Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options

Intercept HTTP history WebSockets history Options

Forward Drop Intercept is off Action Open Browser

Use Burp's embedded browser

There's no need to configure your proxy settings manually. Use Burp's embedded Chromium browser to start testing right away.

Open browser

Use a di

You'll ne
over HTT

View

Using Burp Proxy

If this is your first time using Burp, you might want to take a look at our guide to help you get the most out of your experience.

Burp Proxy options

Reference information about the different options you have for customizing Burp Proxy's behaviour.

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

Proxy Listeners

Burp Proxy uses listeners to receive incoming HTTP requests from your browser. You will need to configure your browser to use one of the listeners as its proxy server.

Add
Edit
Remove

Running	Interface	Invisible	Redirect	Certificate	TLS Protocols
☑	127.0.0.1:8080			Per-host	Default

Each installation of Burp generates its own CA certificate that Proxy listeners can use when negotiating TLS connections. You can import or export this certificate for use in other tools or another installation of B

Import / export CA certificate
Regenerate CA certificate

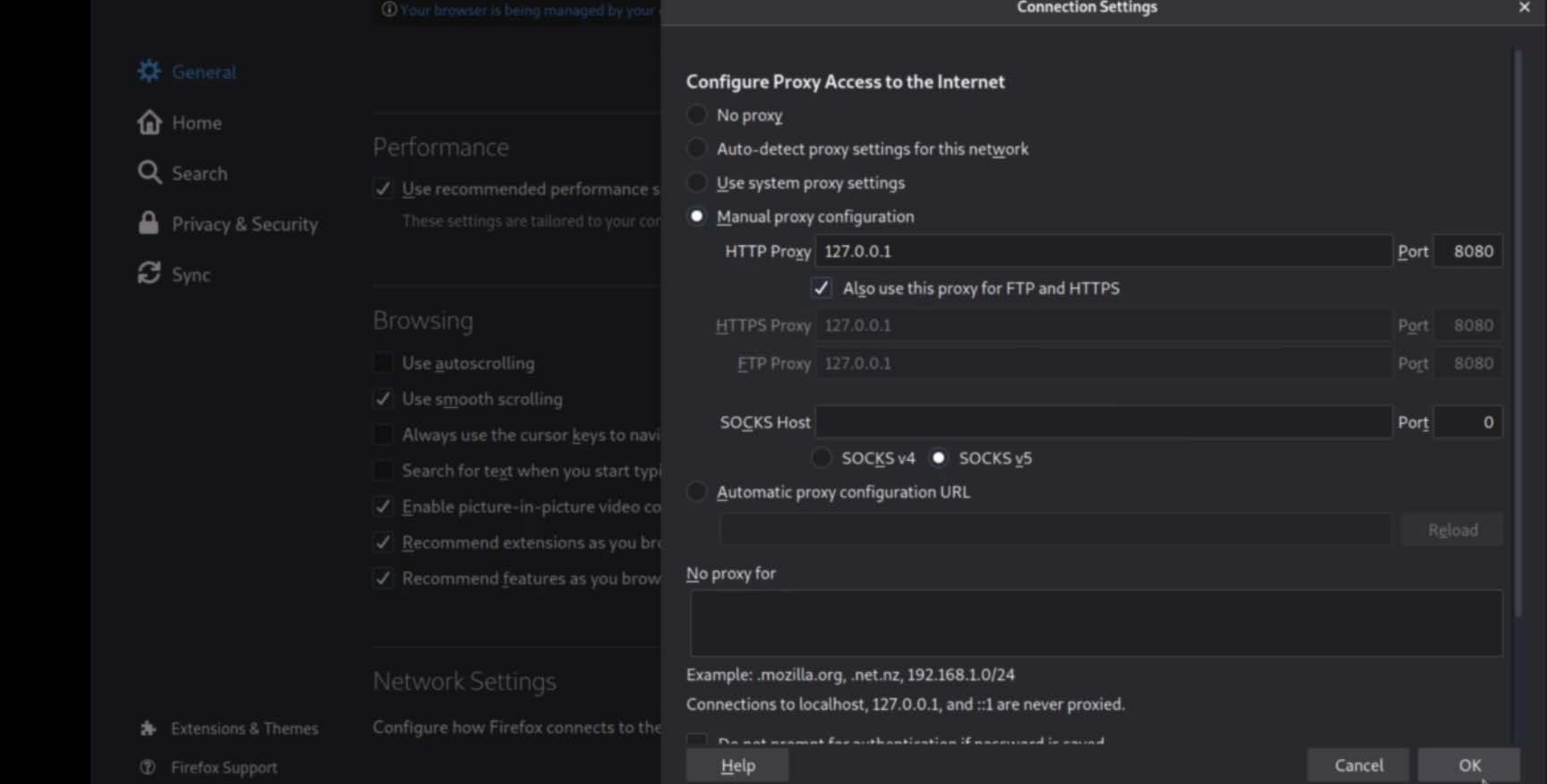
Intercept Client Requests

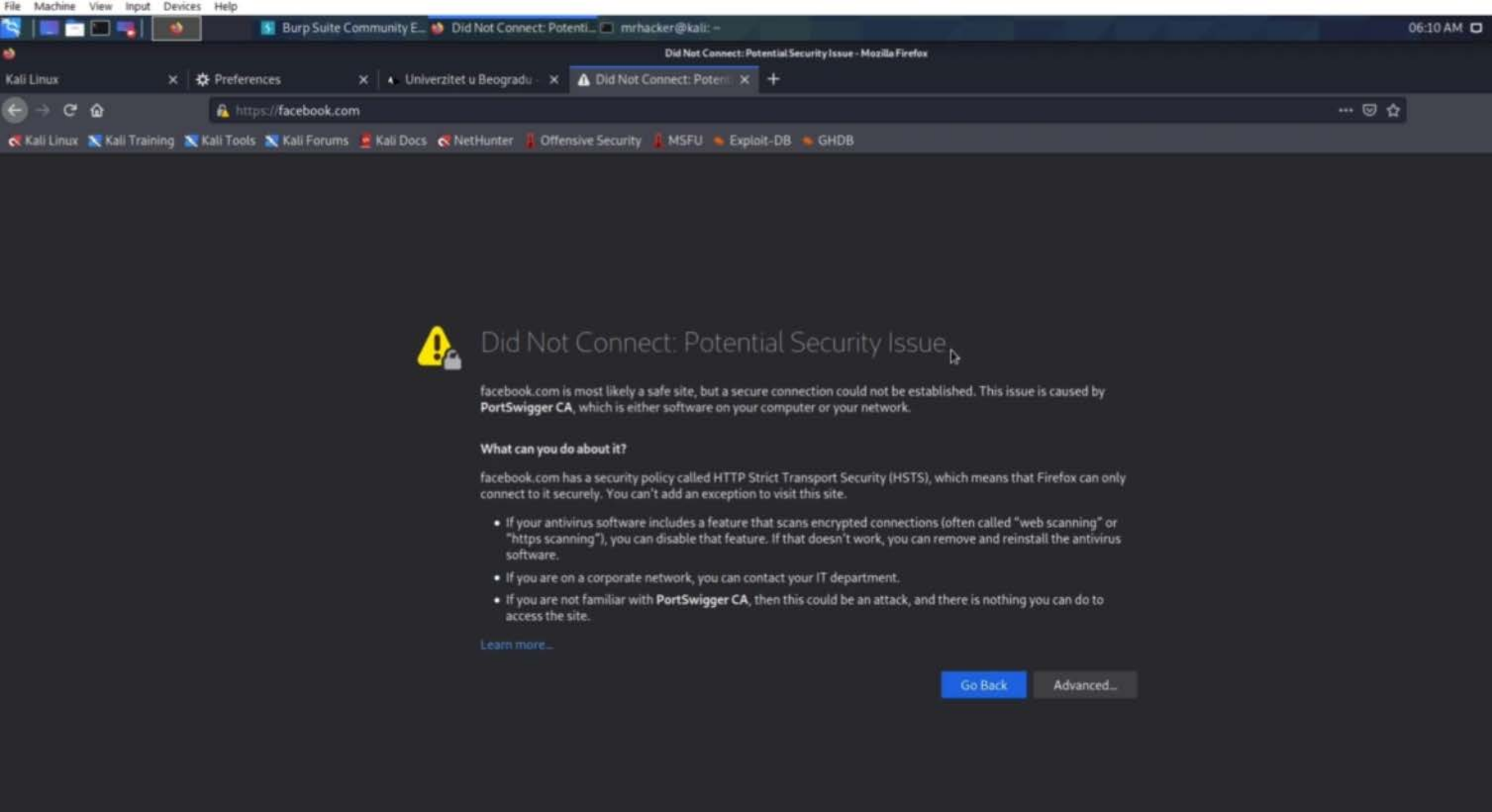
Use these settings to control which requests are stalled for viewing and editing in the Intercept tab.

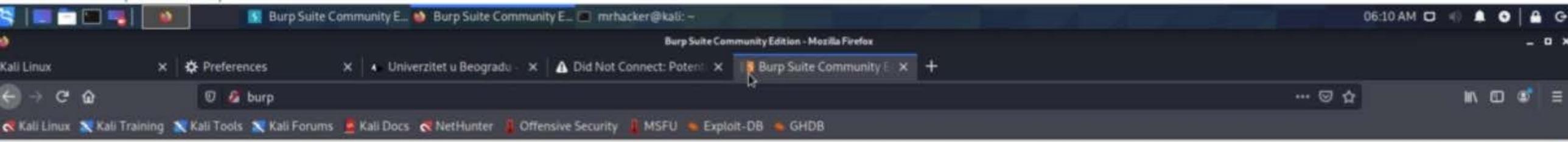
☑ Intercept requests based on the following rules: *Master interception is turned off*

Add
Edit
Remove
Up
Down

Enabled	Operator	Match type	Relationship	Condition
☑		File extension	Does not match	(^gif$\|^jpg$|^png$\|^css$|^js$\|^ico$|...
☐	Or	Request	Contains parameters	
☐	Or	HTTP method	Does not match	(get|post)
☐	And	URL	Is in target scope	


Your browser is being managed by your
General
Home
Search
Privacy & Security
Sync
Performance
Use recommended performance s
These settings are tailored to your cor
Browsing
Use autoscrolling
Use smooth scrolling
Always use the cursor keys to navi
Search for text when you start typi
Enable picture-in-picture video co
Recommend extensions as you br
Recommend features as you brow
Network Settings
Configure how Firefox connects to the
Extensions & Themes
Firefox Support
Connection Settings
Configure Proxy Access to the Internet
No proxy
Auto-detect proxy settings for this network
Use system proxy settings
Manual proxy configuration
HTTP Proxy 127.0.0.1 Port 8080
Also use this proxy for FTP and HTTPS
HTTPS Proxy 127.0.0.1 Port 8080
FTP Proxy 127.0.0.1 Port 8080
SOCKS Host Port 0
SOCKS v4 SOCKS v5
Automatic proxy configuration URL
Reload
No proxy for
Example: .mozilla.org, .net.nz, 192.168.1.0/24
Connections to localhost, 127.0.0.1, and ::1 are never proxied.
Help
Cancel
OK


File Machine View Input Devices Help
Burp Suite Community E...
Did Not Connect: Potenti...
mrhacker@kali: ~
06:10 AM
Did Not Connect: Potential Security Issue - Mozilla Firefox
Kali Linux
Preferences
Univerzitet u Beogradu
Did Not Connect: Poten
https://facebook.com
Kali Linux
Kali Training
Kali Tools
Kali Forums
Kali Docs
NetHunter
Offensive Security
MSFU
Exploit-DB
GHDB
Did Not Connect: Potential Security Issue
facebook.com is most likely a safe site, but a secure connection could not be established. This issue is caused by PortSwigger CA, which is either software on your computer or your network.
What can you do about it?
facebook.com has a security policy called HTTP Strict Transport Security (HSTS), which means that Firefox can only connect to it securely. You can't add an exception to visit this site.
If your antivirus software includes a feature that scans encrypted connections (often called "web scanning" or "https scanning"), you can disable that feature. If that doesn't work, you can remove and reinstall the antivirus software.
If you are on a corporate network, you can contact your IT department.
If you are not familiar with PortSwigger CA, then this could be an attack, and there is nothing you can do to access the site.
Learn more...
Go Back
Advanced...


Burp Suite Community E...
Burp Suite Community E...
mrhacker@kali: ~
06:10 AM
Burp Suite Community Edition - Mozilla Firefox
Kali Linux
Preferences
Univerzitet u Beogradu
Did Not Connect: Poten
Burp Suite Community E
burp
Kali Linux
Kali Training
Kali Tools
Kali Forums
Kali Docs
NetHunter
Offensive Security
MSFU
Exploit-DB
GHDB
Burp Suite Community Edition
CA Certificate
Welcome to Burp Suite Community Edition.

Firefox about:preferences#privacy

Kali Linux Kali Training Kali Tools Kali Forums Kali Docs NetHunter Offensive Security MSFU Exploit-DB GHDB

Your browser is being managed by your organization.

Find in Preferences

- General
- Home
- Search
- Privacy & Security
- Sync

Privacy Notice

Allow Firefox to send technical and interaction data to Mozilla Learn more

Allow Firefox to make personalized extension recommendations Learn more

Allow Firefox to install and run studies View Firefox studies

Allow Firefox to send backlogged crash reports on your behalf Learn more

Security

Deceptive Content and Dangerous Software Protection

- [x] Block dangerous and deceptive content Learn more
  - [x] Block dangerous downloads
  - [x] Warn you about unwanted and uncommon software

Certificates

When a server requests your personal certificate

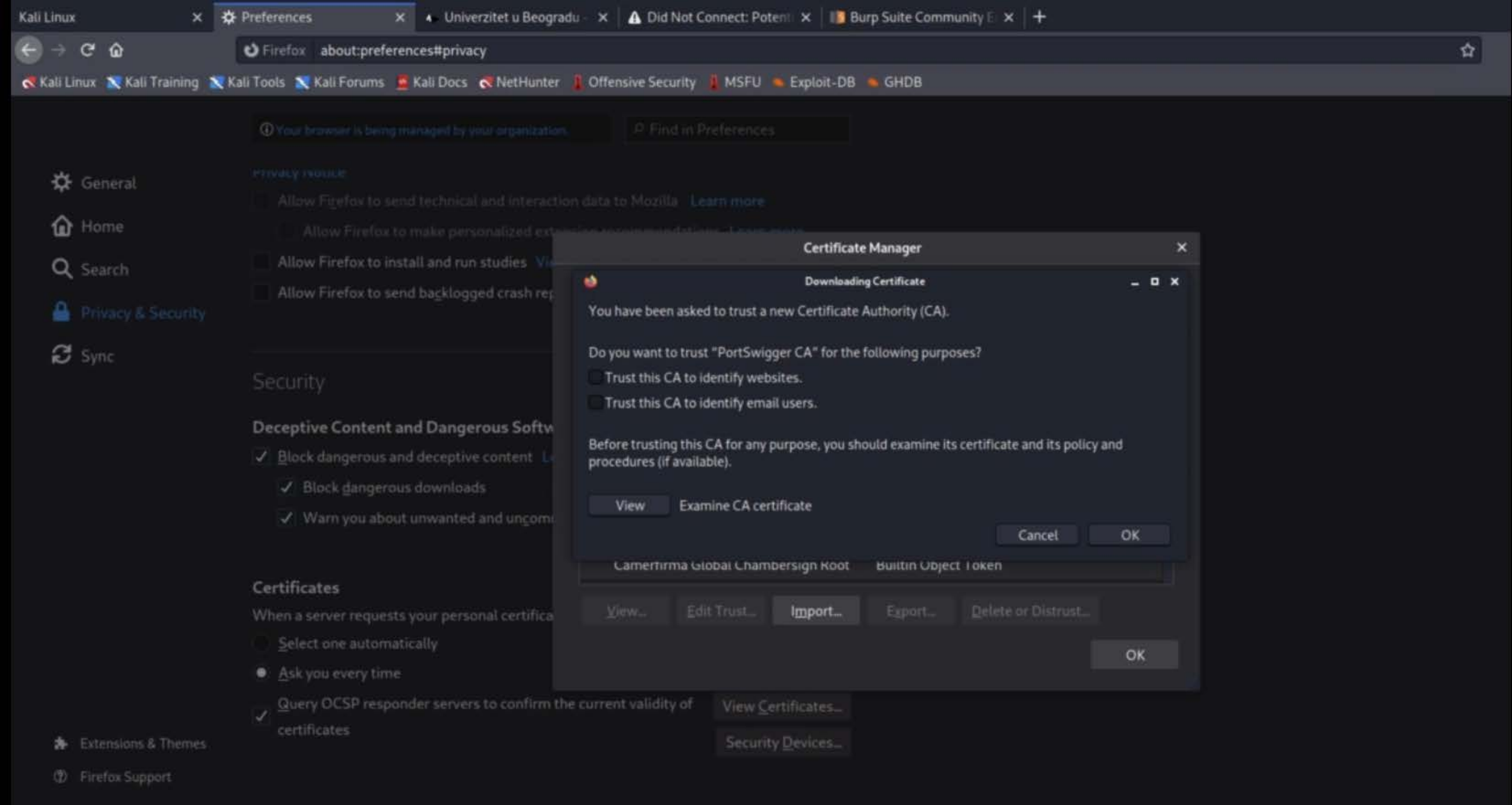
- ( ) Select one automatically
- (•) Ask you every time

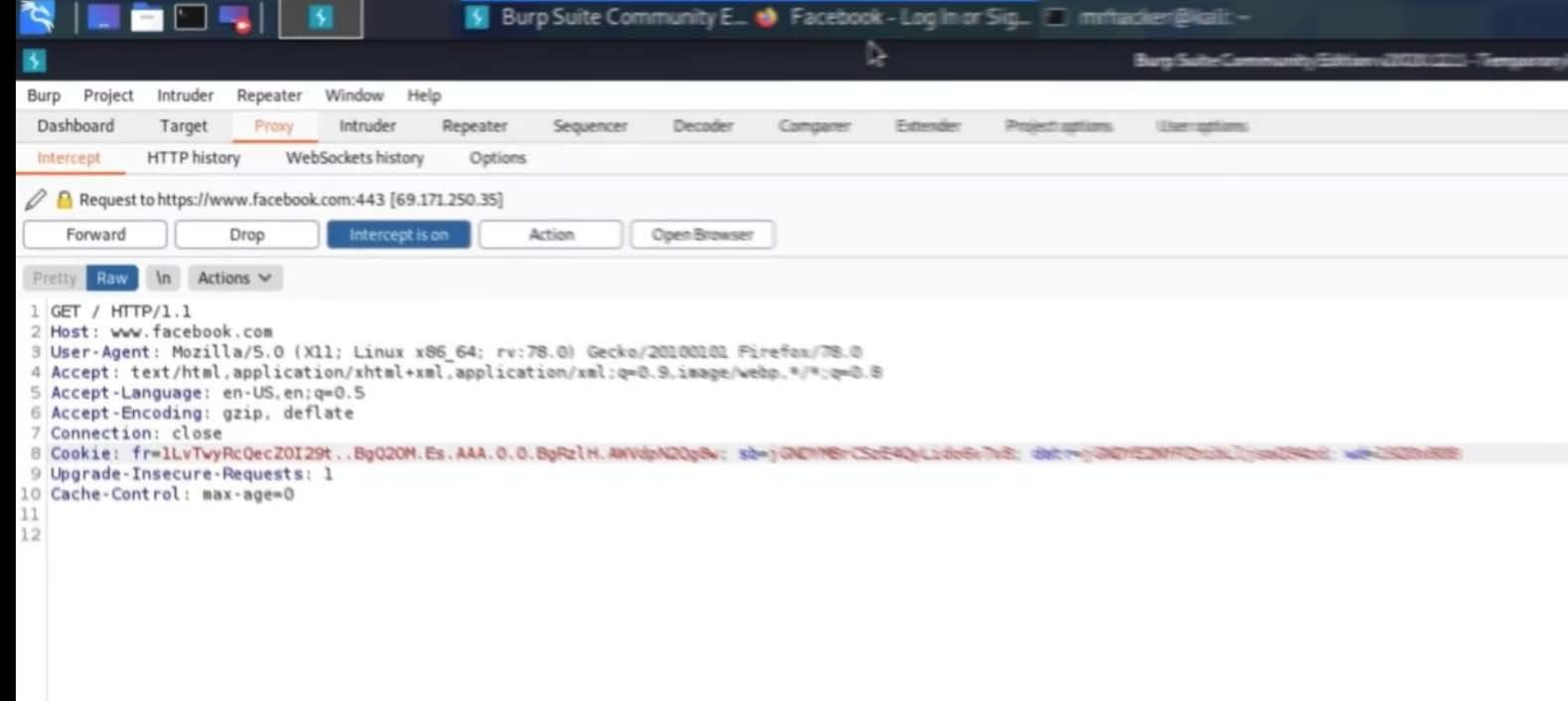
[x] Query OCSP responder servers to confirm the current validity of certificates

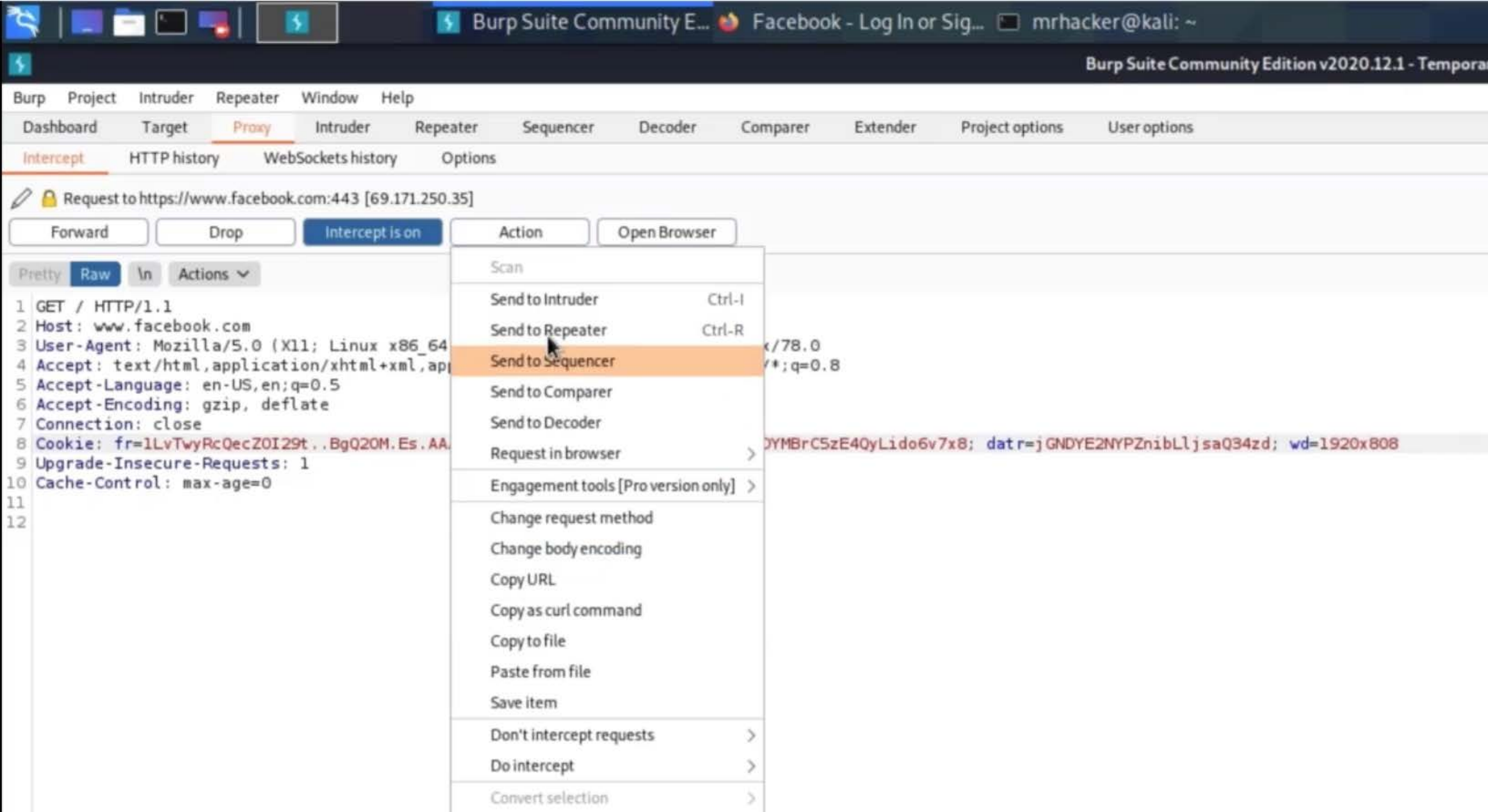
View Certificates...

Security Devices...

Extensions & Themes


Kali Linux
Preferences
Univerzitet u Beogradu
Did Not Connect: Poten
Burp Suite Community E
Firefox about:preferences#privacy
Kali Linux Kali Training Kali Tools Kali Forums Kali Docs NetHunter Offensive Security MSFU Exploit-DB GHDB
Your browser is being managed by your organization.
Find in Preferences
General
Home
Search
Privacy & Security
Sync
Allow Firefox to send technical and interaction data to Mozilla Learn more
Allow Firefox to install and run studies
Allow Firefox to send backlogged crash rep
Security
Deceptive Content and Dangerous Softw
Block dangerous and deceptive content
Block dangerous downloads
Warn you about unwanted and uncom
Certificates
When a server requests your personal certifica
Select one automatically
Ask you every time
Query OCSP responder servers to confirm the current validity of certificates
View Certificates...
Security Devices...
Extensions & Themes
Firefox Support
Certificate Manager
Downloading Certificate
You have been asked to trust a new Certificate Authority (CA).
Do you want to trust "PortSwigger CA" for the following purposes?
Trust this CA to identify websites.
Trust this CA to identify email users.
Before trusting this CA for any purpose, you should examine its certificate and its policy and procedures (if available).
View
Examine CA certificate
Cancel
OK
Camerfirma Global Chambersign Root
Builtin Object Token
View...
Edit Trust...
Import...
Export...
Delete or Distrust...
OK


Burp Suite Community E...
Facebook - Log In or Sig...
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender
Intercept HTTP history WebSockets history Options
Request to https://www.facebook.com:443 [69.171.250.35]
Forward Drop Intercept is on Action Open Browser
Pretty Raw \n Actions
1 GET / HTTP/1.1
2 Host: www.facebook.com
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Cookie: fr=1LvTwyRcQecZOI29t..BgQ2OM.Es.AAA.0.0.BgRzlH.AWVdpN2Qg8w;
9 Upgrade-Insecure-Requests: 1
10 Cache-Control: max-age=0
11
12


Burp Suite Community E...
Facebook - Log In or Sig...
mrhacker@kali: ~
Burp Suite Community Edition v2020.12.1 - Tempora
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 https://www.facebook.com:443 [69.171.250.35]
Forward Drop Intercept is on Action Open Browser
Pretty Raw \n Actions
1 GET / HTTP/1.1
2 Host: www.facebook.com
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64
4 Accept: text/html,application/xhtml+xml,ap
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Cookie: fr=1LvTwyRcQecZOI29t..BgQ2OM.Es.AA
9 Upgrade-Insecure-Requests: 1
10 Cache-Control: max-age=0
11
12
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 [Pro version only]
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

Kali 2021 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Burp Suite Community E... Mozilla Firefox mrhacker@kali: ~ 04:12 AM

Burp Suite Community Edition v2020.12.1 - Temporary Project

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options

Site map Scope Issue definitions

Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

- https://classify-client.services.mozilla.com
- https://normandy.cdn.mozilla.net

Host	Method	URL	Params	Status	Length	MIME type	Title	Comment	Time requested
https://normandy.cdn.mo...	GET	/api/v1/		200	1399	JSON			04:10:27 9 M...
https://normandy.cdn.mo...	GET	/api/v1/action/							
https://normandy.cdn.mo...	GET	/api/v1/action/signed/							
https://normandy.cdn.mo...	GET	/api/v1/approval_request/							
https://normandy.cdn.mo...	GET	/api/v1/extension/							
https://normandy.cdn.mo...	GET	/api/v1/recipe/							
https://normandy.cdn.mo...	GET	/api/v1/recipe/signed/							
https://normandy.cdn.mo...	GET	/api/v1/recipe_revision/							

Request

Pretty Raw \n Actions

```
1 GET /api/v1/ HTTP/1.1
2 Host: normandy.cdn.mozilla.net
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: application/json
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8
9
```

Response

Pretty Raw Render \n Actions

```
1 HTTP/1.1 200 OK
2 Content-Type: application/json
3 Content-Length: 598
4 Connection: close
5 Server: nginx
6 Date: Tue, 09 Mar 2021 09:10:08 GMT
7 Cache-Control: public, max-age=30
8 Allow: GET, HEAD, OPTIONS
9 Content-Security-Policy: base-uri 'none'; frame-src 'none'; object-src 'none'; form-act
10 X-Frame-Options: DENY
11 X-Content-Type-Options: nosniff
12 X-XSS-Protection: 1; mode=block
13 Strict-Transport-Security: max-age=31536000
14 Via: 1.1 google, 1.1 3dca71b0fde541bcd2caf3756ffbc27a.cloudfront.net (CloudFront)
15 Vary: Accept,Origin
16 X-Cache: Hit from cloudfront
17 X-Amz-Cf-Pop: VIE50-C1
18 X-Amz-Cf-Id: aVat2efOqphlpOUKOhOz-Ij_3i3iwyLlsWtdsZd3ZhOZYKV_GxHOHg==
19 Age: 20
20
21 {
  "action-list":"https://normandy.cdn.mozilla.net/api/v1/action/",
  "action-signed":"https://normandy.cdn.mozilla.net/api/v1/action/signed/",
  "approvalrequest-list":"https://normandy.cdn.mozilla.net/api/v1/approval_request/",
  "classify-client":"https://classify-client.services.mozilla.com/api/v1/classify_clien
  "extension-list":"https://normandy.cdn.mozilla.net/api/v1/extension/",
  "recipe-list":"https://normandy.cdn.mozilla.net/api/v1/recipe/",
  "recipe-signed":"https://normandy.cdn.mozilla.net/api/v1/recipe/signed/",
  "reciperevision-list":"https://normandy.cdn.mozilla.net/api/v1/recipe_revision/"
}
```

INSPECTOR

Request Headers (6)

Response Headers (18)

Kali 2021 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Burp Suite Community E... Damn Vulnerable Web A... mrhacker@kali: ~

Burp Suite Community Edition v2020.12.1 - Temporary Project

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options

1 × ...

Send Cancel < > Follow redirection

Request

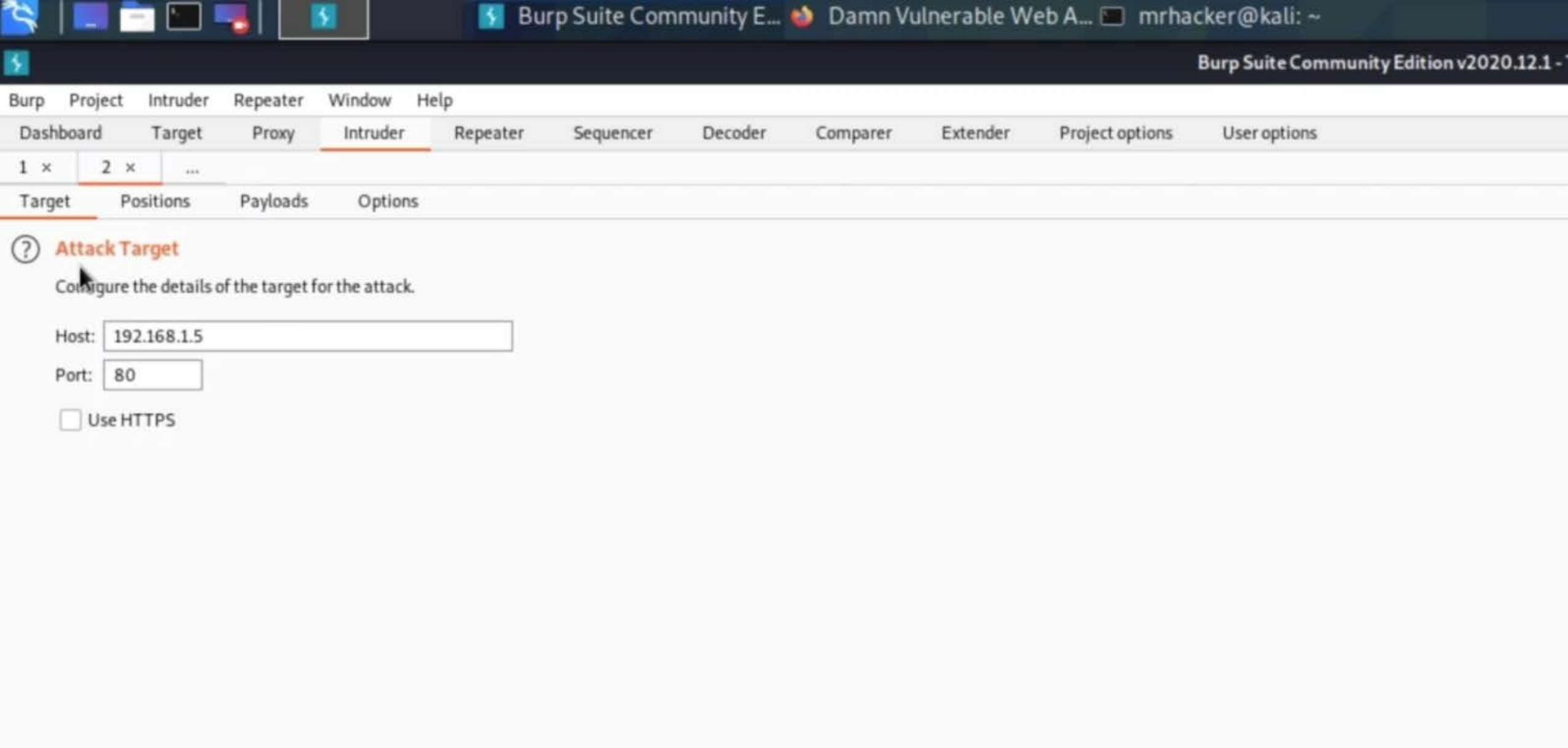
Pretty Raw \n Actions

```
1  POST /dvwa/login.php HTTP/1.1
2  Host: 192.168.1.5
3  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5  Accept-Language: en-US,en;q=0.5
6  Accept-Encoding: gzip, deflate
7  Content-Type: application/x-www-form-urlencoded
8  Content-Length: 39
9  Origin: http://192.168.1.5
10 Connection: close
11 Referer: http://192.168.1.5/dvwa/login.php
12 Cookie: security=low; PHPSESSID=t9vcql2kn0ton0uk8j8nd0lai7; acopendivids=swingset,jotto,phpbb2,redmine;
   acgroupswithpersist=nada
13 Upgrade-Insecure-Requests: 1
14
15 username=test&password=test&Login=Login
```

Response

Pretty Raw Render \n Actions

```
1  HTTP/1.1 302 Found
2  Date: Tue, 09 Mar 2021 09:17:49 GMT
3  Server: Apache/2.2.14 (Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.30 w
4  X-Powered-By: PHP/5.3.2-1ubuntu4.30
5  Expires: Thu, 19 Nov 1981 08:52:00 GMT
6  Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre
7  Pragma: no-cache
8  Location: login.php
9  Vary: Accept-Encoding
10 Content-Length: 0
11 Connection: close
12 Content-Type: text/html
13
14
```


Burp Suite Community E...
Damn Vulnerable Web A...
mrhacker@kali: ~
Burp Suite Community Edition v2020.12.1 -
Burp
Project
Intruder
Repeater
Window
Help
Dashboard
Target
Proxy
Intruder
Repeater
Sequencer
Decoder
Comparer
Extender
Project options
User options
1 ×
2 ×
...
Target
Positions
Payloads
Options
Attack Target
Configure the details of the target for the attack.
Host:
192.168.1.5
Port:
80
Use HTTPS

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options

1 × 2 × 3 × ...

Target Positions Payloads Options

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

```
1  POST /dvwa/login.php HTTP/1.1
2  Host: 192.168.1.5
3  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5  Accept-Language: en-US,en;q=0.5
6  Accept-Encoding: gzip, deflate
7  Content-Type: application/x-www-form-urlencoded
8  Content-Length: 39
9  Origin: http://192.168.1.5
10 Connection: close
11 Referer: http://192.168.1.5/dvwa/login.php
12 Cookie: security=§low§; PHPSESSID=§t9vcql2kn0ton0uk8j8nd0lai7§; acopendivids=§swingset,jotto,phpbb2,redmine§; acgroupswithpersist=§nada§
13 Upgrade-Insecure-Requests: 1
14
15 username=§test§&password=§test§&Login=§Login§
```

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options

1 × 2 × 3 × ...

Target Positions Payloads Options

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

```
1  POST /dvwa/login.php HTTP/1.1
2  Host: 192.168.1.5
3  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5  Accept-Language: en-US,en;q=0.5
6  Accept-Encoding: gzip, deflate
7  Content-Type: application/x-www-form-urlencoded
8  Content-Length: 39
9  Origin: http://192.168.1.5
10 Connection: close
11 Referer: http://192.168.1.5/dvwa/login.php
12 Cookie: security=low; PHPSESSID=t9vcql2kn0ton0uk8j8nd0lai7; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada
13 Upgrade-Insecure-Requests: 1
14
15 username=admin&password=§test§&Login=Login
```

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options

1 × 2 × 3 × ...

Target Positions Payloads Options

Payload Sets

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 typ

Payload set: 1 Payload count: 7

Payload type: Simple list Request count: 7

Payload Options [Simple list]

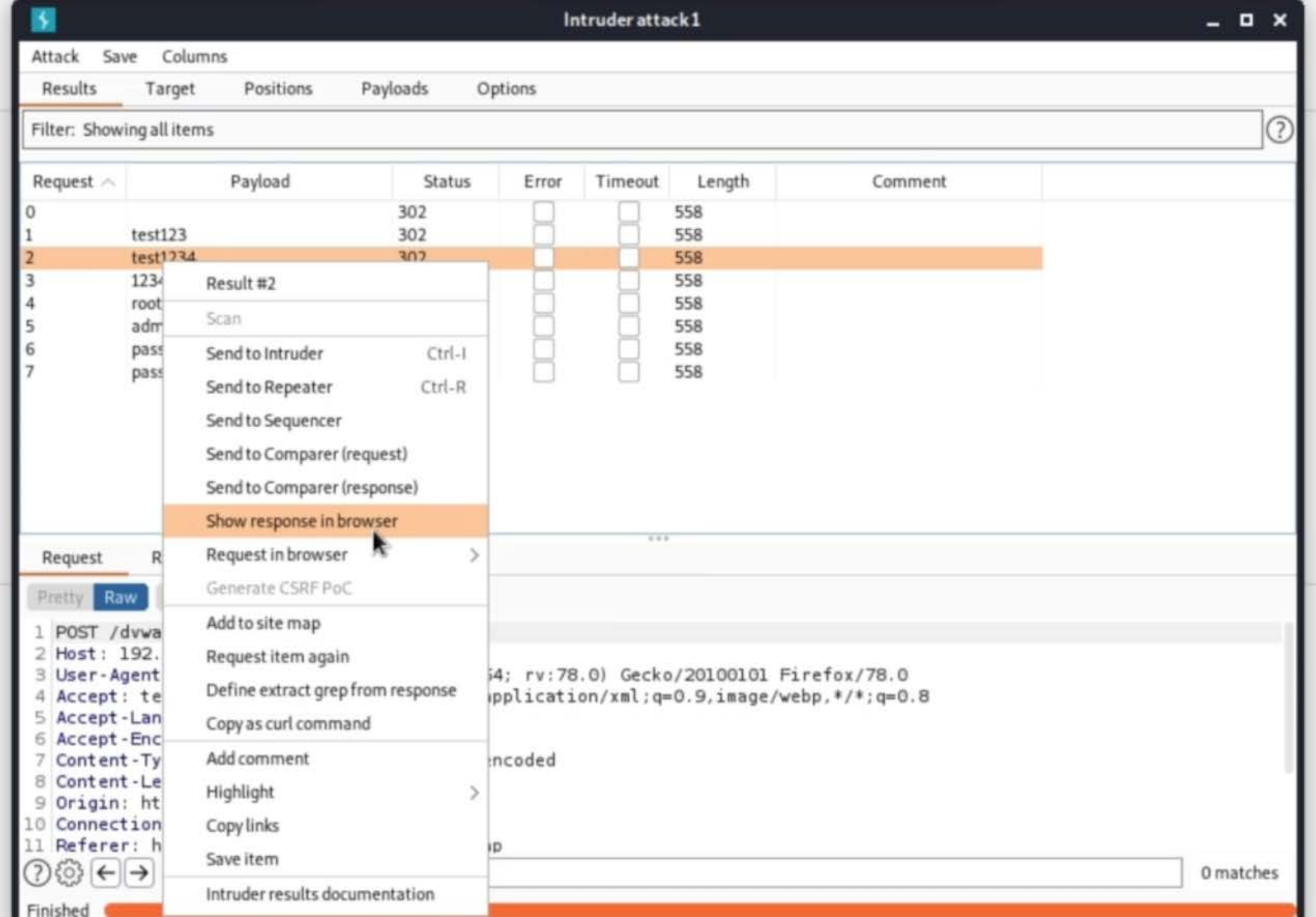
This payload type lets you configure a simple list of strings that are used as payloads.

Paste
Load ...
Remove
Clear

test123
test1234
12345
root
admin
password
password123

Add

Add from list ... [Pro version only]


Intruder attack 1
Attack
Save
Columns
Results
Target
Positions
Payloads
Options
Filter: Showing all items
Request
Payload
Status
Error
Timeout
Length
Comment
0
302
558
1
test123
302
558
2
302
558
3
558
4
558
5
558
6
558
7
558
Result #2
Scan
Send to Intruder Ctrl-I
Send to Repeater Ctrl-R
Send to Sequencer
Send to Comparer (request)
Send to Comparer (response)
Show response in browser
Request in browser
Generate CSRF PoC
Add to site map
Request item again
Define extract grep from response
Copy as curl command
Add comment
Highlight
Copy links
Save item
Intruder results documentation
Request
Pretty
Raw
1 POST /dvwa
2 Host: 192.
3 User-Agent
4 Accept: te
5 Accept-Lan
6 Accept-Enc
7 Content-Ty
8 Content-Le
9 Origin: ht
10 Connection
11 Referer: h
64; rv:78.0) Gecko/20100101 Firefox/78.0
pplication/xml;q=0.9,image/webp,*/*;q=0.8
ncoded
0 matches
Finished