Assignment-1

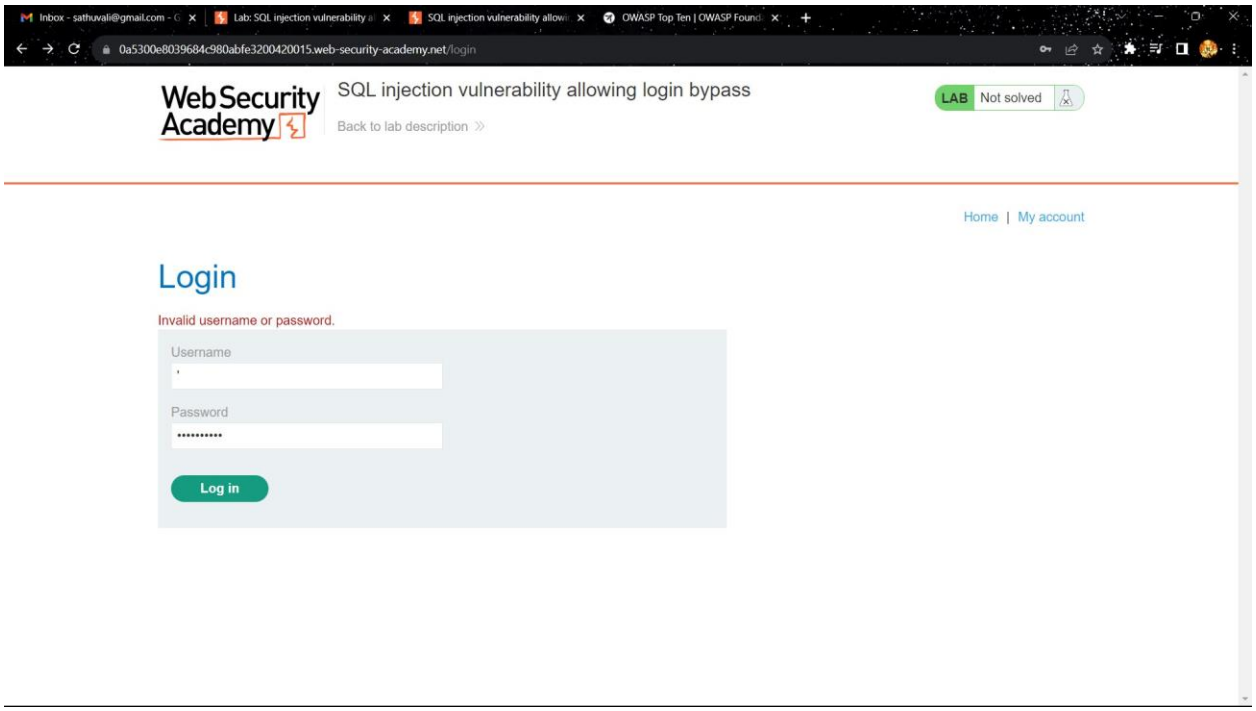
Name: -G. Sathwik

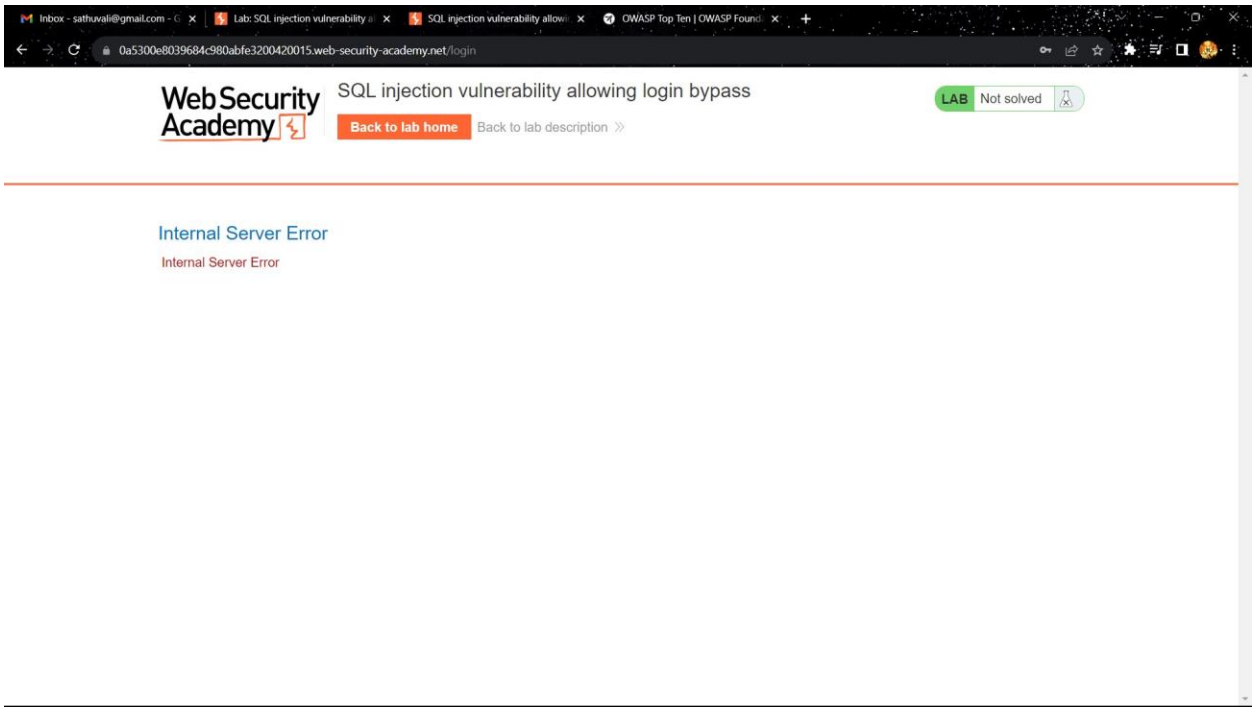
Regno.: - 21bce8137

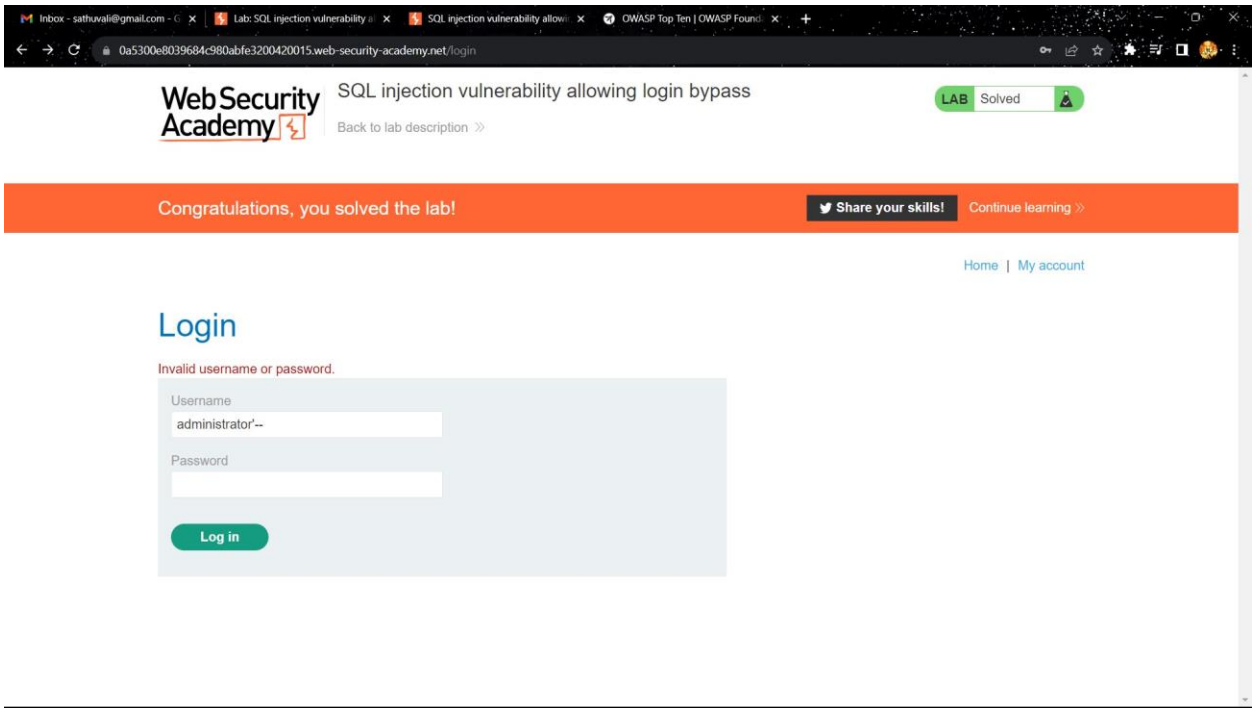
1. **Injection (CWE-89)**: -

Description: Injection vulnerabilities occur when untrusted data is included in a query or command sent to an interpreter. This can include SQL injection, NoSQL injection, OS command injection etc.

Business Impact: Attackers can exploit injection vulnerabilities to execute malicious code or commands on the target system. This can lead to unauthorized access, data breaches, and potential loss of sensitive information, as well as damage to the organization's reputation.



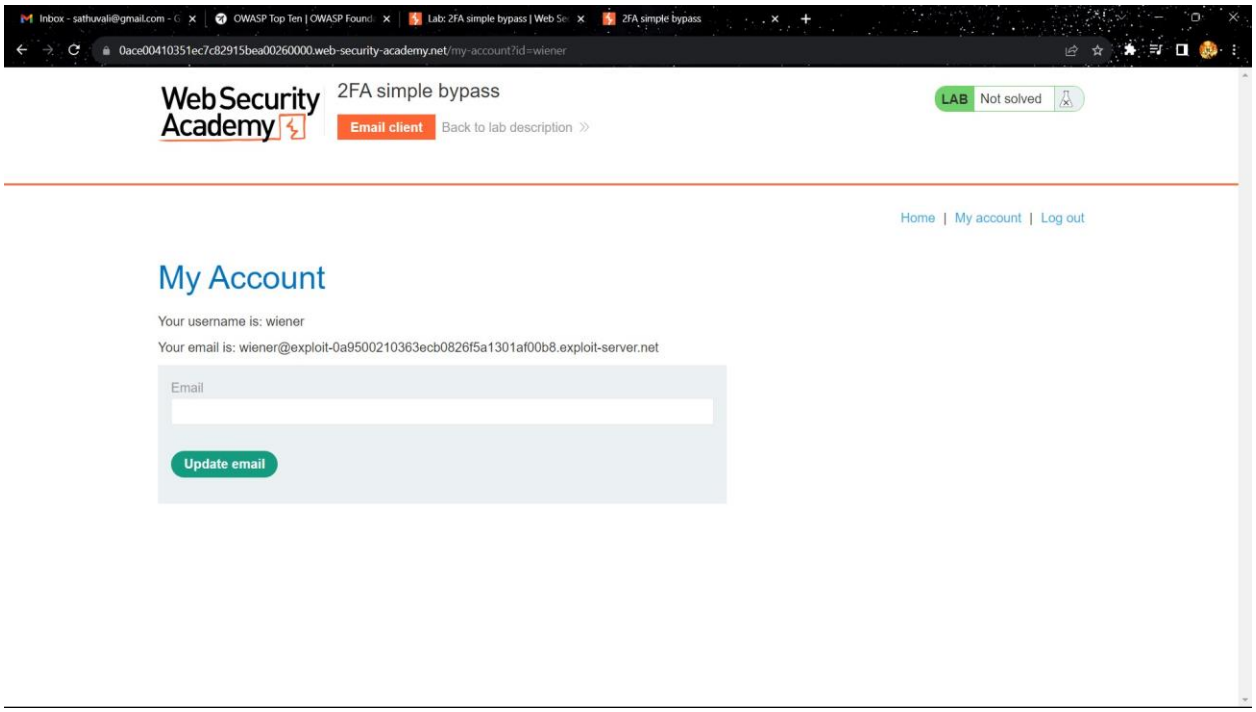

Inbox - sathuvali@gmail.com - G
Lab: SQL injection vulnerability
SQL injection vulnerability allowi
OWASP Top Ten | OWASP Found
0a5300e8039684c980abfe3200420015.web-security-academy.net/login
Web Security Academy
SQL injection vulnerability allowing login bypass
Back to lab home
Back to lab description
LAB Not solved
Internal Server Error
Internal Server Error

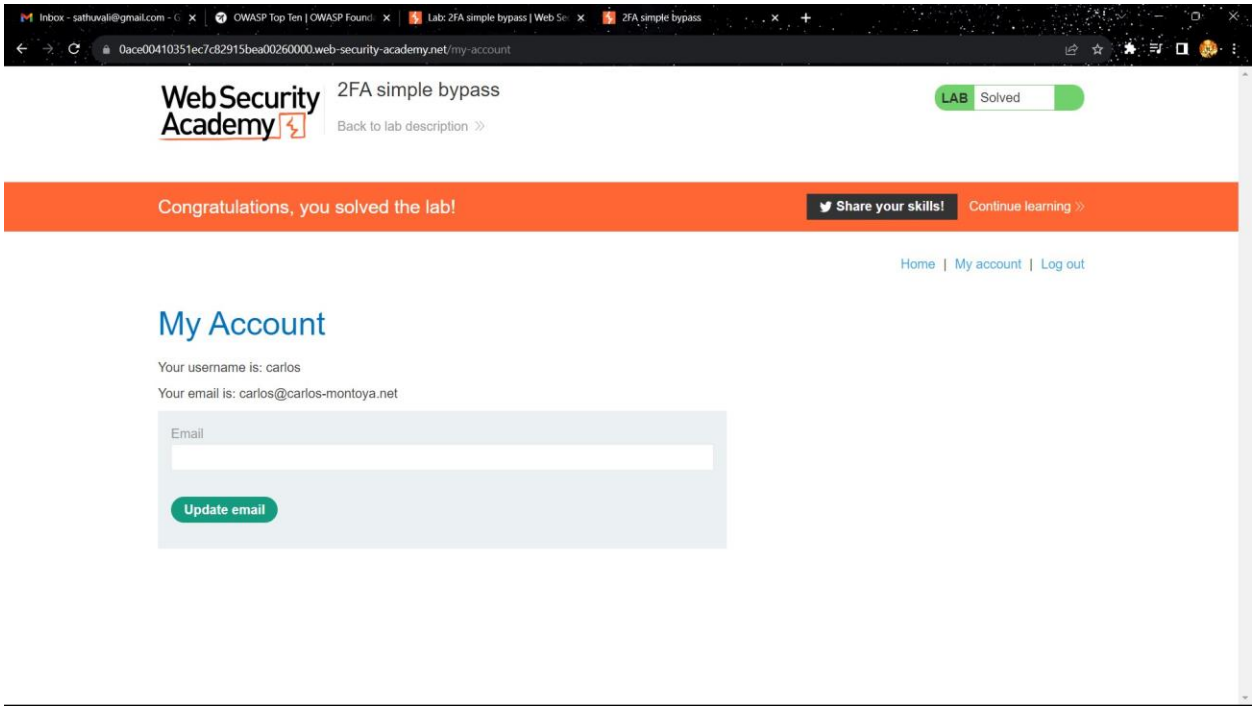

Inbox - sathuvali@gmail.com - G
Lab: SQL injection vulnerability
SQL injection vulnerability allowi
OWASP Top Ten | OWASP Found
0a5300e8039684c980abfe3200420015.web-security-academy.net/login
Web Security Academy
SQL injection vulnerability allowing login bypass
Back to lab description
LAB Solved
Congratulations, you solved the lab!
Share your skills!
Continue learning
Home | My account
Login
Invalid username or password.
Username
administrator'--
Password
Log in

2. **Broken Authentication (CWE-287)**: -

Description: Broken authentication vulnerabilities arise from inadequate or misconfigured authentication mechanisms. This can result in unauthorized users gaining access to sensitive functionality or data.

Business Impact: Successful attacks on broken authentication can lead to unauthorized account access, data breaches, and identity theft. This can harm an organization's reputation, incur regulatory fines, and erode customer trust.

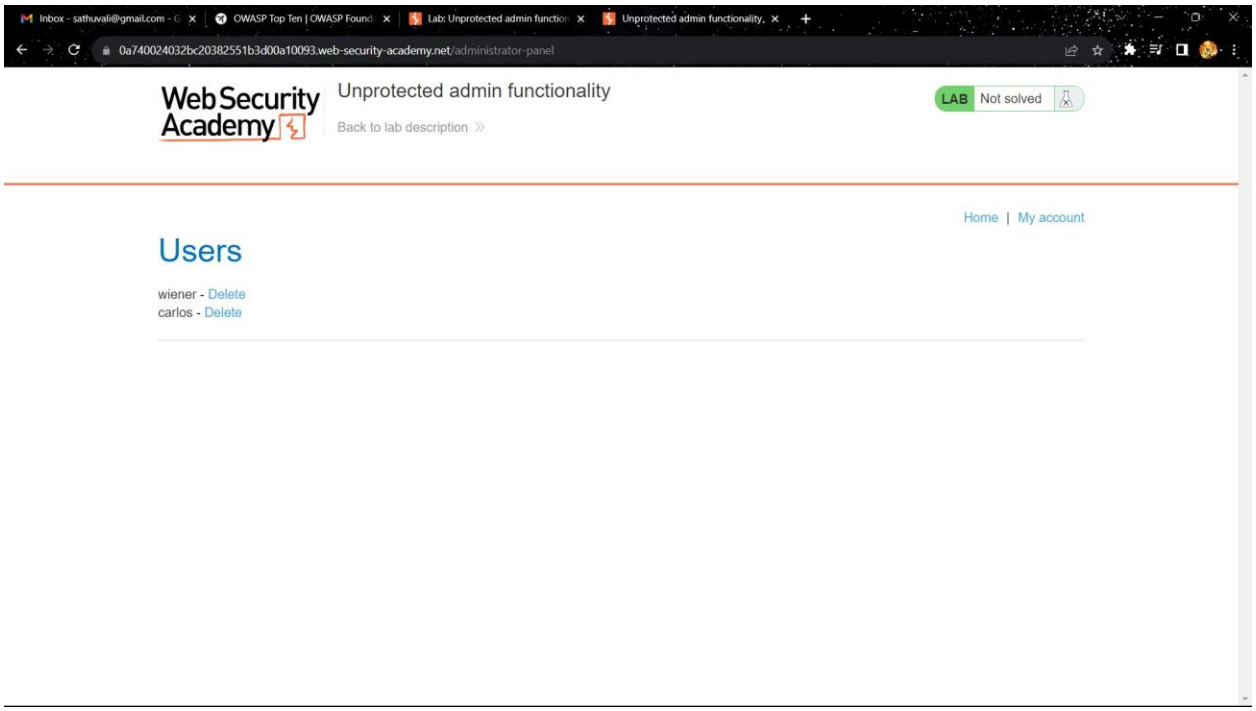


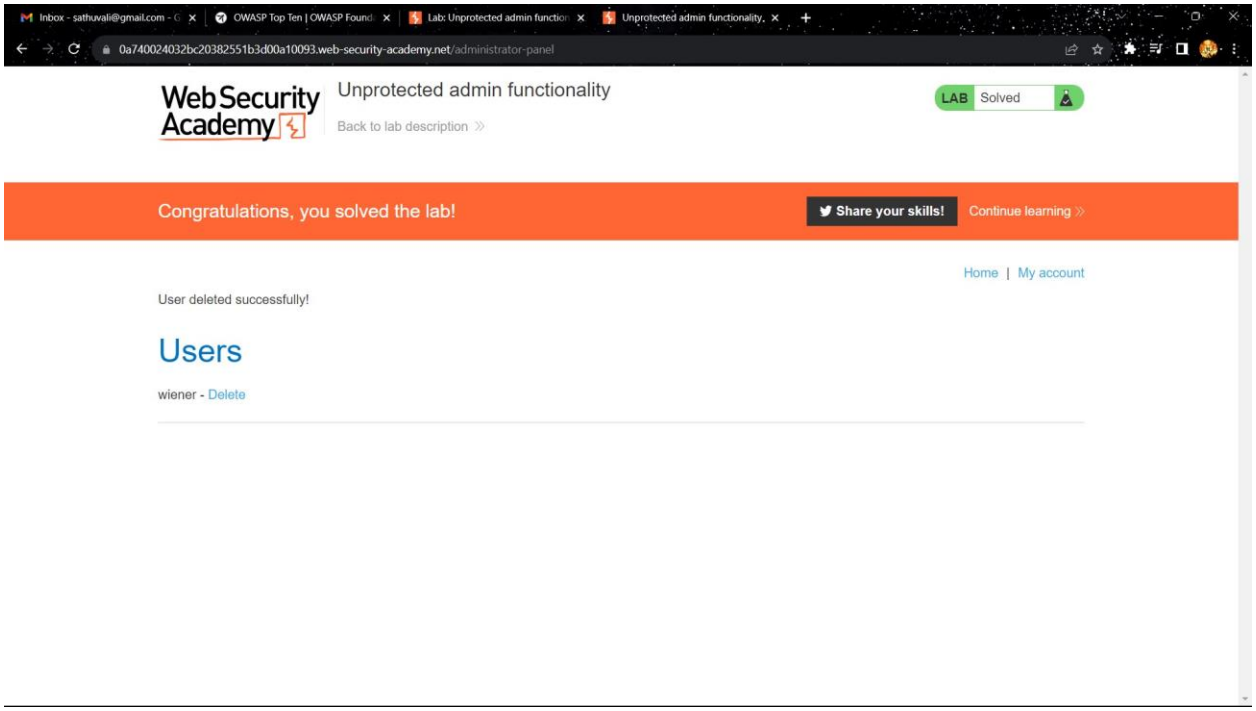


3. **Broken Access Control (CWE-285)**: -

Description: Broken access control occurs when restrictions on what authenticated users can do are not properly enforced. This can enable users to perform actions or access data they shouldn't be able to.

Business Impact: Attackers can exploit broken access control to gain unauthorized access to sensitive functions or data, manipulate user accounts, and perform actions that could harm the application or its users. This can lead to data breaches, financial loss, and damage to an organization's reputation.


Inbox - sathuvali@gmail.com - G
OWASP Top Ten | OWASP Found
Lab: Unprotected admin function
Unprotected admin functionality
0a740024032bc20382551b3d00a10093.web-security-academy.net/administrator-panel
Web Security Academy
Unprotected admin functionality
Back to lab description
LAB Not solved
Home | My account
Users
wiener - Delete
carlos - Delete


Inbox - sathuvali@gmail.com - G
OWASP Top Ten | OWASP Found
Lab: Unprotected admin function
Unprotected admin functionality
0a740024032bc20382551b3d00a10093.web-security-academy.net/administrator-panel
Web Security Academy
Unprotected admin functionality
Back to lab description
LAB Solved
Congratulations, you solved the lab!
Share your skills!
Continue learning
Home | My account
User deleted successfully!
Users
wiener - Delete

4. **Sensitive Data Exposure (CWE-200)**: -

Description: Sensitive data exposure occurs when sensitive information like passwords, credit card numbers, or personal data is exposed without proper protection. This can be due to weak encryption, insecure storage, or inadequate access controls.

Business Impact: Exposure of sensitive data can lead to identity theft, financial loss, legal repercussions, and a loss of trust from customers. Compliance violations and regulatory fines may also result.

5. **XML External Entity (XXE) (CWE-611)**: -

Description: XXE vulnerabilities happen when an XML input is processed by a poorly configured XML parser, allowing attackers to include external entities. This can lead to data disclosure or server-side request forgery (SSRF) attacks.

Business Impact: XXE attacks can lead to the exposure of sensitive internal files, denial of service, or unauthorized data access. They may also enable attackers to interact with internal systems, potentially causing further damage.