

Esercizio Web Application – preparazione ambiente

MATTIA PASTORELLI



CONSEGNA

Nella lezione pratica di oggi vedremo come configurare una DVWA – ovvero damn vulnerable web application in Kali Linux.



PRIMO STEP

Per configurare la nostra DVWA(Damn Vulnerable Web Application) abbiamo bisogno di 3 componenti :

- OS: Kali Linux (Precedentemente installato e configurato)
- Database MySQL
- Web Server Apache

Queste applicazioni vengono utilizzate per simulare attacchi hacker in un sistema protetto, quindi che non va ad intaccare nessun pc /sito /applicazione realmente esistente.

Una volta eseguiti tutti i passaggi per installare i due database, dovremmo riuscire alla pagina di creazione o reset del Database



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: **Enabled**
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: **kali**
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

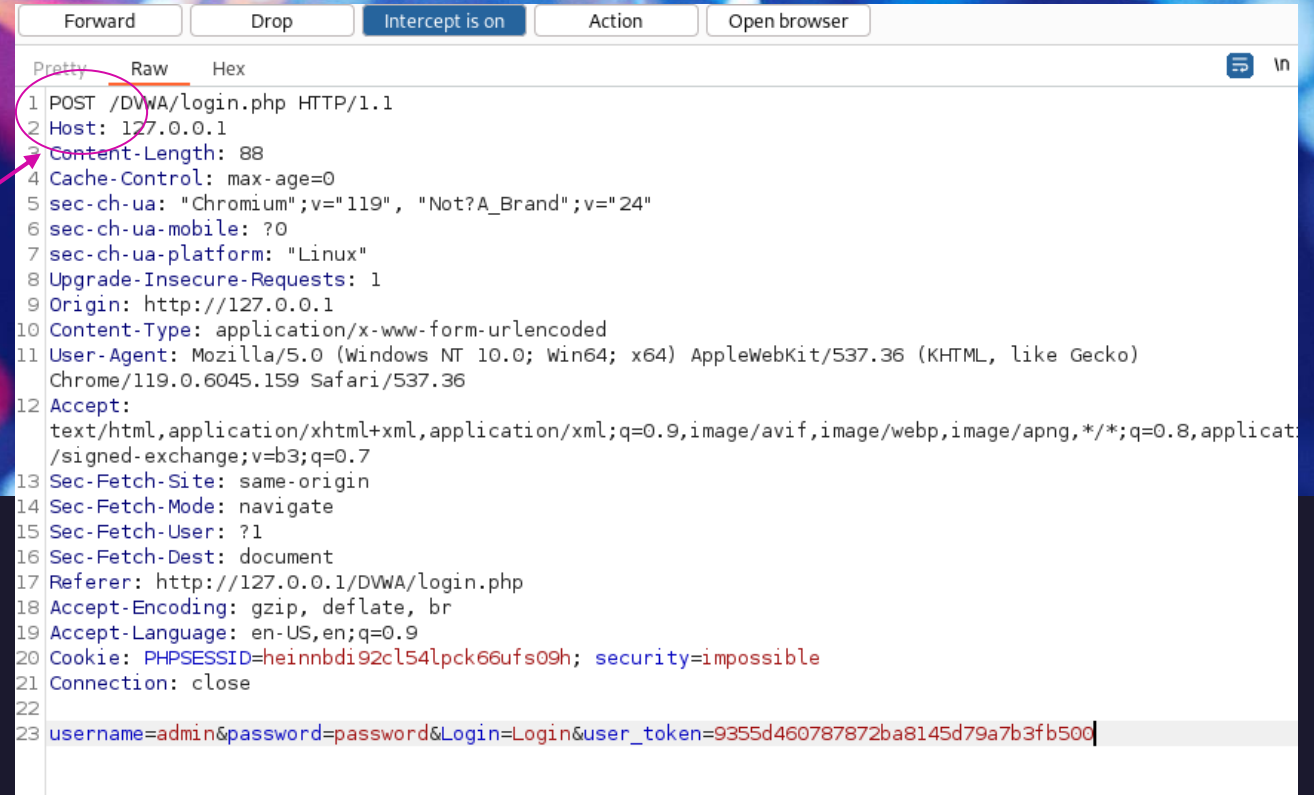
SECONDO STEP

- Una volta loggati nel sito con ID (admin) e Password (password), impostiamo il livello di sicurezza che preferiamo, da un livello basso(poco sicuro) ad un livello Impossibile (molto sicuro).
- Apriamo Burp Suite, questo programma ci servirà da filtro tra noi ed il sito che andiamo a visitare. Funziona come un Proxy avente un proprio certificato SSL, il quale gli permette di fare da intermediario tra le due parti in quanto non viene colpito dalla crittografia del HTTPS. Ciò rende possibile il controllo di ogni passaggio e dei rispettivi Cookies, in quanto «prende il nostro posto». Ci chiederà conferma di ogni passaggio che effettuiamo sul sito web, in più ci mostrerà i dati inseriti in esso.
- Per visualizzare tutti i passaggi bisogna andare nella sezione Proxy, premere su «Intercept is Off» settarlo su On e poi «Open Browser». Burp aprirà il suo browser predefinito «Chromium».

```
Forward Drop Intercept is on Action Open browser
Pretty Raw Hex
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: PHPSESSID=heinnbdi92cl54lpck66ufs09h; security=impossible
21 Connection: close
22
23 username=admin&password=password&Login=Login&user_token=9355d460787872ba8145d79a7b3fb500
```

METODO HTTP

- Il metodo stabilisce il tipo di richiesta, a cui segue la versione del protocollo HTTP. Esistono diversi tipi di metodi ma ad ora vedremo i due in cui ci imatteremo principalmente con Burp Suite:
- Get :Viene utilizzato quando si richiede una risorsa web
- Post:Viene utilizzato per inviare parametri all'interno della richiesta



```
Forward Drop Intercept is on Action Open browser
Pretty Raw Hex
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: PHPSESSID=heinnbdi92cl54lpck66ufs09h; security=impossible
21 Connection: close
22
23 username=admin&password=password&Login=Login&user_token=9355d460787872ba8145d79a7b3fb500
```

TERZO STEP

Una volta entrati nel sito, aver inserito i nostri ID e Password, aver premuto Login, l'applicazione Burp intercetterà i dati e potremo andare ad effettuare dei cambiamenti prima di mandare la richiesta finale di accesso.

- Passando dalla sezione Proxy, premendo tasto destro e Send to Repeater e premendo sulla sezione Repeater, avremo la situazione come in figura.
- Premuto su «Send» e poi su «Follow Redirection», avremo la situazione corrente.
- Possiamo notare il Login Failed, in quanto siamo andati a cambiare ID e Password con Casa e Ciao prima di dare la conferma con Burp.

