**Report on User Role Can be Modified in User Profile**

**Presented By**

**Shikhar Kumar Prasad**

# Table of Content :-

|  |  |  |
| --- | --- | --- |
| **Sr. No.** | **Contents** | **Page No.** |
| 1 | Introduction | 3 |
| 2 | Objectives | 3 |
| 3 | Requirements | 3 |
| 4 | Scope | 4 |
| 5 | Tools Used | 5 |
| 6 | Methodology Used | 5-11 |
| 7 | Recommendation | 12 |
| 8 | Conclusion | 13 |
| 19 | References | 13 |

**1.Introduction:**

This report shows how to change a user's role in their profile by getting access

to a web application's admin panel and performing a specified action with its

privileges. This report covers everything from the objective to the conclusion.

There is an administrative panel at /admin. It is accessible to logged-in users with

the role-id 2. To complete the task, we must modify the user's role from normal

to admin and grant them administrative access.

# 2.Objectives:

Our objective is to demonstrate our ability to exploit access control issues in the web

application. Our aim is to gain unauthorized access to the admin panel, which is

restricted to users with a role ID 2, and use it to delete a user named "carlos".

# 3.Requirements:

1. VirtualBox
2. Kali Linux VM
3. Firefox Browser
4. Foxy proxy
5. Burp suite
6. Access to Lab Environment

# 4.Scope:

1. **Access Control Assessment**: The project would involve a comprehensive assessment of the access control mechanisms implemented within the web application. This includes examining how user roles are defined, assigned, and enforced throughout the application.
2. **Vulnerability Identification**: Conducting a thorough analysis to identify potential vulnerabilities within the access control system. This includes both technical vulnerabilities, such as insufficient validation of user roles, as well as potential process-related vulnerabilities, such as inadequate role assignment procedures.
3. **Exploitation Analysis**: Exploring potential exploitation scenarios to understand the impact of identified vulnerabilities. This may involve simulating attacks or conducting penetration

testing to determine the extent to which unauthorized access can be gained through exploiting access control weaknesses.

1. **Mitigation Recommendations**: Providing recommendations for mitigating identified vulnerabilities and enhancing the overall security of the access control system. This may include implementing additional security controls, improving role assignment procedures, or enhancing monitoring and logging capabilities.
2. **Policy and Procedure Review**: Evaluating existing access control policies and procedures to ensure they align with best practices and regulatory requirements. This may involve reviewing documentation, interviewing stakeholders, and assessing the effectiveness of current practices in mitigating access control risks.
3. **Training and Awareness**: Developing training materials and awareness programs to educate stakeholders about the importance of access control and their roles and responsibilities in maintaining a secure environment. This may include training sessions for administrators, developers, and end-users on access control best practices and security awareness.
4. **Continuous Improvement**: Establishing mechanisms for ongoing monitoring and improvement of the access control system. This includes implementing regular security assessments, reviewing access control policies and procedures, and adapting to evolving

threats and requirements.

1. **Documentation and Reporting**: Documenting the findings, recommendations, and actions taken throughout the project. This may include creating detailed reports for stakeholders, maintaining an inventory of identified vulnerabilities and their status, and documenting

changes made to the access control system.

# 

# 5.Tools Used:

* + - 1. Virtual Box
      2. Kali linux VM
      3. Burp suite
      4. Firefox Browser
      5. Foxy proxy

# 

# 6.Methodology Used:

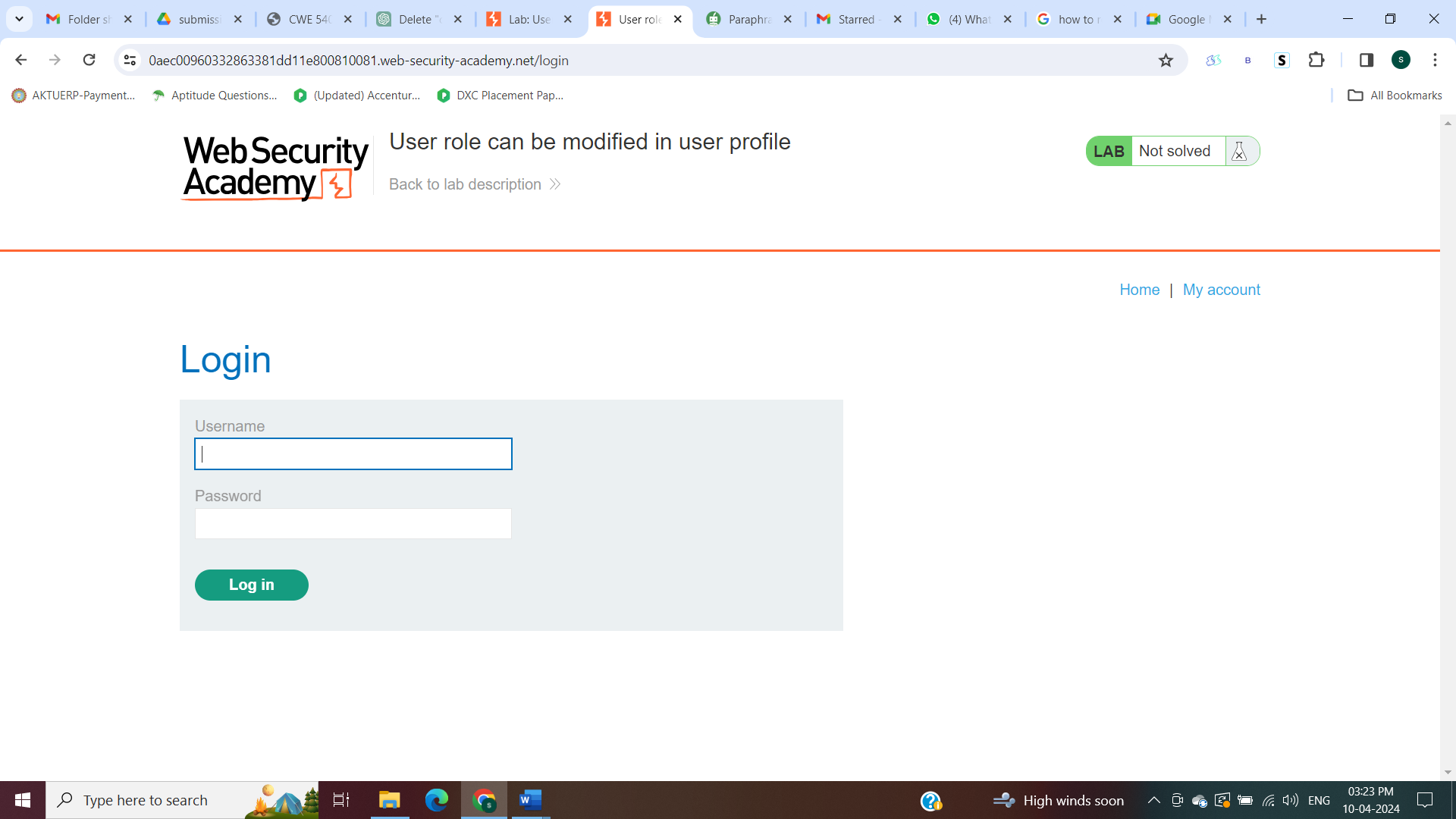
1. **Initial Exploration**:
   * Understand the Objective: The participant reads and understands the objective of the lab, which is to gain access to the admin panel and delete the user "carlos."
   * Review Instructions: Carefully read and review the provided instructions, which outline the steps needed to achieve the objective.
2. **Login and Account Access**:
   * Use the provided credentials (wiener:peter) to log in to the web application.
   * Navigate to the account page or profile section to access the functionality for updating the email address associated with the user account.
3. **Observation of Role ID**:
   * Upon updating the email address, observe the response from the server to ensure that it contains the user's role ID.
   * Confirm that the role ID is present in the response, indicating that the user is authenticated and has the necessary privileges.
4. **Exploitation of Access Control Vulnerability**:
   * Use Burp Repeater or a similar tool to intercept and modify the email submission

request.

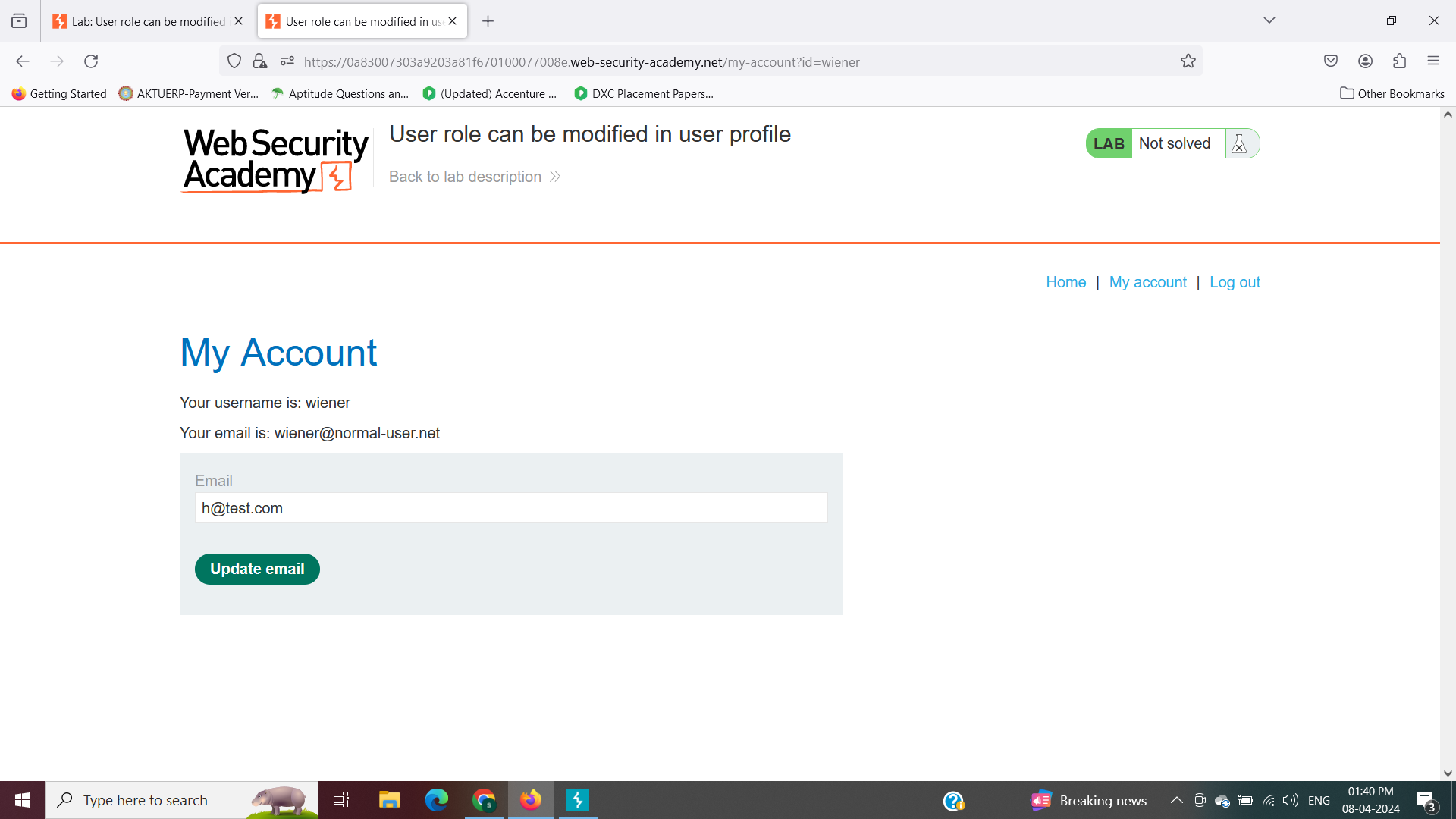
* + Add "roleid":2 into the JSON in the request body to modify the role ID associated with the user account.
  + Resend the modified request and observe the response to confirm that the role ID has changed to 2, granting the user elevated privileges.

1. **Access Admin Panel and User Deletion**:
   * With the modified role ID granting access to the admin panel, navigate to the /admin URL to access the admin interface.
   * Locate the functionality to delete users and proceed to delete the user "carlos" as per the lab's objective.
2. **Verification and Completion**:
   * Verify that the user "carlos" has been successfully deleted from the system.
   * Confirm completion of the lab objective by ensuring that all required steps have been executed successfully and that the desired outcome has been achieved.

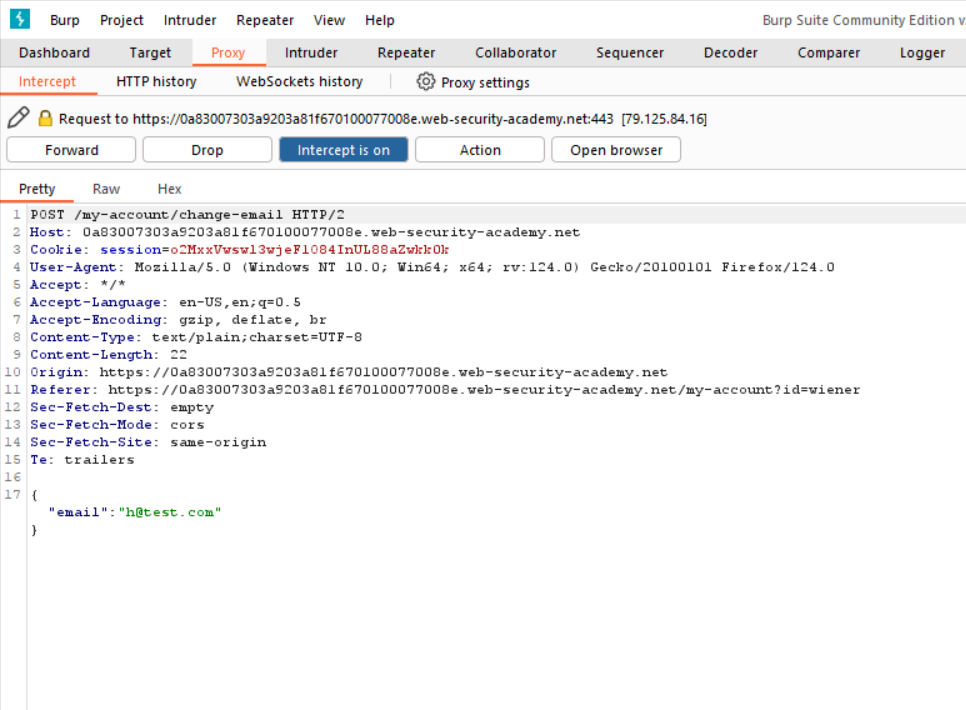
**Step 1:** Go to login page and login using username and password



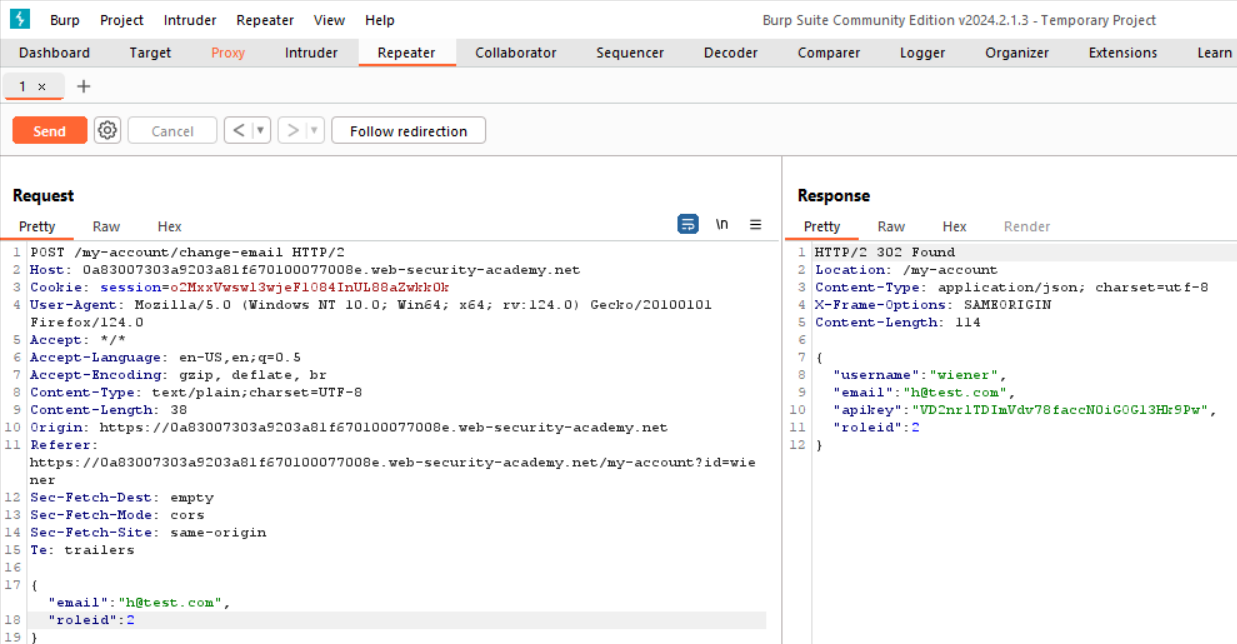
**Step 2:** Use the provided feature to update the email address associated with your account.



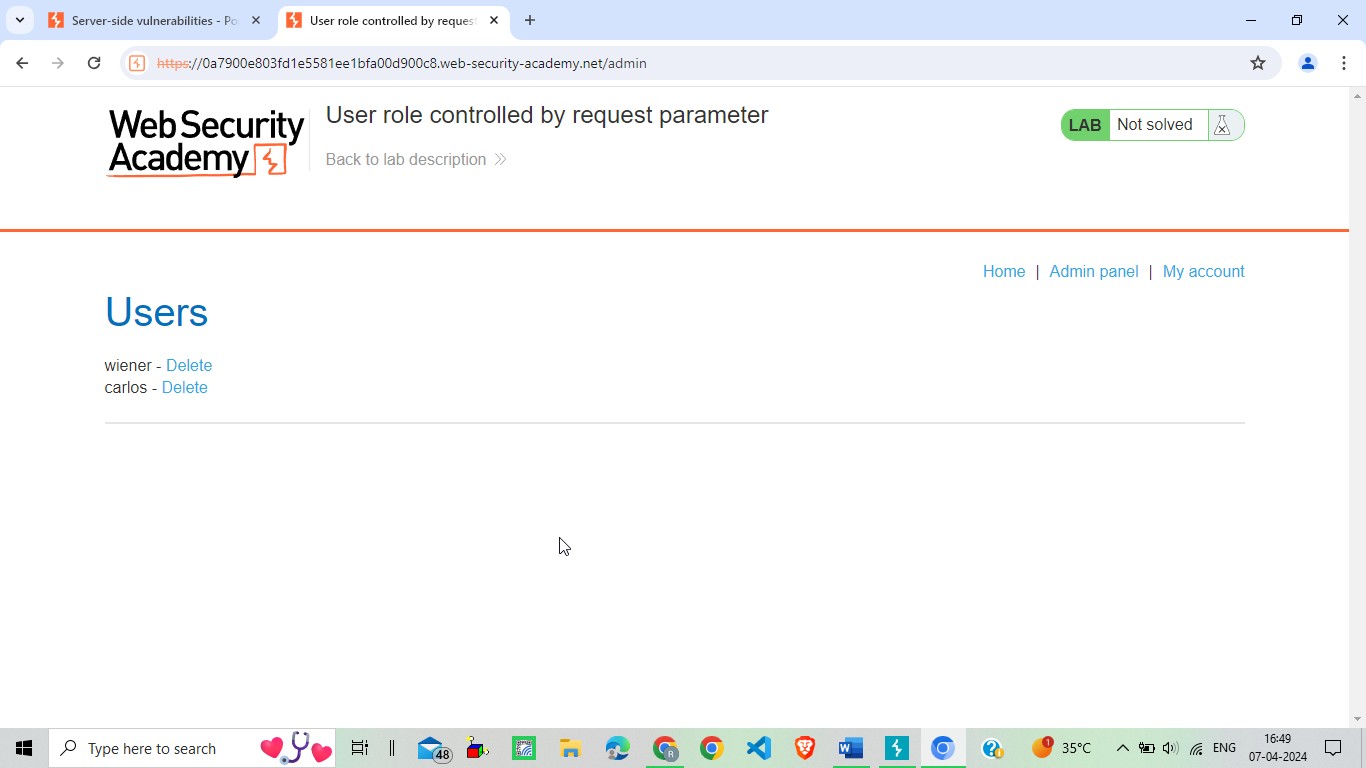
**Step 3**Observe that the response contains your role ID.



1. **Step 4.** Send the email submission request to Burp Repeater, add "roleid":2 into the JSON in the request body, and resend it. Observe that the response shows your role-id has changed to 2.



**Step 5:-** Browse to /admin and delete carlos.



**7.Recommendation: -**

**1.Implement Proper Role-Based Access Control (RBAC)**: Ensure that the web application implements RBAC effectively, with clear definitions of roles and associated permissions. Regularly review and update role assignments to align with the principle of least privilege.

1. **Input Validation and Sanitization**: Implement robust input validation and sanitization mechanisms to prevent injection attacks such as SQL injection or command injection. Validate and sanitize all user-supplied input before processing it to prevent malicious exploitation.
2. **Use of Secure Authentication Mechanisms**: Employ secure authentication mechanisms such as multi-factor authentication (MFA) to enhance user authentication security. Utilize strong password policies and encourage users to use complex passwords to mitigate brute force attacks.
3. **Access Control Logging and Monitoring**: Implement logging and monitoring mechanisms to track access to sensitive functionalities, including the admin panel. Regularly review access logs for suspicious activities and take appropriate action upon detection of unauthorized access attempts.
4. **Regular Security Assessments**: Conduct regular security assessments, including penetration testing and vulnerability scanning, to identify and address access control vulnerabilities proactively. Stay updated on emerging security threats and vulnerabilities relevant to access control mechanisms.
5. **Secure Development Practices**: Follow secure development practices throughout the software development lifecycle (SDLC). Include access control considerations in the design, development, and testing phases to prevent vulnerabilities from being introduced or overlooked.
6. **User Education and Awareness**: Provide training and awareness programs for users, administrators, and developers on access control best practices, common security threats, and how to recognize and respond to security incidents effectively.
7. **Incident Response Plan**: Develop and maintain an incident response plan outlining procedures for responding to security incidents related to access control breaches. Ensure that the plan includes steps for containing the incident, investigating the root cause, and implementing remediation measures promptly.
8. **External Security Audits**: Engage external security auditors or consultants periodically to conduct independent security audits of the web application, including its access control mechanisms. Obtain recommendations and guidance from experts to improve the overall security posture of the application.

# 8.Conclusion:-

The lab scenario "User role can be modified in user profile" highlights the critical importance of robust access control mechanisms in ensuring the security of web applications. Through the exploration and exploitation of access control vulnerabilities, participants gain valuable insights into the potential risks associated with inadequate access controls and the impact they can have on the security posture of an application.

By successfully completing the lab objective of accessing the admin panel and deleting the user "carlos," participants demonstrate their ability to identify, exploit, and mitigate access control vulnerabilities effectively. This hands-on experience equips them with practical knowledge and skills that are invaluable in real-world cybersecurity scenarios.

Moving forward, it is essential to apply the lessons learned from this lab to improve access control practices within web applications. This includes implementing proper role-based access control mechanisms, conducting regular security assessments, and fostering a culture of security awareness and vigilance among users and administrators.

Overall, the lab serves as a valuable learning experience, highlighting the importance of proactive security measures and the ongoing effort required to protect against evolving threats. By addressing access control vulnerabilities effectively, organizations can enhance the resilience of their web applications and safeguard sensitive data from unauthorized access and exploitation.

# 9.References:-

1. Web security Academy
2. https://cyberw1ng.medium.com/7-4-lab-user-role-can-be-modified-in-user-profile-2023-e0ed16ca2d79
3. https://portswigger.net/web-security/access-control/lab-user-role-can-be- modified-in-user-profile