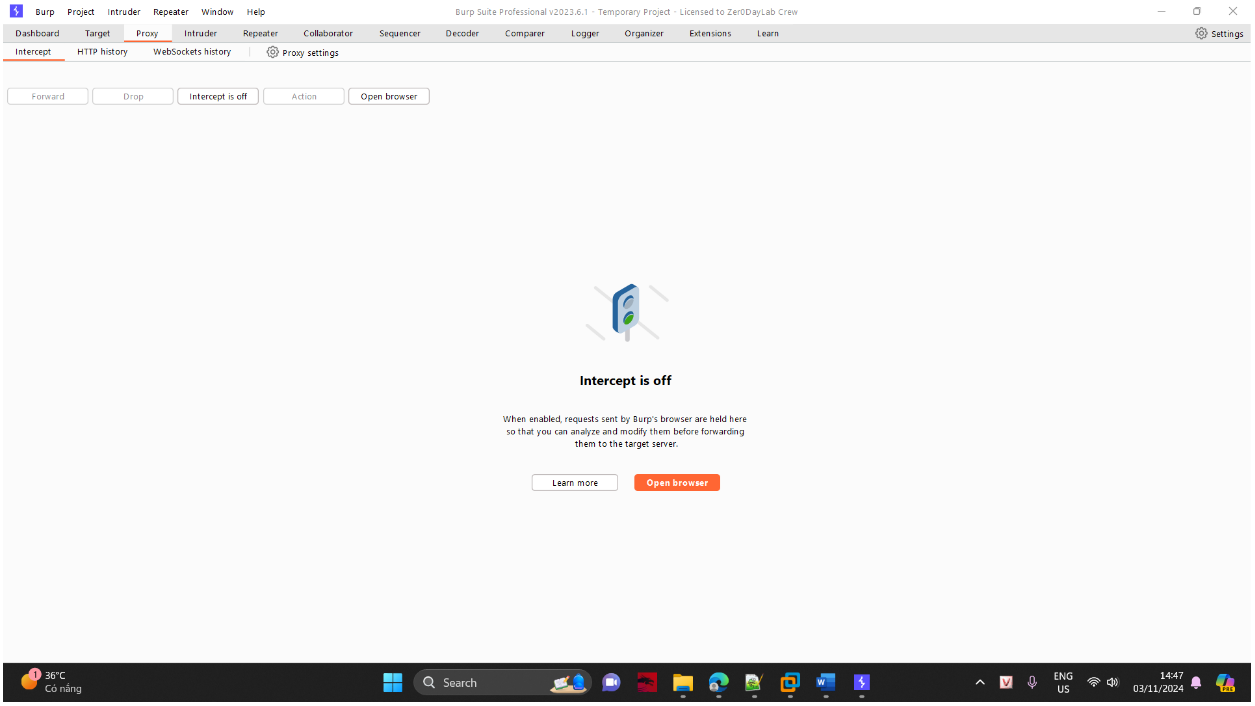
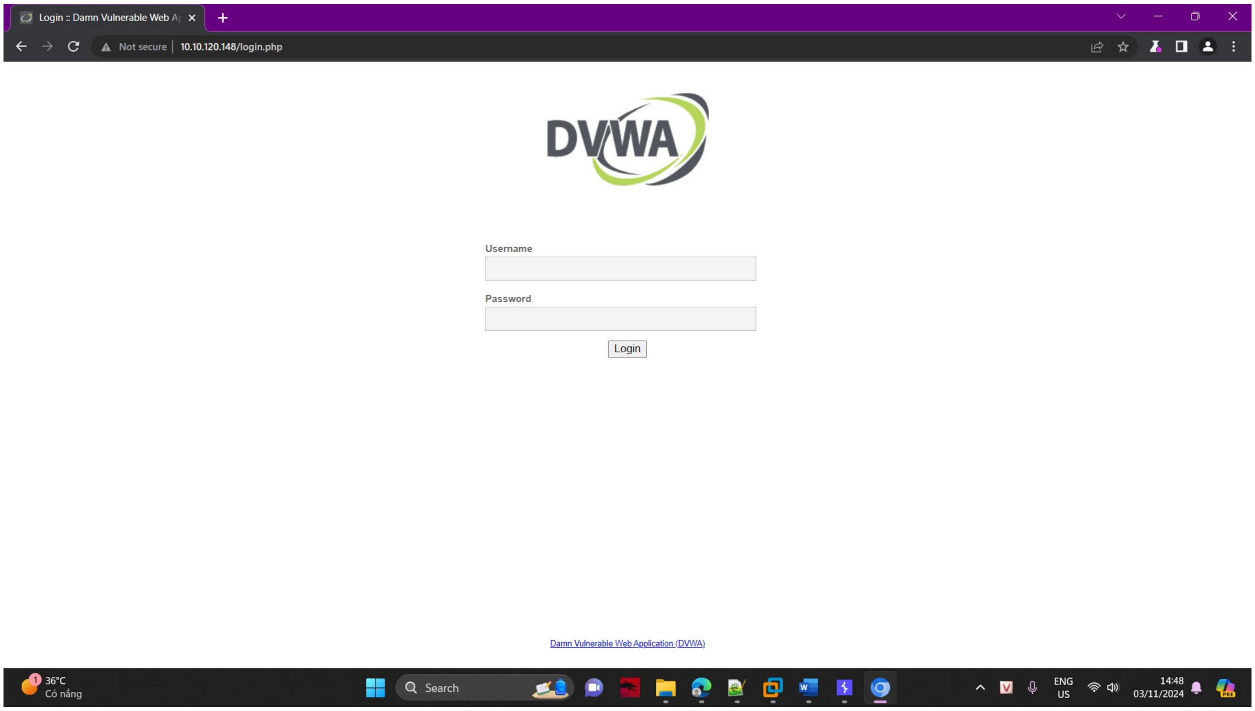
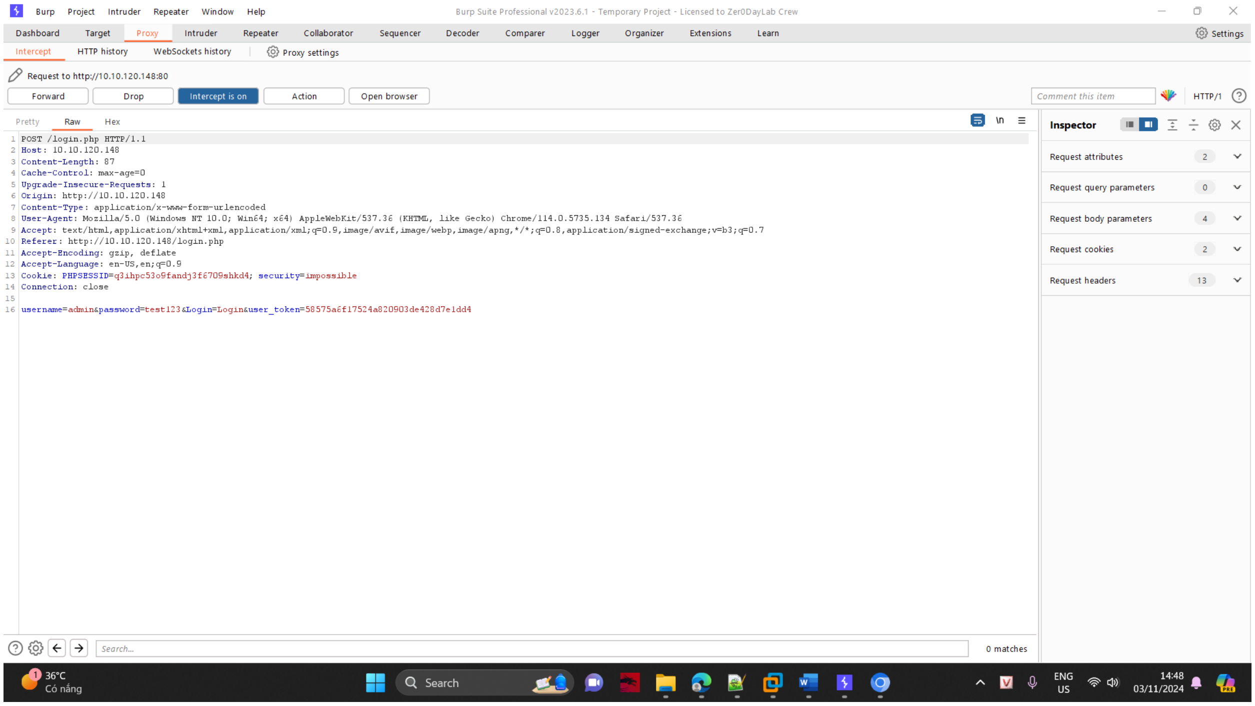
Lab 11: Burp Suite, Man-in-the-middle-attack	
Name	Tran Minh Triet
Student ID	SE172241


Burp Project Intruder Repeater Window Help
Burp Suite Professional v2023.6.1 - Temporary Project - Licensed to Zer0DayLab Crew
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Settings
Intercept HTTP history WebSockets history Proxy settings
Forward
Drop
Intercept is off
Action
Open browser
Learn more
Open browser
36°C
Có nắng
Search
ENG
US
14:47
03/11/2024

Intercept is off

When enabled, requests sent by Burp's browser are held here so that you can analyze and modify them before forwarding them to the target server.

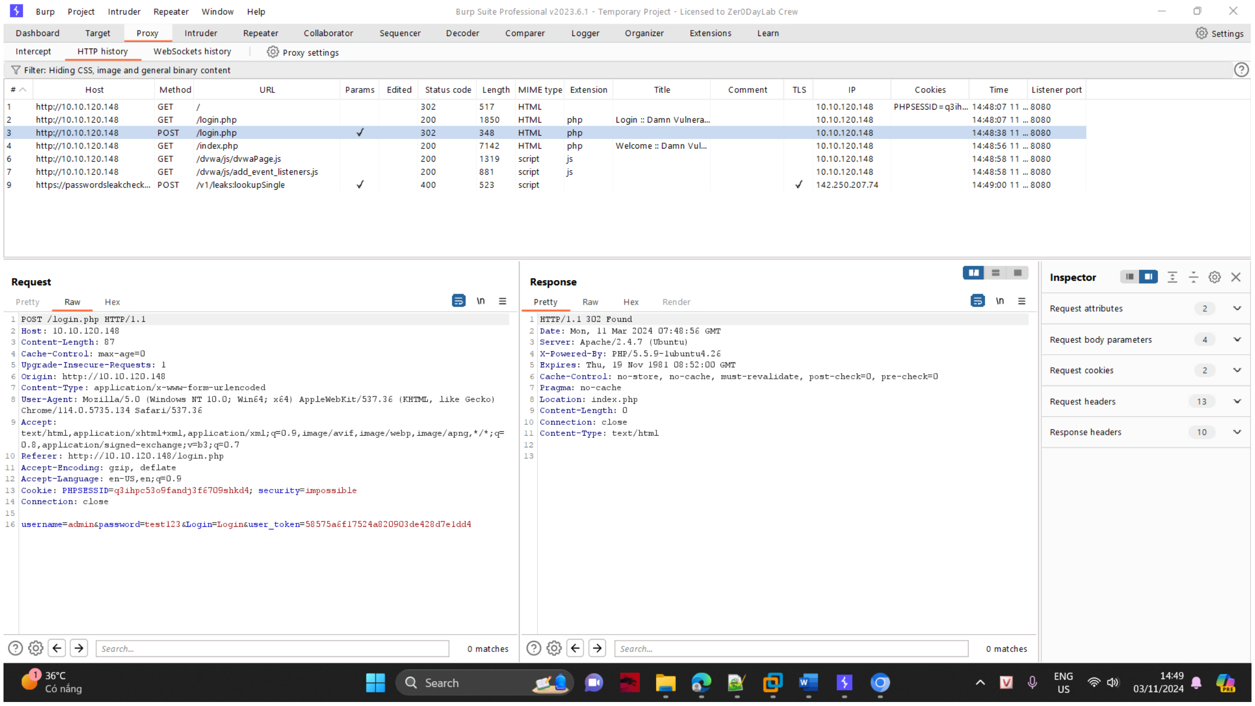



Burp Project Intruder Repeater Window Help
Burp Suite Professional v2023.6.1 - Temporary Project - Licensed to Zer0DayLab Crew
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Settings
Intercept HTTP history WebSockets history Proxy settings
Forward Drop Intercept is on Action Open browser
Comment this item
HTTP/1
Pretty Raw Hex
Inspector
Request attributes 2
Request query parameters 0
Request body parameters 4
Request cookies 2
Request headers 13
Search...
0 matches
36°C
Có nắng
Search
ENG
US
14:48
03/11/2024

Request to http://10.10.120.148:80

```
POST /login.php HTTP/1.1
Host: 10.10.120.148
Content-Length: 87
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://10.10.120.148
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/114.0.5735.134 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://10.10.120.148/login.php
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: PHPSESSID=q3ihpc53o9fandj3f6709shkd4; security=impossible
Connection: close

username=admin&password=test123&Login=Login&user_token=58575a6f17524a820903de428d7e1dd4
```


Burp Project Intruder Repeater Window Help
Burp Suite Professional v2023.6.1 - Temporary Project - Licensed to Zer0DayLab Crew
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Settings
Intercept HTTP history WebSockets history Proxy settings
Request
Pretty Raw Hex
Response
Pretty Raw Hex Render
Inspector
Request attributes 2
Request body parameters 4
Request cookies 2
Request headers 13
Response headers 10
Search...
0 matches
36°C
Có nắng
Search
ENG
US
14:49
03/11/2024

Filter: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Comment	TLS	IP	Cookies	Time	Listener port
1	http://10.10.120.148	GET	/			302	517	HTML					10.10.120.148	PHPSESSID=q3ih...	14:48:07 11 ...	8080
2	http://10.10.120.148	GET	/login.php			200	1850	HTML	php	Login :: Damn Vulnera...			10.10.120.148		14:48:07 11 ...	8080
3	http://10.10.120.148	POST	/login.php	✓		302	348	HTML	php				10.10.120.148		14:48:38 11 ...	8080
4	http://10.10.120.148	GET	/index.php			200	7142	HTML	php	Welcome :: Damn Vul...			10.10.120.148		14:48:56 11 ...	8080
6	http://10.10.120.148	GET	/dvwa/js/dvwaPage.js			200	1319	script	js				10.10.120.148		14:48:58 11 ...	8080
7	http://10.10.120.148	GET	/dvwa/js/add_event_listeners.js			200	881	script	js				10.10.120.148		14:48:58 11 ...	8080
9	https://passwordsleakcheck...	POST	/v1/leaks:lookupSingle	✓		400	523	script				✓	142.250.207.74		14:49:00 11 ...	8080

Request

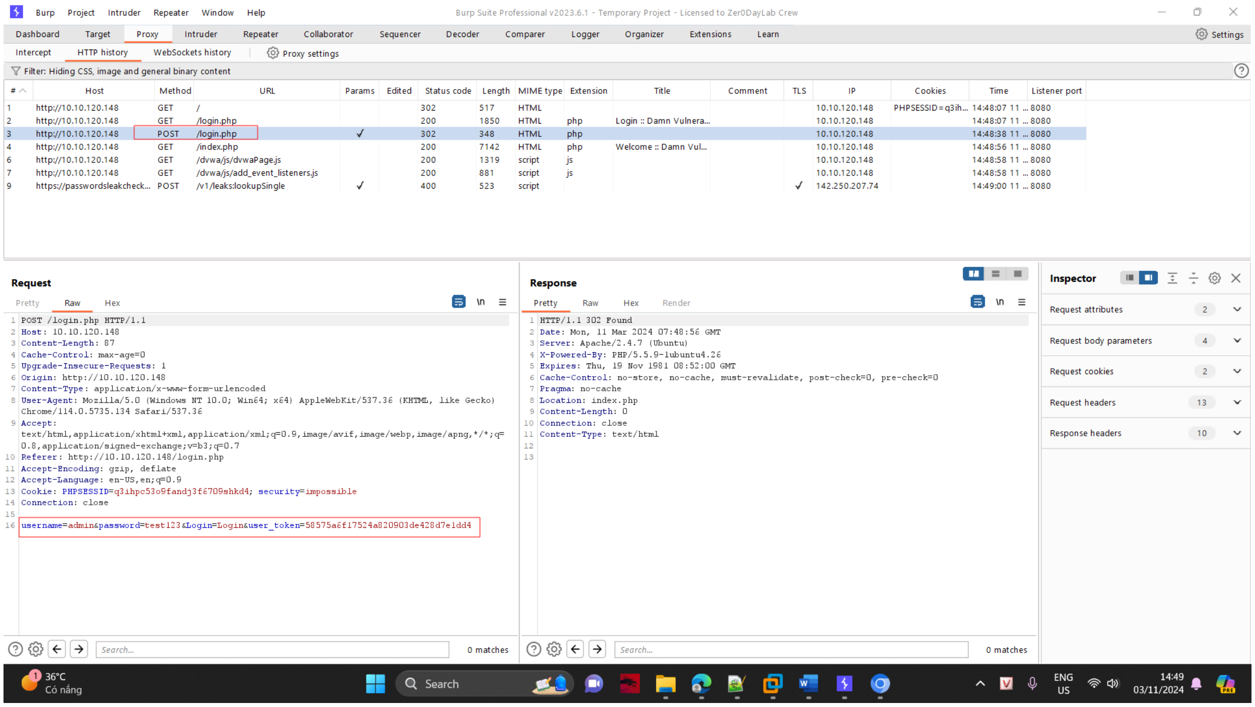
```
POST /login.php HTTP/1.1
Host: 10.10.120.148
Content-Length: 87
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://10.10.120.148
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/114.0.5735.134 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=
0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://10.10.120.148/login.php
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: PHPSESSID=q3ihpc53o9fandj3f6709shkd4; security=impossible
Connection: close

username=admin&password=test123&Login=Login&user_token=58575a6f17524a820903de428d7e1dd4
```

Response

```
HTTP/1.1 302 Found
Date: Mon, 11 Mar 2024 07:48:56 GMT
Server: Apache/2.4.7 (Ubuntu)
X-Powered-By: PHP/5.5.9-1ubuntu4.26
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Location: index.php
Content-Length: 0
Connection: close
Content-Type: text/html


```


Burp Project Intruder Repeater Window Help
Burp Suite Professional v2023.6.1 - Temporary Project - Licensed to Zer0DayLab Crew
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Settings
Intercept HTTP history WebSockets history Proxy settings
Filter: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Comment	TLS	IP	Cookies	Time	Listener port
1	http://10.10.120.148	GET	/			302	517	HTML					10.10.120.148	PHPSESSID=q3ih...	14:48:07 11 ...	8080
2	http://10.10.120.148	GET	/login.php			200	1850	HTML	php	Login :: Damn Vulnera...			10.10.120.148		14:48:07 11 ...	8080
3	http://10.10.120.148	POST	/login.php	✓		302	348	HTML	php				10.10.120.148		14:48:38 11 ...	8080
4	http://10.10.120.148	GET	/index.php			200	7142	HTML	php	Welcome :: Damn Vul...			10.10.120.148		14:48:56 11 ...	8080
6	http://10.10.120.148	GET	/dvwa/js/dvwaPage.js			200	1319	script	js				10.10.120.148		14:48:58 11 ...	8080
7	http://10.10.120.148	GET	/dvwa/js/add_event_listeners.js			200	881	script	js				10.10.120.148		14:48:58 11 ...	8080
9	https://passwordsleakcheck...	POST	/v1/leaks:lookupSingle	✓		400	523	script				✓	142.250.207.74		14:49:00 11 ...	8080

Request

```
POST /login.php HTTP/1.1
Host: 10.10.120.148
Content-Length: 87
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://10.10.120.148
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/114.0.5735.134 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://10.10.120.148/login.php
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: PHPSESSID=q3ihpc53o9fandj3f6709shkd4; security=impossible
Connection: close

username=admin&password=test123&Login=Login&user_token=58575a6f17524a820903de428d7e1dd4
```

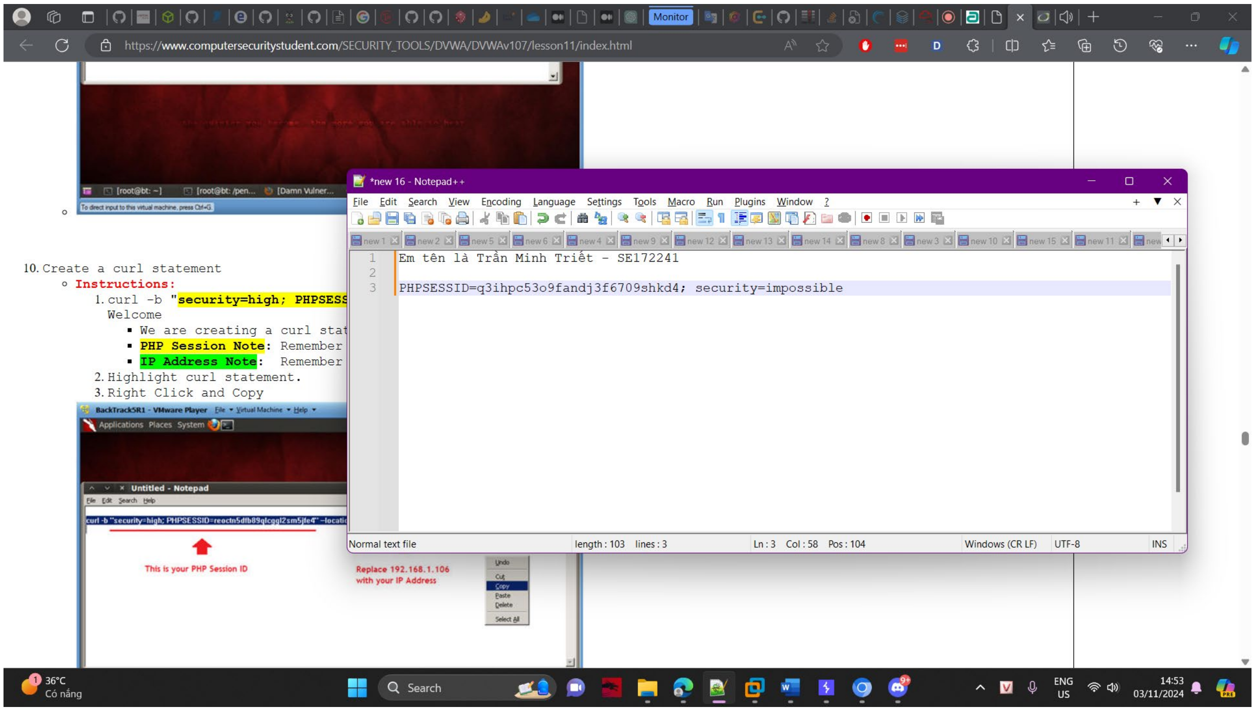
Response

```
HTTP/1.1 302 Found
Date: Mon, 11 Mar 2024 07:48:56 GMT
Server: Apache/2.4.7 (Ubuntu)
X-Powered-By: PHP/5.5.9-1ubuntu4.26
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Location: index.php
Content-Length: 0
Connection: close
Content-Type: text/html
```

Inspector

Request attributes	2
Request body parameters	4
Request cookies	2
Request headers	13
Response headers	10

Search...
0 matches
Search...
0 matches
36°C
Có nắng
Search
ENG
US
14:49
03/11/2024


Monitor
https://www.computersecuritystudent.com/SECURITY_TOOLS/DVWA/DVWAv107/lesson11/index.html
[root@bt: ~]
[root@bt: /pen...
[Damn Vulner...
To direct input to this virtual machine, press Ctrl+G.

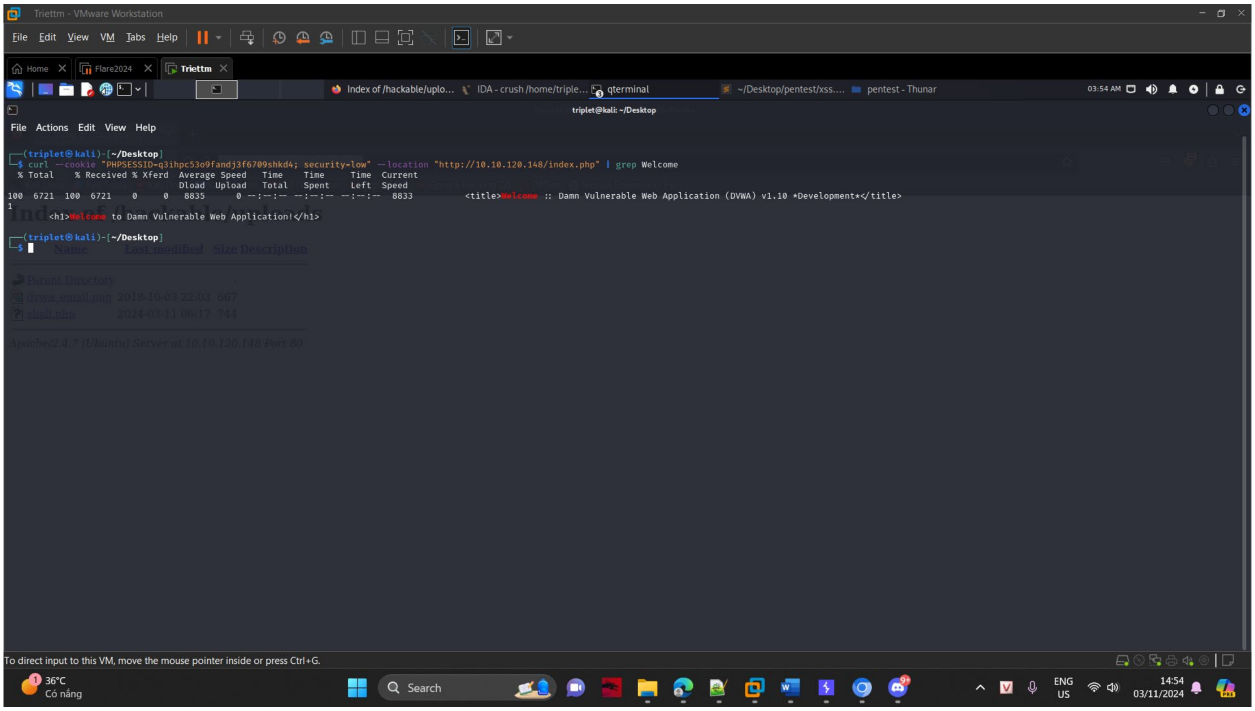
10. Create a curl statement
    - Instructions:
        1. curl -b "security=high; PHPSESS
           Welcome
            - We are creating a curl stat
            - PHP Session Note: Remember
            - IP Address Note: Remember
        2. Highlight curl statement.
        3. Right Click and Copy

BackTrack5R1 - VMware Player File Virtual Machine Help
Applications Places System
Untitled - Notepad
File Edit Search Help
curl -b "security=high; PHPSESSID=reoctn5dfb89qlcggl2sm5jfe4" --locati
This is your PHP Session ID
Replace 192.168.1.106
with your IP Address
Undo
Cut
Copy
Paste
Delete
Select All
*new 16 - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
new 1 new 2 new 5 new 6 new 4 new 9 new 12 new 13 new 14 new 8 new 3 new 10 new 15 new 11 new

```
Em tên là Trần Minh Triết - SE172241

PHPSESSID=q3ihpc53o9fandj3f6709shkd4; security=impossible
```

Normal text file
length : 103 lines : 3
Ln : 3 Col : 58 Pos : 104
Windows (CR LF)
UTF-8
INS
36°C
Có nắng
Search
ENG
US
14:53
03/11/2024



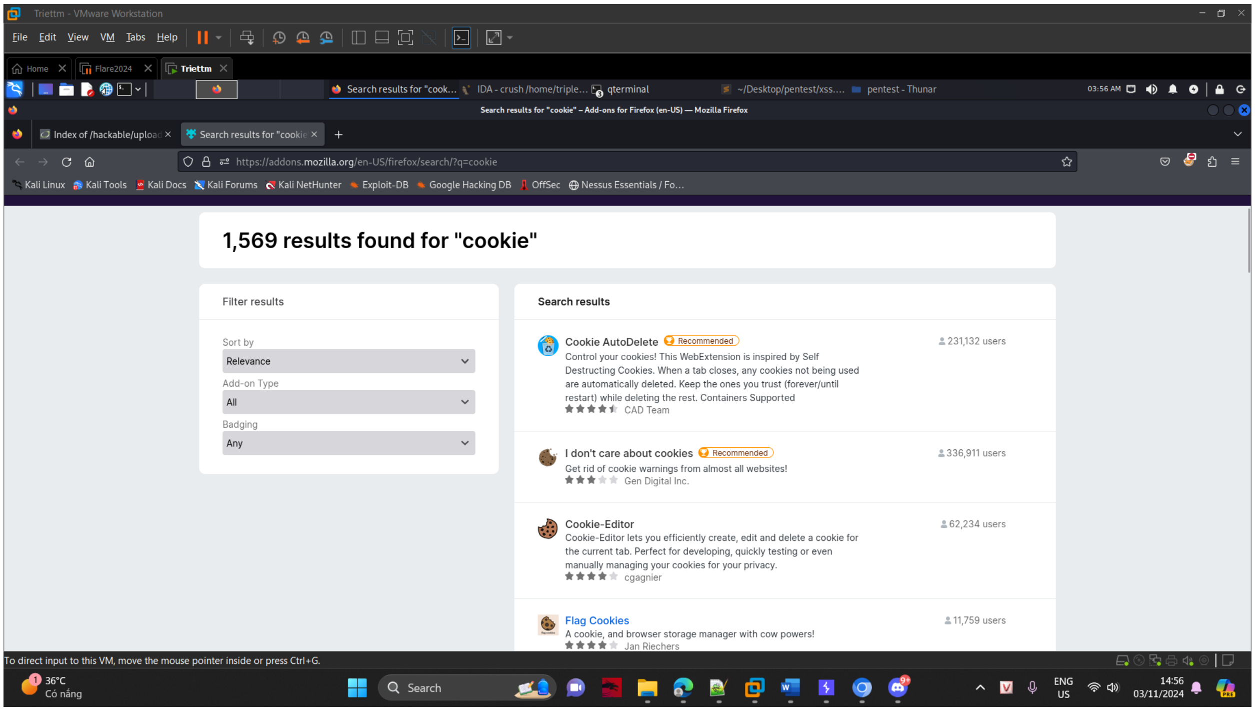
triplet@kali: ~/Desktop

```
┌──(triplet㉿kali)-[~/Desktop]
└─$ curl --cookie "PHPSESSID=q3ihpc53o9fandj3f6709shkd4; security=low" --location "http://10.10.120.148/index.php" | grep Welcome
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  6721  100  6721    0     0   8835      0 --:--:-- --:--:-- --:--:--  8833          <title>Welcome :: Damn Vulnerable Web Application (DVWA) v1.10 *Development*</title>
1
        <h1>Welcome to Damn Vulnerable Web Application!</h1>

┌──(triplet㉿kali)-[~/Desktop]
└─$ 
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Triettm - VMware Workstation
File Edit View VM Tabs Help
Home
Flare2024
Triettm
Index of /hackable/uplo...
IDA - crush /home/triple...
qterminal
~/Desktop/pentest/xss....
pentest - Thunar
03:54 AM
File Actions Edit View Help
36°C
Có nắng
Search
ENG
US
14:54
03/11/2024



Search results for "cookie" – Add-ons for Firefox (en-US) — Mozilla Firefox

https://addons.mozilla.org/en-US/firefox/search/?q=cookie

1,569 results found for "cookie"

Filter results

Sort by: Relevance

Add-on Type: All

Badging: Any

Search results

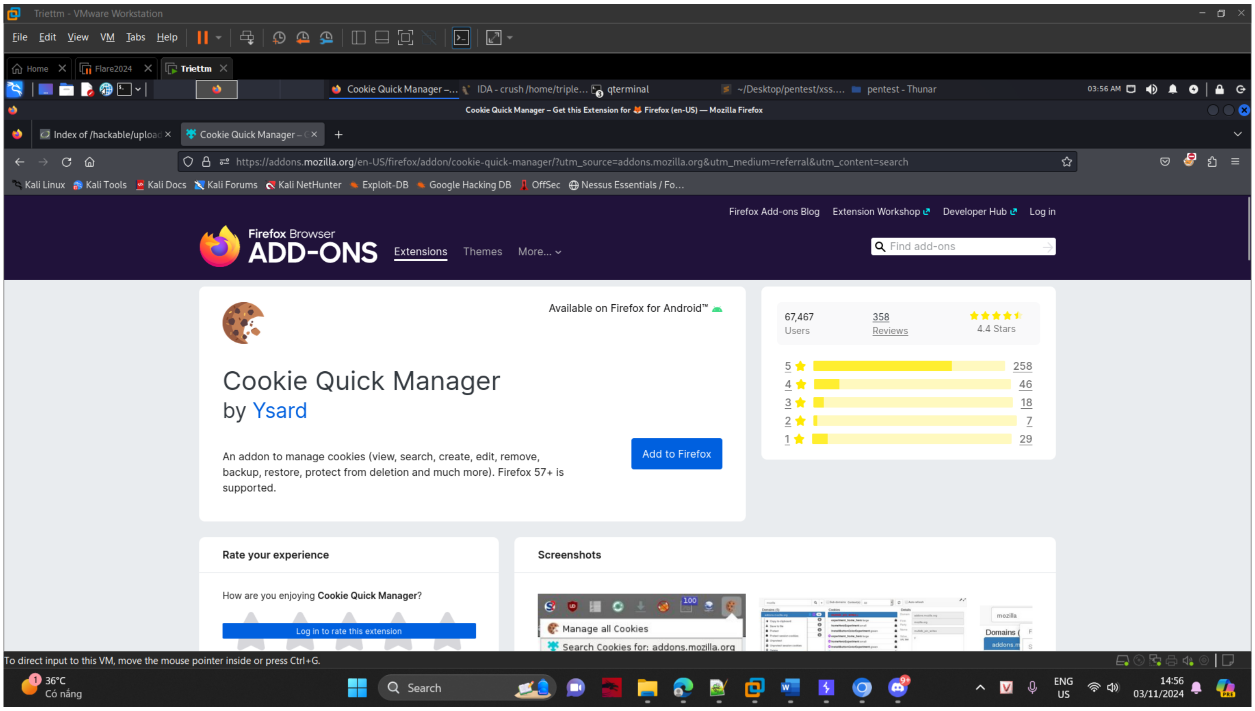
Cookie AutoDelete Recommended — 231,132 users
Control your cookies! This WebExtension is inspired by Self Destructing Cookies. When a tab closes, any cookies not being used are automatically deleted. Keep the ones you trust (forever/until restart) while deleting the rest. Containers Supported
CAD Team

I don't care about cookies Recommended — 336,911 users
Get rid of cookie warnings from almost all websites!
Gen Digital Inc.

Cookie-Editor — 62,234 users
Cookie-Editor lets you efficiently create, edit and delete a cookie for the current tab. Perfect for developing, quickly testing or even manually managing your cookies for your privacy.
cgagnier

Flag Cookies — 11,759 users
A cookie, and browser storage manager with cow powers!
Jan Riechers

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.


Triettm - VMware Workstation
File Edit View VM Tabs Help
Home Flare2024 Triettm
Cookie Quick Manager –... IDA - crush /home/triple... qterminal ~/Desktop/pentest/xss.... pentest - Thunar 03:56 AM
Cookie Quick Manager – Get this Extension for 🦊 Firefox (en-US) — Mozilla Firefox
Index of /hackable/uploa Cookie Quick Manager –
https://addons.mozilla.org/en-US/firefox/addon/cookie-quick-manager/?utm_source=addons.mozilla.org&utm_medium=referral&utm_content=search
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec Nessus Essentials / Fo...
Firefox Add-ons Blog Extension Workshop Developer Hub Log in
Firefox Browser ADD-ONS Extensions Themes More...
Find add-ons

Available on Firefox for Android™

Cookie Quick Manager
by Ysard

An addon to manage cookies (view, search, create, edit, remove, backup, restore, protect from deletion and much more). Firefox 57+ is supported.

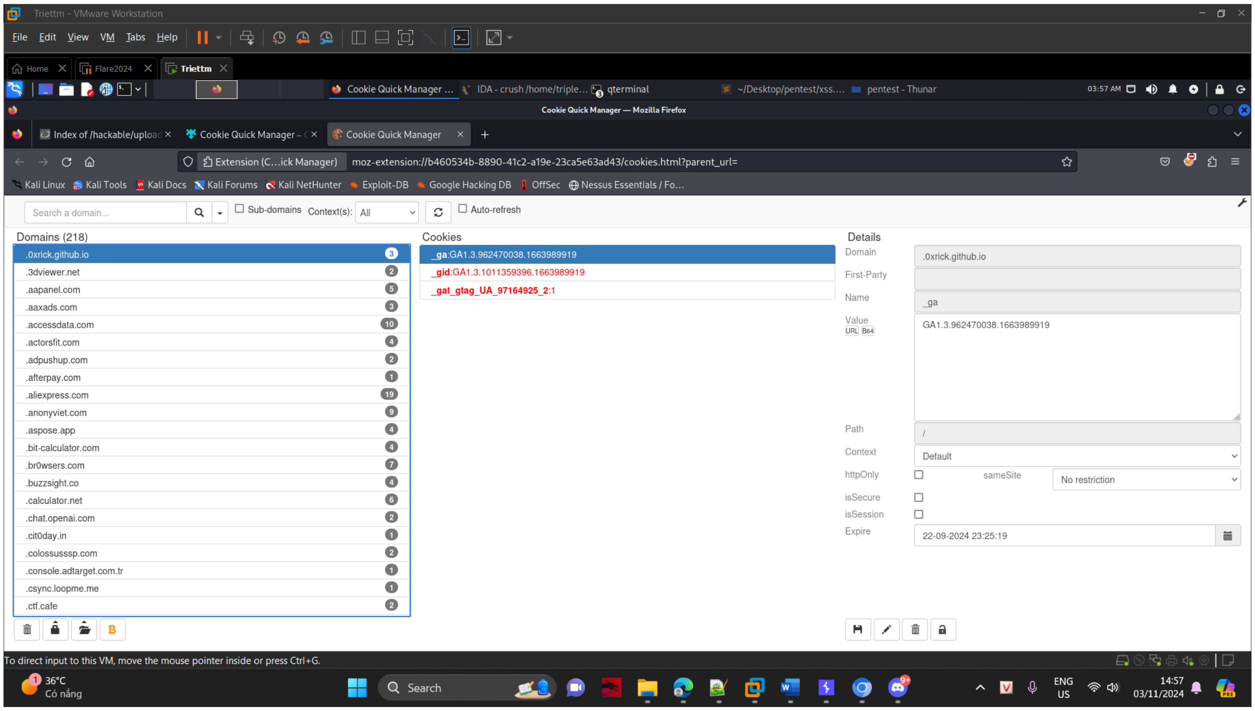
67,467	358	★★★★★
Users	Reviews	4.4 Stars

5 ★	258
4 ★	46
3 ★	18
2 ★	7
1 ★	29

Rate your experience

How are you enjoying **Cookie Quick Manager**?

Log in to rate this extension
Screenshots
Manage all Cookies
Search Cookies for: addons.mozilla.org
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
36°C
Có nắng
Search
ENG
US
14:56
03/11/2024


Triettm - VMware Workstation
File Edit View VM Tabs Help
Home Flare2024 Triettm
Cookie Quick Manager ... IDA - crush /home/triple... qterminal ~/Desktop/pentest/xss.... pentest - Thunar 03:57 AM
Cookie Quick Manager — Mozilla Firefox
Index of /hackable/uploa Cookie Quick Manager – Cookie Quick Manager
Extension (C...ick Manager) moz-extension://b460534b-8890-41c2-a19e-23ca5e63ad43/cookies.html?parent_url=
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec Nessus Essentials / Fo...
Search a domain...
☐ Sub-domains Context(s): All
☐ Auto-refresh

Domains (218)

.0xrick.github.io	3
.3dviewer.net	2
.aapanel.com	5
.aaxads.com	3
.accessdata.com	10
.actorsfit.com	4
.adpushup.com	2
.afterpay.com	1
.aliexpress.com	19
.anonyviet.com	9
.aspose.app	4
.bit-calculator.com	4
.br0wsers.com	7
.buzzsight.co	4
.calculator.net	6
.chat.openai.com	2
.cit0day.in	1
.colossusssp.com	2
.console.adtarget.com.tr	1
.csync.loopme.me	1
.ctf.cafe	2

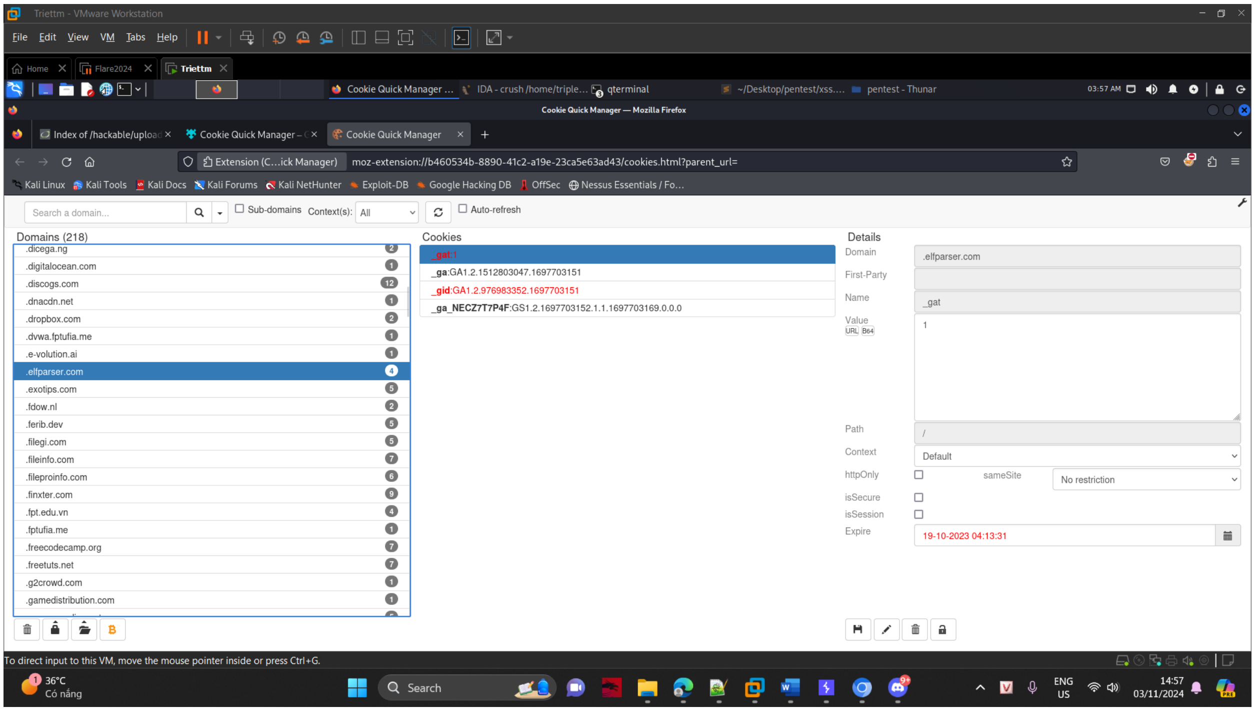
Cookies

- _ga:GA1.3.962470038.1663989919
- _gid:GA1.3.1011359396.1663989919
- _gat_gtag_UA_97164925_2:1

Details

Domain	.0xrick.github.io
First-Party	
Name	_ga
Value	GA1.3.962470038.1663989919
Path	/
Context	Default
httpOnly	☐ sameSite No restriction
isSecure	☐
isSession	☐
Expire	22-09-2024 23:25:19

URL B64
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
36°C
Có nắng
Search
ENG
US
14:57
03/11/2024



moz-extension://b460534b-8890-41c2-a19e-23ca5e63ad43/cookies.html?parent_url=

Domains (218)

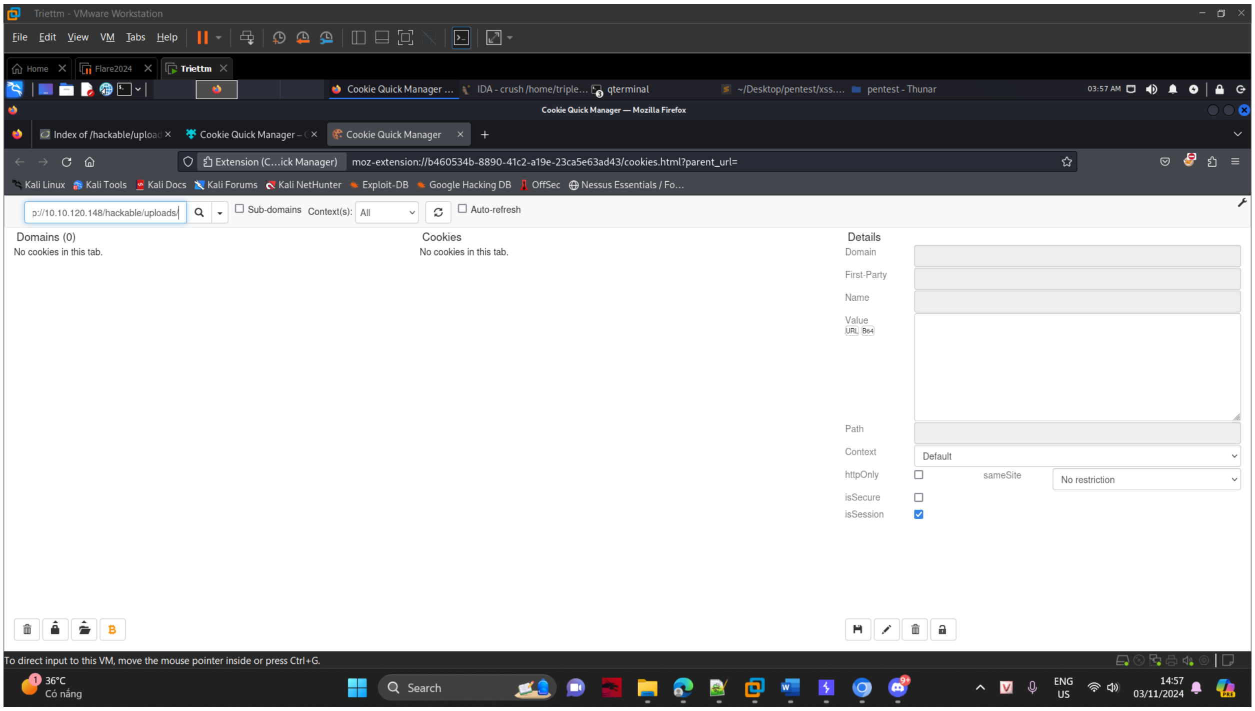
.dicega.ng	2
.digitalocean.com	1
.discogs.com	12
.dnacdn.net	1
.dropbox.com	2
.dvwa.fptufia.me	1
.e-volution.ai	1
.elfparser.com	4
.exotips.com	5
.fdow.nl	2
.ferib.dev	5
.filegi.com	5
.fileinfo.com	7
.fileproinfo.com	6
.finxter.com	9
.fpt.edu.vn	4
.fptufia.me	1
.freecodecamp.org	7
.freetuts.net	7
.g2crowd.com	1
.gamedistribution.com	1

Cookies

_gat:1
_ga:GA1.2.1512803047.1697703151
_gid:GA1.2.976983352.1697703151
_ga_NECZ7T7P4F:GS1.2.1697703152.1.1.1697703169.0.0.0

Details

Domain: .elfparser.com
First-Party:
Name: _gat
Value: 1
Path: /
Context: Default
httpOnly: □ sameSite: No restriction
isSecure: □
isSession: □
Expire: 19-10-2023 04:13:31



moz-extension://b460534b-8890-41c2-a19e-23ca5e63ad43/cookies.html?parent_url=

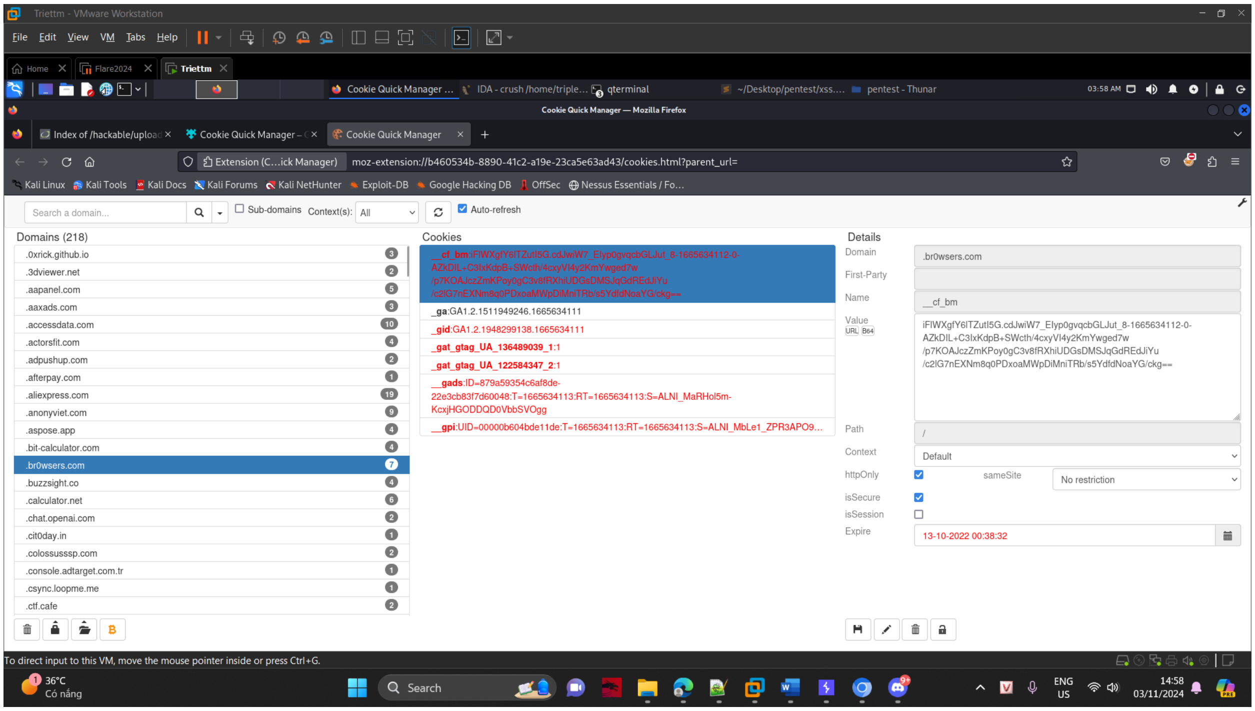
p://10.10.120.148/hackable/uploads/

Domains (0)
No cookies in this tab.

Cookies
No cookies in this tab.

Details

Context: Default
httpOnly: □ sameSite: No restriction
isSecure: □
isSession: ☑



moz-extension://b460534b-8890-41c2-a19e-23ca5e63ad43/cookies.html?parent_url=

Domains (218)

.0xrick.github.io	3
.3dviewer.net	2
.aapanel.com	5
.aaxads.com	3
.accessdata.com	10
.actorsfit.com	4
.adpushup.com	2
.afterpay.com	1
.aliexpress.com	19
.anonyviet.com	9
.aspose.app	4
.bit-calculator.com	4
.br0wsers.com	7
.buzzsight.co	4
.calculator.net	6
.chat.openai.com	2
.cit0day.in	1
.colossusssp.com	2
.console.adtarget.com.tr	1
.csync.loopme.me	1
.ctf.cafe	2

Cookies

```
__cf_bm:iFlWXgfY6lTZutI5G.cdJwiW7_Elyp0gvqcbGLJut_8-1665634112-0-AZkDIL+C3IxKdpB+SWcth/4cxyVI4y2KmYwged7w/p7KOAJczZmKPoy0gC3v8fRXhiUDGsDMSJqGdREdJiYu/c2lG7nEXNm8q0PDxoaMWpDiMniTRb/s5YdfdNoaYG/ckg==
_ga:GA1.2.1511949246.1665634111
_gid:GA1.2.1948299138.1665634111
_gat_gtag_UA_136489039_1:1
_gat_gtag_UA_122584347_2:1
__gads:ID=879a59354c6af8de-22e3cb83f7d60048:T=1665634113:RT=1665634113:S=ALNI_MaRHol5m-KcxjHGODDQD0VbbSVOgg
__gpi:UID=00000b604bde11de:T=1665634113:RT=1665634113:S=ALNI_MbLe1_ZPR3APO9...
```

Details

Domain	.br0wsers.com
First-Party	
Name	__cf_bm
Value URL B64	iFlWXgfY6lTZutI5G.cdJwiW7_Elyp0gvqcbGLJut_8-1665634112-0-AZkDIL+C3IxKdpB+SWcth/4cxyVI4y2KmYwged7w/p7KOAJczZmKPoy0gC3v8fRXhiUDGsDMSJqGdREdJiYu/c2lG7nEXNm8q0PDxoaMWpDiMniTRb/s5YdfdNoaYG/ckg==
Path	/
Context	Default
httpOnly	☑ sameSite No restriction
isSecure	☑
isSession	□
Expire	13-10-2022 00:38:32

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.