

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.

```
# Host: 127.0.0.1
# Database variables 5.0 (X11) - Linux x86_64; rv:128.0 Gecko/20100101 Firefox/128.0
# WARNING: The database specified under db_database WILL BE ENTIRELY DELETED during setup.
# Please use a database dedicated to DVWA.
# Accept-Encoding: gzip, deflate, br
# 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]~[~/etc/php/8.4/apache2] 127.0.0.1 DVWA login page
└─# 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: 443 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.

[Login]
[User]
[Password]
[Login]

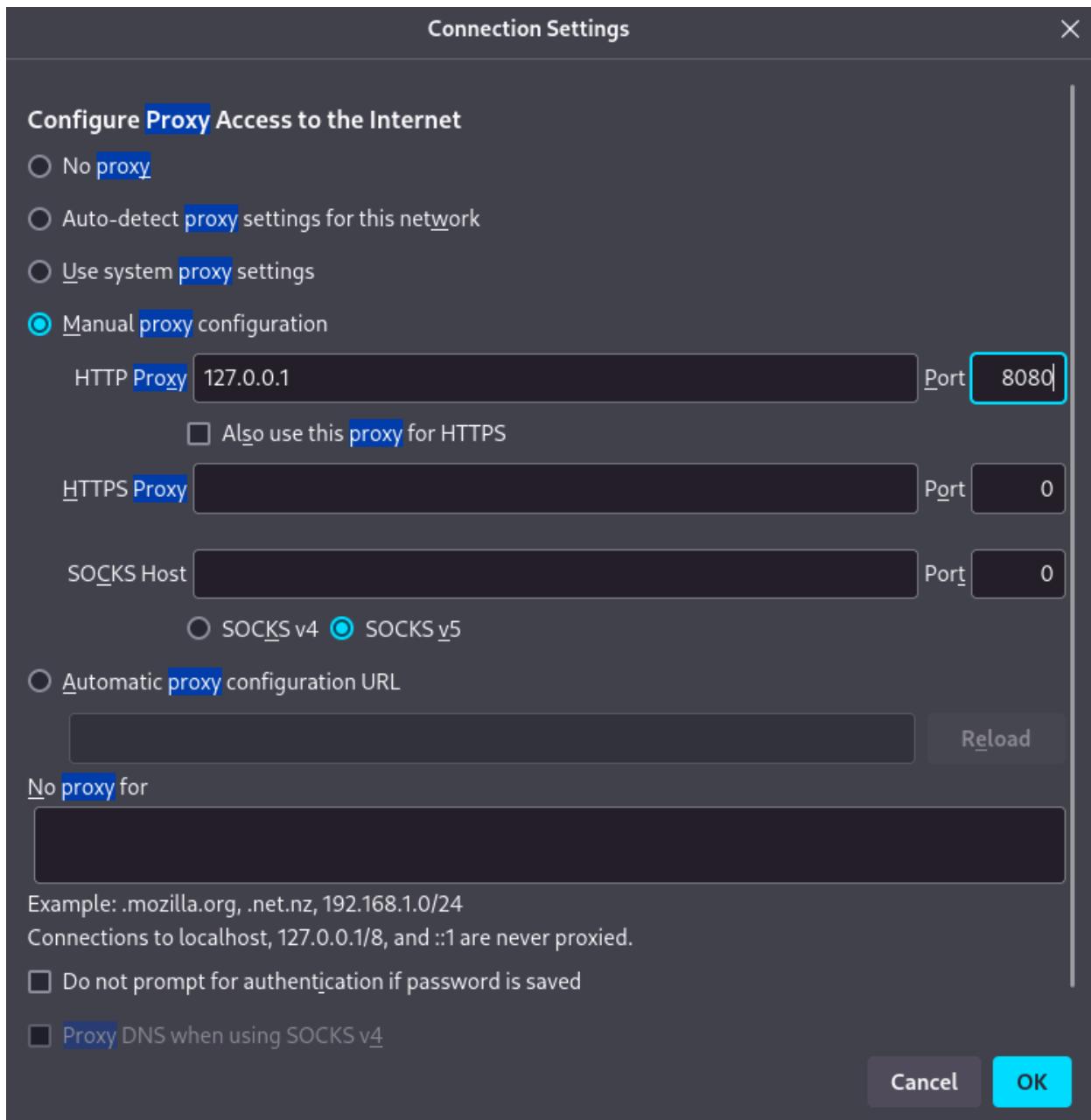
[root@kali]~[~/etc/php/8.4/apache2]
└─# service mysql status
● mariadb.service - MariaDB 11.8.1 database server
  Loaded: loaded (/usr/lib/systemd/system/mariadb.service; disabled; preset: disabled)
  Active: active (running) since Wed 2025-11-12 11:56:52 EST; 5min ago
  Invocation: 8a943a2c80d84521b5269cc4e8ff76da
    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/mysqld (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/wsrep-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!**

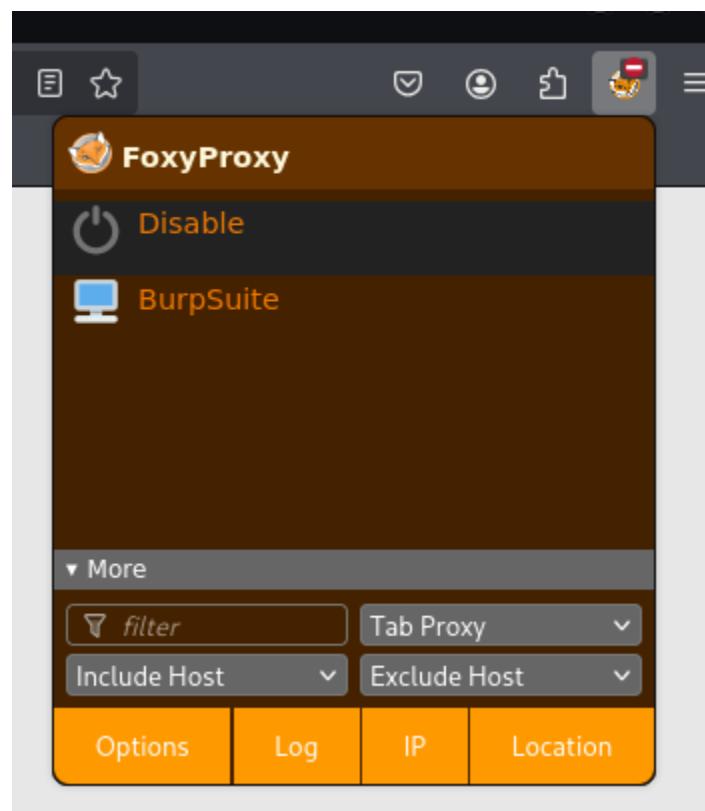
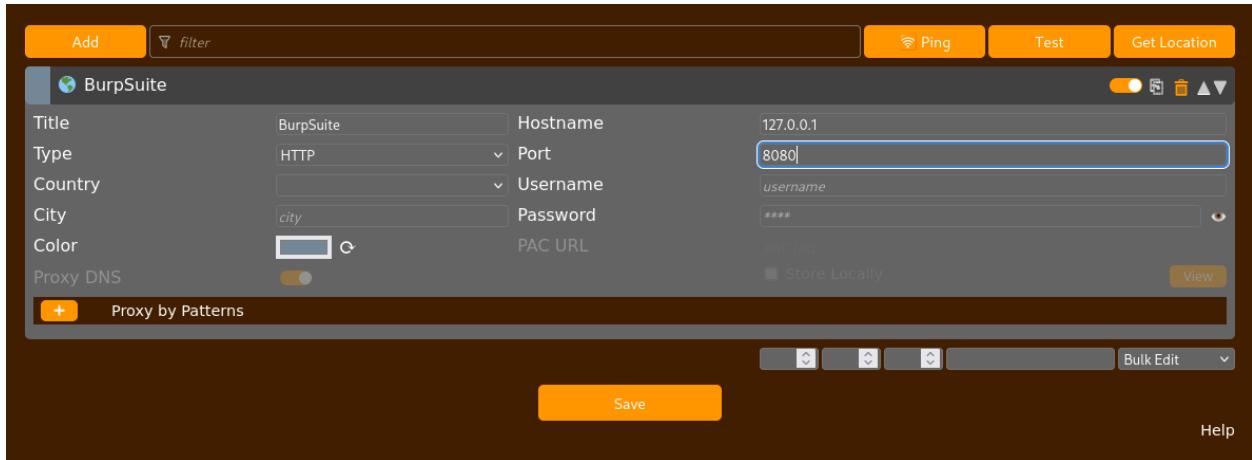


A screenshot of the DVWA security configuration page. The left sidebar contains a list of various security vulnerabilities: Home, Instructions, Setup / Reset DB, Brute Force, Command Injection, CSRF, File Inclusion, File Upload, Insecure CAPTCHA, SQL Injection, SQL Injection (Blind), Weak Session IDs, XSS (DOM), XSS (Reflected), XSS (Stored), CSP Bypass, JavaScript Attacks, Authorisation Bypass, Open HTTP Redirect, Cryptography, and API. The main content area shows the DVWA Security logo with a key icon. It displays the current security level as "impossible". A paragraph explains that the security level can be set to low, medium, high, or impossible, which changes the vulnerability level of DVWA. Below this is a dropdown menu set to "Low" and a "Submit" button. The "Additional Tools" section includes a link to "View Broken Access Control Logs". The bottom navigation bar includes links for DVWA Security, PHP Info, and About.

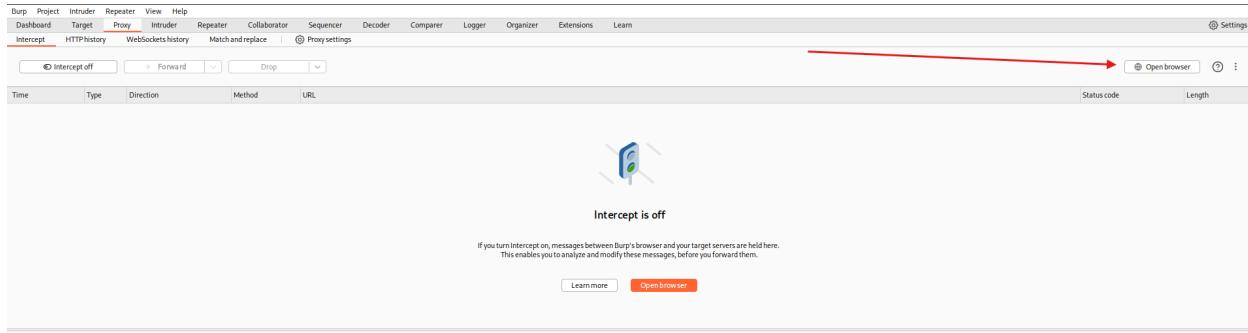
Per riuscire a fare pratica con **Burp Suite**, è stato necessario impostare il proxy su **127.0.0.1:8080**. Questo ha permesso a **Burp Suite** di intercettare le richieste del browser e di analizzarle o modificarle prima che raggiungano il server. Ci sono diversi modi di fare questo tipo di operazione.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



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**.

The screenshot shows the Burp Suite interface with the 'Proxy' tab selected. The 'Intercept on' button is highlighted with a blue bar. In the history list, a request for `http://127.0.0.1/DVWA/login.php` is shown, with the method set to POST. The 'Request' section below shows the raw HTTP request in 'Pretty' format:

```

1 POST /DVWA/login.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 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 88
9 Origin: http://127.0.0.1
10 Connection: keep-alive
11 Referer: http://127.0.0.1/DVWA/login.php
12 Cookie: security=impossible; PHPSESSID=5db0859a5fd8b1dbb6cff3a795bfbbe8
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 Priority: u0, i
19
20 username=admin&password=password&Login=Login&user_token=d3f7c1ae4cb4c50bdfde6b2c373522b6

```

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.

The screenshot shows the OWASp ZAP interface. On the left, there is a 'Request' panel with tabs for 'Pretty', 'Raw', and 'Hex'. A context menu is open over a selected line of the 'Pretty' tab, listing various options like 'Scan', 'Send to Intruder', 'Send to Repeater', etc. The 'Pretty' tab contains the following POST request:

```

1 POST /DVWA/login.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 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 88
9 Origin: http://127.0.0.1
10 Connection: keep-alive
11 Referer: http://127.0.0.1/DVWA/login.php
12 Cookie: security=impossible; PHPSESSID=5db0859a5fd8b1dbb6cff3a795fbbe8
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 Priority: u=0, i
19
20 username=admin&password=password&Login=Login&user_token=d3f7clae4cb4c50bdfde6b2c3

```

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.

The screenshot shows the OWASp ZAP interface with two panels: 'Request' and 'Response'. The 'Request' panel is identical to the one above. The 'Response' panel shows the following HTTP response:

```

HTTP/1.1 302 Found
Date: Wed, 12 Nov 2025 17:09:40 GMT
Server: Apache/2.4.63 (Debian)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Set-Cookie: PHPSESSID=74bc1f525eeff8fd1f908f5a3b75c4dc4; expires=Thu, 19 Nov 2025 17:09:40 GMT; Max-Age=3600; path=/; httpOnly; SameSite=Strict
Location: Login.php
Content-Length: 0
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

```

The screenshot shows the Burp Suite interface. In the Request tab, a GET request to 'DVWA/index.php' is displayed with the following headers:

```

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=f93c89d033bb171b9366e042ee3c0f50
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

```

In the Response tab, the DVWA login page is shown with the title 'Welcome to Damn Vulnerable Web Application'. The page includes a sidebar with links to various modules: Home, Instructions, Setup / Reset DB, Brute Force, Command Injection, CSRF, File Inclusion, File Upload, Insecure CAPTCHA, and SQL Injection.

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.