


DVWA è un'applicazione web scritta in PHP e MySQL, concepita piena zeppa di vulnerabilità più o meno facili da scovare. Progettata per testare il Penetration Testing ed ha la possibilità di configurare diversi livelli di difficoltà.



[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.

Create / Reset Database



[Home](#)
[Instructions](#)
[Setup / Reset DB](#)

DVWA Security

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

[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](#)

Username: admin
Security Level: Impossible
Locale: en

BurpSuite è un Proxy che permette di analizzare e modificare le richieste e le risposte scambiate tra clien-server.

Questo Proxy indaga sui siti Web per verificare la loro sicurezza. Infatti funge da filtro.

Se il client vuole aprire una pagina con protocollo HTML non avrà problemi, perché in chiaro, cioè visibile per tutti, mentre una pagina con protocollo HTTPS, essendo criptata, verrà bloccata non permettendo di procedere.

The screenshot displays the Burp Suite web application interface. At the top, there is a menu bar with options: Burp, Project, Intruder, Repeater, View, and Help. Below this is a sub-menu bar with: Dashboard, Target, Proxy (highlighted), Intruder, Repeater, Collaborator, Sequencer, Decoder, Comparer, Logger, Organizer, Extensions, and Learn. A 'Settings' gear icon is on the far right. Under the 'Proxy' tab, there are links for 'Intercept' (highlighted), 'HTTP history', 'WebSockets history', and 'Proxy settings'.

The main workspace shows a 'Request to http://127.0.0.1:80'. Below this, there are buttons: 'Forward', 'Drop', 'Intercept is on' (highlighted), 'Action', and 'Open browser'. To the right of these buttons is an 'Add notes' text field, a color palette icon, and 'HTTP/1' with a help icon.

The left pane shows the request details in 'Raw' format (selected over 'Pretty' and 'Hex'). The raw text is as follows:

```
1 GET /DVWA HTTP/1.1
2 Host: 127.0.0.1
3 sec-ch-ua: "Chromium"; v="119", "Not?A_Brand"; v="24"
4 sec-ch-ua-mobile: ?0
5 sec-ch-ua-platform: "Linux"
6 Upgrade-Insecure-Requests: 1
7 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
8 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
9 Sec-Fetch-Site: none
10 Sec-Fetch-Mode: navigate
11 Sec-Fetch-User: ?1
12 Sec-Fetch-Dest: document
13 Accept-Encoding: gzip, deflate, br
14 Accept-Language: en-US,en;q=0.9
15 Connection: close
16
17
```

The right pane is titled 'Inspector' and contains a list of request components with expandable dropdowns:

- Request attributes: 2
- Request query parameters: 0
- Request body parameters: 0
- Request cookies: 0
- Request headers: 14

On the far right of the Inspector pane, there are vertical tabs for 'Inspector' (selected) and 'Notes'.

At the bottom of the interface, there is a search bar with a magnifying glass icon and the text '0 highlights'.



Username

Password

Login

[Damn Vulnerable Web Application \(DVWA\)](#)

DashboardTargetProxyIntruderRepeaterCollaboratorSequencerDecoderComparerLoggerOrganizerExtensionsLearn

InterceptHTTP historyWebSockets historyProxy settings

Request to http://127.0.0.1:80

ForwardDropIntercept is onActionOpen browser

Add notesHTTP/1

PrettyRawHex

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="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/DVWA/login.php

18 Accept-Encoding: gzip, deflate, br

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

20 Cookie: security=impossible; PHPSESSID=iv59846c7ishe13nphositqt6l

21 Connection: close

22

23 username=admin&password=password&Login=Login&user_token=c2b2b77a5b385b598d74bde6d5de7ac8

Inspector

Request attributes2

Request query parameters0

Request body parameters4

Request cookies2

Request headers...

InspectorNotes

0 highlights

Request

Pretty

Raw

Hex

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: security=impossible; PHPSESSID=iv59846c7ishe13nphositqt6l

21

Connection: close

22

23

username=ciao&password=ciao&Login=Login&user_token=c2b2b77a5b385b598d74bde6d5de7ac8

Response

Pretty

Raw

Hex

Render

Inspector

Request attributes

2

Request query parameters

0

Request body parameters

4

Request cookies

2

Request headers

20

Inspector

Notes

Request

PrettyRawHex

1POST /DVWA/login.php HTTP/1.1

2Host: 127.0.0.1

3Content-Length: 83

4Cache-Control: max-age=0

5sec-ch-ua: "Chromium";v="119", "Not?A_Brand";v="24"

6sec-ch-ua-mobile: ?0

7sec-ch-ua-platform: "Linux"

8Upgrade-Insecure-Requests: 1

9Origin: http://127.0.0.1

10Content-Type: application/x-www-form-urlencoded

11User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.6045.159 Safari/537.36

12Accept: 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

13Sec-Fetch-Site: same-origin

14Sec-Fetch-Mode: navigate

15Sec-Fetch-User: ?1

16Sec-Fetch-Dest: document

17Referer: http://127.0.0.1/DVWA/login.php

18Accept-Encoding: gzip, deflate, br

19Accept-Language: en-US,en;q=0.9

20Cookie: security=impossible; PHPSESSID=iv59846c7ishe13nphositqt6l

21Connection: close

22

23username=ciao&password=ciao&Login=Login&user_token=c2b2b77a5b385b598d74bde6d5de7ac8

0 highlights

Response

PrettyRawHexRender

1HTTP/1.1 302 Found

2Date: Tue, 12 Dec 2023 14:02:00 GMT

3Server: Apache/2.4.58 (Debian)

4Expires: Thu, 19 Nov 1981 08:52:00 GMT

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

6Pragma: no-cache

7Location: login.php

8Content-Length: 0

9Connection: close

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

11

12

0 highlights

Inspector

Request attributes2

Request query parameters0

Request body parameters4

Request cookies2

Request headers20

Response headers9

InspectorNotes

Burp Project Intruder Repeater View Help

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn Settings

1 x +

Send Cancel < >

Target: http://127.0.0.1 HTTP/1

Request

Pretty Raw Hex

```
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="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,
10 like Gecko) Chrome/119.0.6045.159 Safari/537.36
11 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/
12 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/DVWA/login.php
18 Accept-Encoding: gzip, deflate, br
19 Accept-Language: en-US,en;q=0.9
20 Cookie: security=impossible; PHPSESSID=iv59846c7ishe13nphositqt6l
21 Connection: close
```

Response

Pretty Raw Hex Render

```
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 db30a5efc12c4ca47c2cfaddefb1094f' />
61
62 </form>
63
64 <div class="message">
65   Login failed
66 </div>
67
68 <br />
69 <br />
70 <br />
71 <br />
72 <br />
73 <br />
```

Inspector

Selection 12 (0xc)

Selected text

Login failed

Request attributes 2

Request query parameters 0

Request body parameters 0

Request cookies 2

Request headers 18

Response headers 9

Done 1,672 bytes | 43 millis

Questo esercizio prevede:

- la configurazione di una DVWA su Kali Linux;
- Creare un'utenza sul db di MySQL assegnando i privilegi;
- Andare all'indirizzo 127.0.0.1/DVWA/setup.php e creare un db e, cliccando su DVWA Security, scegliere i livello di sicurezza;
- Avviare BurnSuite e cambiare alcuni valori (tipo User e password).

Avviando BurpSuite, ed aprendo la pagina 127.0.0.1/DVWA col browser proprietario e selezionando “Intercep is On”, viene caricata una lista con tutte le informazioni di quella pagina.

Infatti troviamo:

- GET: indica la risorsa web;
- Host: l’indirizzo IP;

Per continuare la navigazione su questo sito dobbiamo cliccare su “Forward”, dando così il permesso tramite BurpSuite a vedere la pagina successiva.

Nella pagina successiva inserire username e password vedendo che BurpSuite blocca ulteriormente il proseguimento della navigazione.

Notiamo che su BurpSuite vengono visualizzate altre informazioni, tra cui username e password utilizzate.

Continuando a dare il permesso si riesce ad entrare sul sito.

Se sulla schermata dove vengono visualizzate username e password queste vengono cambiate, BurpSuite non permette di continuare la navigazione.