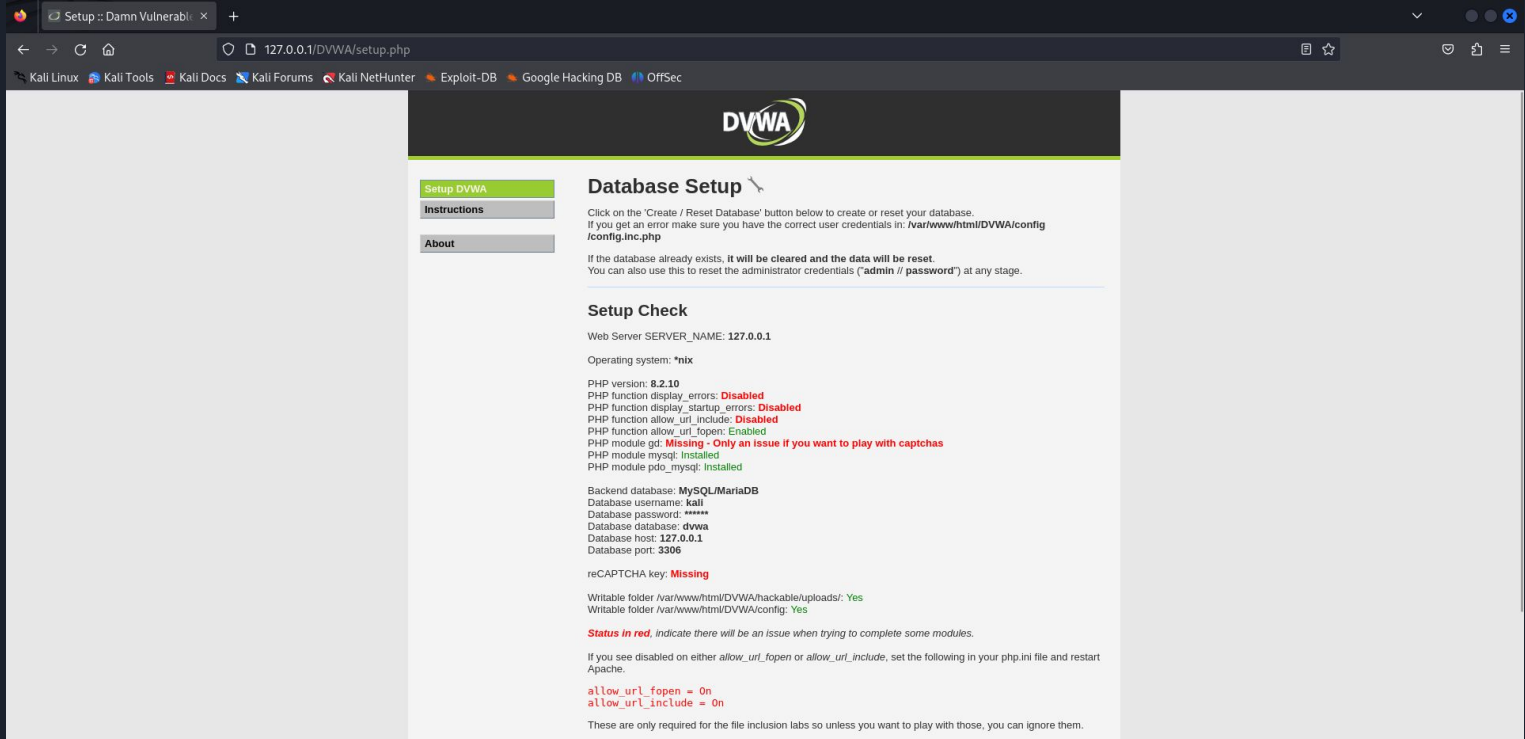




Consegna S3/L3 Cybersecurity

Riccardo Agostino Monti

Seguendo le slide tutto funziona correttamente.



The screenshot shows a web browser window with the address bar displaying `127.0.0.1/DVWA/setup.php`. The browser's tab is titled "Setup - Damn Vulnerable". The page content is for the "Database Setup" section of the DVWA application. On the left, there is a sidebar with three tabs: "Setup DVWA" (highlighted in green), "Instructions", and "About". The main content area has a dark header with the DVWA logo. Below the header, the "Database Setup" section is titled. It contains instructions on how to create or reset the database, mentioning the correct user credentials in `/var/www/html/DVWA/config/config.inc.php`. It also states that if the database already exists, it will be cleared and the data will be reset. Below this, there is a "Setup Check" section that displays various system and configuration details. These details include the web server name (`127.0.0.1`), operating system (`*nix`), PHP version (`8.2.10`), and various PHP functions and modules. Some items are marked as "Disabled" in red, while others are "Enabled" or "Installed" in green. The backend database is identified as `MySQL/MariaDB` with the username `kali` and password `*****`. The database name is `dvwa` and the host is `127.0.0.1`. The port is `3306`. The reCAPTCHA key is marked as "Missing" in red. Writable folders are confirmed as "Yes". A note at the bottom states that items in red indicate issues when trying to complete some modules. It also provides instructions on how to fix disabled functions by editing the `php.ini` file and restarting Apache. Finally, it mentions that some modules are only required for file inclusion labs.

Setup DVWA

Instructions

About

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: `8.2.10`
PHP function display_errors: **Disabled**
PHP function display_startup_errors: **Disabled**
PHP function allow_url_include: **Disabled**
PHP function allow_url_fopen: **Enabled**
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**

Writable folder `/var/www/html/DVWA/hackable/uploads/`: **Yes**
Writable folder `/var/www/html/DVWA/config/`: **Yes**

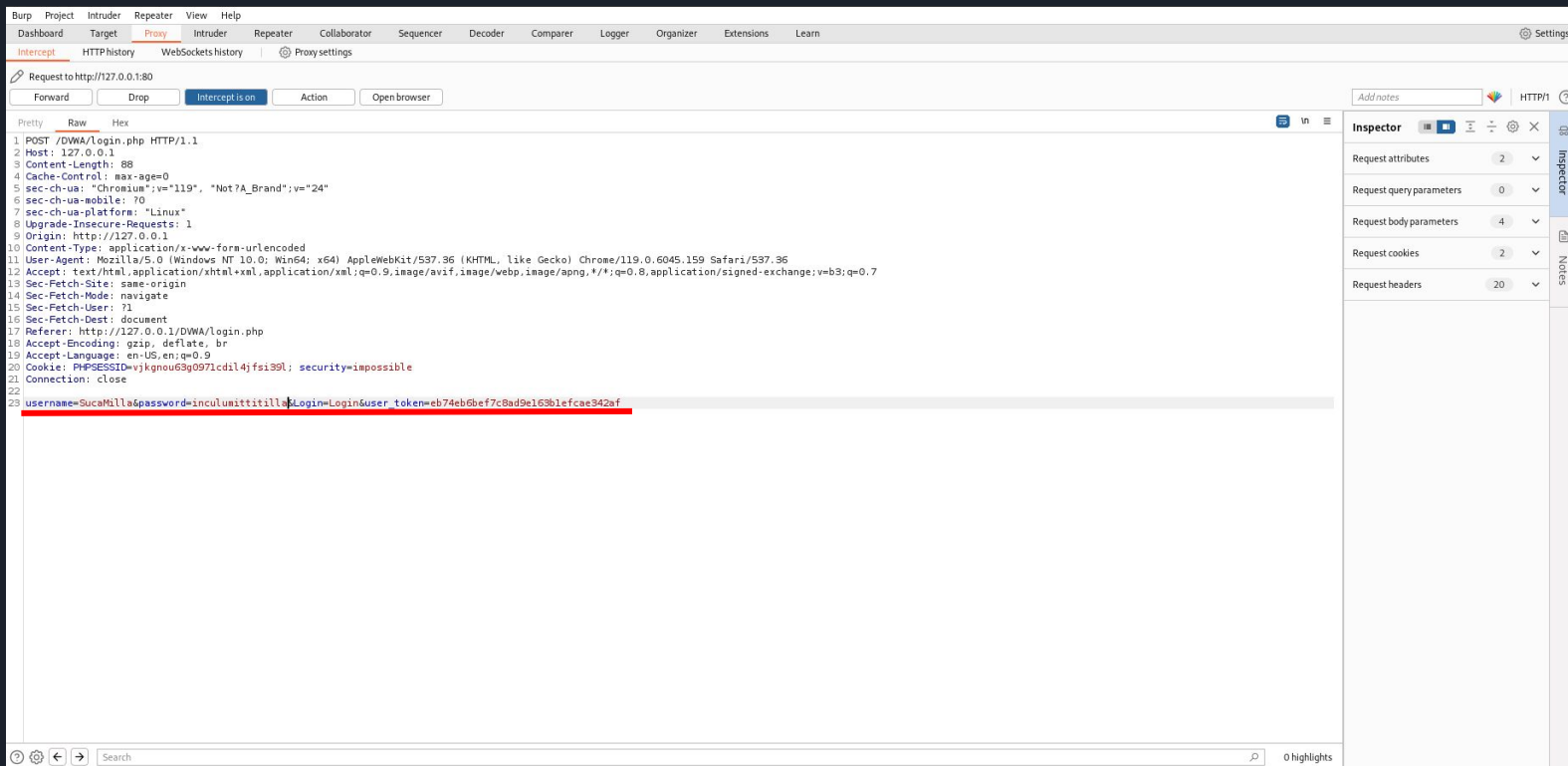
Status in red, indicate there will be an issue when trying to complete some modules.

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.

Cambiamo le credenziali inviate

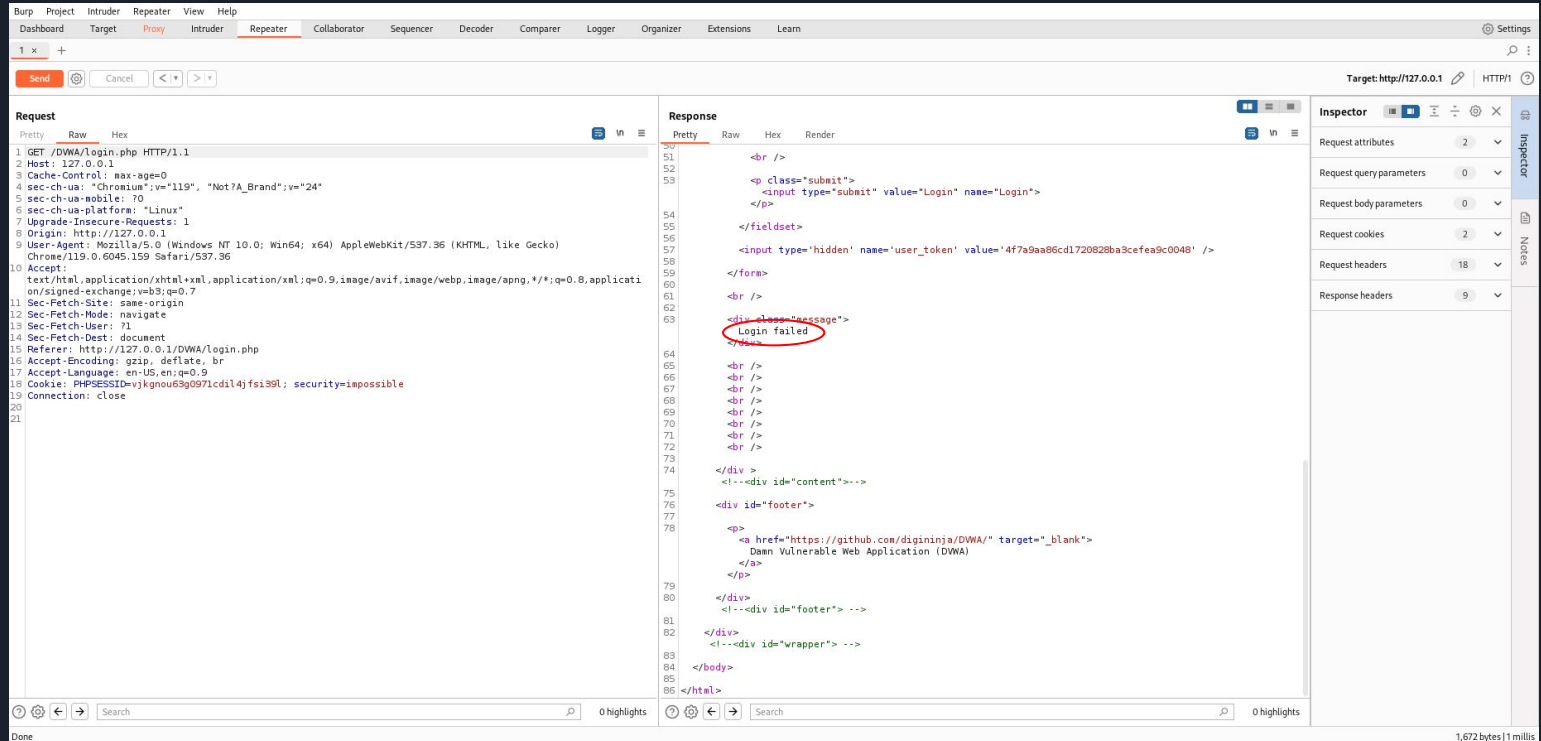


Burp Suite interface showing an intercepted HTTP request to `http://127.0.0.1:80`. The request is a POST to `/DWA/login.php` with the following body:

```
1 POST /DWA/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="119", "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/119.0.6045.159 Safari/537.36
12 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
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/DWA/login.php
18 Accept-Encoding: gzip, deflate, br
19 Accept-Language: en-US,en;q=0.9
20 Cookie: PHPSESSID=vjkgno69y097lcdil4jfsi39l; security=impossible
21 Connection: close
22
23 username=SuccaMilla&password=inculumittitillo&Login=Login&user_token=eb74eb6bef7c8ad9e163b1efcae342af
```

The request body is highlighted in red. The interface also shows the 'Inspector' panel on the right, which displays the request details.

Mandiamo tutto al repeater e come ci aspettavamo il risultato è "Login Failed"



The screenshot displays the Burp Suite Repeater interface. The 'Request' tab on the left shows an HTTP GET request to `/DWA/login.php` with various headers including `Cache-Control: max-age=0`, `sec-ch-ua: "Chromium";v="119"`, `Origin: http://127.0.0.1`, and `User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.6045.159 Safari/537.36`. The 'Response' tab on the right shows the server's reply, which is an HTML page. A red circle highlights the text `Login failed` within the response body. The right sidebar contains the 'Inspector' panel with expandable sections for Request attributes, Request query parameters, Request body parameters, Request cookies, Request headers, and Response headers.

Request

```
1 GET /DWA/login.php HTTP/1.1
2 Host: 127.0.0.1
3 Cache-Control: max-age=0
4 sec-ch-ua: "Chromium";v="119", "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/119.0.6045.159 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 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/DWA/login.php
16 Accept-Encoding: gzip, deflate, br
17 Accept-Language: en-US,en;q=0.9
18 Cookie: PHPSESSID=vjkgnou63g097lclil4jfsi99l; security=impossible
19 Connection: close
20
21
```

Response

```
50 <br />
51
52 <p class="submit">
53   <input type="submit" value="Login" name="Login">
54 </p>
55
56 </fieldset>
57
58 <input type="hidden" name="user_token" value="4f7a9aa86cd1720828ba3cefa9c0048" />
59
60 </form>
61 <br />
62
63 <div class="message">
64   Login failed
65 </div>
66 <br />
67 <br />
68 <br />
69 <br />
70 <br />
71 <br />
72 <br />
73
74 </div>
75 <!--div id="content"-->
76
77 <div id="footer">
78
79   <a href="https://github.com/digininga/DWA/" target="_blank">
80     Dawn Vulnerable Web Application (DWA)
81   </a>
82 </div>
83 <!--div id="footer"-->
84
85 </div>
86 <!--div id="wrapper"-->
87
88 </body>
89
90 </html>
```

Target: http://127.0.0.1 HTTP/1

Inspector

- Request attributes: 2
- Request query parameters: 0
- Request body parameters: 0
- Request cookies: 2
- Request headers: 18
- Response headers: 9

Done

1,672 bytes | 1 millis