

DVWA e Burp Suite

L'obiettivo di questo lab pratico era prendere confidenza con la configurazione iniziale di **DVWA** e, soprattutto, iniziare a usare **Burp Suite** come strumento di **web-app testing**. Ho seguito le istruzioni di setup previste per il setup in locale di **DVWA**. Sono stati configurati i servizi **Apache2** e **MySQL**, e mi sono assicurato che entrambi fossero attivi e pronti a gestire correttamente l'applicazione web.

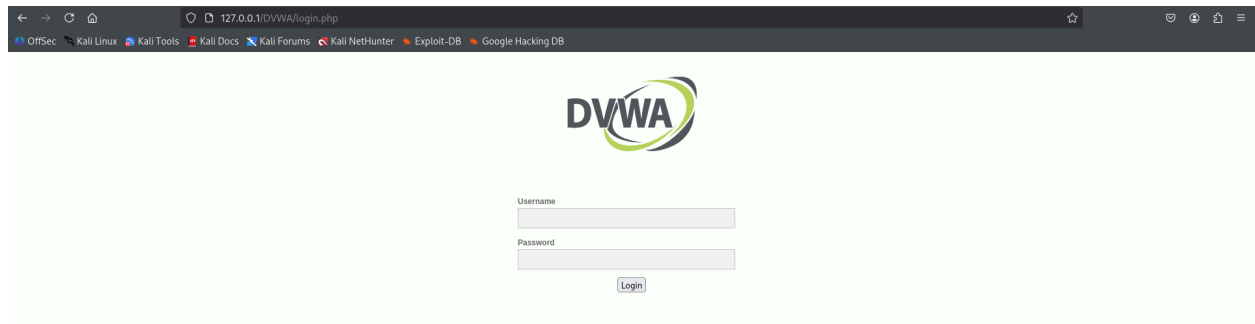
```
# Database variables
# WARNING: The database specified under db_database WILL BE ENTIRELY DELETED during setup.
# Please use a database dedicated to DVWA.
#
# If you are using MariaDB then you cannot use root, you must use create a dedicated DVWA user.
# See README.md for more information on this.
$DVWA = array();
$DVWA['db_server'] = getenv('DB_SERVER') ?: '127.0.0.1';
$DVWA['db_database'] = getenv('DB_DATABASE') ?: 'dvwa';
$DVWA['db_user'] = getenv('DB_USER') ?: 'kali';
$DVWA['db_password'] = getenv('DB_PASSWORD') ?: 'kali';
$DVWA['db_port'] = getenv('DB_PORT') ?: '3306';
```



```
(root@kali)~# service apache2 status
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/apache2.service; disabled; preset: disabled)
   Active: active (running) since Wed 2025-11-12 11:58:57 EST; 2min 59s ago
     Invocation: 90f4e495703542ea936a686d718a938f
       Docs: https://httpd.apache.org/docs/2.4/
   Process: 4433 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
    Main PID: 4449 (apache2)
       Tasks: 8 (limit: 4538)
      Memory: 25.5M (peak: 27.8M)
         CPU: 132ms
    CGroup: /system.slice/apache2.service
            └─4449 /usr/sbin/apache2 -k start
              └─4452 /usr/sbin/apache2 -k start
                └─4453 /usr/sbin/apache2 -k start
                  └─4454 /usr/sbin/apache2 -k start
                    └─4455 /usr/sbin/apache2 -k start
                      └─4456 /usr/sbin/apache2 -k start
                        └─5821 /usr/sbin/apache2 -k start
                          └─6118 /usr/sbin/apache2 -k start

Nov 12 11:58:57 kali systemd[1]: Starting apache2.service - The Apache HTTP Server...
Nov 12 11:58:57 kali apachectl[4448]: AH00558: apache2: Could not reliably determine the server's fully qualified domain name, using 127.0.1.1. Set the
Nov 12 11:58:57 kali systemd[1]: Started apache2.service - The Apache HTTP Server.

(root@kali)~# service mysql status
● mariadb.service - MariaDB 11.8.1 database server
   Loaded: loaded (/usr/lib/systemd/system/mariadb.service; disabled; preset: disabled)
   Active: active (running) since Wed 2025-11-12 11:56:52 EST; 5min ago
     Invocation: 8a943a2c80d84521b5269cc4e8ff76da
       Docs: man:mariadb(8)
            https://mariadb.com/kb/en/library/systemd/
   Process: 3242 ExecStartPre=/usr/bin/install -m 755 -o mysql -g root -d /var/run/mysql (code=exited, status=0/SUCCESS)
   Process: 3244 ExecStartPre=/bin/sh -c [ ! -e /usr/bin/galera_recovery ] && VAR=|| VAR=/usr/bin/galera_recovery; [ $? -eq 0 ] && echo _WSREP_
   Process: 3318 ExecStartPost=/bin/rm -f /run/mysql/wsrp-start-position (code=exited, status=0/SUCCESS)
   Process: 3320 ExecStartPost=/etc/mysql/debian-start (code=exited, status=0/SUCCESS)
    Main PID: 3297 (mariadb)
      Status: "Taking your SQL requests now..."
       Tasks: 13 (limit: 2995)
      Memory: 332M (peak: 421.7M)
         CPU: 2.850s
    CGroup: /system.slice/mariadb.service
            └─3297 /usr/sbin/mariadb
```

Una volta attivati i servizi, ho aperto il browser e navigato verso l'indirizzo **127.0.0.1/setup.php** per inizializzare il database dell'applicazione. Inizializzato il database sono stato reindirizzato in automatico all'endpoint **/login.php**. A questo punto la **Damn Vulnerable Web Application** era funzionante e **ready-to-rock**!





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 Attacks

Authorisation Bypass

Open HTTP Redirect

Cryptography

API

DVWA Security

PHP Info

About

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'.

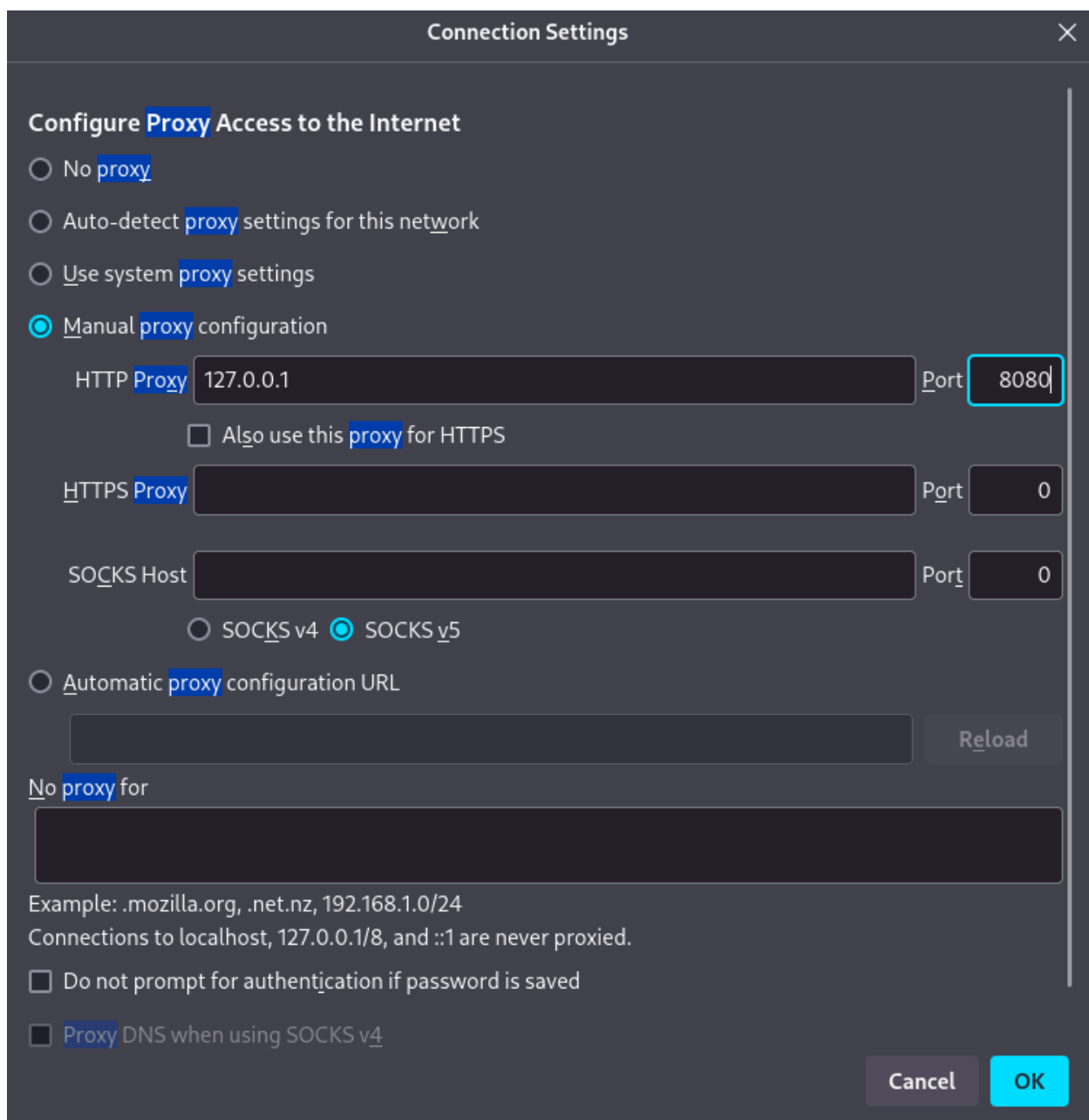
Low

Submit

Additional Tools

- [View Broken Access Control Logs](#) - View access logs for the Broken Access Control vulnerability

Per riuscire a fare pratica con **Burp Suite**, è stato necessario impostare il proxy su **127.0.0.1:8080**. Questo ha permesso a **Burp Suite** di intercettare le richieste del browser e di analizzarle o modificarle prima che raggiungano il server. Ci sono diversi modi di fare questo tipo di operazione. Il primo è quello di configurare il proxy manualmente in **Firefox** dalle impostazioni.



The image shows the 'Connection Settings' dialog box in Firefox. The 'Manual proxy configuration' option is selected. The HTTP Proxy is set to '127.0.0.1' and the Port is '8080'. The 'Also use this proxy for HTTPS' checkbox is unchecked. The HTTPS Proxy and SOCKS Host fields are empty, and their ports are set to '0'. The SOCKS version is set to 'SOCKS v5'. The 'Automatic proxy configuration URL' option is also unchecked, with an empty text field and a 'Reload' button. The 'No proxy for' section has an empty text field. At the bottom, there are checkboxes for 'Do not prompt for authentication if password is saved' and 'Proxy DNS when using SOCKS v4', both of which are unchecked. 'Cancel' and 'OK' buttons are at the bottom right.

Connection Settings

Configure Proxy Access to the Internet

- ☐ No proxy
- ☐ Auto-detect proxy settings for this network
- ☐ Use system proxy settings
- ☒ Manual proxy configuration

HTTP Proxy 127.0.0.1 Port 8080

☐ Also use this proxy for HTTPS

HTTPS Proxy Port 0

SOCKS Host Port 0

☐ SOCKS v4 ☒ SOCKS v5

☐ Automatic proxy configuration URL

Reload

No proxy for

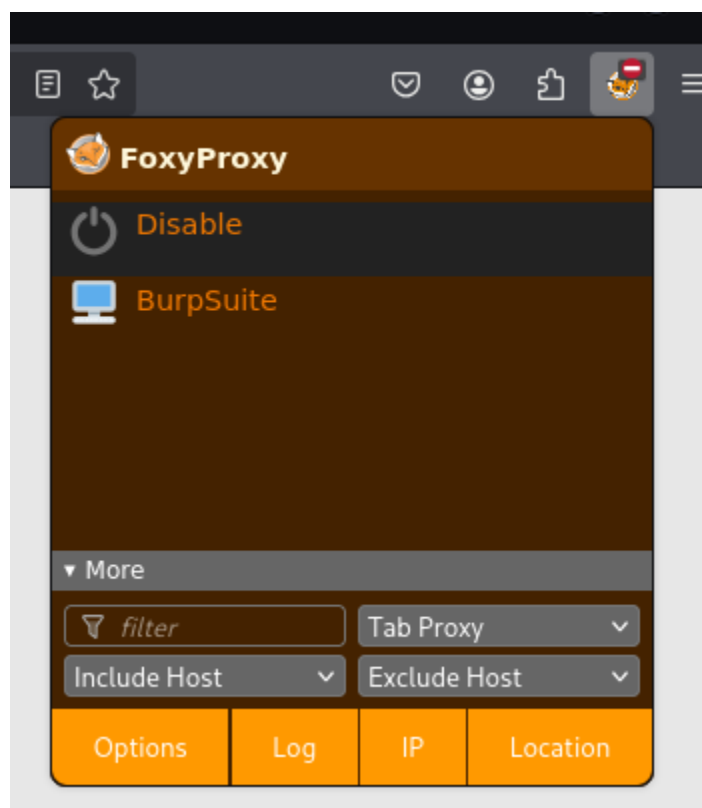
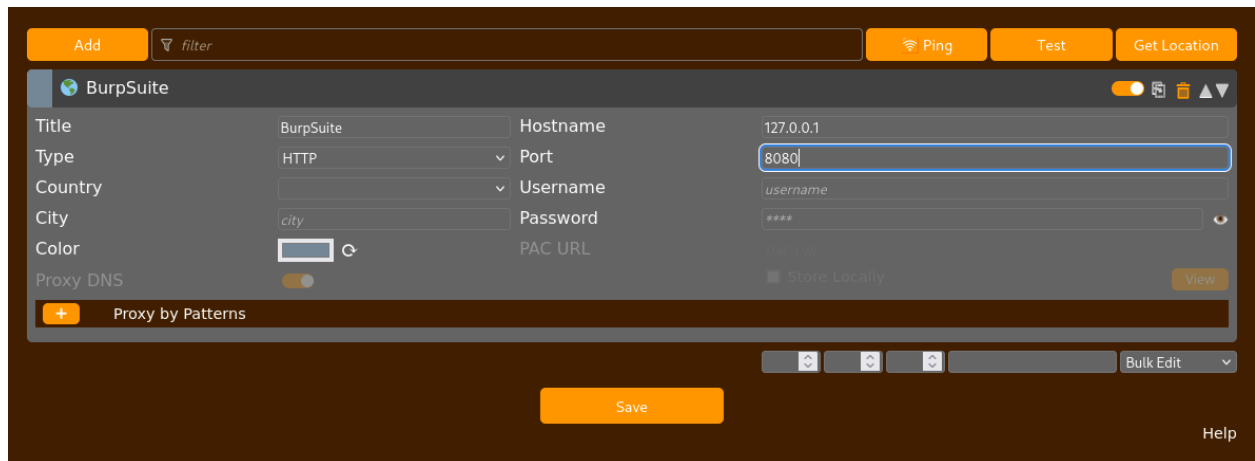
Example: .mozilla.org, .net.nz, 192.168.1.0/24
Connections to localhost, 127.0.0.1/8, and ::1 are never proxied.

☐ Do not prompt for authentication if password is saved

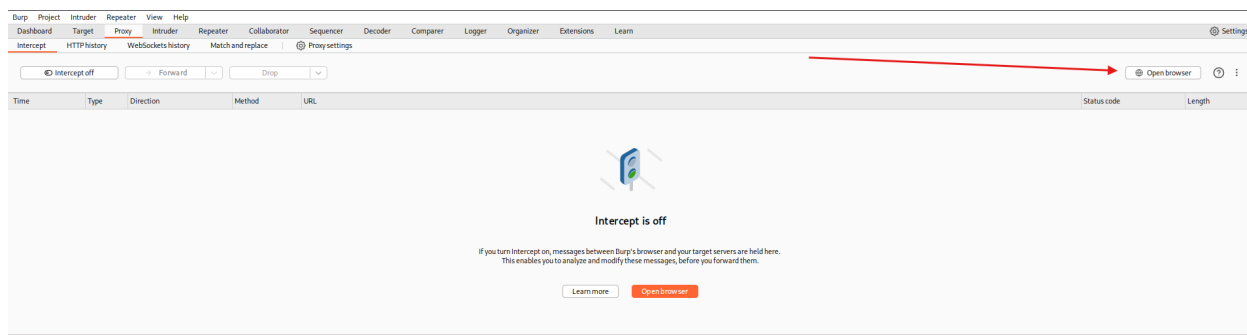
☐ Proxy DNS when using SOCKS v4

Cancel OK

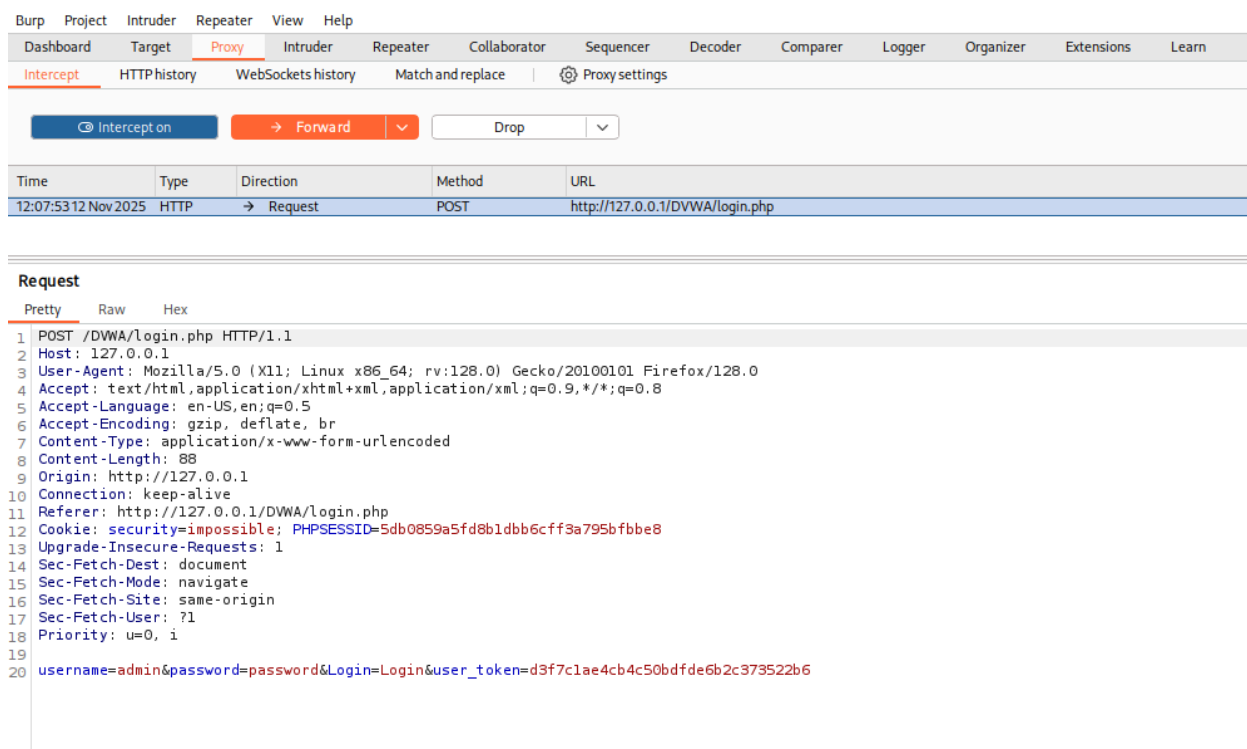
Per rendere il flusso più comodo e veloce è possibile (e consigliabile) utilizzare l'estensione **FoxyProxy**, che permette di passare con un click tra proxy diversi senza dover andare ogni volta nelle impostazioni del browser.



In alternativa (o per evitare di toccare le impostazioni del browser di sistema) è possibile utilizzare il browser integrato di **Burp** (basato su **Chromium**), già configurato per inviare richieste e ricevere risposte attraverso **Burp** senza ulteriori settaggi.



A questo punto **Burp Suite** poteva intercettare le mie richieste. Ho attivato l'**Interceptor**, sono andato sulla pagina **/login.php** e ho inviato una richiesta di login, che è stata poi intercettata da **Burp**.



Ho cliccato col tasto destro sulla richiesta e l'ho inviata a **Repeater**. A questo punto, senza modificarla ho lasciato che la richiesta arrivasse al server.

Request

PrettyRawHex

1POST /DVWA/login.php HTTP/1.1

2Host: 127.0.0.1

3User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0

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

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

6Accept-Encoding: gzip, deflate, br

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

8Content-Length: 88

9Origin: http://127.0.0.1

10Connection: keep-alive

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

12Cookie: security=impossible; PHPSESSID=5db0859a5fd8b1dbb6cff3a795bfbbe8

13Upgrade-Insecure-Requests: 1

14Sec-Fetch-Dest: document

15Sec-Fetch-Mode: navigate

16Sec-Fetch-Site: same-origin

17Sec-Fetch-User: ?1

18Priority: u=0, i

19

20username=admin&password=password&Login=Login&user_token=d3f7c1ae4cb4c50bdfde6b2c373522b6

Scan

Send to IntruderCtrl+I

Send to RepeaterCtrl+R

Send to Sequencer

Send to Comparer

Send to Decoder

Send to OrganizerCtrl+O

Insert Collaborator payload

Request in browser>

Engagement tools [Pro version only]>

Change request method

Change body encoding

CopyCtrl+C

Copy URL

Copy as curl command (bash)

Copy to file

Paste from file

Save item

Don't intercept requests>

Do intercept>

Convert selection>

URL-encode as you type

La risposta del server indicava un **302 Found** che puntava verso **index.php**; seguendo il redirect e renderizzando la pagina, ho potuto verificare che il login era avvenuto con successo e che ero autenticato correttamente.

1 x +

Send

Cancel

<>

>>

Follow redirection

Request

PrettyRawHex

1POST /DVWA/login.php HTTP/1.1

2Host: 127.0.0.1

3User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0

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

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

6Accept-Encoding: gzip, deflate, br

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

8Content-Length: 88

9Origin: http://127.0.0.1

10Connection: keep-alive

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

12Cookie: security=impossible; PHPSESSID=5db0859a5fd8b1dbb6cff3a795bfbbe8

13Upgrade-Insecure-Requests: 1

14Sec-Fetch-Dest: document

15Sec-Fetch-Mode: navigate

16Sec-Fetch-Site: same-origin

17Sec-Fetch-User: ?1

18Priority: u=0, i

19

20username=admin&password=password&Login=Login&user_token=d3f7c1ae4cb4c50bdfde6b2c373522b6

Response

PrettyRawHexRender

1HTTP/1.1 302 Found

2Date: Wed, 12 Nov 2025 17:09:40 GMT

3Server: Apache/2.4.63 (Debian)

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

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

6Pragma: no-cache

7Set-Cookie: PHPSESSID=74bc1f525eef8fd1f908f5a3b75c4dc4; expires=Thu, 13 Nov 2025 17:09:40 GMT; Max-Age=86400; path=/; HttpOnly; SameSite=Strict

8Location: login.php

9Content-Length: 0

10Keep-Alive: timeout=5, max=100

11Connection: Keep-Alive

12Content-Type: text/html; charset=UTF-8

13

14

The screenshot shows the Burp Suite interface with the **Repeater** tab selected. The **Request** pane on the left displays a raw HTTP request:

```
1 GET /DVWA/index.php HTTP/1.1
2 Host: 127.0.0.1
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;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: keep-alive
9 Referer: http://127.0.0.1/DVWA/login.php
10 Cookie: security=impossible; PHPSESSID=f33c83d033bb171b9966e042ee3c0f50
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 Priority: u=0, i
17
18
```

The **Response** pane on the right shows the rendered HTML of the DVWA homepage:

Welcome to Damn Vulnerable Web Appli

Damn Vulnerable Web Application (DVWA) is a PHP/MySQL web application that is da goal is to be an aid for security professionals to test their skills and tools in a legal envi developers better understand the processes of securing web applications and to aid bo learn about web application security in a controlled class room environment.

The aim of DVWA is to practice some of the most common web vulnerabilities, with difficulty, with a simple straightforward interface.

General Instructions

It is up to the user how they approach DVWA. Either by working through every module selecting any module and working up to reach the highest level they can before moving is not a fixed object to complete a module; however users should feel that they have su system as best as they possible could by using that particular vulnerability.

Please note: there are both documented and undocumented vulnerabilities with this

Ho ripetuto l'operazione usando **Repeater** e ho provato a inserire delle credenziali casuali. Ho inviato la richiesta al server e ho ricevuto una **302 Found** che questa volta puntava a **/login.php**. Questo ad indicare che il login non è riuscito e che sono stato reindirizzato nuovamente alla pagina di accesso.