🔍 Explanation of the Vulnerability

What is SQL Injection?

SQL Injection is a web security vulnerability that allows an attacker to interfere with the queries that an application makes to its database.

How it Works:

DVWA takes user input and directly inserts it into an SQL query without validating or sanitizing it.

When we submit `' OR 1=1 --`, it changes the SQL query from:

sql

```
SELECT * FROM users WHERE id = '1';
```

sql

```
SELECT * FROM users WHERE id = '' OR 1=1 -- ';
```

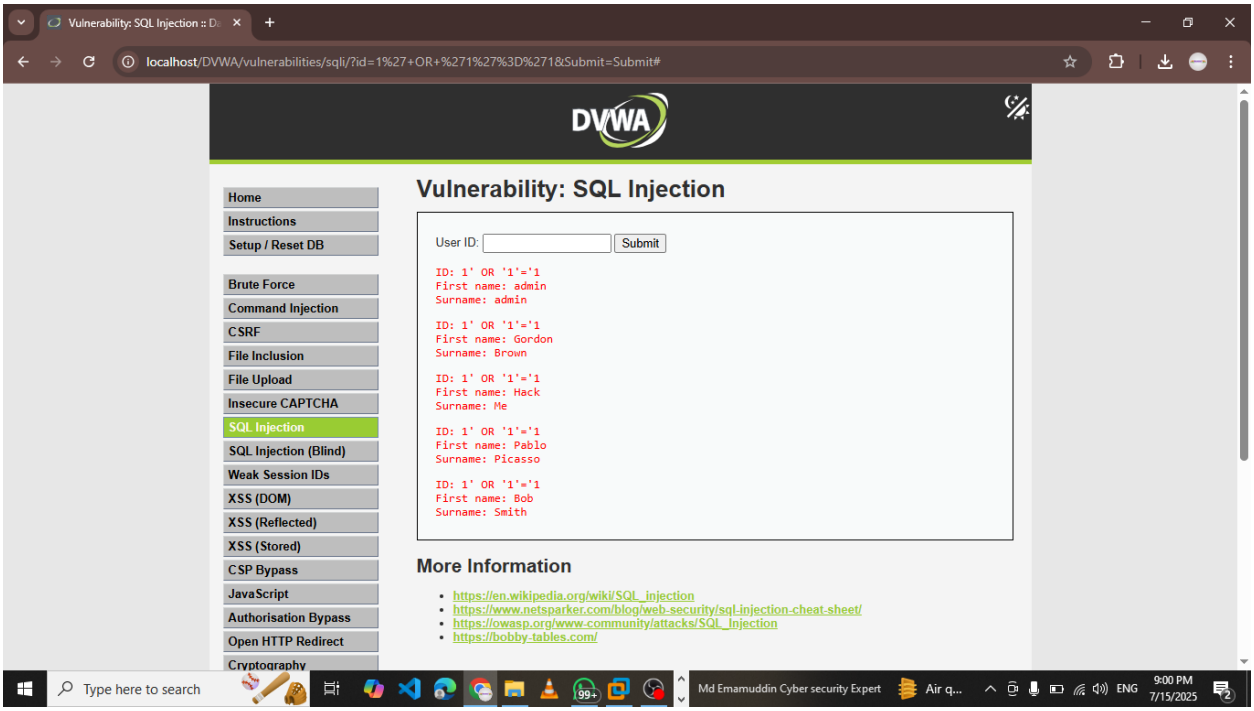
The condition `1=1` is always true, so the query returns **all users** from the database.

Risk in Real World:

- An attacker can **bypass login**, **steal data**, or **manipulate the database**.
- If advanced injection is used, attackers can even **delete data** or **gain shell access**.

How to Prevent:

- Use **parameterized queries (Prepared Statements)**
- Validate and sanitize all user inputs
- Use security tools like **WAF (Web Application Firewall)**
- Keep web applications and databases updated


Vulnerability: SQL Injection :: D
localhost/DVWA/vulnerabilities/sqli/?id=1%27+OR+%271%27%3D%271&Submit=Submit#
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)
CSP Bypass
JavaScript
Authorisation Bypass
Open HTTP Redirect
Cryptography
Vulnerability: SQL Injection
User ID:
Submit
ID: 1' OR '1'='1
First name: admin
Surname: admin
ID: 1' OR '1'='1
First name: Gordon
Surname: Brown
ID: 1' OR '1'='1
First name: Hack
Surname: Me
ID: 1' OR '1'='1
First name: Pablo
Surname: Picasso
ID: 1' OR '1'='1
First name: Bob
Surname: Smith
More Information
https://en.wikipedia.org/wiki/SQL_injection
https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/
https://owasp.org/www-community/attacks/SQL_Injection
https://bobby-tables.com/
Type here to search
Md Emamuddin Cyber security Expert
Air q...
ENG
9:00 PM
7/15/2025