

ESERCIZIO W8D1

L'esercizio ci porterà ad analizzare le richieste inviate ad DVWA(Damn Vulnerable Web Application) per mezzo dell'intercepting proxy Burpsuite. Prepariamo l'ambiente su Kali Linux seguendo i vari passaggi.

Modifica file interfaces

Per effettuare l'analisi delle richieste tra Client e Server abbiamo bisogno guardacaso della connessione alla rete. Una volta cambiata la scheda di rete in "scheda con bridge", accediamo al foglio interfaces, seguendo il percorso etc/network/interfaces, ed apportiamo le modifiche richieste.

```
# The loopback network interface
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet dhcp
#iface eth0 inet static
address 192.168.32.100/24
netmask 255.255.255.0
#gateway 192.168.32.1
```

modifiche foglio interfaces

Installazione e modifica DVWA/config

```
(kali@kali)-[/var/www/html]
$ sudo git clone https://github.com/digininja/DVWA
[sudo] password for kali:
Cloning into 'DVWA' ...
remote: Enumerating objects: 4440, done.
remote: Counting objects: 100% (215/215), done.
remote: Compressing objects: 100% (148/148), done.
remote: Total 4440 (delta 98), reused 148 (delta 64), pack-reused 4225
Receiving objects: 100% (4440/4440), 2.18 MiB | 2.15 MiB/s, done.
Resolving deltas: 100% (2100/2100), done.
```

git clone

Una volta entrati nella cartella html tramite il comando `cd /var/www/html`, cloniamo la repository git specificata nel percorso.

```
(kali㉿kali)-[/var/www/html]
$ sudo chmod -R 777 DVWA

(kali㉿kali)-[/var/www/html]
$ ls-l
ls-l: command not found

(kali㉿kali)-[/var/www/html]
$ ls -l
total 20
drwxrwxrwx 12 root root 4096 Dec 12 14:00 DVWA
-rw-r--r-- 1 root root 10701 May 23 2023 index.html
-rw-r--r-- 1 root root 615 May 23 2023 index.nginx-debian.html
```

Tutti i permessi

Poi doniamo alla repository clonata, e al suo contenuto, tutti i privilegi con il comando `sudo chmod -R 777 DVWA`. Nel caso siamo insicuri sull'esito possiamo anche appurare dare un'occhiata ai permessi grazie al comando `ls -l`.

```
(kali㉿kali)-[/var/www/html]
$ cd DVWA/config

(kali㉿kali)-[/var/www/html/DVWA/config]
$ cp config.inc.php.dist config.inc.php

(kali㉿kali)-[/var/www/html/DVWA/config]
$ ls
config.inc.php  config.inc.php.dist

(kali㉿kali)-[/var/www/html/DVWA/config]
$ sudo nano config.inc.php
```

copia del file e modifica

Creiamo una copia del file config di DWVA attraverso il comando `cp config.inc.php.dist config.inc.php`. A questo punto non ci resta che entrare dentro il file di configurazione appena copiato per modificare le credenziali di accesso. Usiamo `sudo nano config.inc.php`.

```
$_DVWA = array();
$_DVWA[ 'db_server' ] = getenv( 'DB_SERVER' ) ?: '127.0.0.1';
$_DVWA[ 'db_database' ] = 'dvwa';
$_DVWA[ 'db_user' ] = 'kali';
$_DVWA[ 'db_password' ] = 'kali';
$_DVWA[ 'db_port' ] = '3306';
```

Cambio utente e password

Attivazione Mysql

Ci decidiamo finalmente ad attivare i privilegi root (sorry) ed attiviamo così il servizio Mysql. Per accedere al monitor useremo infine il comando `mysql -u root -p`. Inseriamo la password per root, e siamo dentro.

```
(kali@kali)-[/var/www/html/DVWA/config]
$ sudo su
(root@kali)-[/var/www/html/DVWA/config]
# service mysql start

(root@kali)-[/var/www/html/DVWA/config]
# mysql -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 31
Server version: 10.11.4-MariaDB-1 Debian 12

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)]>
```

attivazione MariaDB...

Creazione utente con privilegi

All'interno del monitor di MariaDB, che altro non sarebbe se non la versione free di Mysql. Creiamo un nuovo utente Mysql chiamato kali con la password kali, e decidiamo di relegare l'accesso solo al computer locale. Prima di uscire, ricordiamoci di fornire tutti i privilegi all'utente kali.

```
MariaDB [(none)]> create user 'kali'@'127.0.0.1' identified by 'kali';
Query OK, 0 rows affected (1.692 sec)

MariaDB [(none)]> grant all privileges on dvwa.* to 'kali'@'127.0.0.1' identified by 'kali';
Query OK, 0 rows affected (0.104 sec)

MariaDB [(none)]> exit
Bye
```

Creazione utente e permessi

Attivazione web server

Dopo la configurazione possiamo passare all'attivazione del server apache mediante `service apache2 start`. Seguiamo il percorso `/etc/php/8.2/apache2` ed apriamo il file `php.ini`, così da apportare qualche modifica. `Ctrl + F` ci viene in aiuto per cercare tra le righe interessate.

```
; 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
```

settings php.ini

```
(root@kali)~[/var/www/html/DVWA/config]
# cd /etc/php

(root@kali)~[/etc/php]
# ls
8.2

(root@kali)~[/etc/php]
# cd 8.2

(root@kali)~[/etc/php/8.2]
# ls
apache2 cli mods-available

(root@kali)~[/etc/php/8.2]
# cd apache2

(root@kali)~[/etc/php/8.2/apache2]
# ls
conf.d php.ini

(root@kali)~[/etc/php/8.2/apache2]
# service apache2 stop

(root@kali)~[/etc/php/8.2/apache2]
# service apache2 start
```

modifica php e
restart
apache2

Il riquadro qui sotto invece mostra le azioni all'interno del terminale di Linux. Dopo le modifiche riavviamo apache 2.

Sessione Browser

Quando è tutto pronto, apriamo il browser e scriviamo 127.0.0.1/DVWA/setup.php nella barra degli indirizzi. L'icona da cliccare nella pagina visualizzata riporterà Create/Reset Database.

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

Create / Reset Database

Settaggio difficoltà DWVA

Visto che non siamo così esperti, è meglio scegliere la difficoltà che più rappresenta l'esperienza attuale. Su DWVA security scegliamo dunque il livello Low.

Security Level

Security level is currently: **low**.

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'.

Low

▼

Submit

Security level set to low

settaggio difficoltà

Burp Suite



inserimento
credenziali

Username

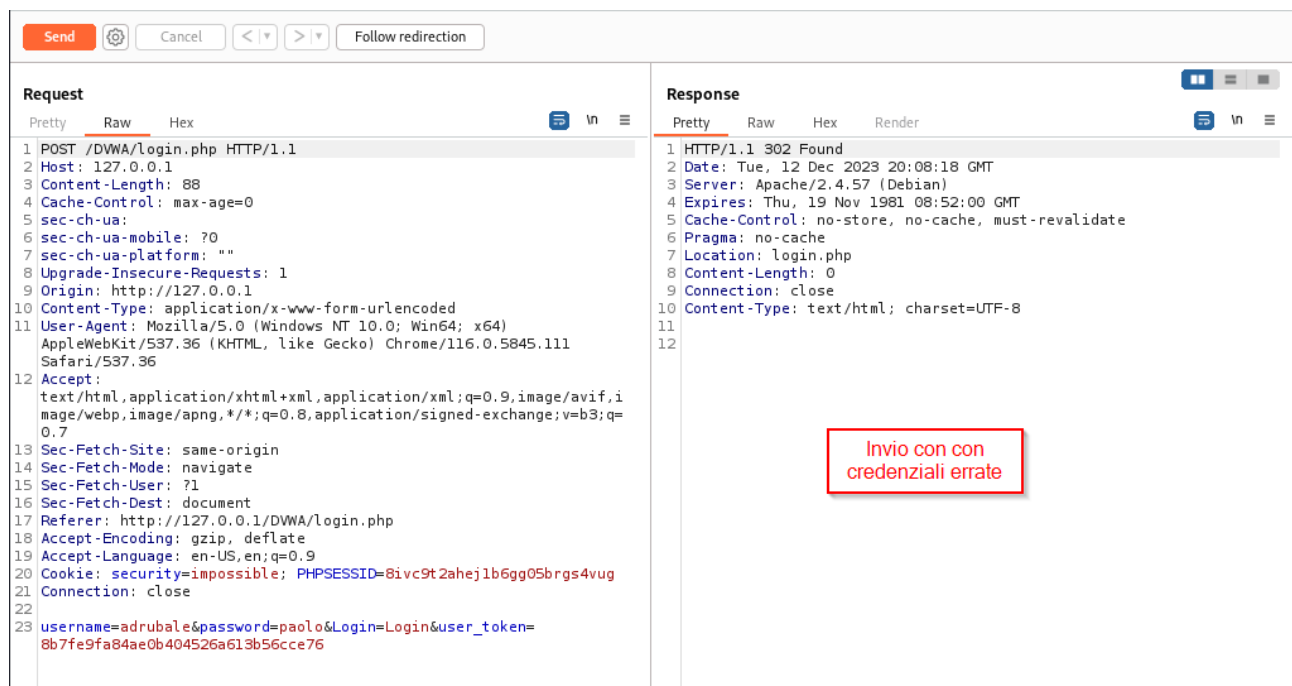
admin

Password

••••••••

Login

Lanciamo Burp Suite e scegliamo un progetto temporaneo. Per cominciare la scansione apriamo il browser partendo dalla pagina vuota del software. Inseriamo l'indirizzo della nostra DVWA, ovvero 1270.0.1/DVWA, dopo di che, clicchiamo su Proxy e Intercept ON. Queste azioni metteranno il browser in soft lock, visto che andremo a raccogliere la richiesta POST della pagina di login.



The screenshot displays the Burp Suite interface with a request and response view. The 'Request' tab on the left shows a POST request to /DVWA/login.php with various headers and a body containing login credentials. The 'Response' tab on the right shows the server's response, which is an HTTP 302 Found status, indicating a redirect. A red box with the text 'Invio con con credenziali errate' (Send with wrong credentials) is overlaid on the response area.

Request

```
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:
6 sec-ch-ua-mobile: ?0
7 sec-ch-ua-platform: ""
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/116.0.5845.111
    Safari/537.36
12 Accept:
    text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,i
    mage/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
19 Accept-Language: en-US,en;q=0.9
20 Cookie: security=impossible; PHPSESSID=8ivc9t2ahej1b6gg05brgs4vug
21 Connection: close
22
23 username=adrubale&password=paolo&Login=Login&user_token=
    8b7fe9fa84ae0b404526a613b56cce76
```

Response

```
1 HTTP/1.1 302 Found
2 Date: Tue, 12 Dec 2023 20:08:18 GMT
3 Server: Apache/2.4.57 (Debian)
4 Expires: Thu, 19 Nov 1981 08:52:00 GMT
5 Cache-Control: no-store, no-cache, must-revalidate
6 Pragma: no-cache
7 Location: login.php
8 Content-Length: 0
9 Connection: close
10 Content-Type: text/html; charset=UTF-8
11
12
```

Invio con con credenziali errate

Da qui abbiamo la possibilità di modificare le credenziali inserite nella richiesta POST. Per vedere cosa succede, clicchiamo il tasto destro ed a seguire send to repeater. Premendo Send osserviamo i risultati della richiesta da parte del Server.

```
<br />
<div class="message">
  Login failed
</div>
```

Ovviamente, quest'ultimo non ci concede le risorse richieste e ci invia un login failed. Proviamo a vedere cosa succede se inviamo una richiesta con le credenziali giuste.

```
<div class="body_padded">
  <h1>
    Welcome to Damn Vulnerable Web Application!
  </h1>
  <p>
    Damn Vulnerable Web Application (DWVA) is a
    PHP/MySQL web application that is damn vulnerable.
    Its main goal is to be an aid for security
    professionals to test their skills and tools in a
    legal environment, help web developers better
    understand the processes of securing web
    applications and to aid both students & teachers to
    learn about web application security in a controlled
    class room environment.
  </p>
  <p>
    The aim of DWVA is to <em>
      practice some of the most common web
      vulnerabilities
    </em>
    , with <em>
      various levels of difficulty
    </em>
    , with a simple straightforward interface.
  </p>
  <hr />
  <br />

  <h2>
    General Instructions
  </h2>
  </div>
```

Come è possibile constatare, il server ha risposto inviandoci la risorsa richiesta. Vediamo il testo html che ci presenta la nostra Damn Vulnerable Web Application.