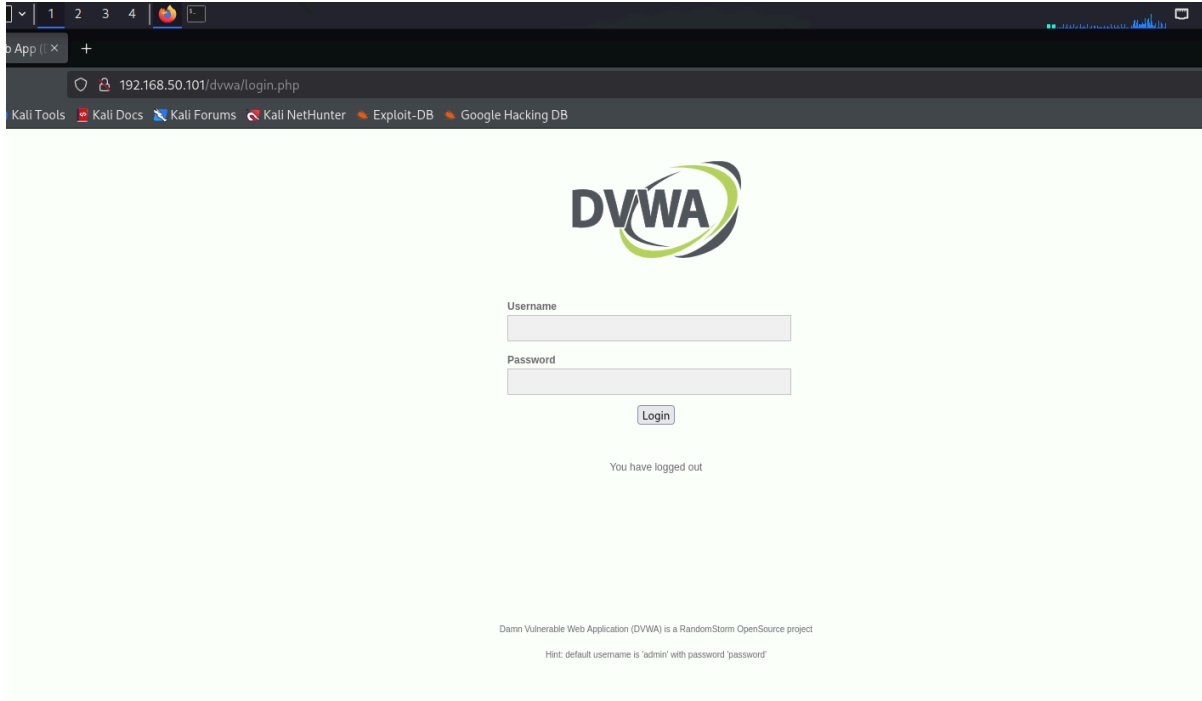
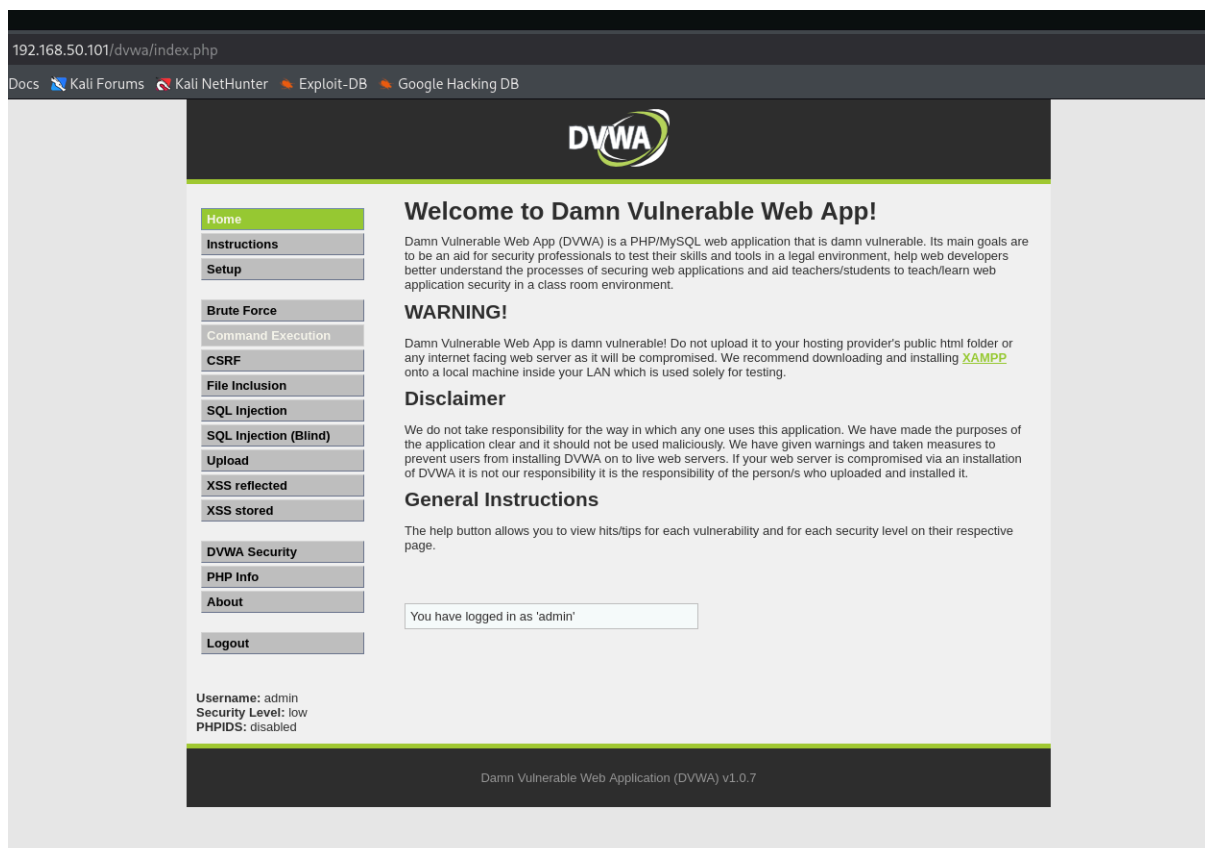


W8D1 - DVWA e Burpsuite

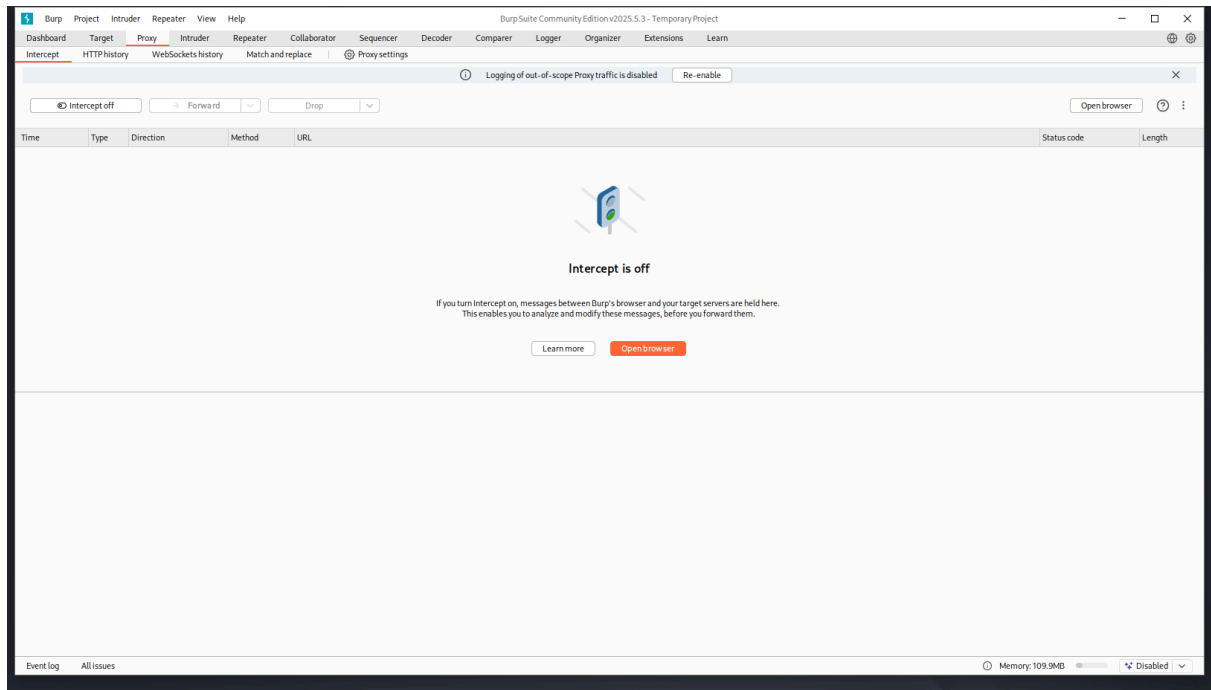
ecco sotto la home di DVWA tramite metasploitable con IP 192.168.50.101



Facciamo l'accesso con
username: admin
password: password



apriamo Burpsuite e clicchiamo “Open browser”



con intercept attivo, entriamo su DVWA e facciamo il login con le credenziali

Burp Suite Community Edition v2025.5.3 - Temporary Project

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn

Site map Scope Issues

Logging of out-of-scope Proxy traffic is disabled Re-enable

Site map filter: Hiding out of scope and not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

> 192.168.50.101

Host	Method	URL	Params	Status code	Length	MIME type	Title	Notes
http://192.168.50.101	GET	/		200	1124	HTML	Metasploitable2 - Linux	
http://192.168.50.101	GET	/dwva/dwva/js/dwvaPage.js		200	1086	script		
http://192.168.50.101	GET	/dwva/index.php		200	4933	HTML	Damn Vulnerable Web App (DVWA...)	
http://192.168.50.101	GET	/dwva/login.php		200	1636	HTML	Damn Vulnerable Web App (DVWA...)	
http://192.168.50.101	GET	/dwva/		302	482			
http://192.168.50.101	POST	/dwva/login.php	✓	302	392			
http://192.168.50.101	GET	/dav/						
http://192.168.50.101	GET	/dwva/about.php						

Request

Pretty Raw Hex

```
1 POST /dwva/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/137.0.0.0 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/dwva/login.php
12 Accept-Encoding: gzip, deflate, br
13 Cookie: security=high; PHPSESSID=0e741f0e9937780b04d8c76410dc35ec
14 Connection: keep-alive
15
16 username=admin&password=password&Login=Login
```

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 302 Found
2 Date: Mon, 01 Sep 2025 20:57:25 GMT
3 Server: Apache/2.2.8 (Ubuntu) DAV/2
4 X-Powered-By: PHP/5.2.4-2ubuntu5.10
5 Expires: Thu, 19 Nov 1981 08:52:00 GMT
6 Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
7 Pragma: no-cache
8 Location: index.php
9 Content-Length: 0
10 Keep-Alive: timeout=15, max=100
11 Connection: Keep-Alive
12 Content-Type: text/html
13
14
```

Inspector

Request attributes

Request body parameters

Request cookies

Request headers

Response headers

Event log All issues

Memory: 109.9MB

andando su Target si può vedere le attività di login su DVWA, la richiesta e la risposta con anche le credenziali. Se facciamo tasto destro e si seleziona “Send to Repeater” fa vedere la richiesta dove si può fare delle modifiche e vedere che risposta ci può dare. Per esempio se cambio la password e invio questa è la risposta:

The screenshot shows the Burp Suite Repeater interface. The 'Request' tab is active, displaying a POST request to `/dvwa/login.php`. The request body contains the following data:

```
POST /dvwa/login.php HTTP/1.1
Host: 192.168.50.101
Content-Length: 43
Cache-Control: max-age=0
Accept-Language: en-US,en;q=0.9
Origin: http://192.168.50.101
Content-Type: application/x-www-form-urlencoded
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=0e741f0e9937780b04d8c76410dc35ec
Connection: keep-alive
username=admin&password=Pippo23&Login=Login
```

The 'Response' tab is also visible, showing the server's response:

```
HTTP/1.1 302 Found
Date: Mon, 01 Sep 2025 21:14:30 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Location: login.php
Content-Length: 0
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Content-Type: text/html
```

come si può vedere la risposta da come location ancora `login.php` e non `index.php`, per l'appunto se clicchiamo “Follow redirection” ci fa vedere il codice HTML della risposta e nella body si legge `Login failed`

The screenshot shows the 'Response' tab in Burp Suite Repeater, displaying the HTML body of the response. The code is as follows:

```
44
45
46      <label for="pass">
          Password
        </label>
        <input type="password" class="loginInput" AUTOCOMPLETE="
off" size="20" name="password">
        <br />
47
48
49      <p class="submit">
          <input type="submit" value="Login" name="Login">
        </p>
50
51      </fieldset>
52
53    </form>
54
55
56    <br />
57
58    <div class="message">
        Login failed
    </div>
59
60    <br />
61    <br />
62    <br />
63    <br />
64    <br />
65    <br />
```

FACOLTATIVO:

sinceramente non ho potuto vedere dei cambiamenti a parte nella richiesta su Cookie:
security=low/medium/high