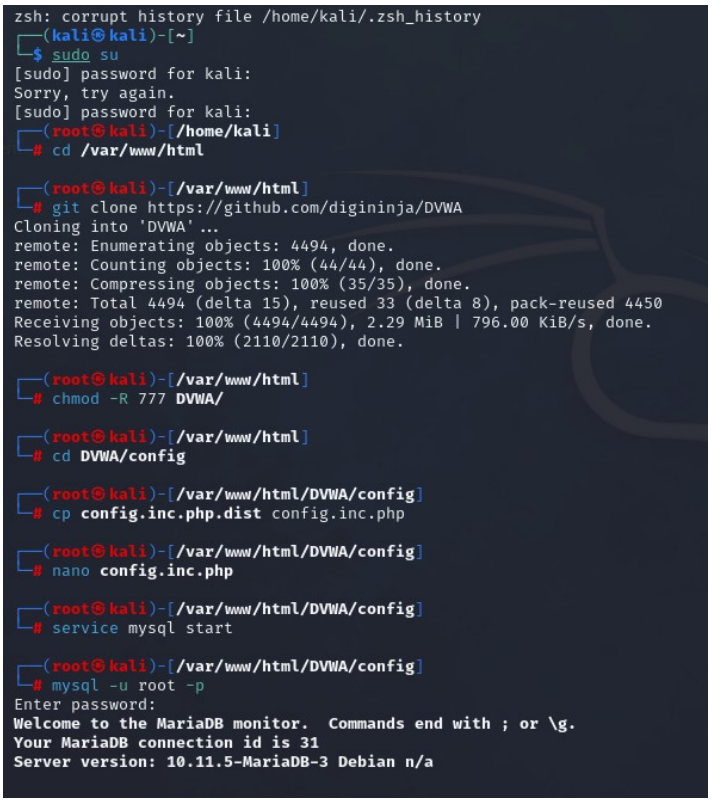
Esercizio Web Application – preparazione ambiente S3/L2

Manuel Di Gangi 6 febbraio 2024

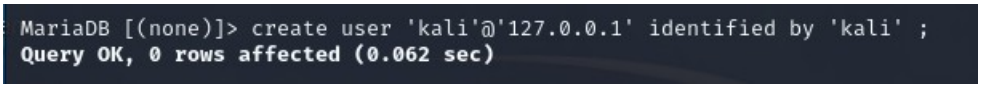
TRACCIA

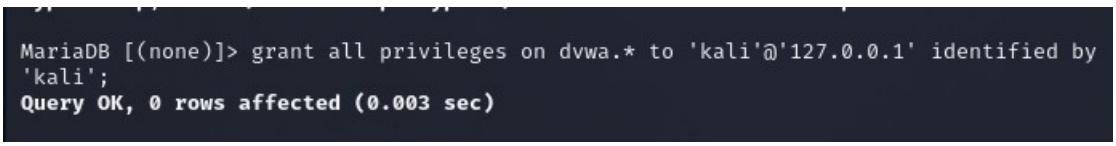
Nella lezione pratica di oggi vedremo come configurare una DVWA – ovvero damn vulnerable web application in Kali Linux. La DVWA ci sarà molto utile per i nostri test.

1. Aprite un terminale su Kali, utilizzate l'utenza di root, eseguendo il comando «sudo su» e poi eseguite i comandi seguenti:
   - cd /var/www/html
   - git clone https://github.com/digininja/DVWA
   - chmod –R 777 DVWA/
   - cd DVWA/config
   - cp config.inc.php.dist config.inc.php
   - nano config.inc.php



2. Facciamo partire il servizio mysql, connettiamoci al DB e creiamo un'utenza;



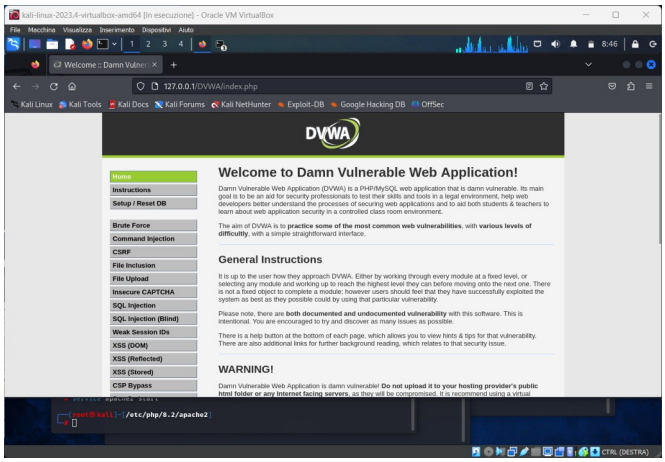


3. Facciamo partire il servizio apache (il web server) e modifichiamo le voci allow_url_fopen e allow_url_include come sotto

```
; 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 = On
```

4. Creiamo il database ed effettuiamo il login.



5. Ora che l'ambiente è creato, eseguiamo delle prove con Burpsuite.

Effettuiamo il login dal browser all'indirizzo 127.0.0.1/DVWA
Utente: admin
Password: password

Intercettiamo la richiesta del client al server e andiamo a modificare le credenziali di accesso

Utente: utente
Password: spagliato

```
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,applicati
   on/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: security=impossible; PHPSESSID=hi5ldoho0bppqoo5rj52afage5
21 Connection: close
22
23 username=admin&password=password&Login=Login&user_token=9de9cb862e795afaa6cf02beb3d40d23
```

```
username=utente&password=spagliato&Login=Login&user_token=9de9cb862e795afaa6cf02beb3d40d23
```

6. Come ci aspettavamo con le credenziali errate non riusciamo ad entrare.