# **HACKING WEBSITES**

#### **OBJECTIVE**

The objective of this report includes understanding of potential weaknesses in web systems, assessing the impact of these vulnerabilities, and providing recommendations for mitigation.

By conducting controlled security assessments, the project aims to contribute to the broader objective of enhancing website security and safeguarding user data.

We will see the SQL Injection methodology in this report.

#### **TOOLS**

The tools required are a web browser and knowledge of SQL Injection techniques.

#### **METHODOLOGY**

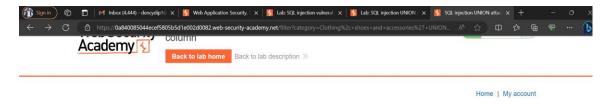
There are two ways for hacking websites which includes Script kiddle methods such as Keylogger and phishing. The other way is by use of Offensive hacking methods by using Terminal and Scripting.

SQL injection is a code injection technique used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker).

SQL injection must exploit a security vulnerability in an application's software, for example, when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and unexpectedly executed. SQL injection is mostly known as an attack vector for websites but can be used to attack any type of SQL database.

Below example shows the process involved in SQL Injection.

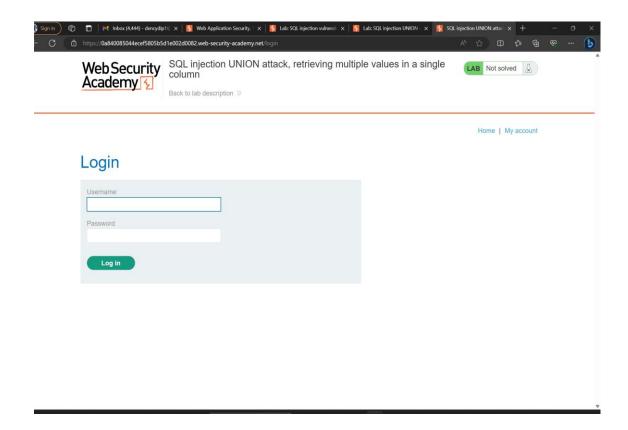
### **PROOF OF CONCEPT**

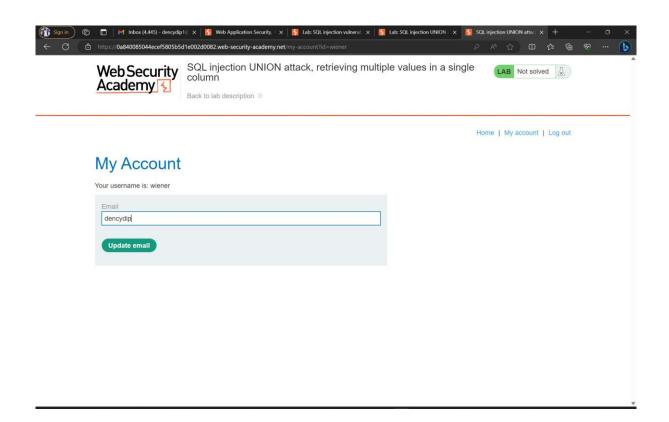


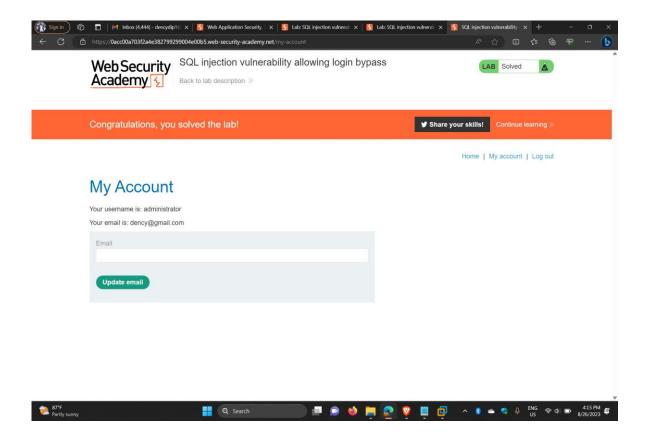


# Clothing, shoes and accessories' UNION SELECT NULL, username||'~'||password FROM users--









## **CONCLUSION**

In summary, ethical hacking stands as a proactive defense strategy. By identifying vulnerabilities, evaluating risks, and fortifying web systems, it safeguards data, maintains trust, and fosters cybersecurity awareness. Adhering to legal and ethical guidelines, ethical hacking contributes to a secure digital landscape and a culture of protection.