

+

127.0.0.1/DVWA/setup.php

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

Authorisation Bypass

Open HTTP Redirect

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: 8.2.12
PHP function display_errors: **Disabled**
PHP function display_startup_errors: **Disabled**
PHP function allow_url_include: **Enabled**
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.

Create / Reset Database

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

POST /DVWA/login.php HTTP/1.1

Host: 127.0.0.1

Content-Length: 75

Cache-Control: max-age=0

sec-ch-ua: "Not A Brand";v="0", "Chromium";v="120"

sec-ch-ua-mobile: ?0

sec-ch-ua-platform: "Linux"

Upgrade-Insecure-Requests: 1

Origin: http://127.0.0.1

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

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.6099.216 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

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, br

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

Cookie: security=impossible; PHPSESSID=q2074hrve77be6704k4eeqrvi

Connection: close

username=admin&password=ciao&login_login_token=082ae8885ca48396441edf2808ee7f

Inspector

Request attributes

Request query parameters

Request body parameters

Request cookies

Request headers

127.0.0.1/DVWA/login.php

DVWA

Username

Password

Login

Login failed