

M2_W8D2

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

Security Level

Security level is currently: **impossible**.

You can set the security level to low, medium, high or impossible. The security level changes the vulnerability level of DVWA:

1. Low - This security level is completely vulnerable and **has no security measures at all**. It's use is to be as an example of how web application vulnerabilities manifest through bad coding practices and to serve as a platform to teach or learn basic exploitation techniques.
2. Medium - This setting is mainly to give an example to the user of **bad security practices**, where the developer has tried but failed to secure an application. It also acts as a challenge to users to refine their exploitation techniques.
3. High - This option is an extension to the medium difficulty, with a mixture of **harder or alternative bad practices** to attempt to secure the code. The vulnerability may not allow the same extent of the exploitation, similar in various Capture The Flags (CTFs) competitions.
4. Impossible - This level should be **secure against all vulnerabilities**. It is used to compare the vulnerable source code to the secure source code.
Prior to DVWA v1.9, this level was known as 'high'.

Impossible ▾

Submit

Intercettazione del traffico con BURP SUITE sulla pagina di Log In

Burp Suite Community Edition v2023.12.1.3 - Temporary Project

Burp

Project

Intruder

Repeater

View

Help

Dashboard

Target

Proxy

Intruder

Repeater

Collaborator

Sequencer

Decoder

Comparer

Logger

Organizer

Extensions

Intercept

HTTP history

WebSockets history

Proxy settings

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 User-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:109.0) Gecko/20100101 Firefox/115.0

4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8

5 Accept-Language: en-US,en;q=0.5

6 Accept-Encoding: gzip, deflate, br

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

8 Content-Length: 88

9 Origin: http://127.0.0.1

10 Connection: close

11 Referer: http://127.0.0.1/DVWA/login.php

12 Cookie: security=impossible; PHPSESSID=e0rfb112fpvp432enlhgogjmgn

13 Upgrade-Insecure-Requests: 1

14 Sec-Fetch-Dest: document

15 Sec-Fetch-Mode: navigate

16 Sec-Fetch-Site: same-origin

17 Sec-Fetch-User: ?1

18

19 username=admin&password=password&Login=Login&user_token=a05f2d909ec1fc3e53e3fb84951fe0f2

Request		Response	
Pretty	Raw	Pretty	Raw
<pre> 1 POST /DVWA/login.php HTTP/1.1 2 Host: 127.0.0.1 3 User-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:109.0) Gecko/20100101 Firefox/115.0 4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif, image/webp,*/*;q=0.8 5 Accept-Language: en-US,en;q=0.5 6 Accept-Encoding: gzip, deflate, br 7 Content-Type: application/x-www-form-urlencoded 8 Content-Length: 85 9 Origin: http://127.0.0.1 10 Connection: close 11 Referer: http://127.0.0.1/DVWA/login.php 12 Cookie: PHPSESSID=gps8h3qlu54lm43ikuvorga9sq; security=low 13 Upgrade-Insecure-Requests: 1 14 Sec-Fetch-Dest: document 15 Sec-Fetch-Mode: navigate 16 Sec-Fetch-Site: same-origin 17 Sec-Fetch-User: ?1 18 19 username=pippo&password=baudo&Login=Login&user_token= 241b09dc0114fed071718c37cbaca492 </pre>		<pre> 1 HTTP/1.1 302 Found 2 Date: Wed, 31 Jan 2024 14:30:47 GMT 3 Server: Apache/2.4.58 (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 Set-Cookie: PHPSESSID=q53usfe19h4q7h9ckq56jl2d7g; expires=Thu, 01 Feb 2024 14:30:47 GMT; Max-Age=86400; path=/ 8 Location: login.php 9 Content-Length: 0 10 Connection: close 11 Content-Type: text/html; charset=UTF-8 12 13 </pre>	

Send

Cancel

< ▾

> ▾

Request

PrettyRawHex

in

1 GET /DVWA/login.php HTTP/1.1

2 Host: 127.0.0.1

3 User-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:109.0) Gecko/20100101 Firefox/115.0

4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8

5 Accept-Language: en-US,en;q=0.5

6 Accept-Encoding: gzip, deflate, br

7 Origin: http://127.0.0.1

8 Connection: close

9 Referer: http://127.0.0.1/DVWA/login.php

10 Cookie: PHPSESSID=s016lut730k49hkeu7dg6o4s02; security=impossible

11 Upgrade-Insecure-Requests: 1

12 Sec-Fetch-Dest: document

13 Sec-Fetch-Mode: navigate

14 Sec-Fetch-Site: same-origin

15 Sec-Fetch-User: ?1

16

17

Response

PrettyRawHexRender

in

1 HTTP/1.1 200 OK

2 Date: Wed, 31 Jan 2024 14:57:35 GMT

3 Server: Apache/2.4.58 (Debian)

4 Expires: Tue, 23 Jun 2009 12:00:00 GMT

5 Cache-Control: no-cache, must-revalidate

6 Pragma: no-cache

7 Vary: Accept-Encoding

8 Content-Length: 1342

9 Connection: close

10 Content-Type: text/html; charset=utf-8

11

12 <!DOCTYPE html>

13

14 <html lang="en-GB">

15

16 <head>

17

18 <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />

19

20 <title>

21 Login :: Damn Vulnerable Web Application (DVWA)

22 </title>

23

24 <link rel="stylesheet" type="text/css" href="dvwa/css/login.css" />

25

26 </head>

27

28 <body>

29

30 <div id="wrapper">