

## BURP SUITE

### Analizzare ed intercettare una richiesta di login

Per questa attività utilizziamo la web application **DVWA**, configurandola come in foto:

## Database Setup

Click on the 'Create / Reset Database' button below to create or reset your database.  
If you get an error make sure you have the correct user credentials in: `/var/www/html/DVWA/config/config.inc.php`

If the database already exists, **it will be cleared and the data will be reset.**  
You can also use this to reset the administrator credentials ("**admin // password**") at any stage.

---

## Setup Check

Web Server SERVER\_NAME: **127.0.0.1**

Operating system: **\*nix**

PHP version: **8.1.5**  
 PHP function display\_errors: **Disabled**  
 PHP function safe\_mode: **Disabled**  
 PHP function allow\_url\_include: **Disabled**  
 PHP function allow\_url\_fopen: **Enabled**  
 PHP function magic\_quotes\_gpc: **Disabled**  
 PHP module gd: **Missing - Only an issue if you want to play with captchas**  
 PHP module mysql: **Installed**  
 PHP module pdo\_mysql: **Installed**

Backend database: **MySQL/MariaDB**  
 Database username: **kali**  
 Database password: **\*\*\*\*\***  
 Database database: **dvwa**  
 Database host: **127.0.0.1**  
 Database port: **3306**

reCAPTCHA key: **Missing**

[User: root] Writable folder /var/www/html/DVWA/hackable/uploads/: **Yes**  
 [User: root] Writable file /var/www/html/DVWA/external/phpids/0.6/lib/IDS/tmp/phpids\_log.txt: **Yes**

[User: root] Writable folder /var/www/html/DVWA/config: **Yes**  
**Status in red**, indicate there will be an issue when trying to complete some modules.

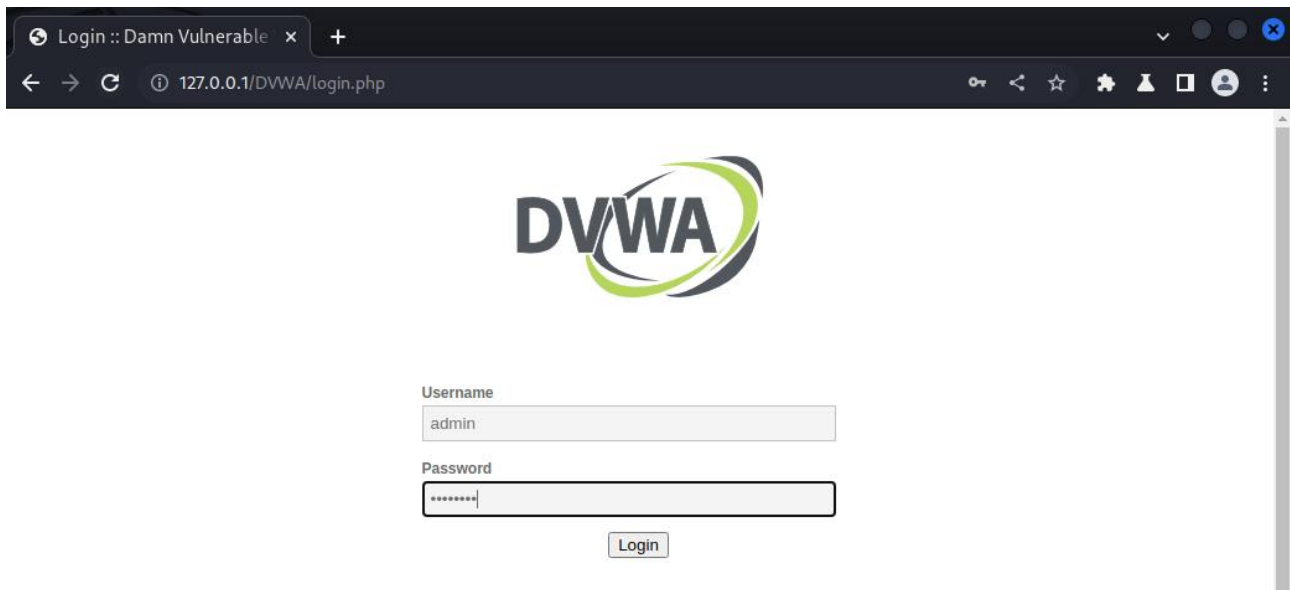
If you see disabled on either `allow_url_fopen` or `allow_url_include`, set the following in your `php.ini` file and restart Apache.

**allow\_url\_fopen = On**  
**allow\_url\_include = On**

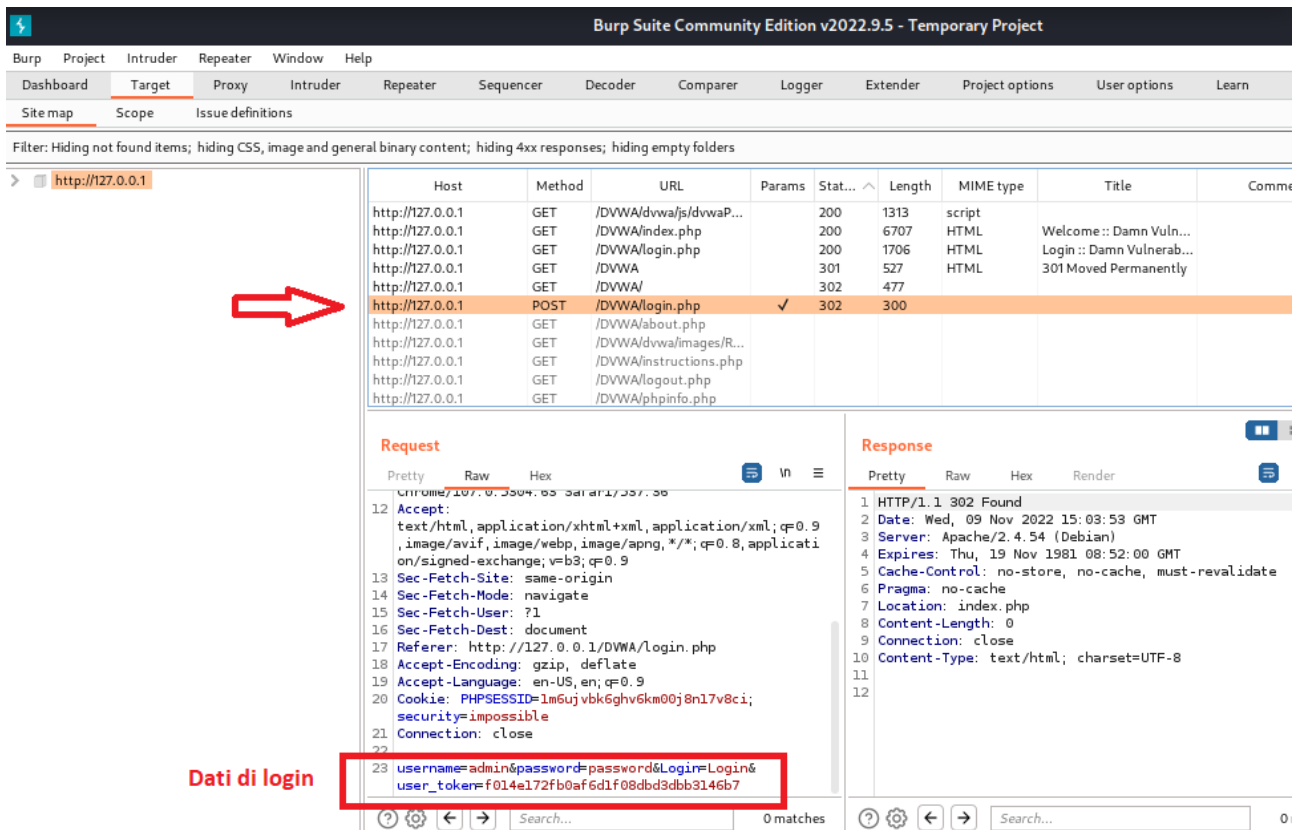
These are only required for the file inclusion labs so unless you want to play with those, you can ignore them.

[Create / Reset Database](#)

Adesso avviamo il tool BurpSuite e accediamo da browser all'indirizzo **127.0.0.1/DVWA** utilizzando le credenziali **admin** e **password**



Nello stesso momento, intercettiamo ed analizziamo le richieste HTTP focalizzandoci sulla richiesta con metodo **POST**, che contiene i dati di login inviati dal client al server. Selezionandola, possiamo vedere in chiaro le credenziali usate per il login.



Burp Suite Community Edition v2022.9.5 - Temporary Project

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

Site map Scope Issue definitions

Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

Host	Method	URL	Params	Stat...	Length	MIME type	Title	Comme
http://127.0.0.1	GET	/DVWA/dvwa/js/dvwaP...		200	1313	script		
http://127.0.0.1	GET	/DVWA/index.php		200	6707	HTML	Welcome :: Damn Vuln...	
http://127.0.0.1	GET	/DVWA/login.php		200	1706	HTML	Login :: Damn Vulnerab...	
http://127.0.0.1	GET	/DVWA/		301	527	HTML	301 Moved Permanently	
http://127.0.0.1	POST	/DVWA/login.php		✓ 302	300			
http://127.0.0.1	GET	/DVWA/about.php						
http://127.0.0.1	GET	/DVWA/dvwa/images/R...						
http://127.0.0.1	GET	/DVWA/instructions.php						
http://127.0.0.1	GET	/DVWA/logout.php						
http://127.0.0.1	GET	/DVWA/phpinfo.php						

**Request**

Pretty Raw Hex

```
12 Chrome/107.0.5304.65 Safari/537.36
13 Accept:
14 text/html,application/xhtml+xml,application/xml;q=0.9
15 ,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
16 Sec-Fetch-Site: same-origin
17 Sec-Fetch-Mode: navigate
18 Sec-Fetch-User: ?1
19 Referer: http://127.0.0.1/DVWA/login.php
20 Accept-Encoding: gzip, deflate
21 Accept-Language: en-US,en;q=0.9
22 Cookie: PHPSESSID=1m6ujvbk6ghv6km00j8n17v8ci;
23 security=impossible
24 Connection: close
25
26 username=admin&password=password&Login=Login&
27 user_token=f014e172fb0af6d1f08dbd3dbb3146b7
```

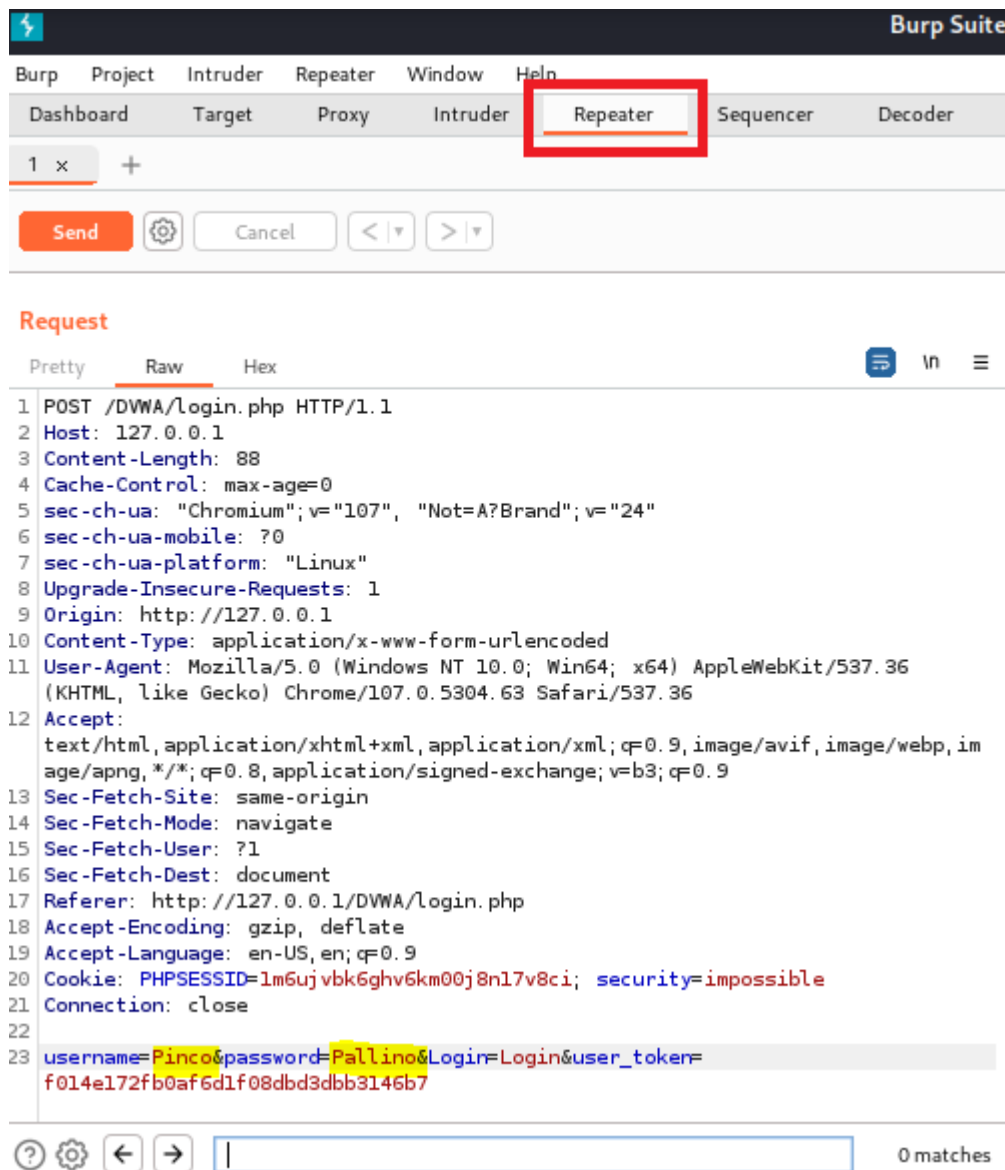
**Dati di login**

**Response**

Pretty Raw Hex Render

```
1 HTTP/1.1 302 Found
2 Date: Wed, 09 Nov 2022 15:03:53 GMT
3 Server: Apache/2.4.54 (Debian)
4 Expires: Thu, 19 Nov 1981 08:52:00 GMT
5 Cache-Control: no-store, no-cache, must-revalidate
6 Pragma: no-cache
7 Location: index.php
8 Content-Length: 0
9 Connection: close
10 Content-Type: text/html; charset=UTF-8
11
12
```

Proviamo adesso, tramite il modulo **repeater**, a modificare la richiesta di login con credenziali inventate:



The screenshot shows the Burp Suite interface with the Repeater module selected. The 'Request' tab is active, displaying a list of request details. The request is a POST to /DVWA/login.php. The body contains login credentials: username=Pinco&password=Pallino&Login=Login&user\_token=f014e172fb0af6d1f08dbd3dbb3146b7. The Repeater module is highlighted with a red box.

**Burp Suite**

Menu: Burp, Project, Intruder, Repeater, Window, Help

Toolbar: Dashboard, Target, Proxy, Intruder, **Repeater**, Sequencer, Decoder

1 x +

Buttons: Send, Cancel, <|, >|

**Request**

Pretty Raw Hex

```
1 POST /DVWA/login.php HTTP/1.1
2 Host: 127.0.0.1
3 Content-Length: 88
4 Cache-Control: max-age=0
5 sec-ch-ua: "Chromium"; v="107", "Not=A?Brand"; v="24"
6 sec-ch-ua-mobile: ?0
7 sec-ch-ua-platform: "Linux"
8 Upgrade-Insecure-Requests: 1
9 Origin: http://127.0.0.1
10 Content-Type: application/x-www-form-urlencoded
11 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
    (KHTML, like Gecko) Chrome/107.0.5304.63 Safari/537.36
12 Accept:
    text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,im
    age/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-User: ?1
16 Sec-Fetch-Dest: document
17 Referer: http://127.0.0.1/DVWA/login.php
18 Accept-Encoding: gzip, deflate
19 Accept-Language: en-US,en;q=0.9
20 Cookie: PHPSESSID=1m6ujvbk6ghv6km00j8n17v8ci; security=impossible
21 Connection: close
22
23 username=Pinco&password=Pallino&Login=Login&user_token=
    f014e172fb0af6d1f08dbd3dbb3146b7
```

0 matches

Adesso inviamo la richiesta. Come si può vedere, nel body della pagina html visualizziamo il feedback che riceviamo è **“login failed”**.

The screenshot displays the Burp Suite interface with the 'Repeater' tab selected. The 'Request' pane on the left shows an HTTP GET request to `/DVWA/login.php` with various headers including `Host: 127.0.0.1`, `Cache-Control: max-age=0`, `sec-ch-ua: "Chromium"; v="107", "Not=A?Brand"; v="24"`, `sec-ch-ua-mobile: ?0`, `sec-ch-ua-platform: "Linux"`, `Upgrade-Insecure-Requests: 1`, `Origin: http://127.0.0.1`, `User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.5304.63 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=0.9`, `Sec-Fetch-Site: same-origin`, `Sec-Fetch-Mode: navigate`, `Sec-Fetch-User: ?1`, `Sec-Fetch-Dest: document`, `Referer: http://127.0.0.1/DVWA/login.php`, `Accept-Encoding: gzip, deflate`, `Accept-Language: en-US,en;q=0.9`, and a cookie `PHPSESSID=lm6ujvbk6ghv6km00j8n17v8ci; security=impossible`. The 'Response' pane on the right shows the HTML output, which includes a submit button and a hidden input field. A red arrow points to the message `Login failed` within a `<div class="message">` block.

**Request**

```
1 GET /DVWA/login.php HTTP/1.1
2 Host: 127.0.0.1
3 Cache-Control: max-age=0
4 sec-ch-ua: "Chromium"; v="107", "Not=A?Brand"; v="24"
5 sec-ch-ua-mobile: ?0
6 sec-ch-ua-platform: "Linux"
7 Upgrade-Insecure-Requests: 1
8 Origin: http://127.0.0.1
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
  (KHTML, like Gecko) Chrome/107.0.5304.63 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=0.9
11 Sec-Fetch-Site: same-origin
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-User: ?1
14 Sec-Fetch-Dest: document
15 Referer: http://127.0.0.1/DVWA/login.php
16 Accept-Encoding: gzip, deflate
17 Accept-Language: en-US,en;q=0.9
18 Cookie: PHPSESSID=lm6ujvbk6ghv6km00j8n17v8ci; security=impossible
19 Connection: close
20
21
```

**Response**

```
50
51 <br />
52
53 <p class="submit">
54   <input type="submit" value="Login" name="Login">
55 </p>
56
57 </fieldset>
58
59 <input type='hidden' name='user_token' value='
60   f39612b2d4233147486090e4a468c02f' />
61
62 </form>
63
64 <br />
65
66 <div class="message">
67   Login failed
68 </div>
69
70 <br />
71 <br />
72 <br />
73 <br />
74 <br />
75 <br />
76 <br />
77 <br />
78 <br />
79 <br />
80 <br />
81 <br />
82 <br />
83 <br />
84 <br />
85 <br />
86 <br />
87 <br />
88 <br />
89 <br />
90 <br />
91 <br />
92 <br />
93 <br />
94 <br />
95 <br />
96 <br />
97 <br />
98 <br />
99 <br />
100 <br />
```