


ESERCIZIO WEB APPLICATION

setup.php

NetHunter Exploit-DB Google Hacking DB OffSec



Home

Instructions

Setup / Reset DB

Brute Force

Command Injection

CSRF

File Inclusion

File Upload

Insecure CAPTCHA

SQL Injection

SQL Injection (Blind)

Weak Session IDs

XSS (DOM)

XSS (Reflected)

XSS (Stored)

CSP Bypass

JavaScript

DVWA Security

PHP Info

About

Logout

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: 8.1.12
PHP function display_errors: Disabled
PHP function safe_mode: Disabled
PHP function allow_url_include: Enabled
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.

kali-linux-2022.4-virtualbox-amd64 [In esecuzione] - Oracle VM VirtualBox

File Macchina Visualizza Inserimento Dispositivi Aiuto

DVWA Security :: Damn Vulnerable

127.0.0.1/DVWA/login.php



Username
admin

Password

Login

You have logged out

Burp Suite Community Edition v2022.9.6 - Temporary Project

Dashboard Project Intruder Repeater Window Help

Intercept HTTP History WebSockets History Options

Request to http://127.0.0.1:80

Forward Drop Intercept is on Action Open Browser

Pretty Raw Hex

```
1 POST /DVWA/login.php HTTP/1.1
2 Host: 127.0.0.1
3 Content-Length: 80
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/107.0.5304.107 Safari/537.36
12 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml;q=0.9,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=v26vdeutlg27qg3pdfnv442ikt; security=impossible
21 Connection: close
22
23 username=admin&password=password&Login=Login&user_token=b606ea28056dec9b615d442a1f1923f2
```

Cambio Username e Password:

The image shows a Kali Linux virtual machine with DVWA Security installed. The browser window displays the DVWA login page with the username 'admin' and a masked password. The Burp Suite interface is open, showing an intercepted POST request to http://127.0.0.1/DVWA/login.php. The request body is visible in the 'Raw' tab, showing a standard login attempt with user 'admin' and a password. The 'Intercept' tab is active, and the 'Intercept is on' button is highlighted.

Send to Repeater:

The image shows the Burp Suite Repeater tab. A request has been sent to http://127.0.0.1/DVWA/login.php. The response is displayed in the 'Response' tab, showing an HTML page with the title 'Login :: Damn Vulnerable Web Application (DVWA) v1.10 *Development*'. The response body contains a login form with a 'Login' button. The 'Request' tab is also visible, showing the details of the intercepted request.

Login Fallito:

burp project intruder repeater window help

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

1 x +

Send Cancel < >

Request

Pretty Raw Hex

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="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/107.0.5304.107 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/DWA/login.php

16 Accept-Encoding: gzip, deflate

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

18 Cookie: PHPSESSID=v26vdeudtg27qg3pdfnv442ikt; security=impossible

19 Connection: close

20

21

Response

Pretty Raw Hex Render

52

53 <p class="submit">

54 <input type="submit" value="Login" name="Login">

55 </p>

56 </fieldset>

57 <input type="hidden" name="user_token" value="184003da83bf0b5432f52c04c3b452a0" />

58 </form>

59

60

61 <div class="message">

62 Login failed

63 </div>

64

65

66

67

68

69

70

71

72

73

