**Name** : Vaibhav Soni

**Enrolment No.** : IU2141230287

**Branch** : CSE – A

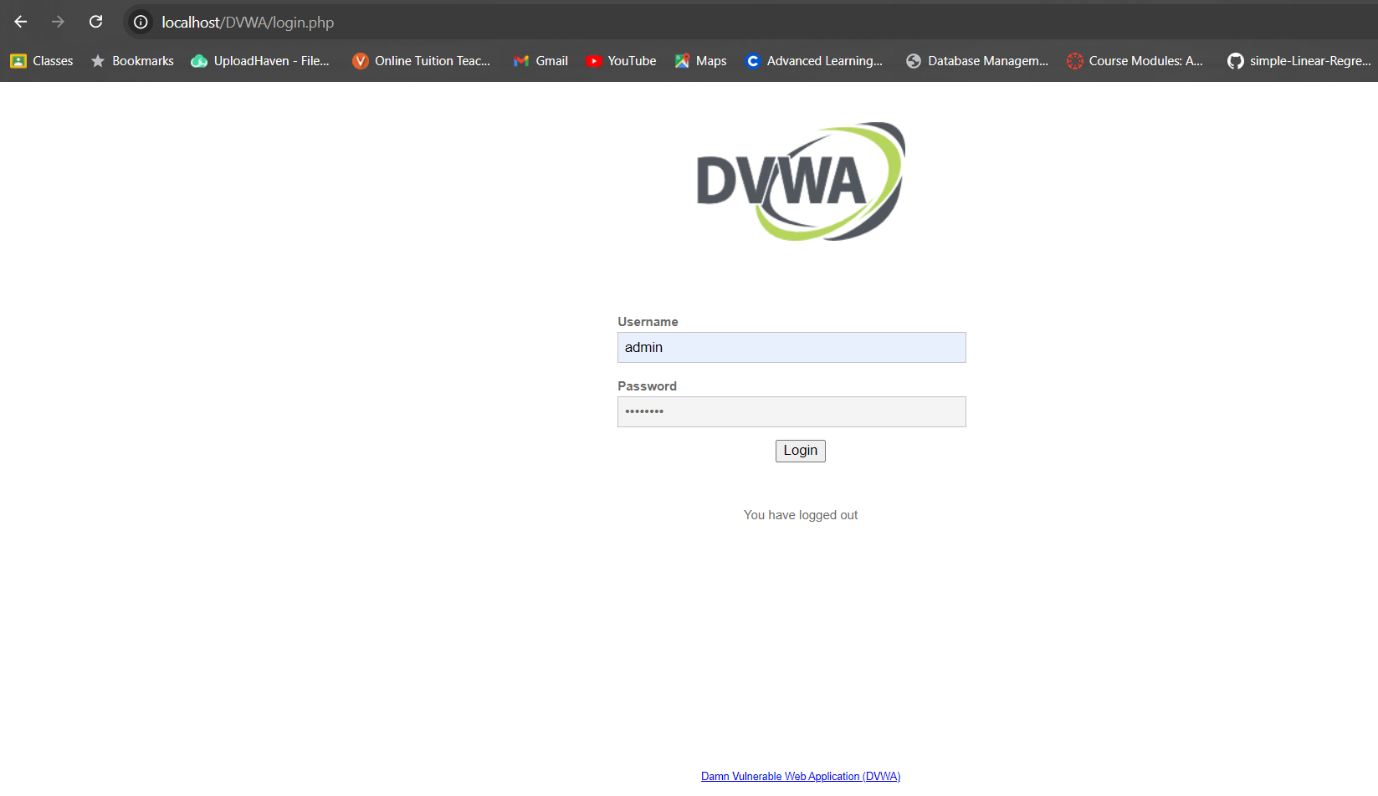
**Sem** : 7

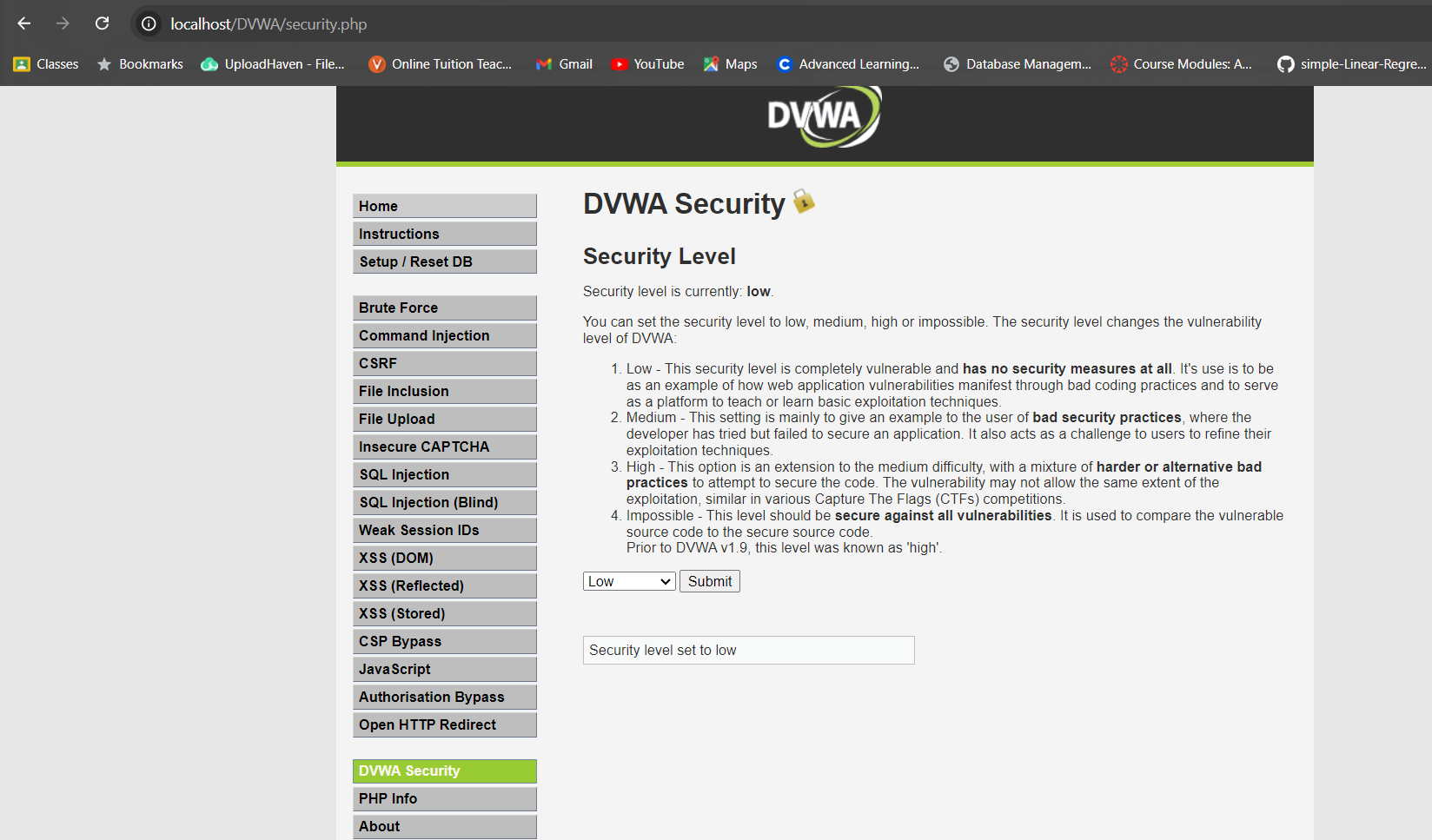
**Subject** : Cyber Security

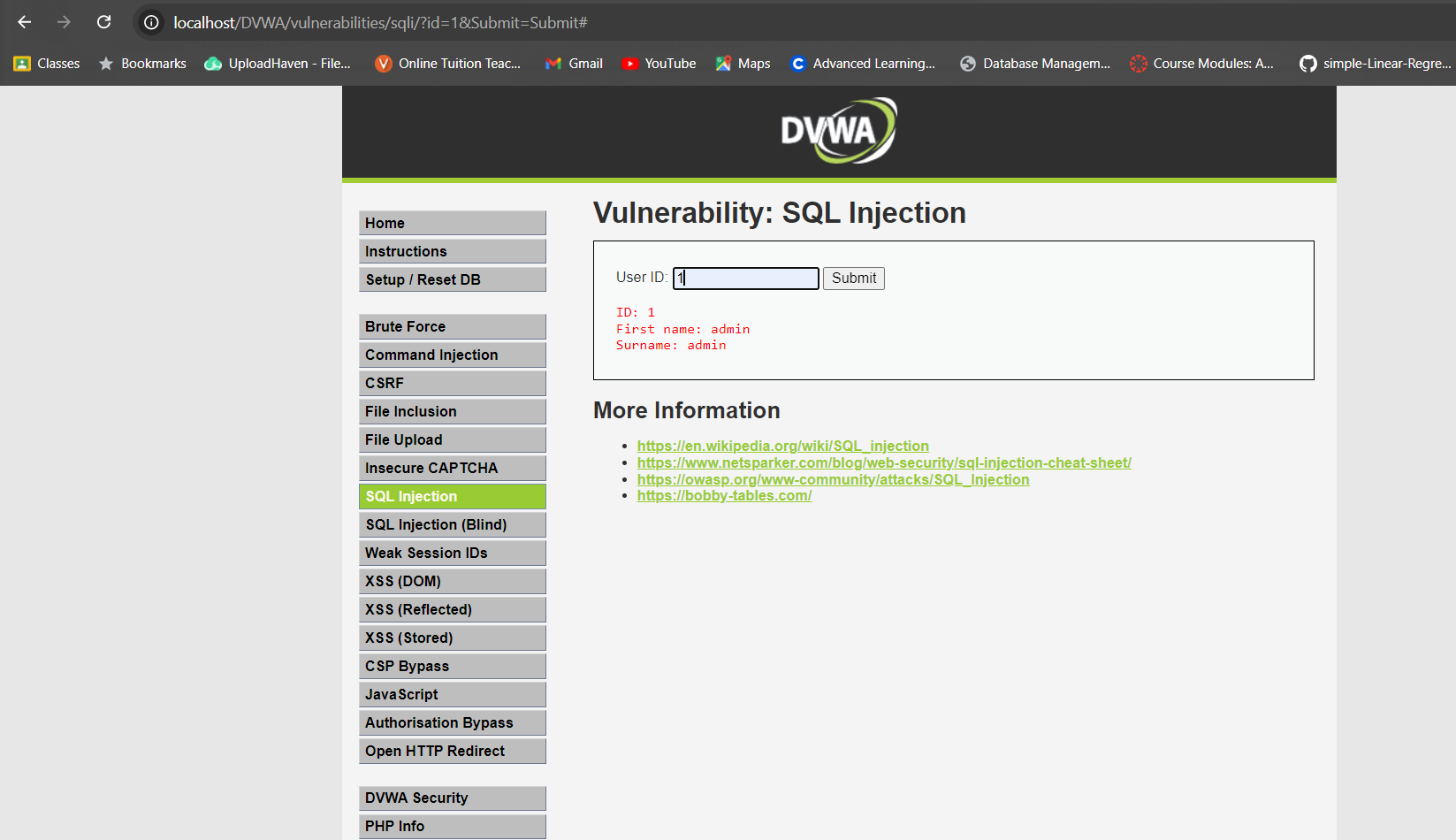
**Lab – 6**

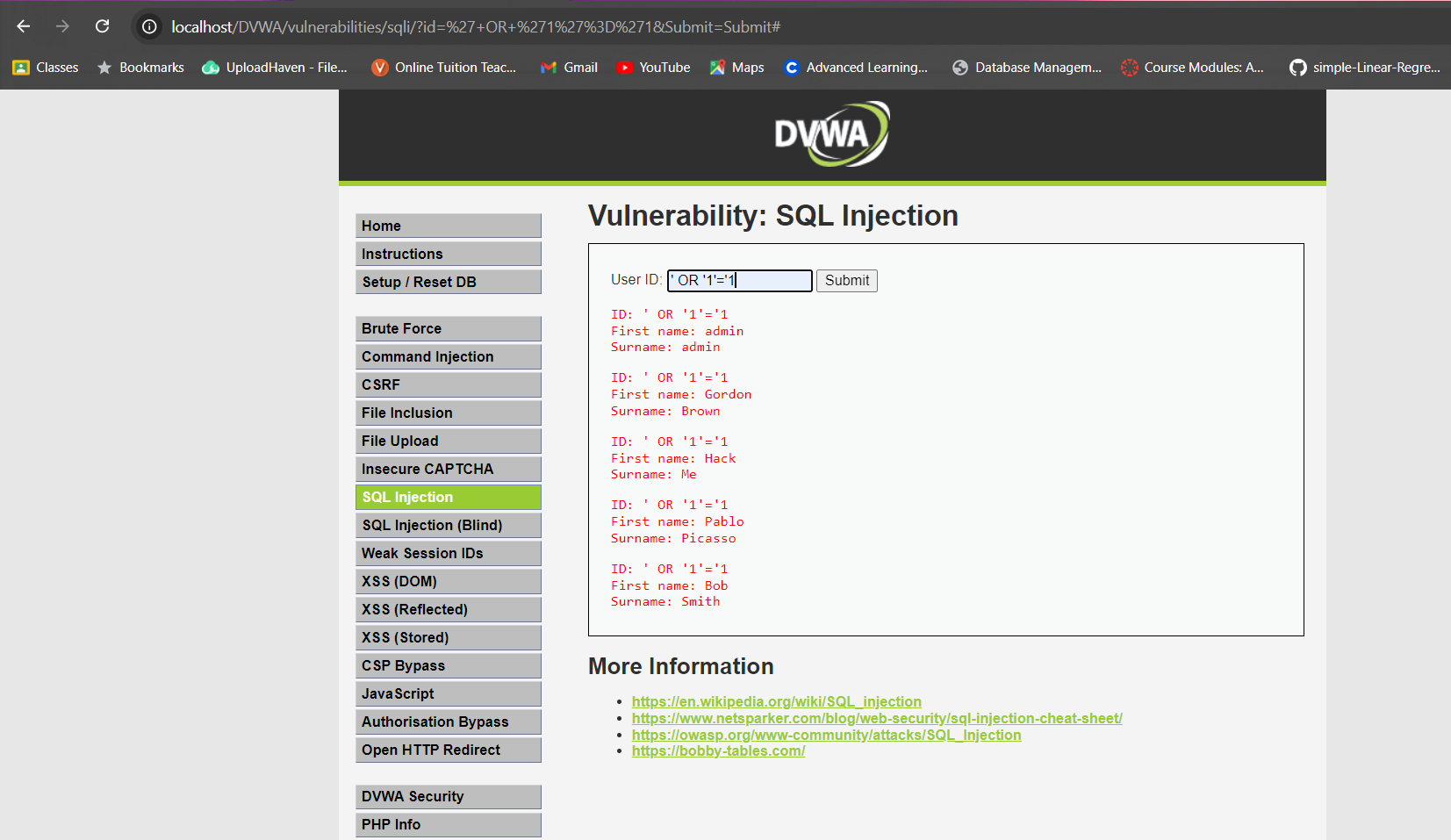
**Aim :** Demonstration of SQL Injection using DVWA.

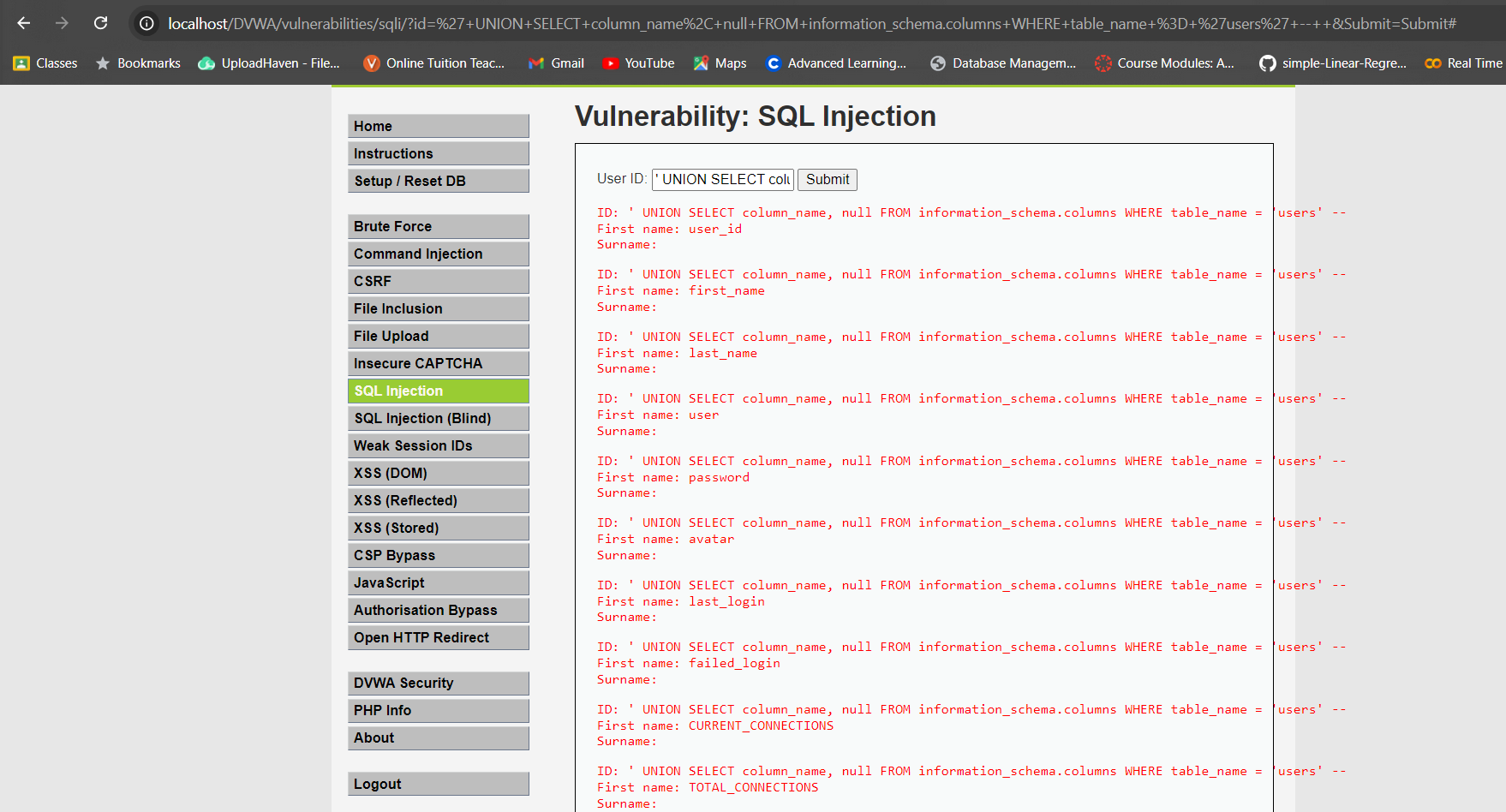
**Screenshots :**

****

****

****

****

****

* During this lab, I gained hands-on experience with SQL injection attacks by exploiting vulnerable SQL queries. Specifically, I used two injection techniques to manipulate the database and retrieve sensitive information. The first payload, **`' OR '1'='1' --`**, was a classic SQL injection that creates an always-true condition in the query, bypassing authentication and allowing access to all records in the database. This simple payload demonstrates how attackers can exploit weak input validation to gain unauthorized access to user data.
* The second payload, **`' UNION SELECT column\_name, null FROM information\_schema.columns WHERE table\_name = 'users' --`**, took advantage of a union-based SQL injection. This allowed me to extract metadata about the database, specifically the column names of the `users` table. By leveraging the `information\_schema.columns`, I was able to identify the structure of the table and gather critical information like column names, which could be used for further attacks or data extraction. Through this lab, I learned how vulnerable SQL queries can be exploited to manipulate databases, and it emphasized the importance of securing applications with prepared statements and proper input sanitization.