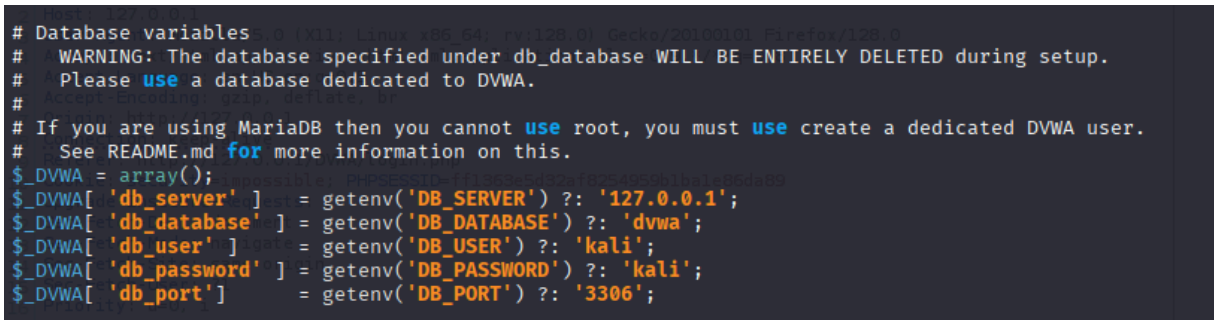
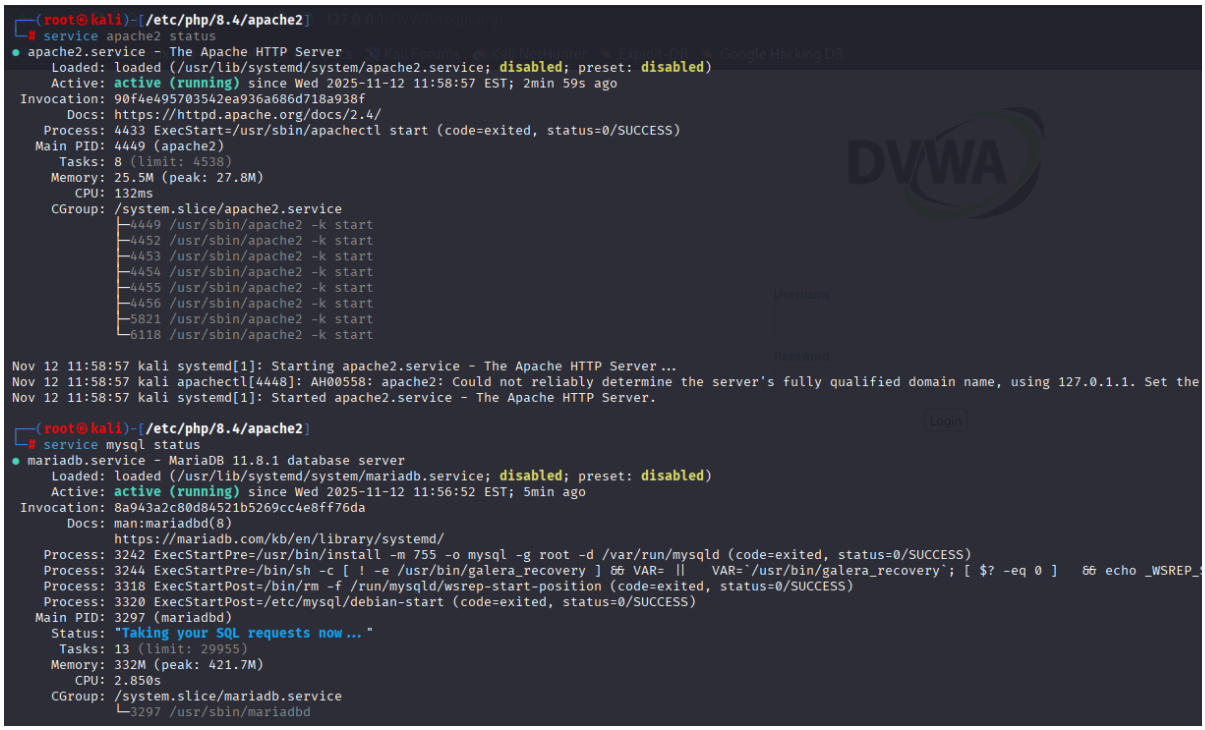
DVWA e Burp Suite

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.

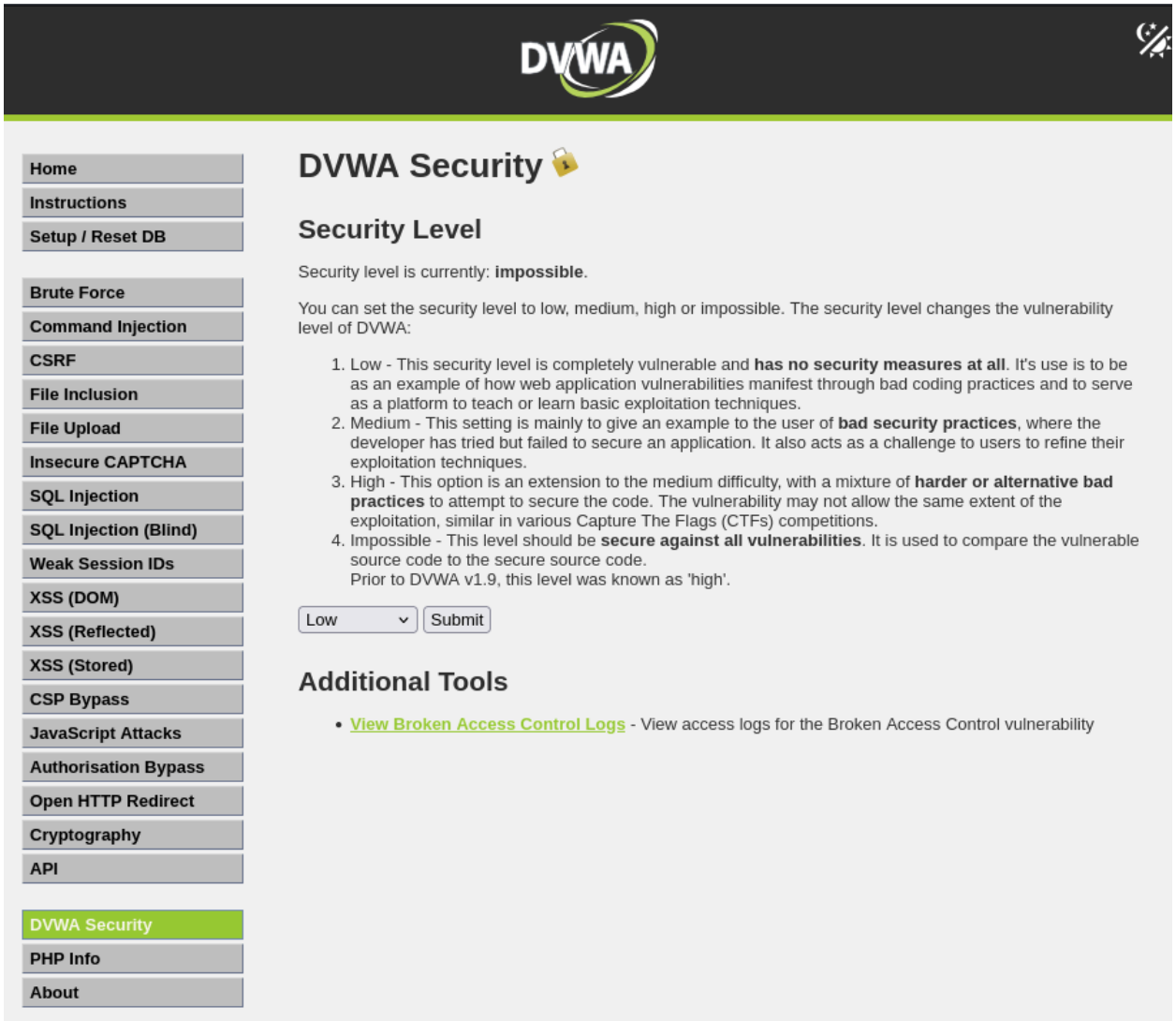


```
# Database variables
#   WARNING: The database specified under db_database WILL BE ENTIRELY DELETED during setup.
#   Please use a database dedicated to DVWA.
#
# If you are using MariaDB then you cannot use root, you must use create a dedicated DVWA user.
#   See README.md for more information on 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';
```

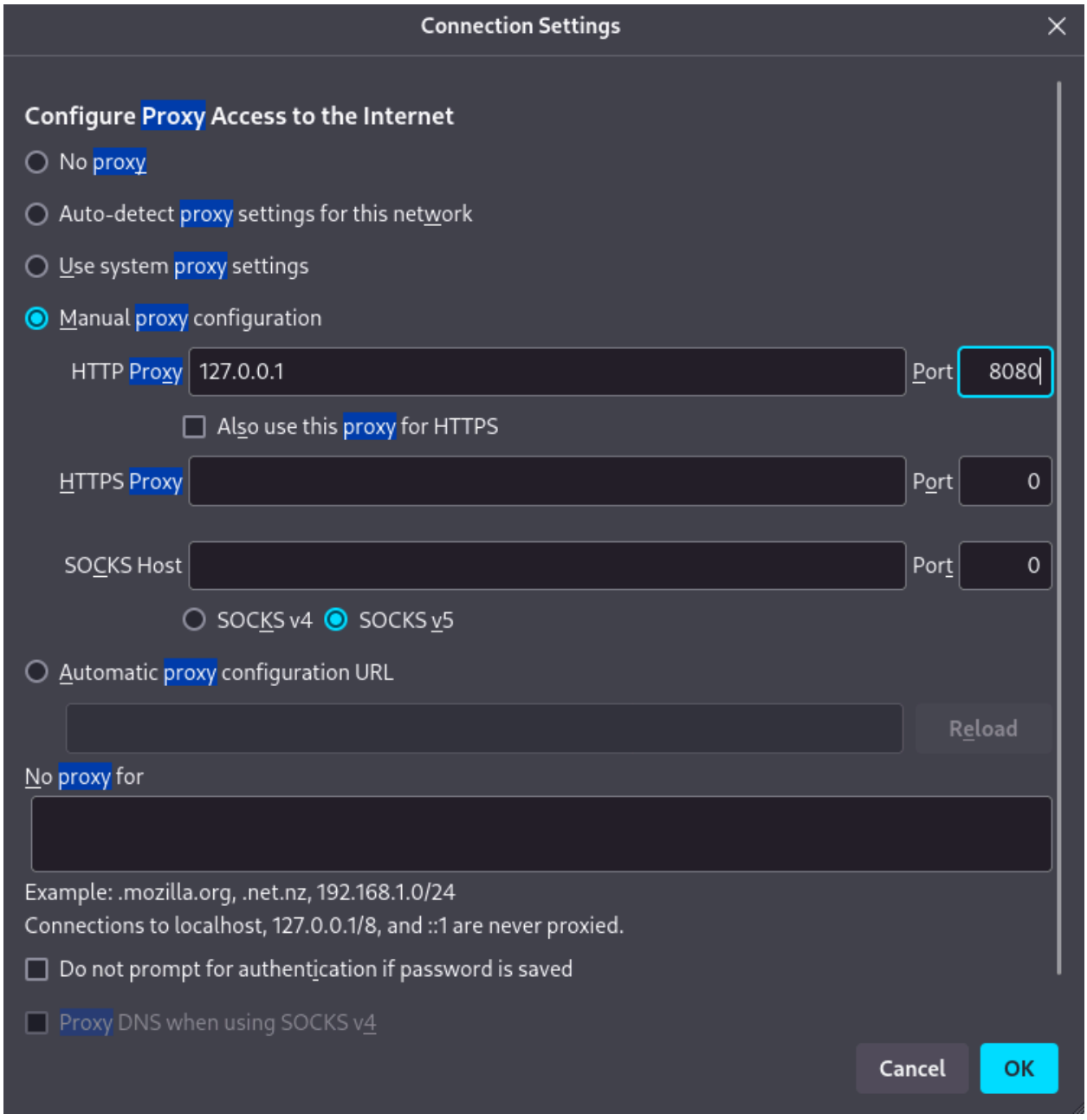


```
┌──(root㉿kali)-[/etc/php/8.4/apache2]
└─# service apache2 status
● apache2.service - The Apache HTTP Server
     Loaded: loaded (/usr/lib/systemd/system/apache2.service; disabled; preset: disabled)
     Active: active (running) since Wed 2025-11-12 11:58:57 EST; 2min 59s ago
 Invocation: 90f4e495703542ea936a686d718a938f
       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)-[/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:mariadbd(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/mysqld/wsrep-start-position (code=exited, status=0/SUCCESS)
    Process: 3320 ExecStartPost=/etc/mysql/debian-start (code=exited, status=0/SUCCESS)
   Main PID: 3297 (mariadbd)
     Status: "Taking your SQL requests now..."
      Tasks: 13 (limit: 29955)
     Memory: 332M (peak: 421.7M)
        CPU: 2.850s
     CGroup: /system.slice/mariadb.service
             └─3297 /usr/sbin/mariadbd
```

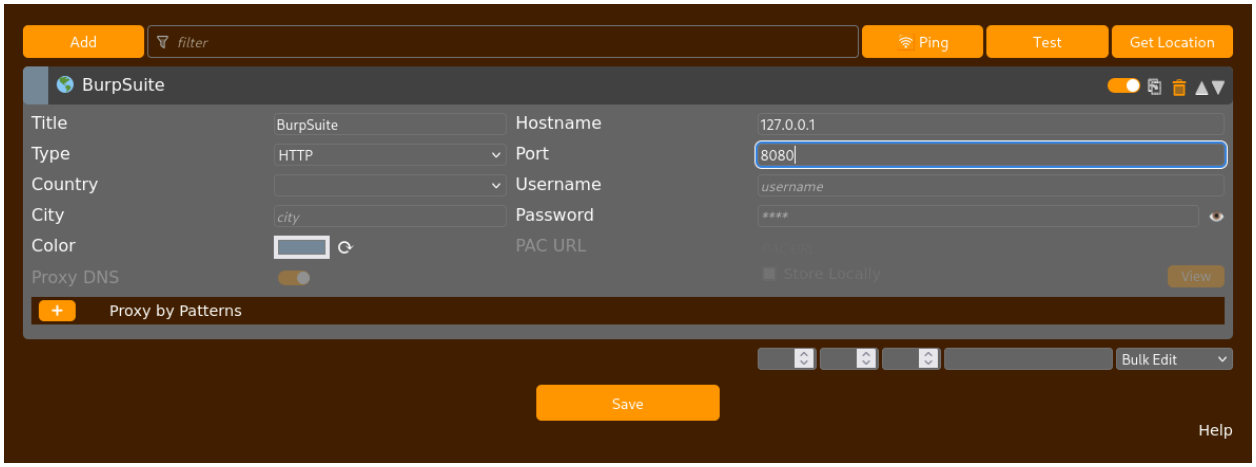
Una volta attivati i servizi, ho aperto il browser e navigato verso l'indirizzo **127.0.0.1/setup.php** per inizializzare il database dell'applicazione. Inizializzato il database sono stato reindirizzato in automatico all'endpoint **/login.php**. A questo punto la **Damn Vulnerable Web Application**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

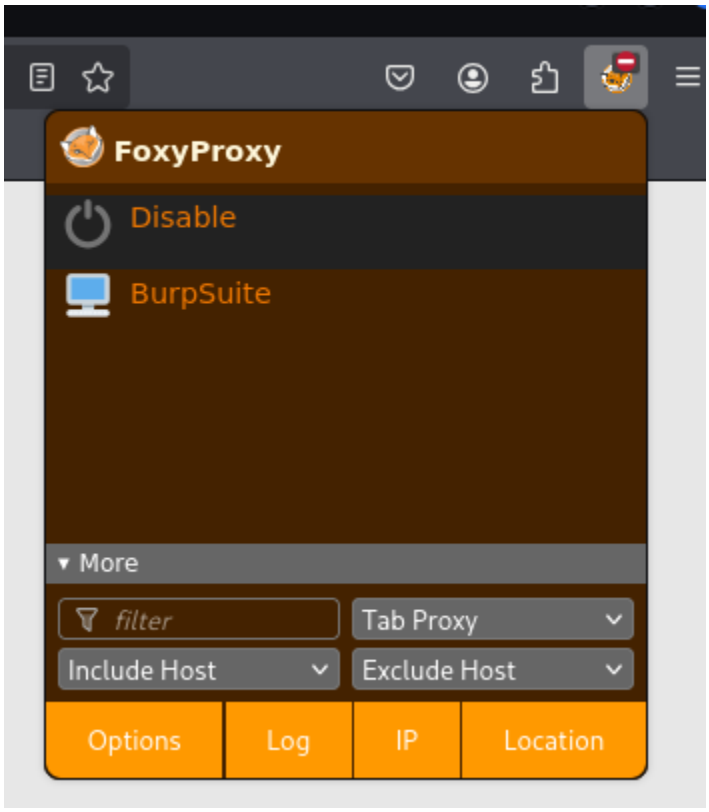


Per riuscire a fare pratica con **Burp Suite**, è stato necessario impostare il proxy su **127.0.0.1:8080**. Questo ha permesso a **Burp Suite** di intercettare le richieste del browser e di analizzarle o modificarle prima che raggiungano il server. Ci sono diversi modi di fare questo tipo di operazione.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

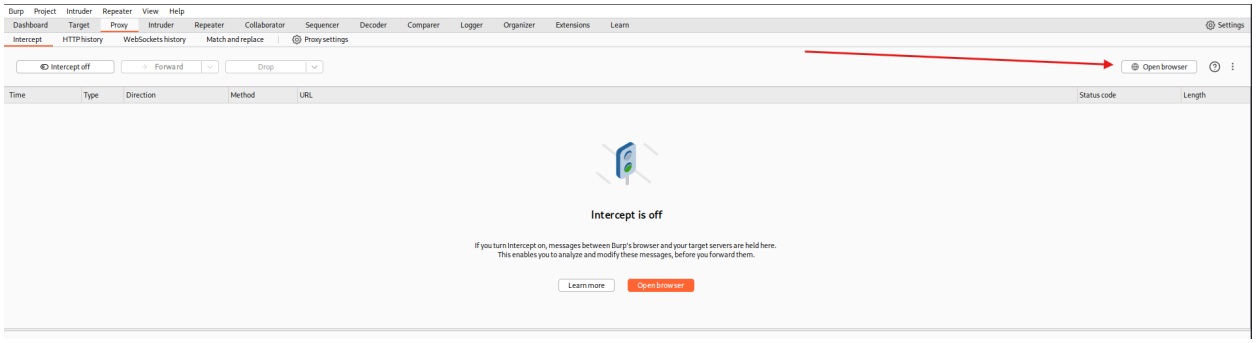


Per rendere il flusso più comodo e veloce è possibile (e consigliabile) utilizzare l'estensione **FoxyProxy**, che permette di passare con un click tra proxy diversi senza dover andare ogni volta nelle impostazioni del browser.

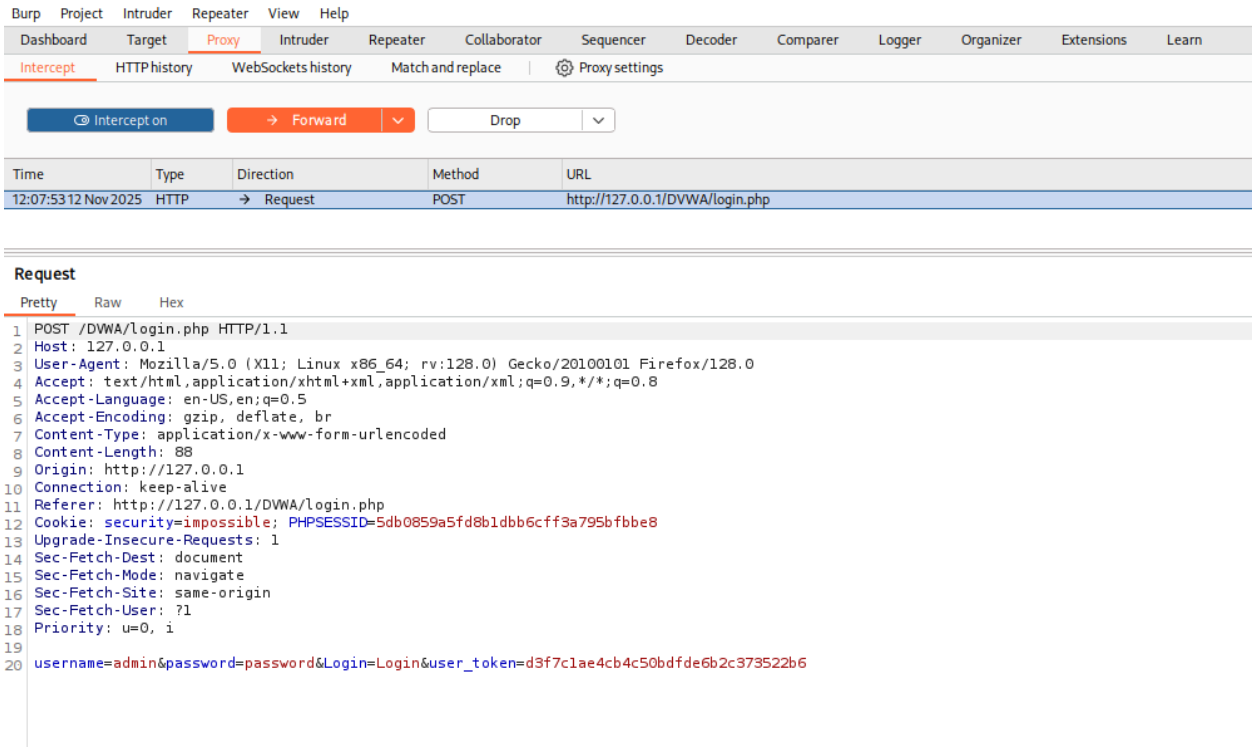




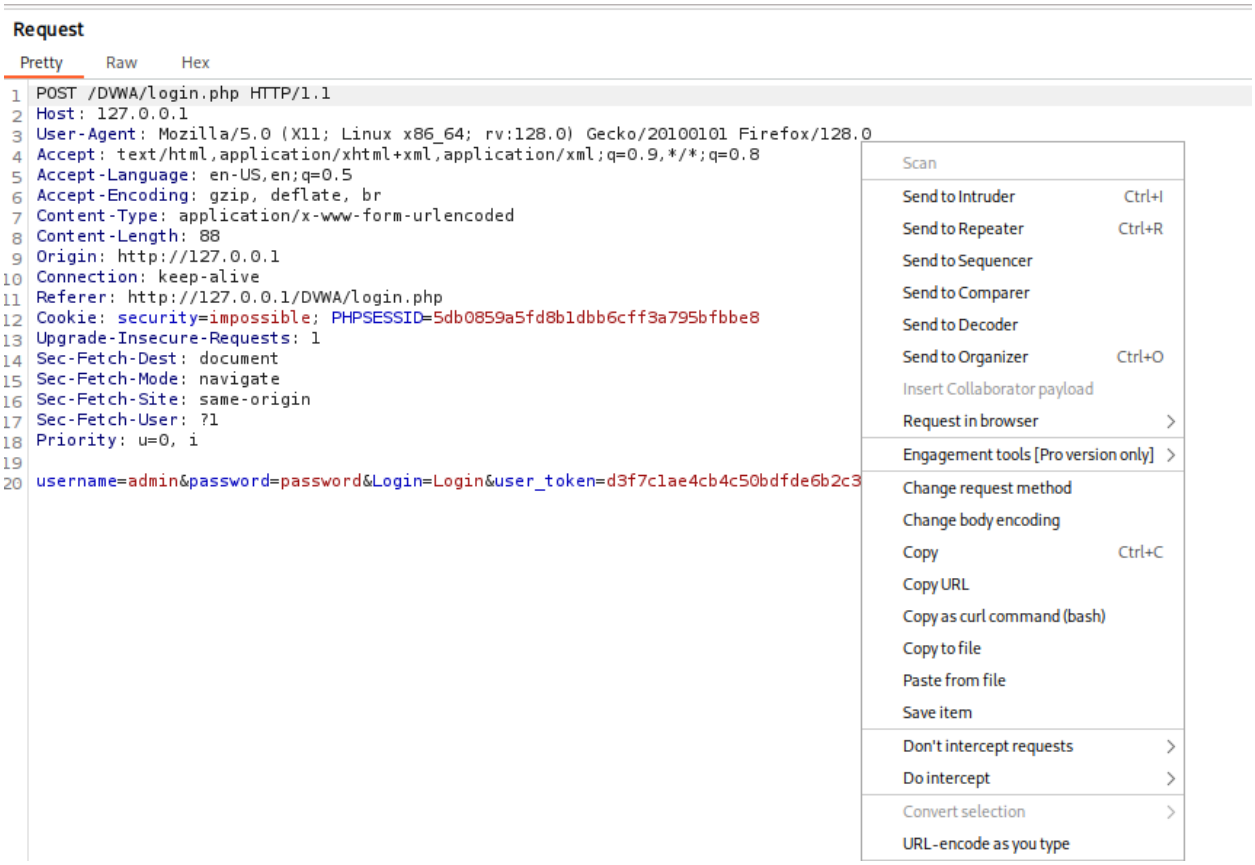
In alternativa (o per evitare di toccare le impostazioni del browser di sistema) è possibile utilizzare il browser integrato di **Burp** (basato su **Chromium**), già configurato per inviare richieste e ricevere risposte attraverso **Burp** senza ulteriori settaggi.



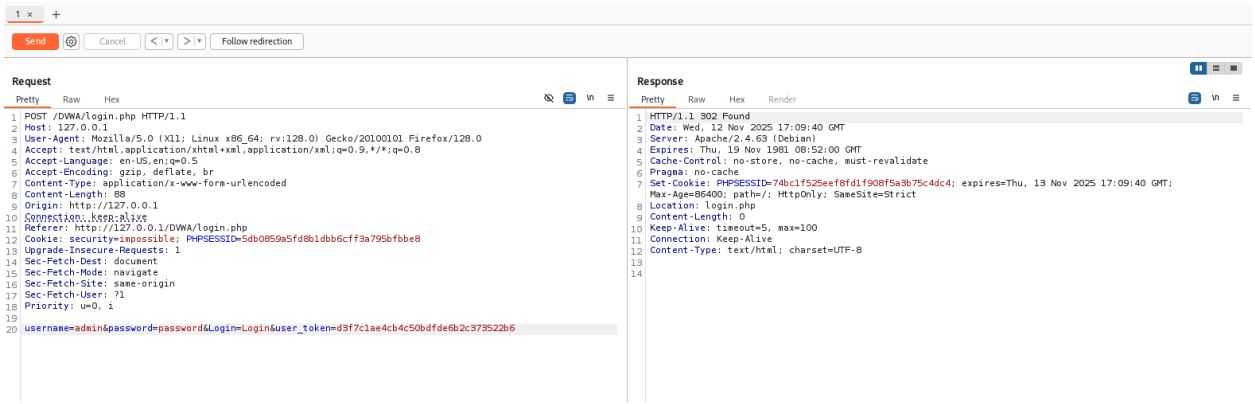
A questo punto **Burp Suite** poteva intercettare le mie richieste. Ho attivato l'**Interceptor**, sono andato sulla pagina **/login.php** e ho inviato una richiesta di login, che è stata poi intercettata da **Burp**.

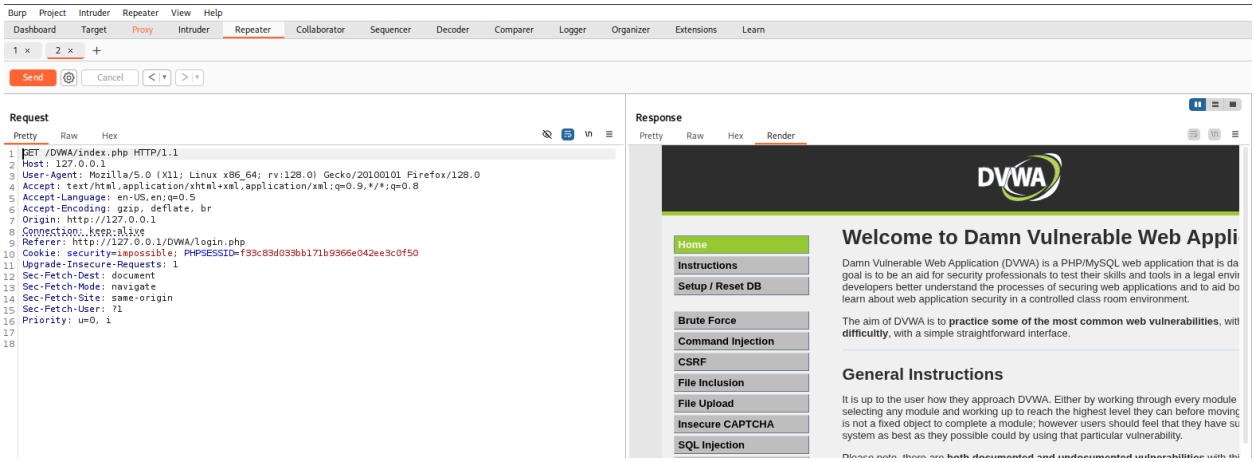


Ho cliccato col tasto destro sulla richiesta e l'ho inviata a **Repeater**. A questo punto, senza modificarla ho lasciato che la richiesta arrivasse al server.



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.





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.