Exploit DVWA - XSS e SQL injection

S6/L2

14/01/2025

Argomento:

Sfruttamento delle Vulnerabilità XSS e SQL Injection sulla DVWA

Obiettivi:

Configurare il laboratorio virtuale per sfruttare con successo le vulnerabilità XSS e SQL Injection sulla Damn Vulnerable Web Application (DVWA).

Istruzioni per l'Esercizio:

1. **Configurazione del Laboratorio:**

- Configurate il vostro ambiente virtuale in modo che la macchina DVWA sia raggiungibile dalla macchina Kali Linux (l'attaccante).
- Verificate la comunicazione tra le due macchine utilizzando il comando ping.
-

2. **Impostazione della DVWA:**

- Accedete alla DVWA dalla macchina Kali Linux tramite il browser.
- Navigate fino alla pagina di configurazione e settate il livello di sicurezza a LOW.
-

3. **Sfruttamento delle Vulnerabilità:**

- Scegliete una vulnerabilità XSS reflected e una vulnerabilità SQL Injection (non blind)

Svolgimento:

Ho configurato le due macchine da far comunicare e ho testato tramite un ping che comunicassero:

```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.60.2
PING 192.168.60.2 (192.168.60.2) 56(84) bytes of data.
64 bytes from 192.168.60.2: icmp_seq=1 ttl=64 time=1.37 ms
64 bytes from 192.168.60.2: icmp_seq=2 ttl=64 time=1.81 ms
64 bytes from 192.168.60.2: icmp_seq=3 ttl=64 time=1.30 ms
64 bytes from 192.168.60.2: icmp_seq=4 ttl=64 time=0.952 ms
^C
— 192.168.60.2 ping statistics —
4 packets transmitted, 4 received, 0% packet loss, time 3003ms
rtt min/avg/max/mdev = 0.952/1.358/1.814/0.306 ms

┌──(kali㉿kali)-[~]
└─$
```

```
msfadmin@metasploitable:~$ ping 192.168.60.5
PING 192.168.60.5 (192.168.60.5) 56(84) bytes of data.
64 bytes from 192.168.60.5: icmp_seq=1 ttl=64 time=1.38 ms
64 bytes from 192.168.60.5: icmp_seq=2 ttl=64 time=0.542 ms
64 bytes from 192.168.60.5: icmp_seq=3 ttl=64 time=0.566 ms
64 bytes from 192.168.60.5: icmp_seq=4 ttl=64 time=0.920 ms

--- 192.168.60.5 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3000ms
rtt min/avg/max/mdev = 0.542/0.854/1.389/0.343 ms
msfadmin@metasploitable:~$ _
```

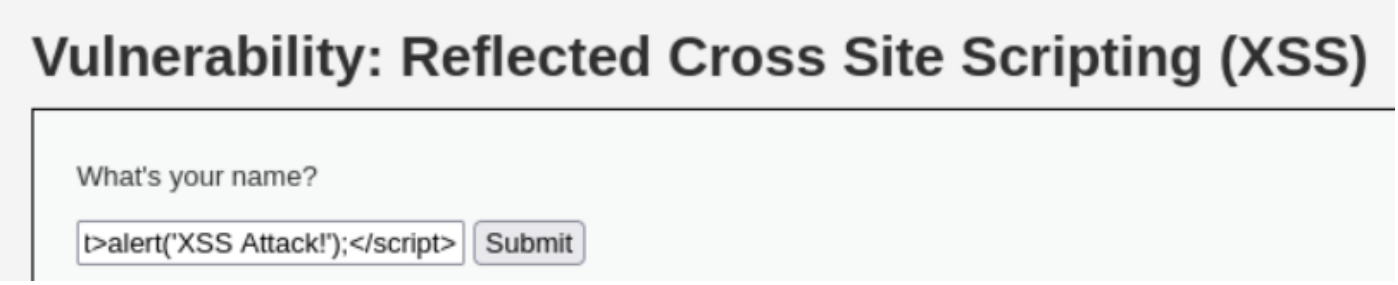
Nel browser di kali sono entrato nella DVWA di Metasploitable digitando il suo indirizzo IP-----> 192.168.60.2

Andiamo su DVWA security ed impostiamo la sicurezza in LOW in modo da poter sfruttare le vulnerabilità in modo più semplice.

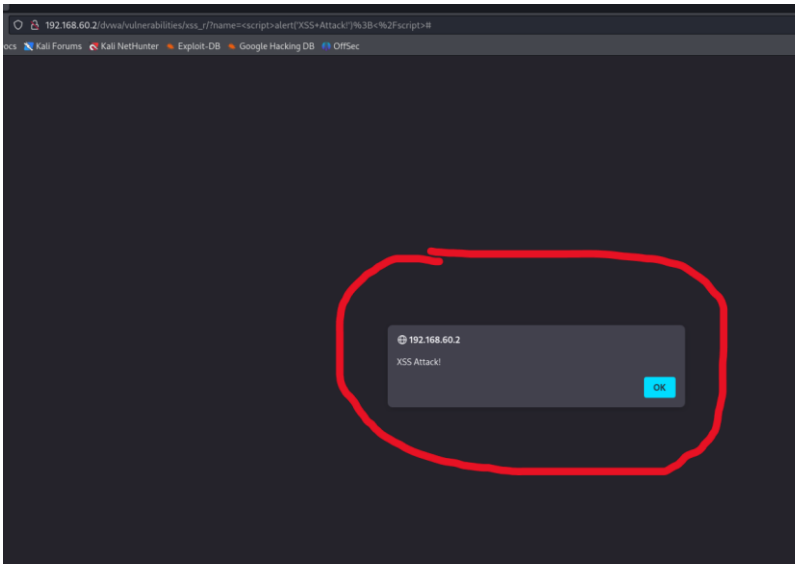
XSS REFLECTED

Andiamo nella pagina XSS reflected per poter testare l'attacco:

Da qui possiamo cominciare con i nostri test.
Ho copiato il payload presente nelle slide per fare una prova e l'ho scritto nello spazio apposito: <script>alert('XSS Attack!');</script>

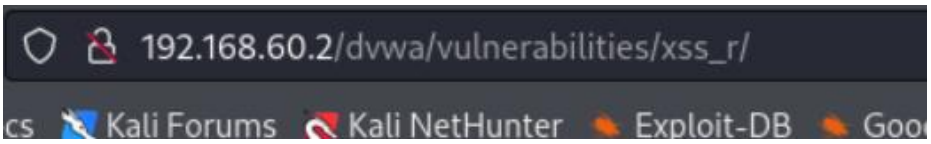


Clicchiamo su Submit e ci aspetteremo che esca fuori un banner di allert che ci avvisa di un attacco XSS:

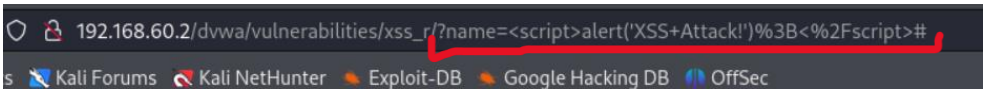


Cliccando su ok torneremo nella pagina della DVWA e possiamo vedere che il payload è stato inserito nella URL della pagina:

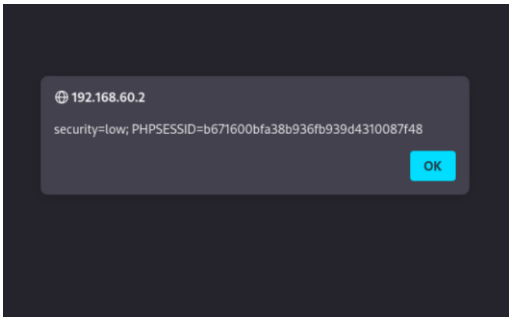
PRIMA



DOPO



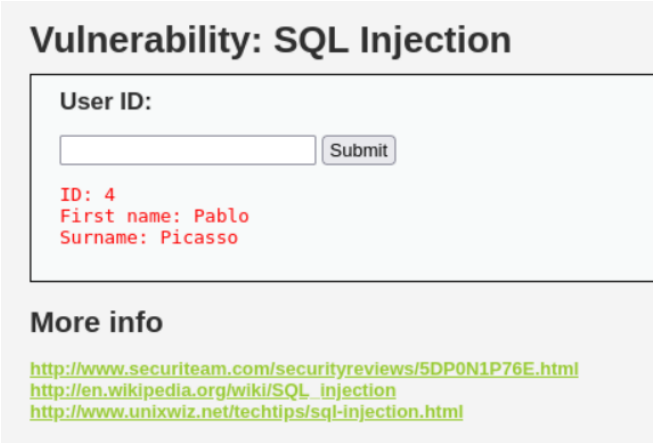
Riporto altre prove che ho fatto:

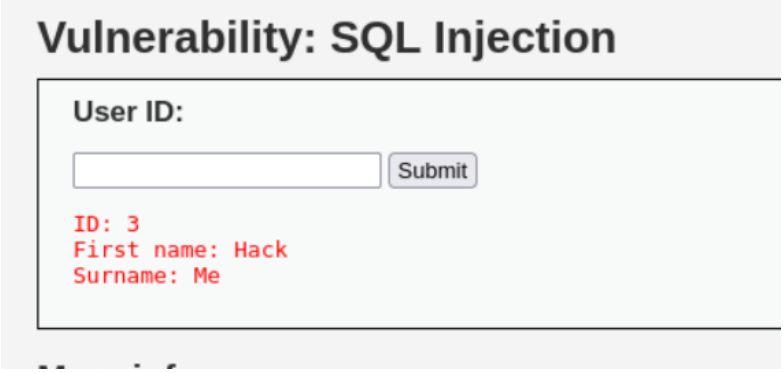


SQL injection

Andiamo nella pagina di SQL injection per fare i test:

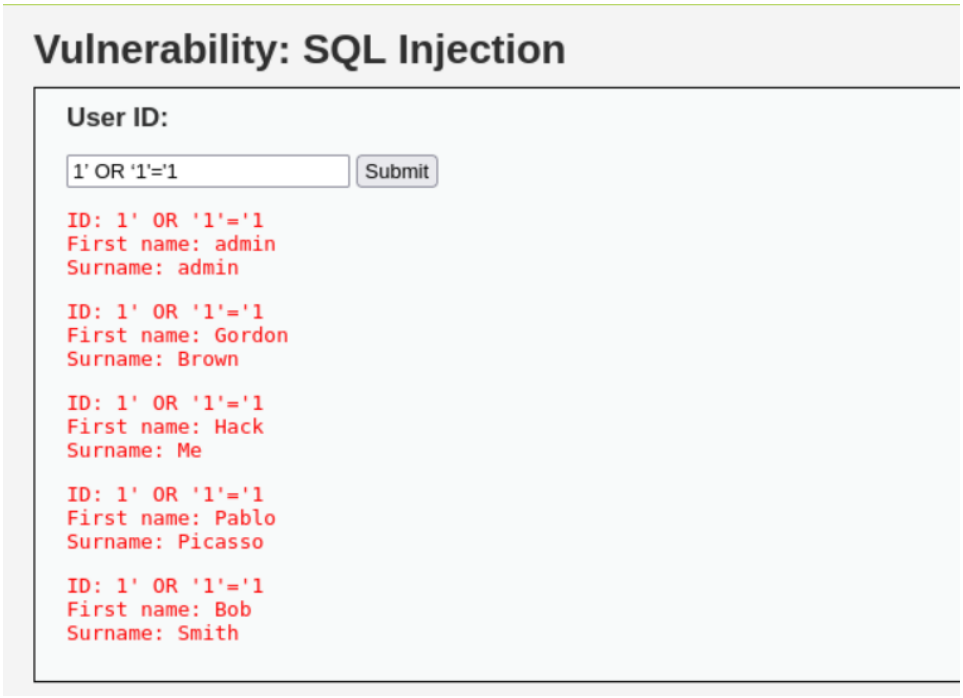
Proviamo a inserire un ID e vediamo che come risultato ci stampa il nome dell'utente che corrisponde a quell'id:



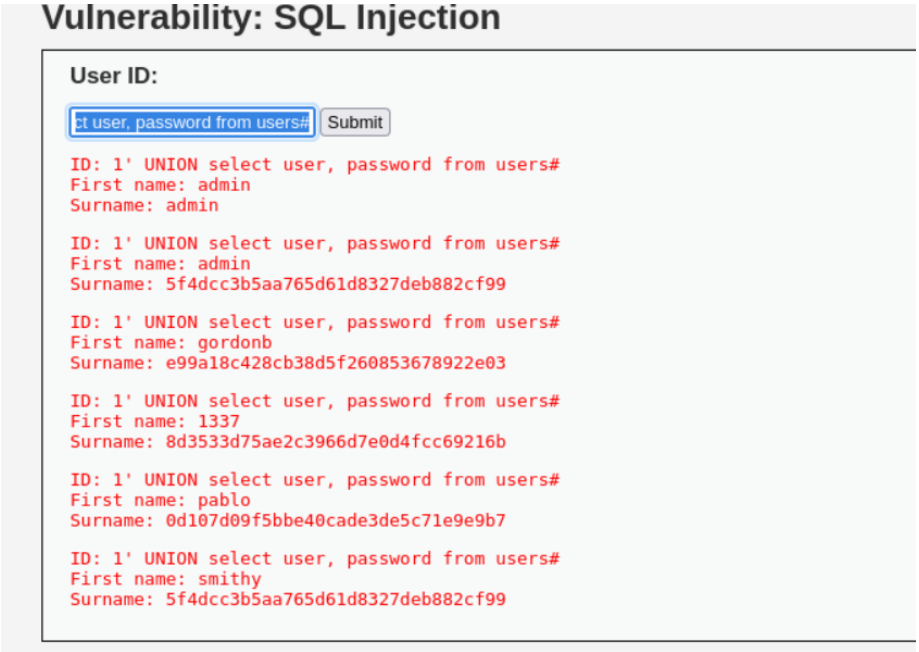


Se vogliamo prenderci tutto il database dobbiamo dargli una condizione che sia sempre vera--------> ‘ or ‘ a ’=‘a

1’ or ‘1’=’1



Ho poi provato a fare una sql injection union per trovare anche i nomi utenti e le password degli users:
1' UNION select user, password from users# -------> questa è la query



Possiamo vedere che come risultato ci ha dato il nome utente e la sua password per tutti gli User ID del database.