



Burpsuite

Kali

Sommario

Traccia esercizio	2
Esercizio principale	2
Esercizio facoltativo	2
Procedimento esercizio principale	3
Installazione Database MySQL.....	3
Configurazione Apache service.....	4
Configurazione Web Server DVWA	5
Burpsuite	6
Test con Burp e DVWA	8
Procedimento esercizio facoltativo	10
Livello di sicurezza medio	10
Livello di sicurezza alto	10
Livello di sicurezza impossibile	11
Spiegazione	11

Traccia esercizio

Esercizio principale

In questa lezione pratica vedremo come configurare una DVWA – ovvero damn vulnerable web application in Kali Linux. La DVWA ci sarà molto utile per i nostri test, in cui vedremo da vicino le tecniche per sfruttare le vulnerabilità nella fase di exploit.

Prerequisiti:

per installare la DVWA vi servirà connettività ad internet da Kali Linux, avete 2 possibilità:

- Per chi avesse già installato una nuova Kali con scheda di rete bridged in lezione 2 potete utilizzare quella;
- Altrimenti, potete modificare le impostazioni della scheda di rete della vostra istanza di Kali, aggiungendo una scheda di rete bridged.

Assicuratevi di avere accesso ad internet. Qualora doveste avere problemi con la configurazione della scheda di rete, vi consigliamo di ricreare una macchina Kali con la scheda di rete bridged abilitata. Per installare la DVWA abbiamo bisogno di 3 componenti:

- OS: Kali Linux (OK)
- Database MySQL (da installare)
- Web Server Apache (da installare)

Vedi traccia completa sul PDF W8D1 – Pratica da pagina 5 a pagina 13 per il procedimento dell'installazione dei requisiti.

Esercizio facoltativo

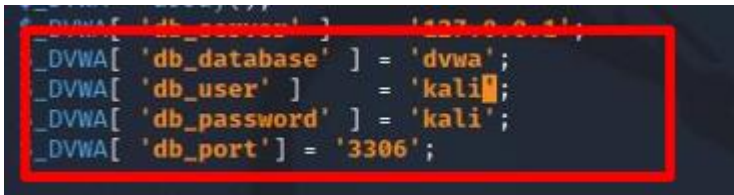
Ripetere tutti i passi visti, con livello di sicurezza “Medium” e “High”. Cosa cambia?

Procedimento esercizio principale

Installazione Database MySQL

Eseguire i seguenti comandi da terminale di Kali in utenza di root.

1. Dal terminale inserire comando **sudo su** per ottenere i privilegi di amministratore.
Recarsi alla cartella html da terminale con **cd /var/www/html**
2. Copiare/ scaricare la cartella DVWA dal link fornito dalla traccia dell'esercizio, comando **git clone <https://github.com/digininja/DVWA>** .
3. Cambiare I privilegi della cartella DVWA in R(4)+W(2)+X(1) = 7 per ogni gruppo quindi 777, comando **chmod -R 777 DVWA/** -R è usato per la modifica dei permessi valida anche per i file all'interno della cartella.
4. Recarsi nella cartella config, comando **cd DVWA/config** .
5. Copiare i contenuti, comando **cp config.inc.php.dist config.inc.php** .
6. Modificare il file tramite nano, comando **nano config.inc.php** .
Attraverso i comandi nano, modificare username e password in kali.

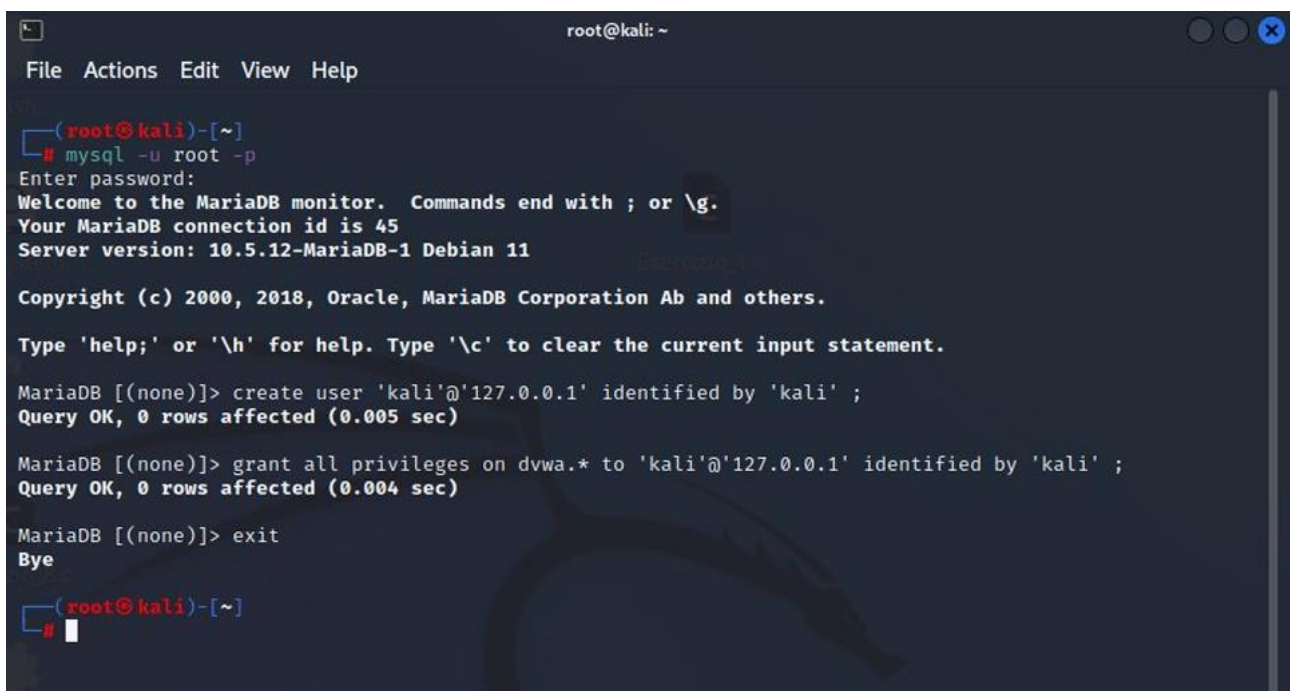


```

DVWA[ 'db_server' ] = '127.0.0.1';
DVWA[ 'db_database' ] = 'dvwa';
DVWA[ 'db_user' ] = 'kali';
DVWA[ 'db_password' ] = 'kali';
DVWA[ 'db_port' ] = '3306';

```

7. Avviare il servizio mysql, comando **service mysql start** .
8. Connettere il database all'utenza di root, comando **mysql -u root -p** .
9. Creare l'utenza e i privilegi sul database, comandi **create user 'kali'@'127.0.0.1' identified by 'kali' ;**
e **grant all privileges on dvwa.* to 'kali'@'127.0.0.1' identified by 'kali' ;**
10. Uscire con **exit**



```

root@kali: ~
File Actions Edit View Help

(root@kali)-[~]
# mysql -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 45
Server version: 10.5.12-MariaDB-1 Debian 11

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> create user 'kali'@'127.0.0.1' identified by 'kali' ;
Query OK, 0 rows affected (0.005 sec)

MariaDB [(none)]> grant all privileges on dvwa.* to 'kali'@'127.0.0.1' identified by 'kali' ;
Query OK, 0 rows affected (0.004 sec)

MariaDB [(none)]> exit
Bye

(root@kali)-[~]
#

```

Configurazione Apache service

Sempre da terminale in modalità utente root **sudo su**

1. Avviare il servizio apache, comando **service apache2 start**
2. Recarsi nella cartella di apache 2, comando **cd /etc/php/x/apache2** (x è il numero della versione)
In questo caso con il comando **ls** si scopre che la versione è la 8.2.

```
(kali㉿kali)-[~]
$ sudo su
[sudo] password for kali:
(kali㉿kali)-[/home/kali]
# cd /etc/php/

(kali㉿kali)-[/etc/php]
# ls
8.2

(kali㉿kali)-[/etc/php]
# cd 8.2/apache2

(kali㉿kali)-[/etc/php/8.2/apache2]
#
```

4

3. Aprire il file php.ini, comando **nano php.ini**

```
(kali㉿kali)-[/etc/php]
# cd 8.2/apache2

(kali㉿kali)-[/etc/php/8.2/apache2]
# ls
conf.d  php.ini

(kali㉿kali)-[/etc/php/8.2/apache2]
# nano php.ini
```

4. Modificare la voce "allow_url_include" in **On** e assicurarsi che "allow_url_fopen" sia anch'esso **On**

```
; Whether to allow the treatment of URLs (like http:// or ftp://) as files.
; https://php.net/allow-url-fopen
allow_url_fopen = On

; Whether to allow include/require to open URLs (like https:// or ftp://) as files.
; https://php.net/allow-url-include
allow_url_include = Off
```

Per aiutarsi a trovarlo si può usare la funzione di nano **CTRL+F** per usare la funzione di ricerca.

Per salvare CTRL+O invio e CTRL+X invio

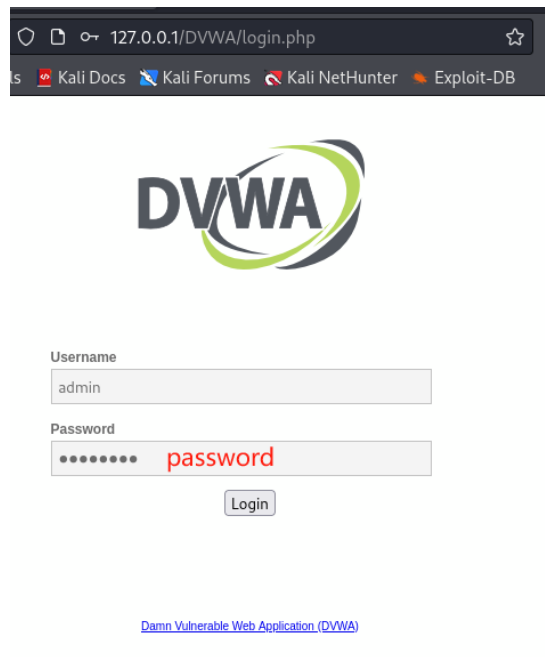
5. Avviare il servizio, comando **service apache2 start**
6. Aprire un browser di Kali e scrivere l'indirizzo per il Setup del Web Server.
Link <http://127.0.0.1/DVWA/setup.php>
7. Cliccate su «Create / Reset Database» nella parte bassa della pagina

These are only required for the file inclusion labs so unless you want to play with those, you can ignore them.

Create / Reset Database

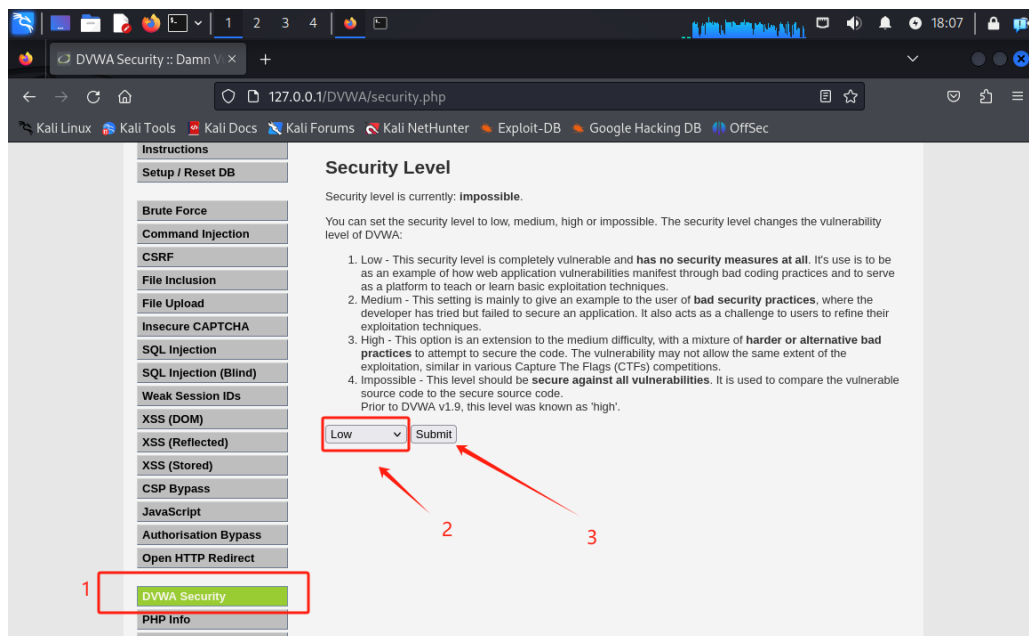
Configurazione Web Server DVWA

Le credenziali di default sono admin e password.



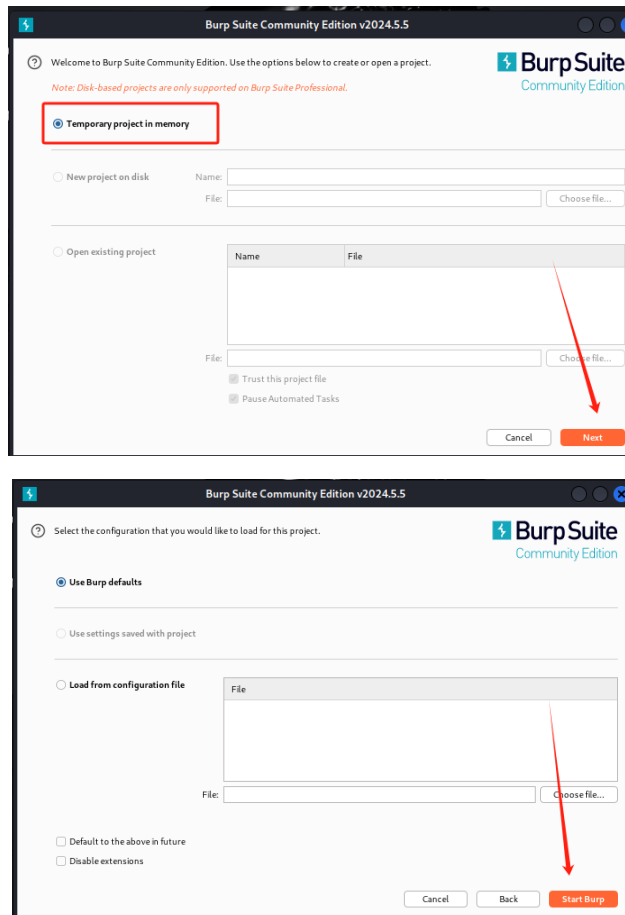
5

Impostare la sicurezza su livello basso

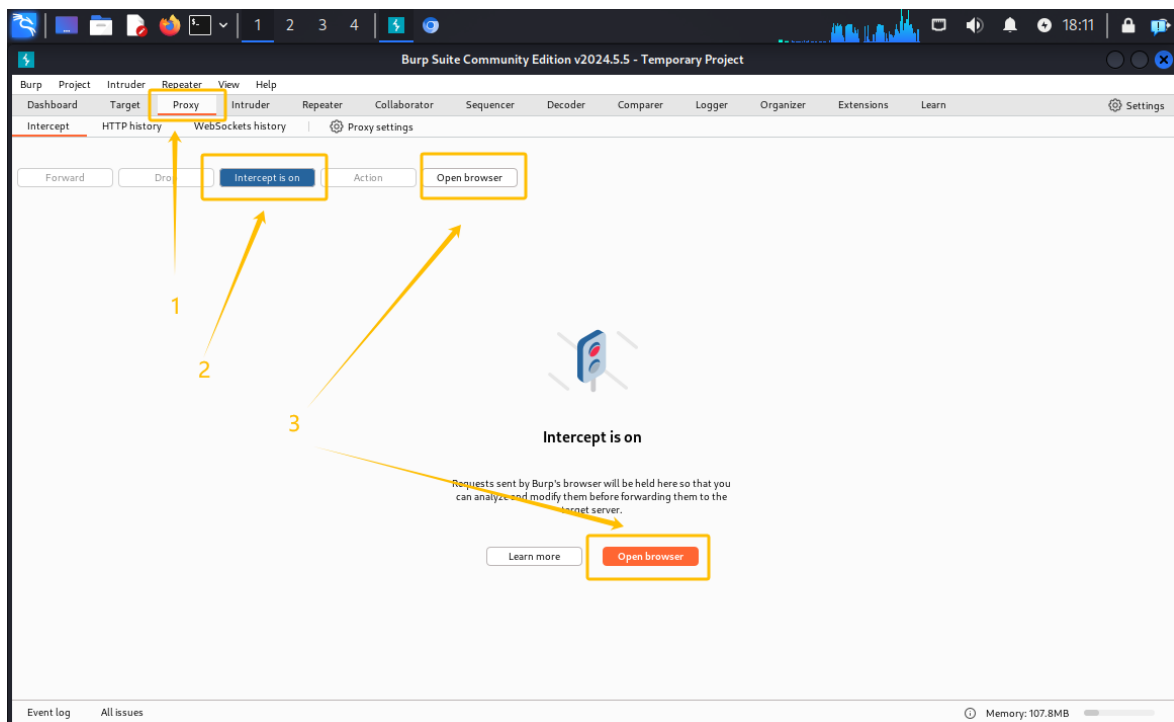


Burpsuite

Cercare Burpsuit tra le app di Kali ed avviarlo come da immagini.

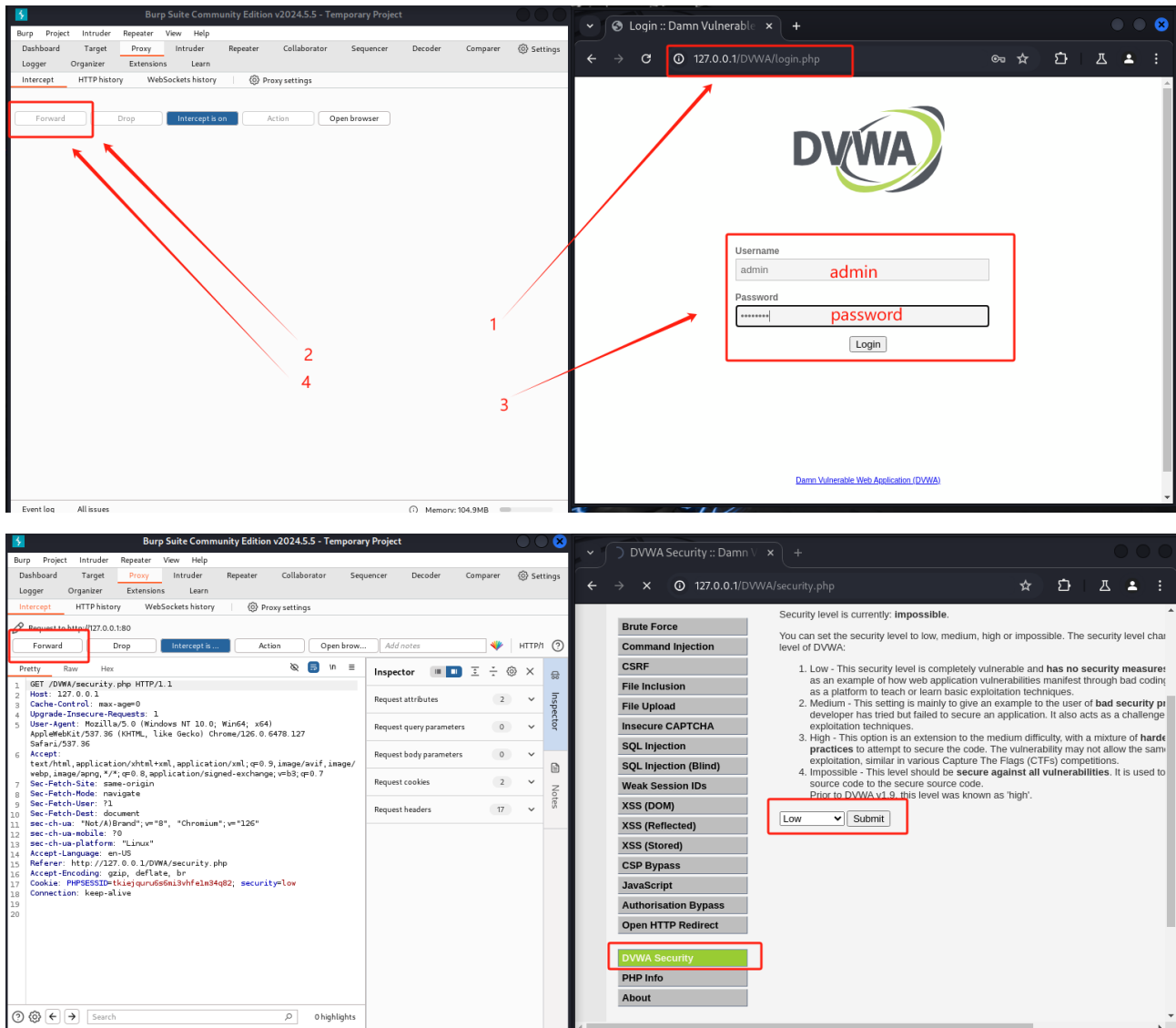


Recarsi nella sezione Proxy, attivare Intercept is on e aprire il browser, vedi immagine:



Nel browser di Burp Suite recarsi all'indirizzo <http://127.0.0.1/DVWA/> ed effettuare la modifica al livello di sicurezza su basso, come spiegato nel precedente paragrafo "Configurazione Web Server DVWA".

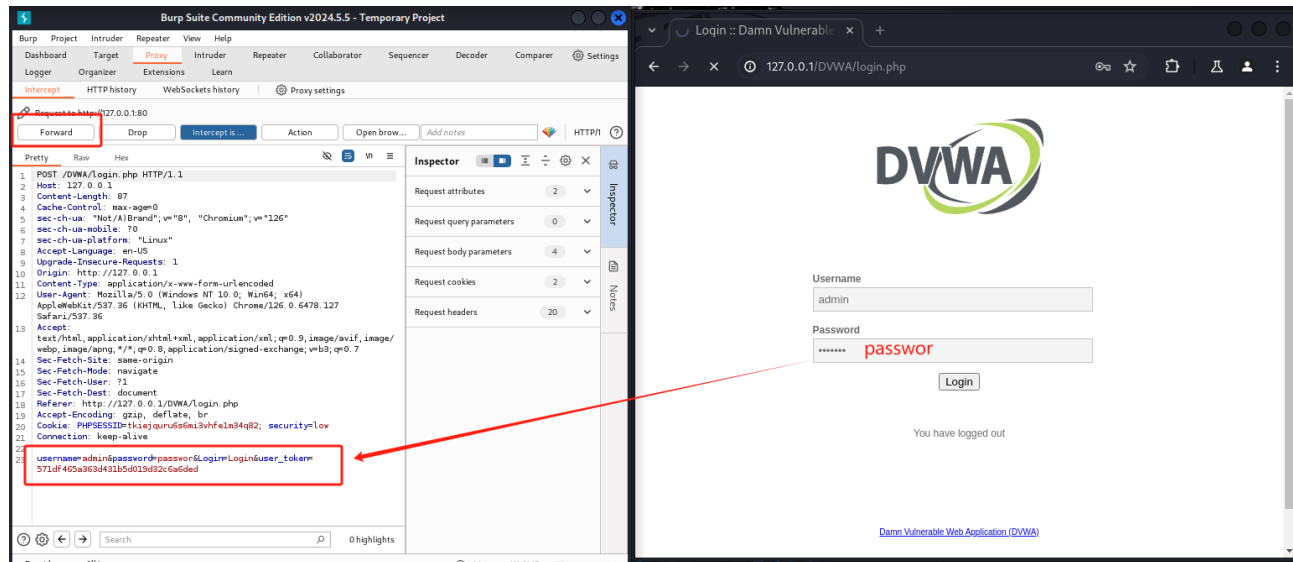
Per caricare la pagina premere **Forward** su Burpsuite, anche più volte consecutive, finché il browser non carica la pagina web.



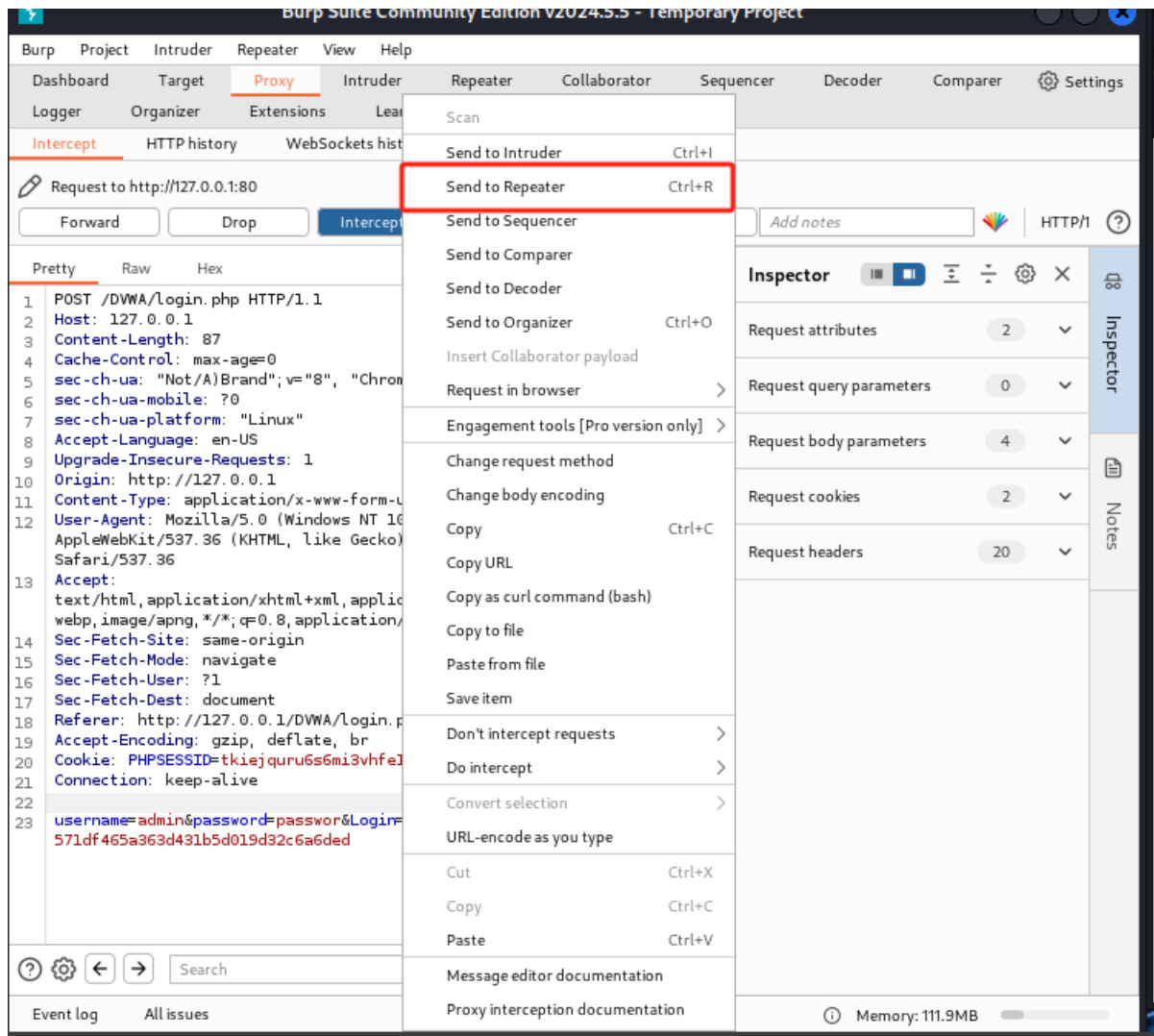
Dopo aver impostato il livello di sicurezza su basso, fare **logout** e cominciare ad effettuare i test.

Test con Burp e DVWA

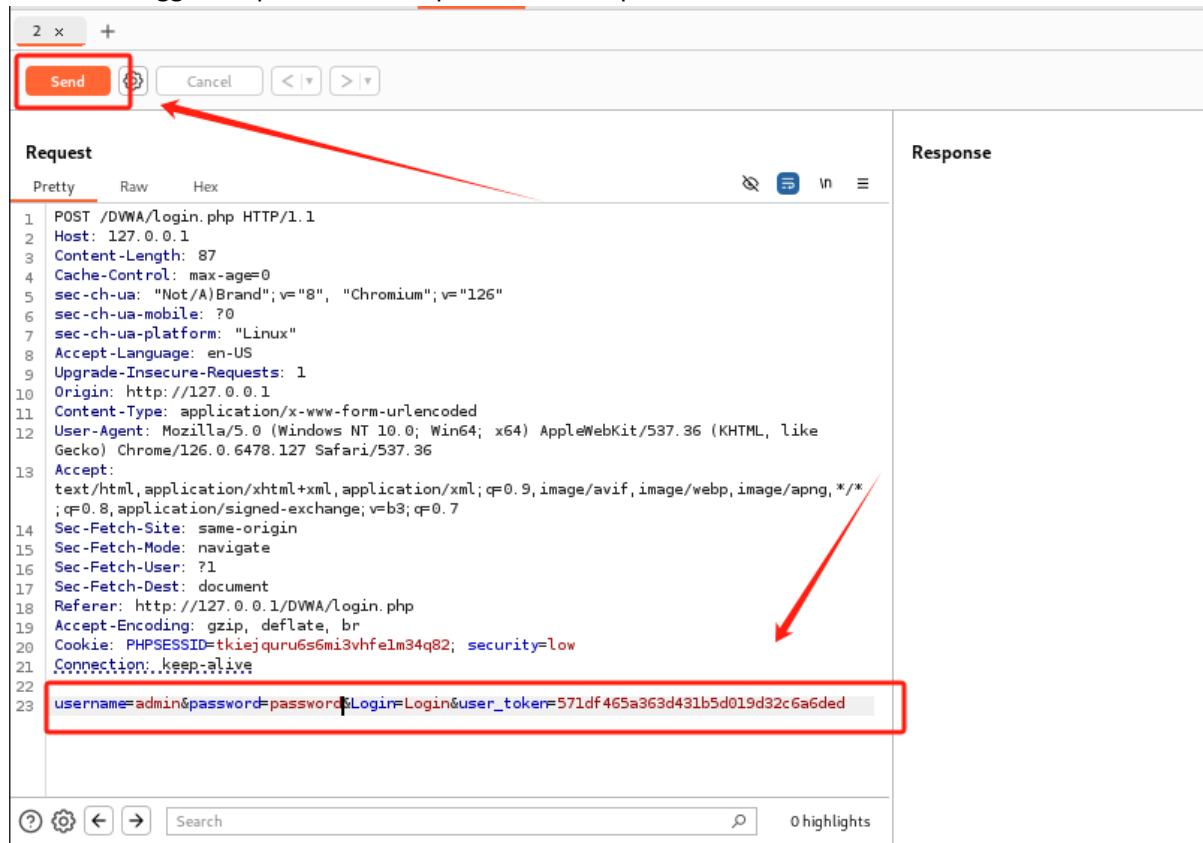
Inserire una qualsiasi credenziale non corretta come in immagine e intercettarla con Burp.



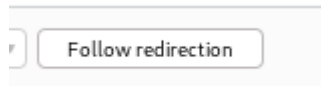
Premere Ctrl+R oppure tasto destro Send to Repeater per inviare alla sezione Repeater il cookie intercettato.



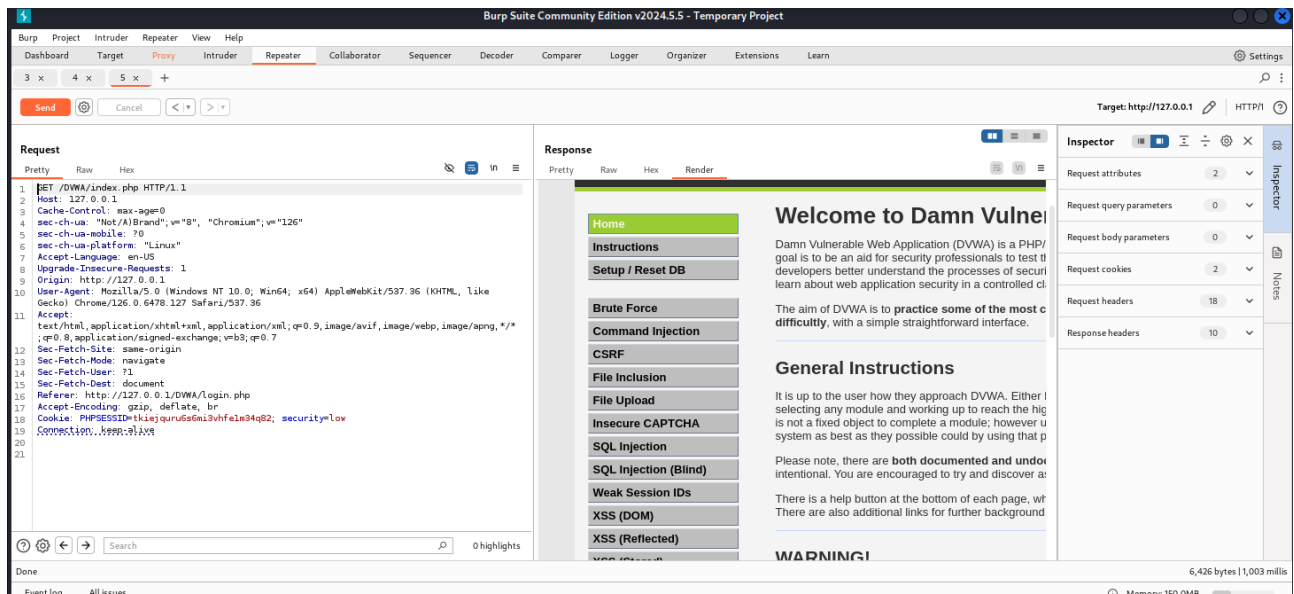
Correggere la password con quella corretta “password” e inviare una richiesta al server.



Se necessario premere Follow redirection, se il server lo prevedesse.



L'esercizio si conclude con l'avvenuto login nel server tramite il cookie con la password corretta.



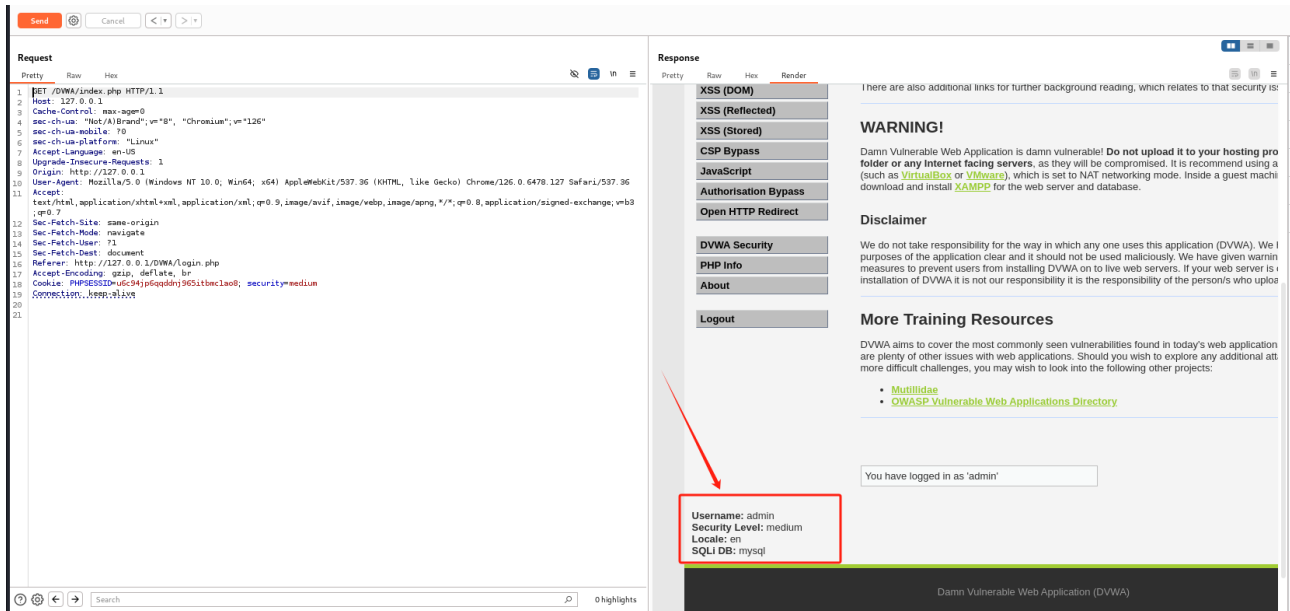
Il tentativo di rubare la sessione tramite il cookie intercettato è riuscito.

Procedimento esercizio facoltativo

Livello di sicurezza medio

Recarsi nella pagina di configurazione utilizzando le credenziali corrette, vedi paragrafo antecedente “Configurazione Web Server DVWA” e impostare su livello di sicurezza “medium”.

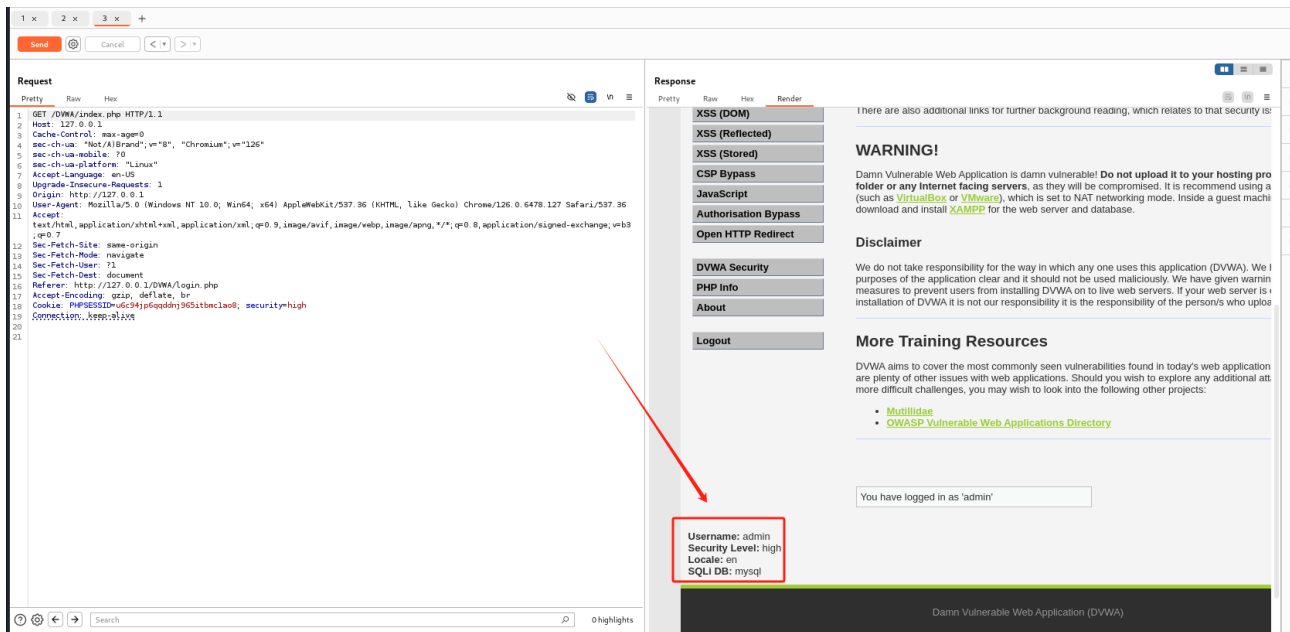
Ripetere lo stesso procedimento del paragrafo precedente “Test con Burp e DVWA”.



Si constata che anche a livello di sicurezza medio si può intercettare e accedere ugualmente.

Livello di sicurezza alto

Analogamente al paragrafo precedente con il livello medio, impostare a livello alto e riprovare il test.



Si constata che anche a livello di sicurezza alto si può intercettare e accedere ugualmente.

Livello di sicurezza impossibile

Analogamente si fa lo stesso test con il livello impossibile.

The screenshot shows a network request from a browser to a DVWA login page. The request headers include a 'Cookie' field with a session ID. A red box highlights this field, and a red arrow points from it to the 'Cookie' field in the browser's address bar. The response shows the DVWA login page with a 'Username' field, a 'Password' field, and a 'Login' button.

Solo in questo caso, nonostante le credenziali fossero stati intercettati, il server non ha garantito l'accesso tramite il cookie clonato, pertanto la sessione non è stato possibile rubare.

Spiegazione

Nella scheda di impostazione del livello di sicurezza, si constata che solo un livello che sia impostato contro tutte le vulnerabilità è in grado di riconoscere che il cookie intercettato non è autorizzato ad accedere.

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'.