Name: Samarth Jain

USN: 4SU20CS081

Course: Cybersecurity

Trainer: Bharath Kumar

Date: 09/09/2023

Assignment Details

Assigned Date: 08/09/2023

Due Date: 09/09/2023

Topic: Privilege Escalation

Introduction

Privilege escalation is a cybersecurity term that refers to the process by which an attacker gains unauthorized access to higher levels of privilege or authority within a computer system, application, or network. Privilege escalation can occur in two main forms: horizontal privilege escalation and vertical privilege escalation.

Horizontal privilege escalation involves an attacker gaining access to the same level of privilege as their current user account but for a different user or entity. For example, if an attacker with a standard user account manages to compromise another standard user's credentials, they can then access resources and perform actions as that user. This form of privilege escalation is often used to move laterally within a network, increasing an attacker's reach and potential impact.

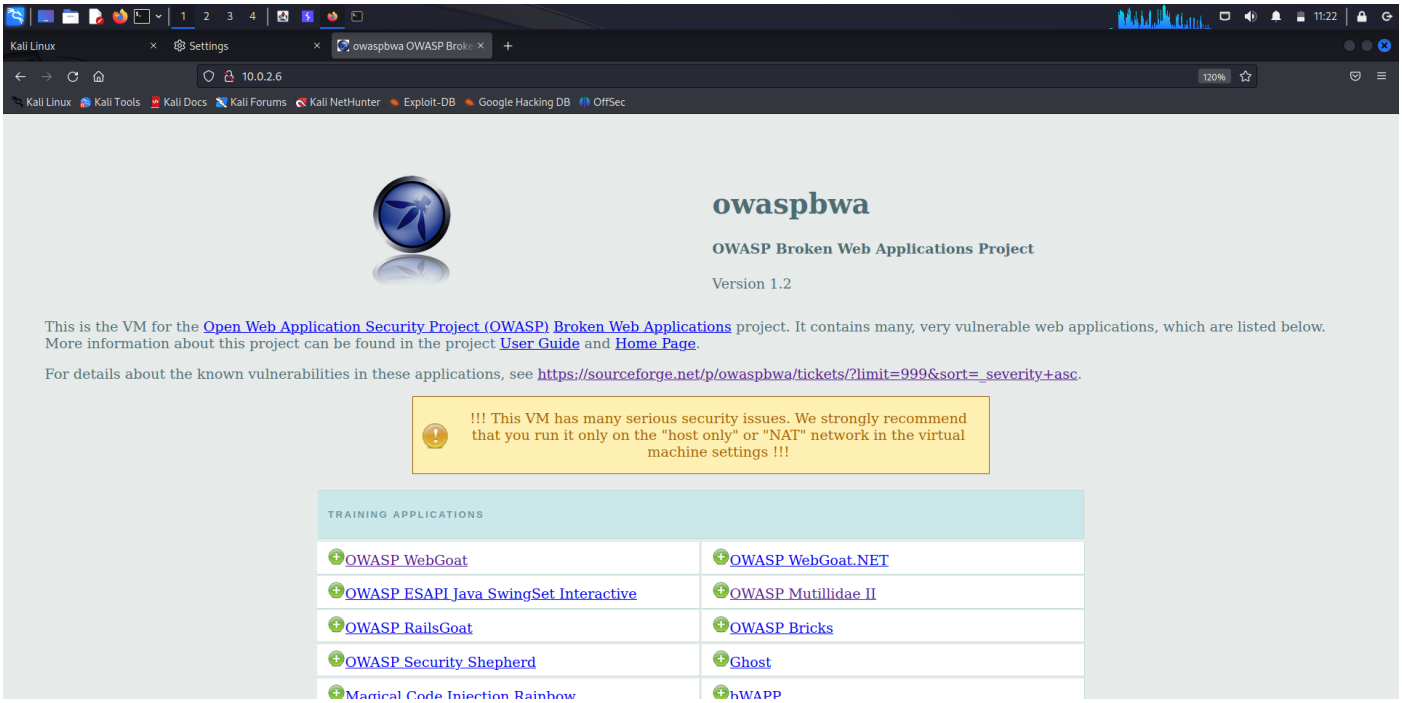
Vertical privilege escalation, on the other hand, involves an attacker moving from a lower level of privilege to a higher one. This typically occurs when an attacker exploits vulnerabilities or weaknesses in a system or application to gain administrative or root-level access. Once an attacker achieves vertical privilege escalation, they can potentially control the entire system, making it a more critical and dangerous form of escalation.

Privilege escalation is a significant concern in cybersecurity because it can lead to unauthorized access, data breaches, and the ability to carry out malicious actions with elevated privileges. Organizations need to implement robust security measures, including access controls, regular patching, and monitoring, to detect and prevent privilege escalation attempts, both horizontal and vertical, in order to safeguard their systems and data. Failure to do so can result in serious security breaches and data loss.

Content

Horizontal Privilege Escalation

Open the OWASP Broken Web Application

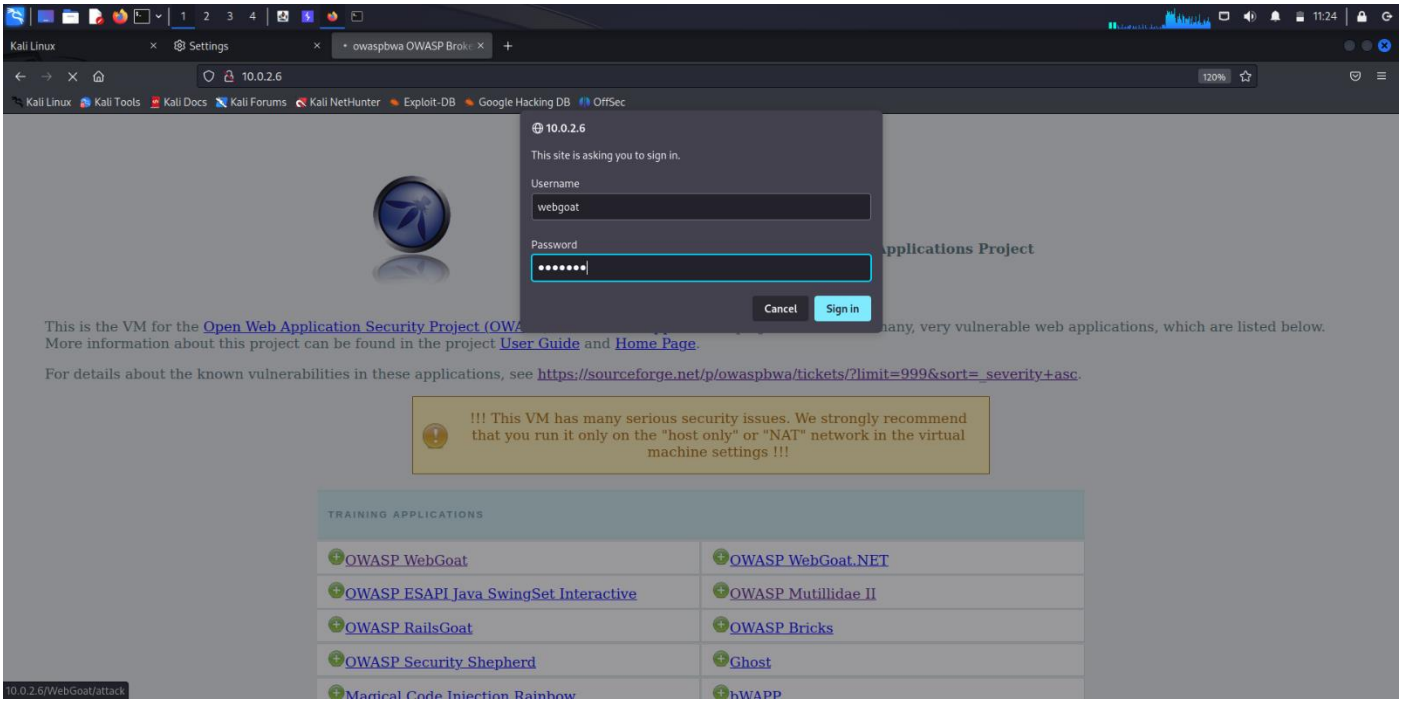


Open WebGoat web application

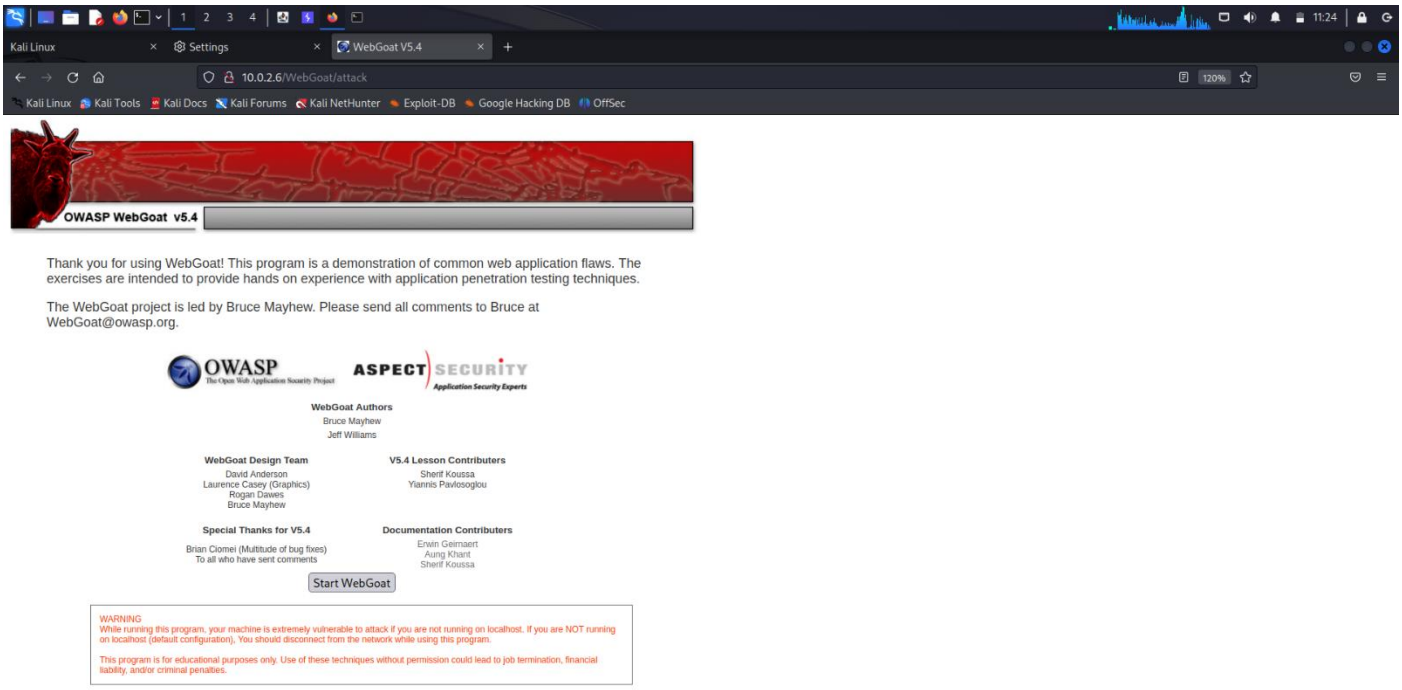
Signing in to OWASP WebGoat

Username: webgoat

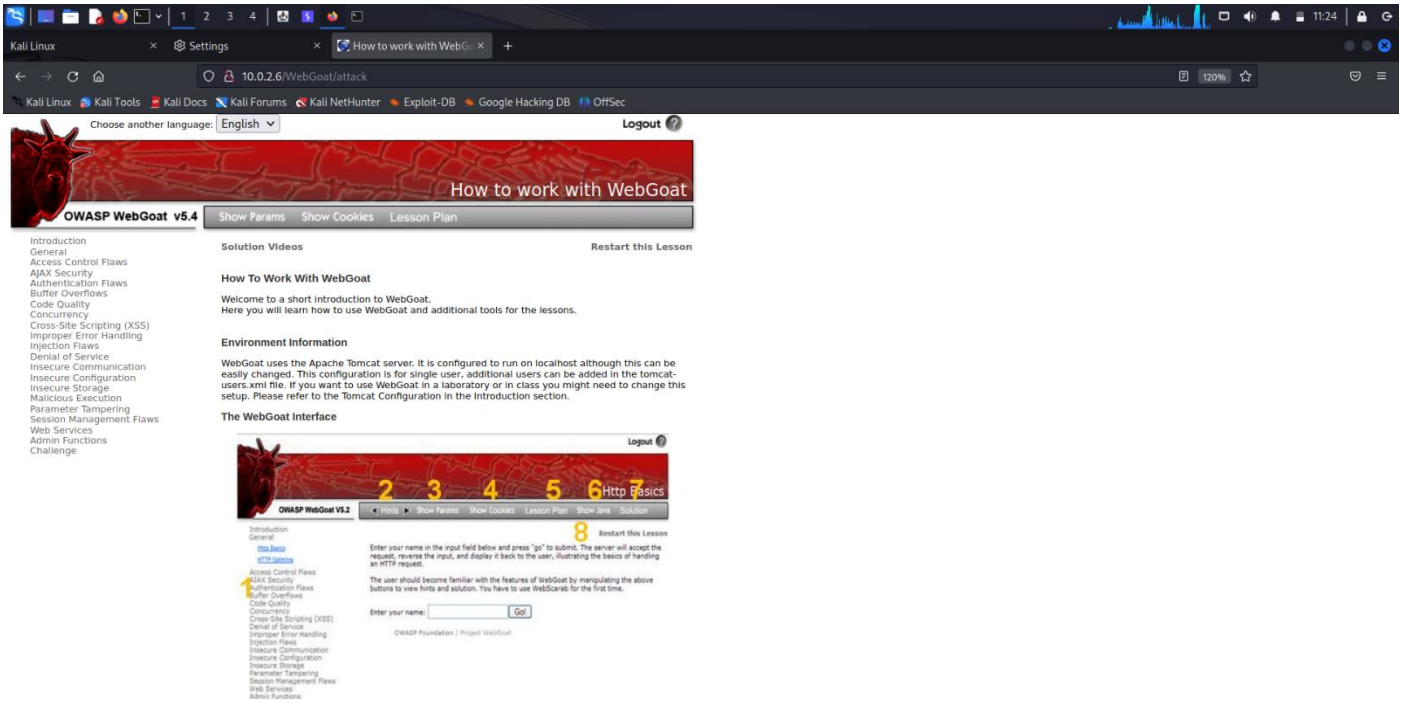
Password: webgoat



Starting WebGoat



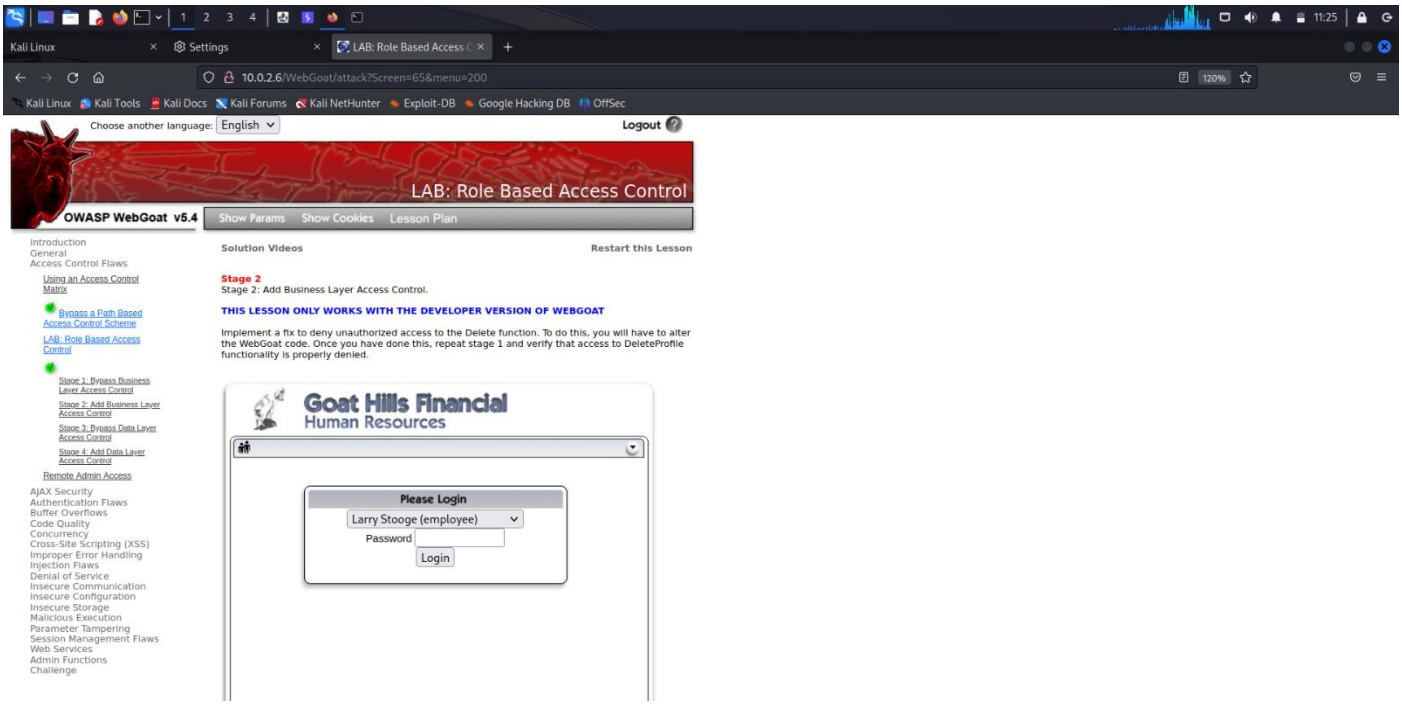
Home page of the WebGoat web application



Open Access Control Flaws

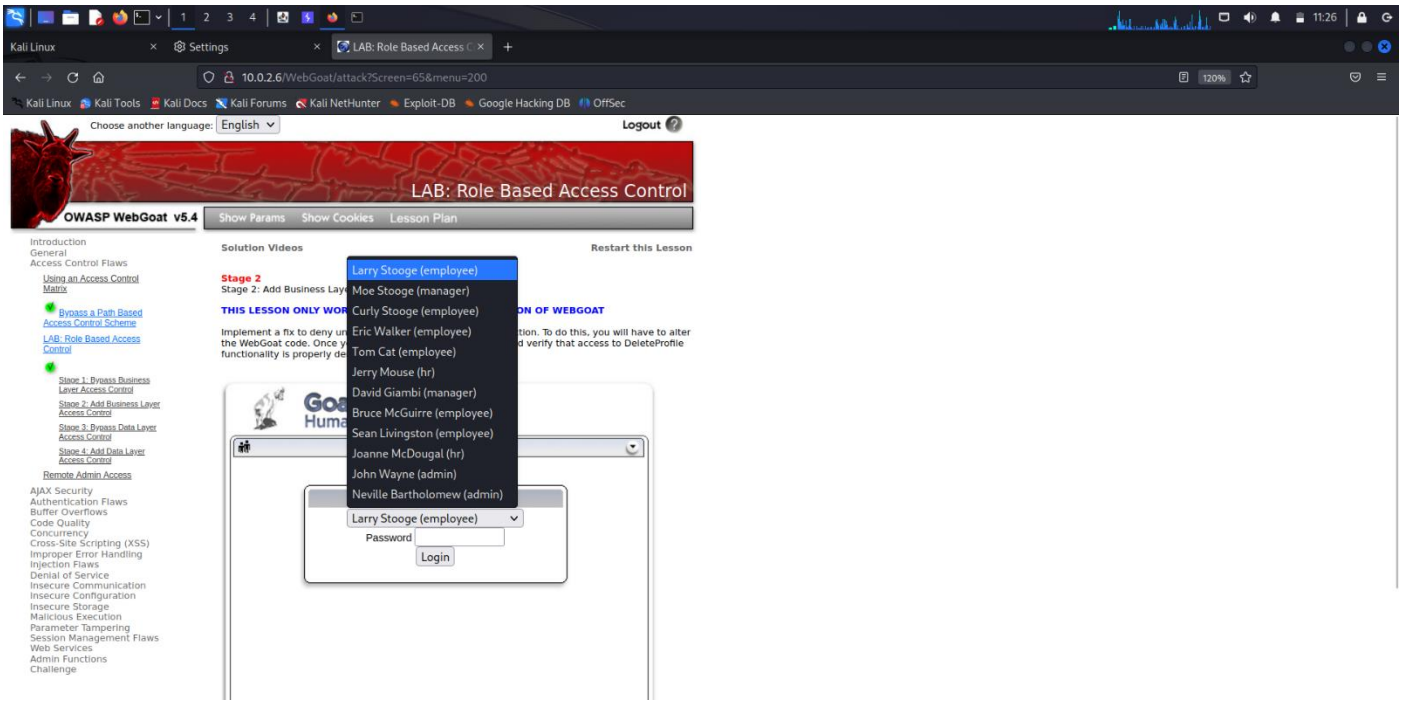
Click on LAB: Role Based Access Control

Human Resources department of Goat Hills Financial is shown. The login page for the employees is shown below.



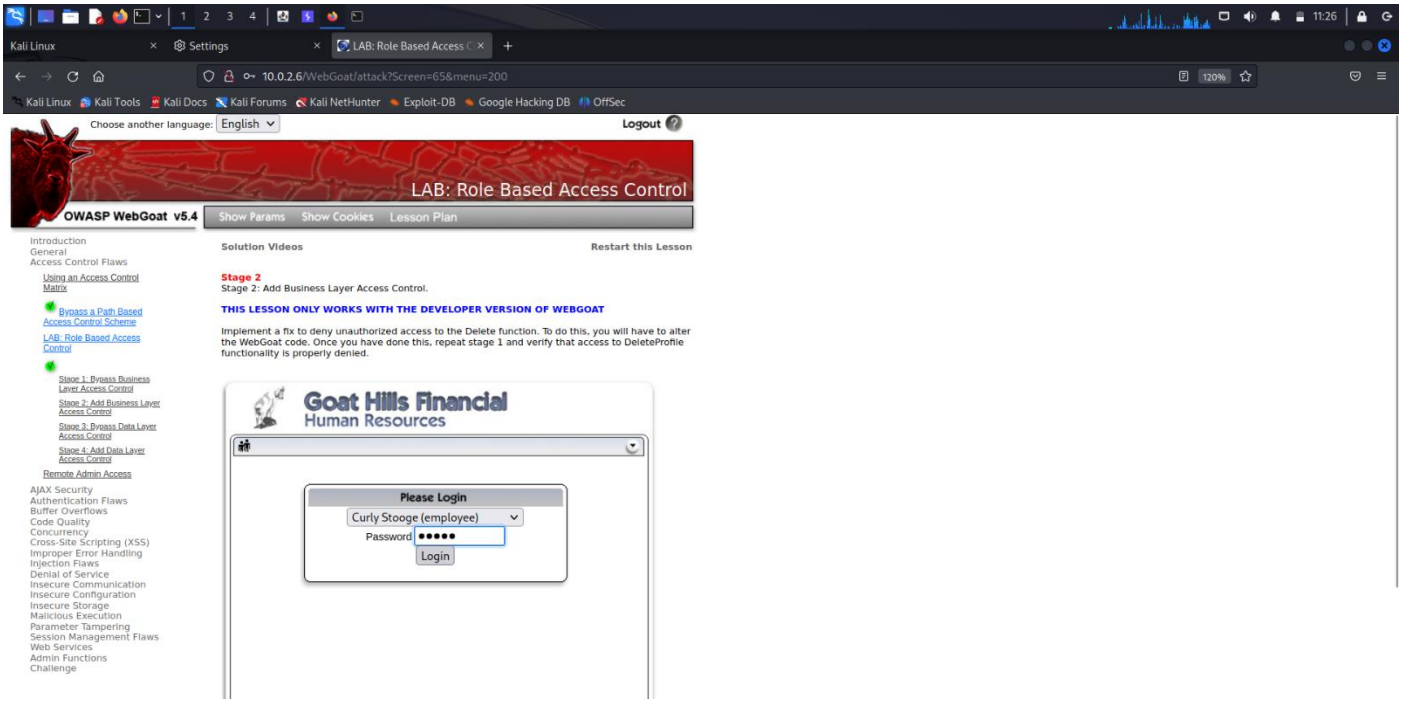
Description:

The drop-down list shows all the employees of the Goat Hills Financial corporation. Goat Hills Financial's Human Resources department contains employees with any one of employee/manager/hr/admin privilege. Consider yourself as the user Larry Stooge(employee). We are going to perform Horizontal Privilege Escalation on another employee, say Curly Stooge. Only we can Edit our Profile except admins. We perform ***Horizontal Privilege Escalation*** by editing another employee's(Curly Stooge's) Profile.



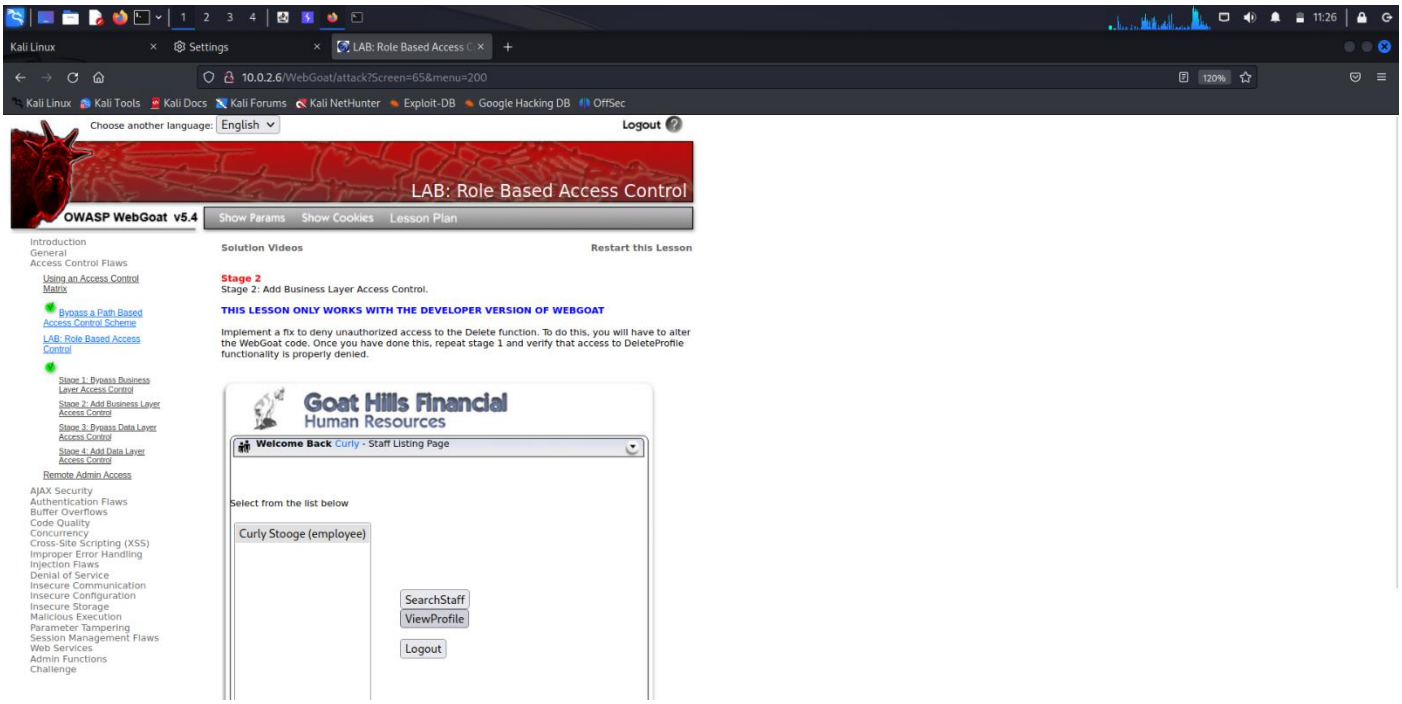
The victim Curly Stooge logs in using her credentials.

Password: curly



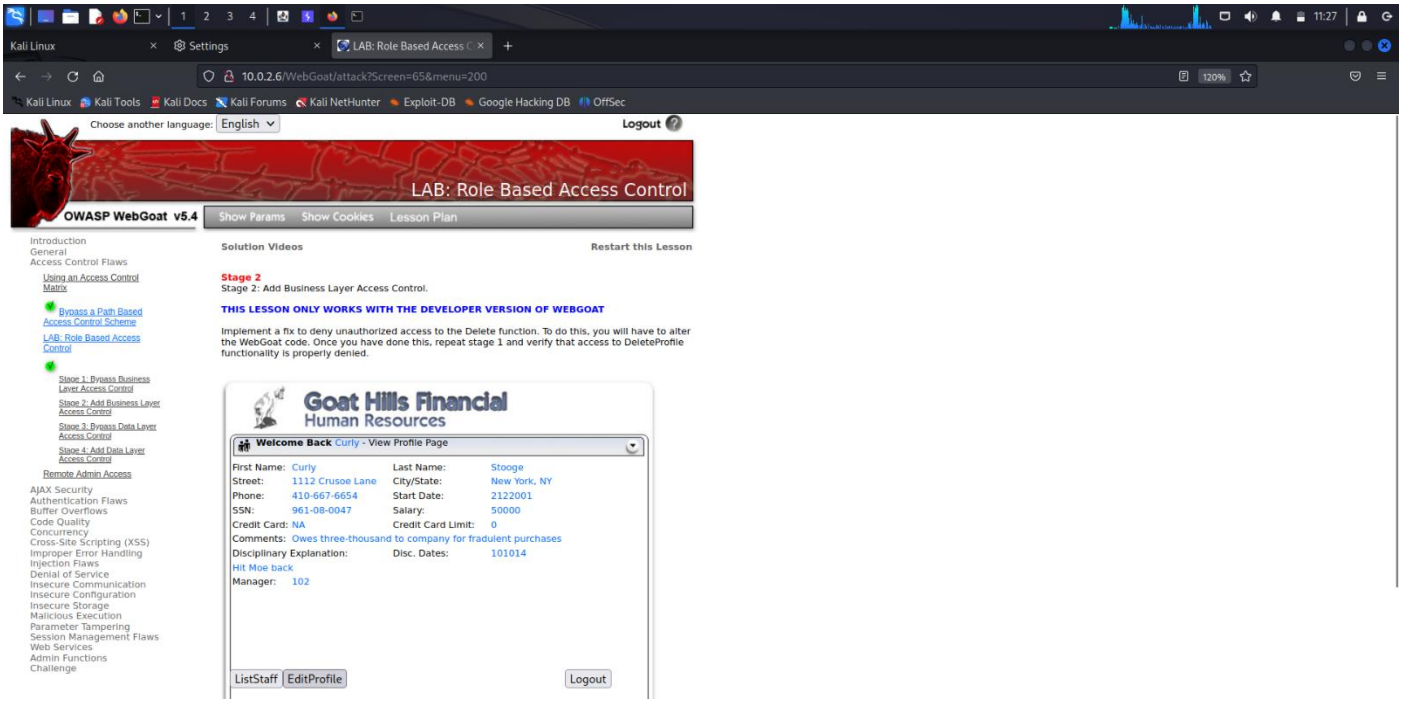
Curly wants to edit her profile.

Curly clicks on ViewProfile button.



Curly enters the View Profile Page.

She clicks on EditProfile button to edit her profile.

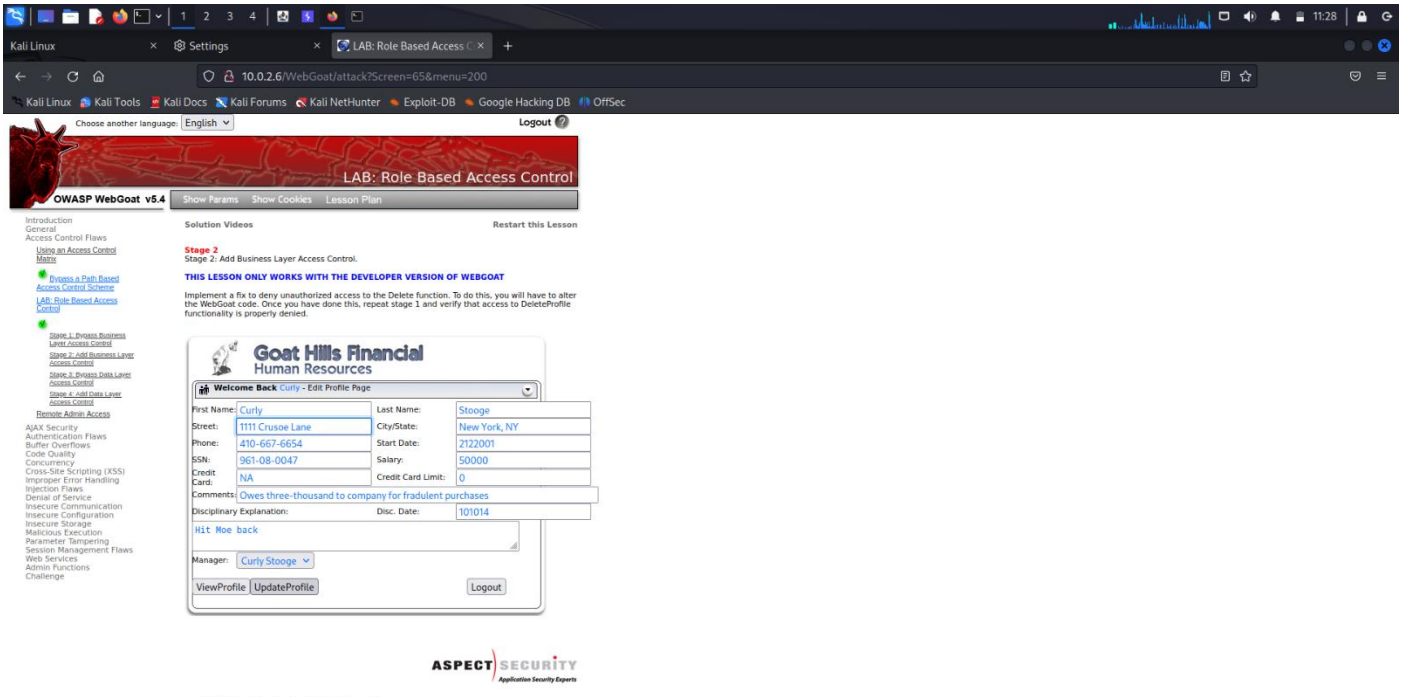


Curly makes changes to her profile in Edit Profile Page.

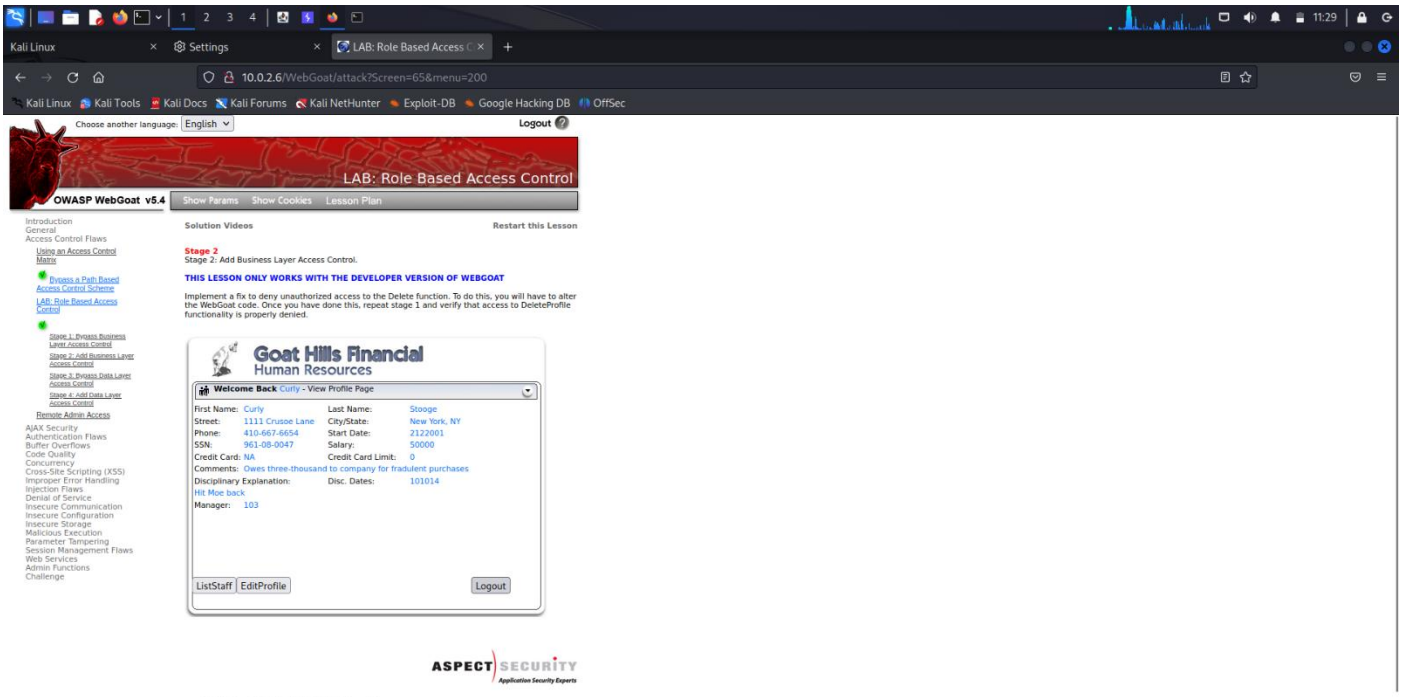
Before: Street: 1112 Crusoe Lane

After: Street: 1111 Crusoe Lane

She updates her profile by clicking UpdateProfile button.

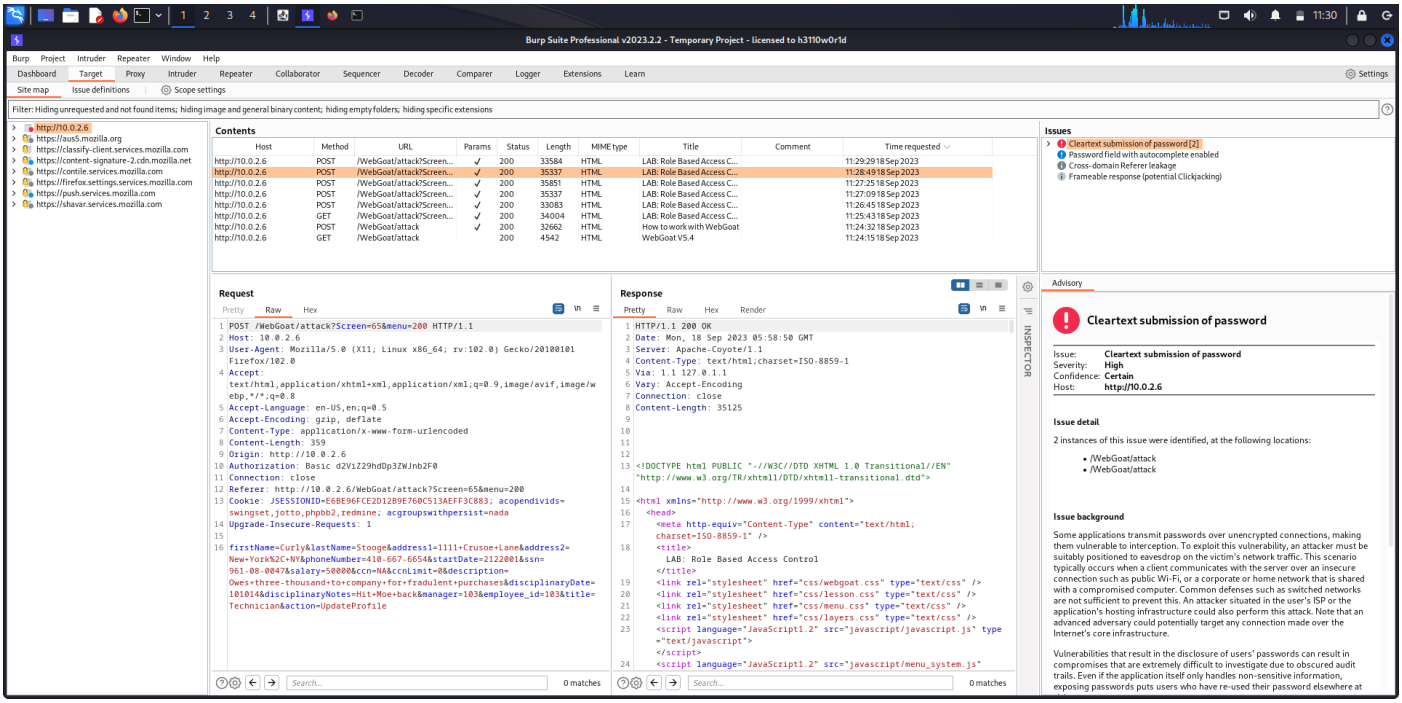


Curly logs out by clicking the Logout button.

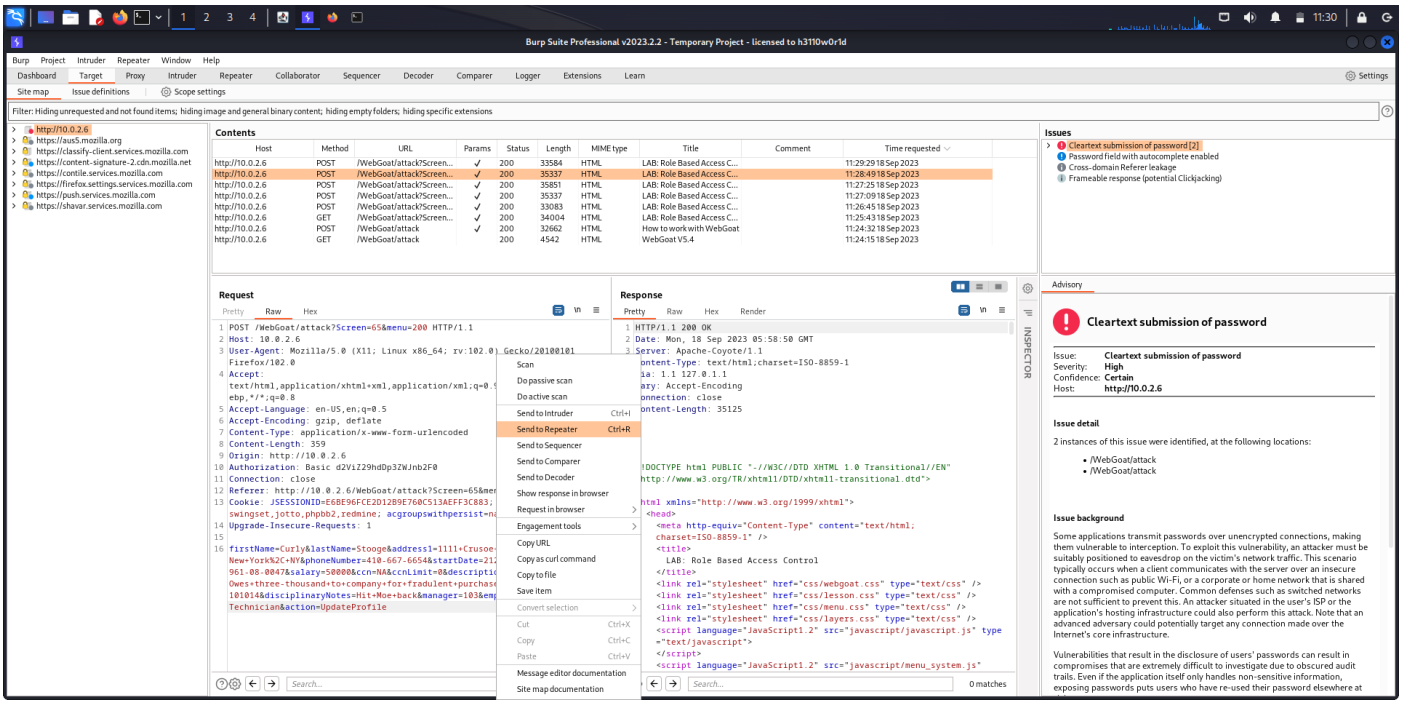


The action=UpdateProfile HTTP Request message is captured in the burpsuite.

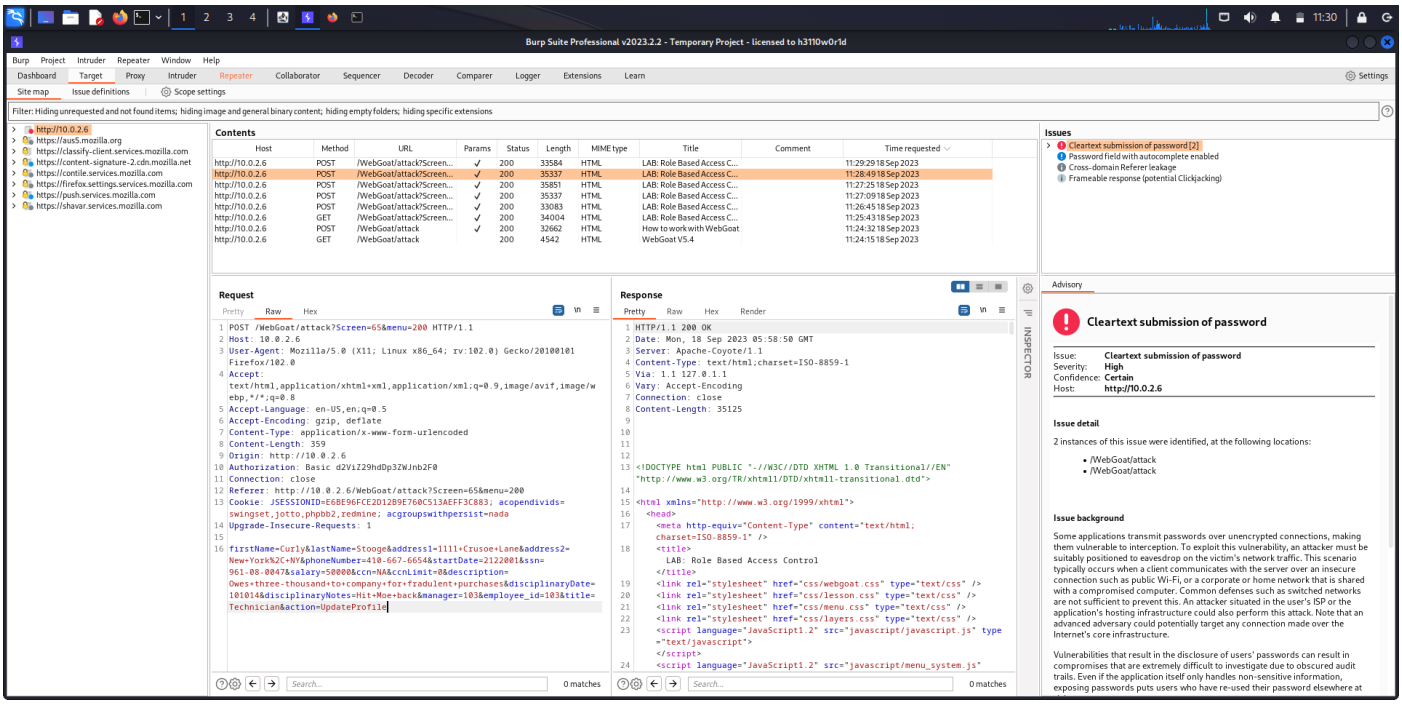
We can see the changes made by Curly in the HTTP Request message and the HTTP Response message sent by the server.



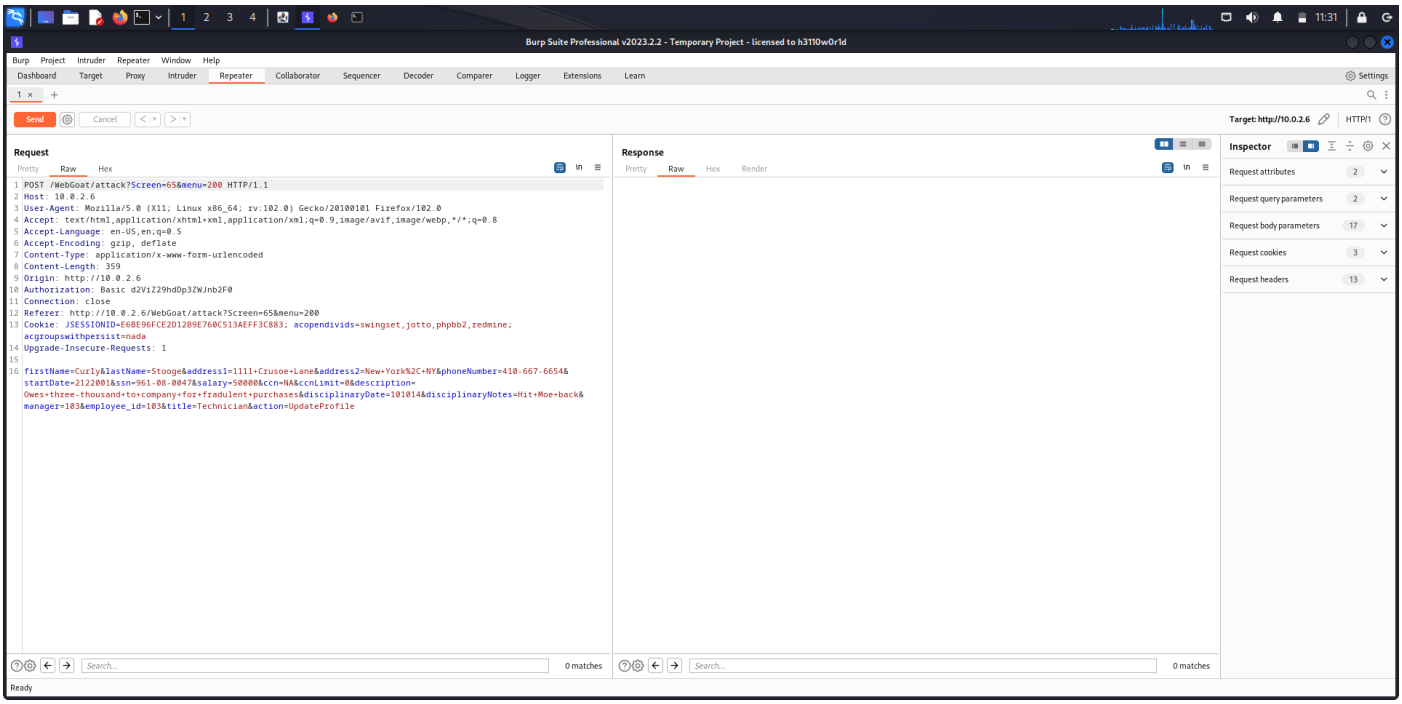
Right click on the HTTP Request message and click on Send to Repeater.



The HTTP Request message has been sent to the Repeater as it is indicated by highlighting the Repeater tab in red.

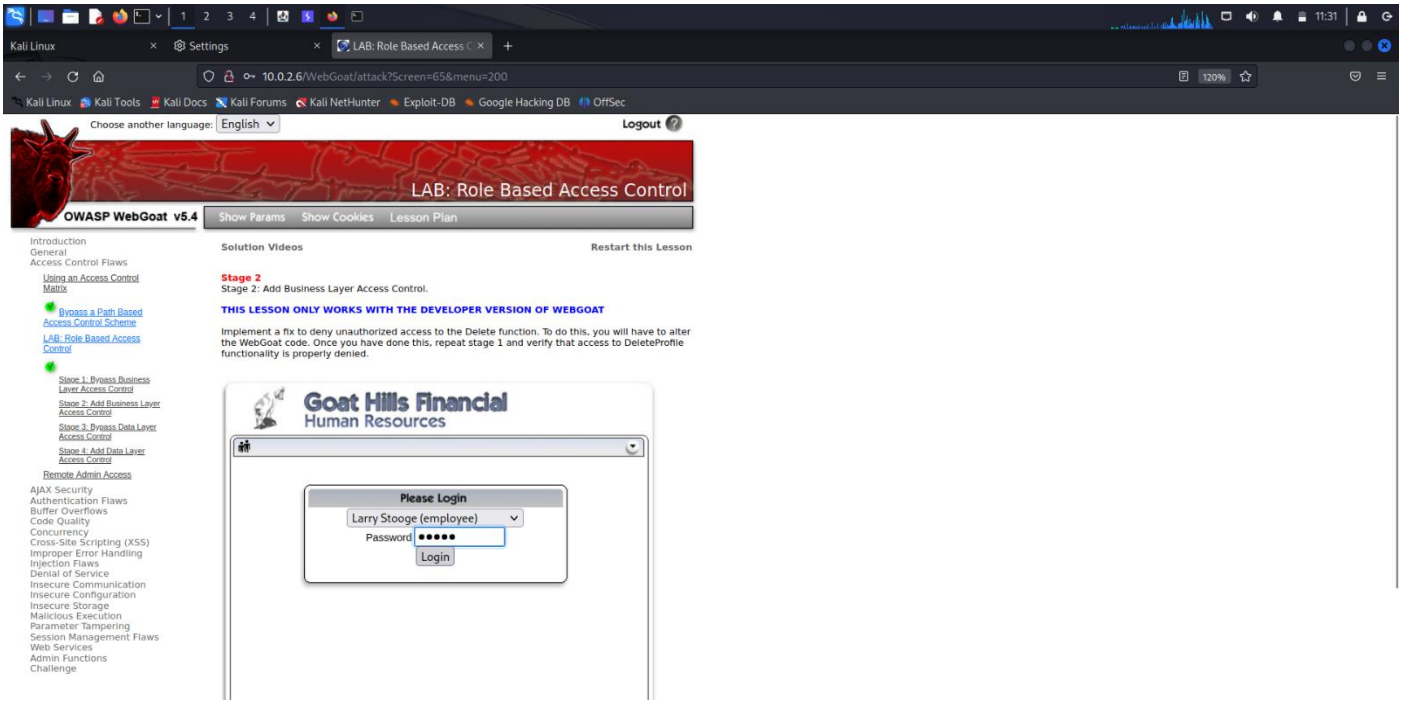


First payload has been received in the Repeater tab.

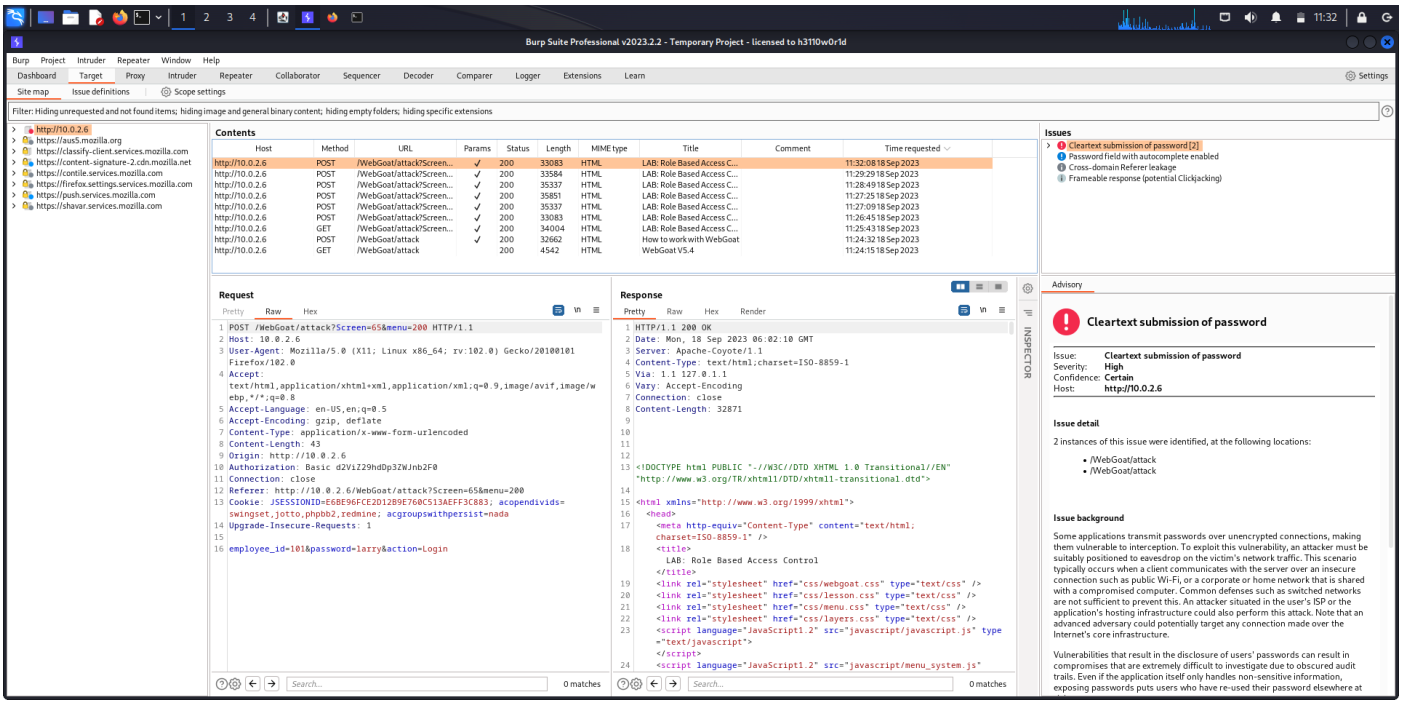


The attacker Larry logs into the Login Page using his credentials.

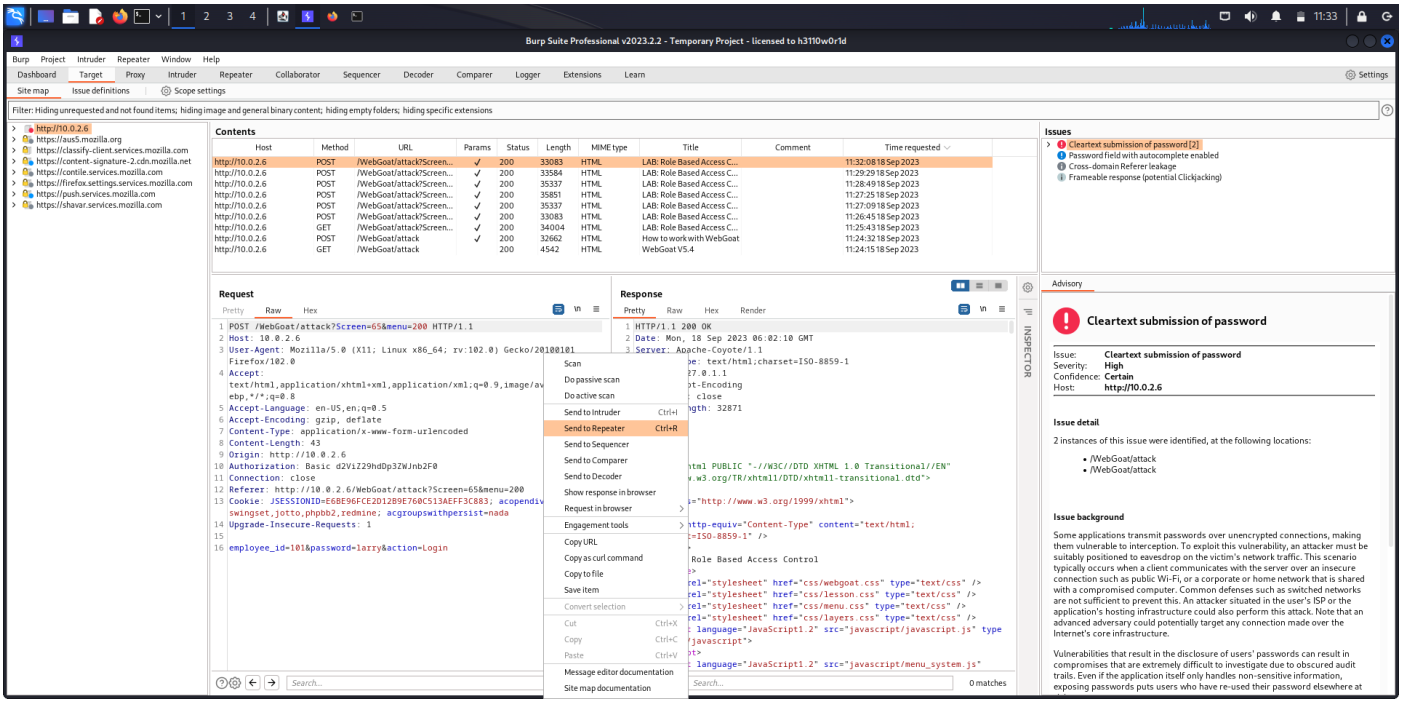
Password: larry



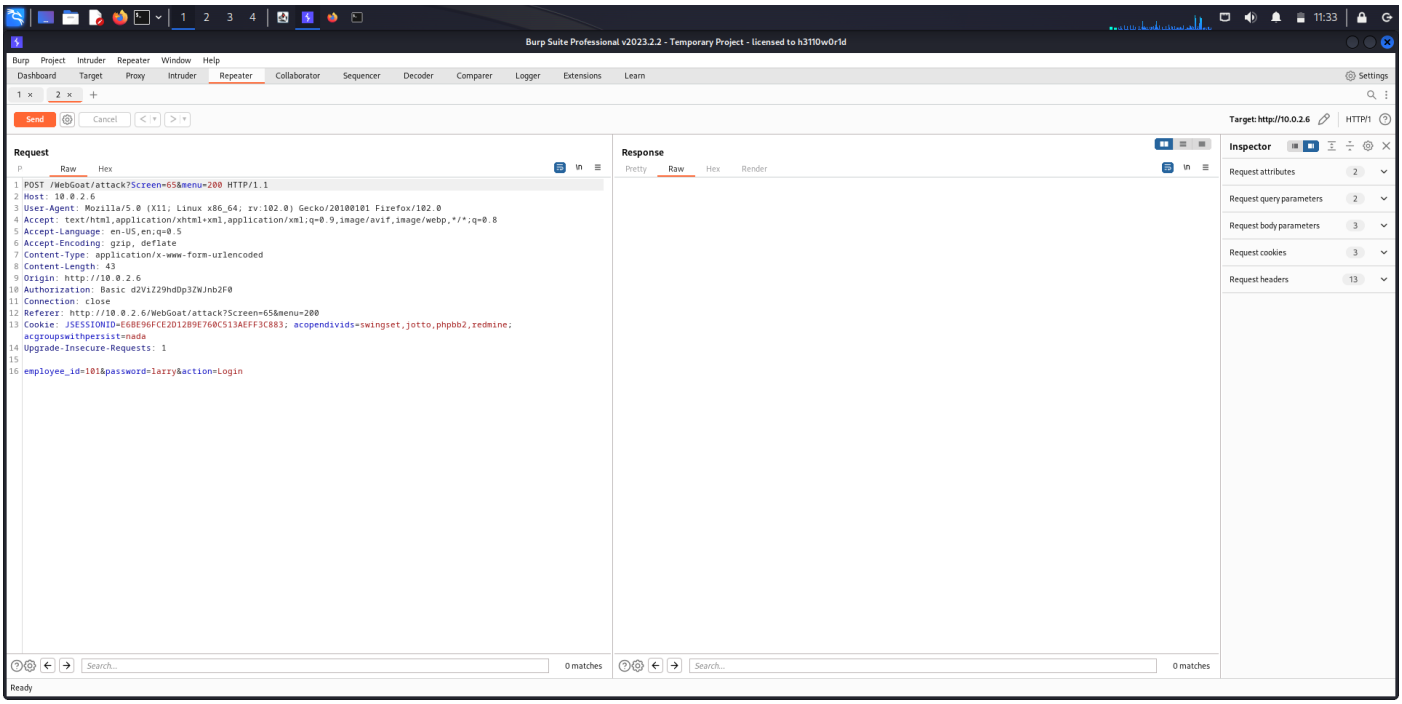
The action=Login HTTP Request message is captured in the burpsuite.



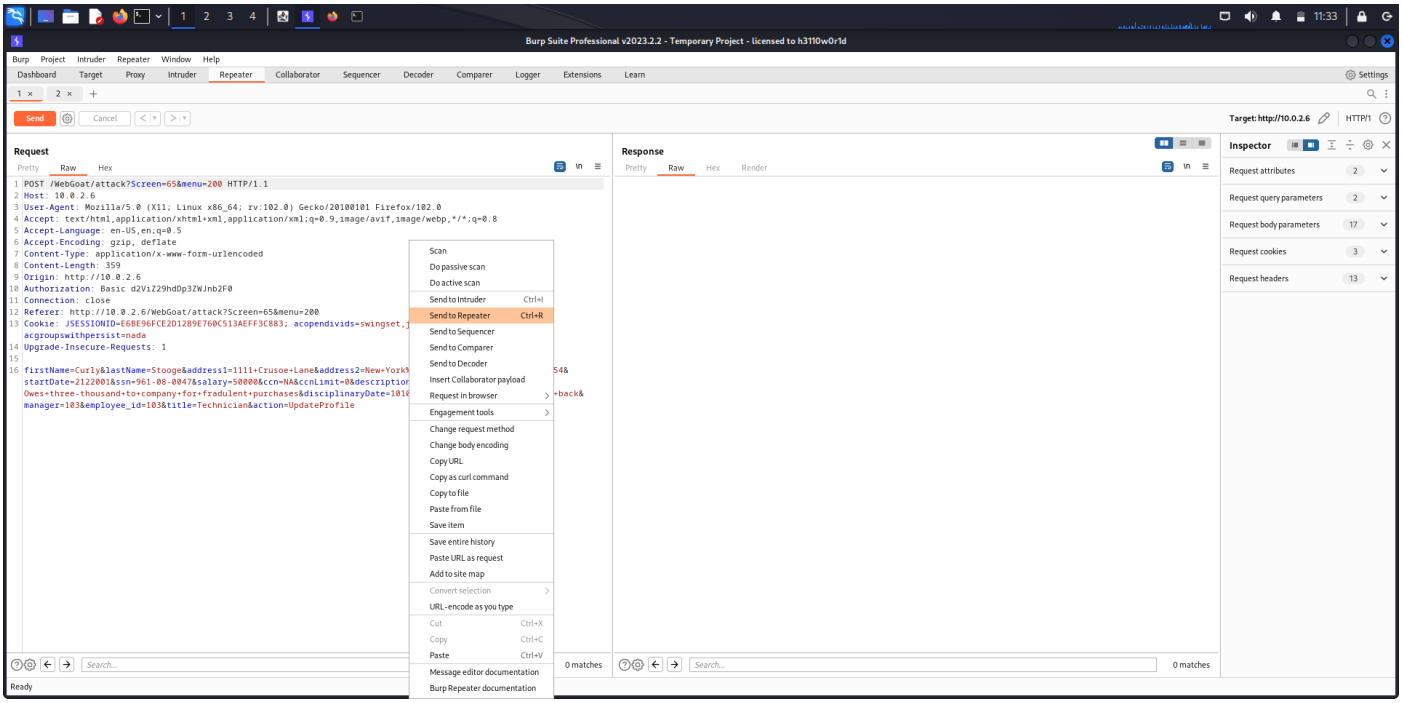
Right click on the HTTP Request message and click on Send to Repeater.



Second payload has been received in the Repeater tab.



Right click on the first payload and send it to Repeater again.

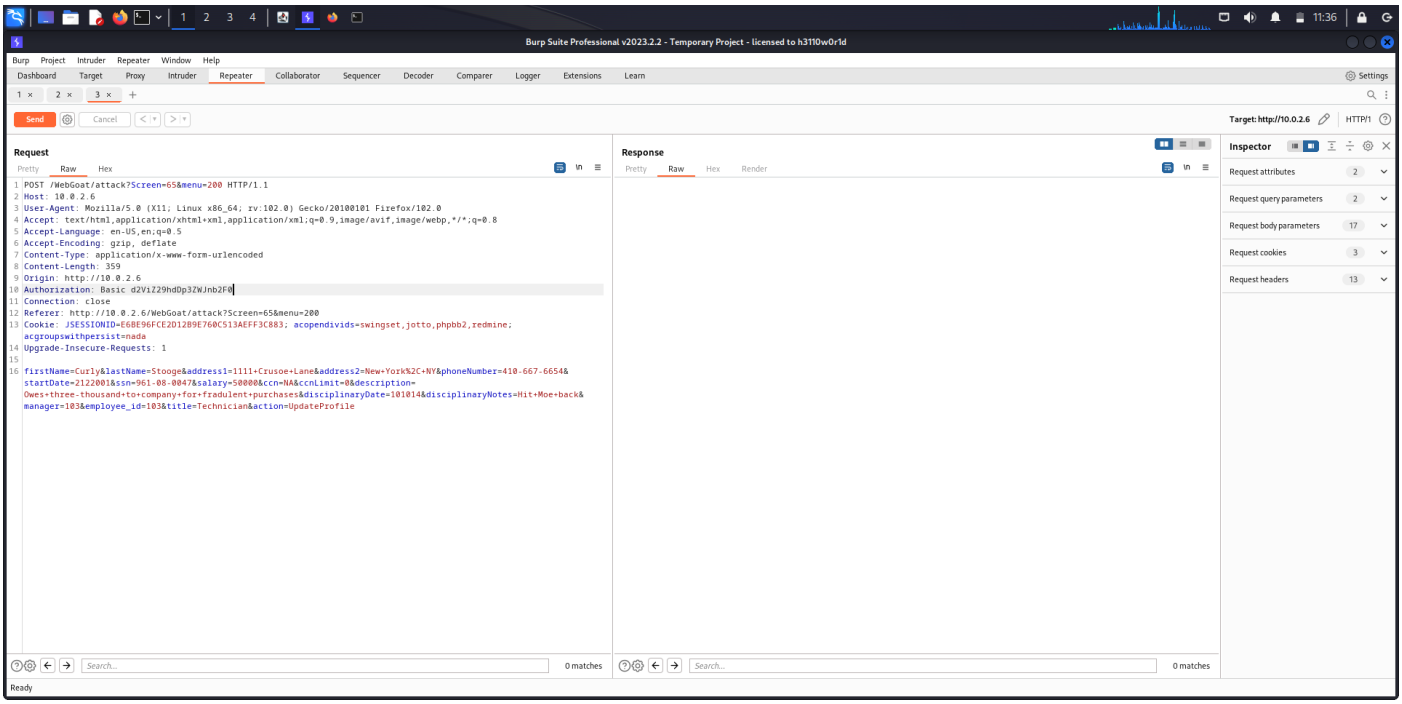


Copy the Authorization token and Cookie Session ID from second payload and paste it in the third payload.

Now, first payload contains Curly's UpdateProfile HTTP Request message

second payload contains Larry's Login HTTP Request message

third payload contains Curly's HTTP Request Message with Cookie and Authorization of Larry.



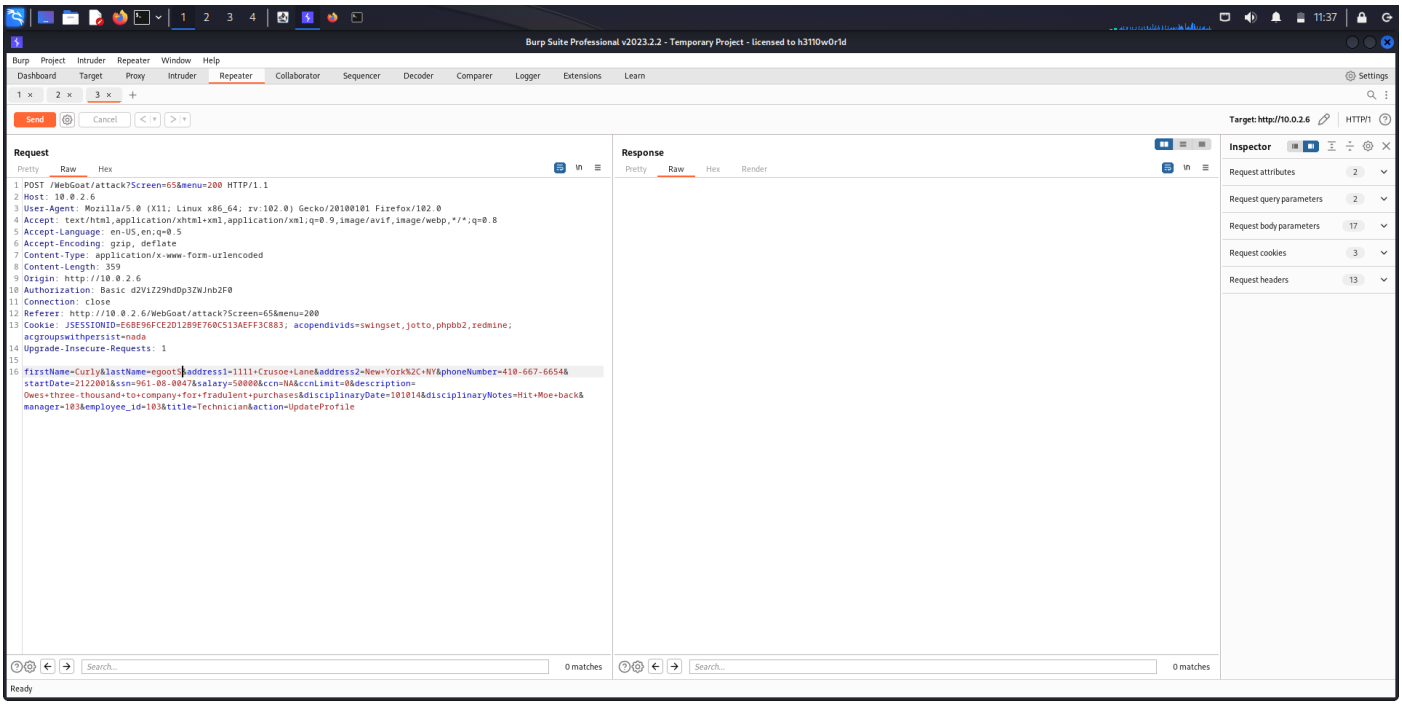
The attacker makes changes to Curly’s profile by editing the third payload.

In this case, the attacker changes the Last Name of Curly’s profile.

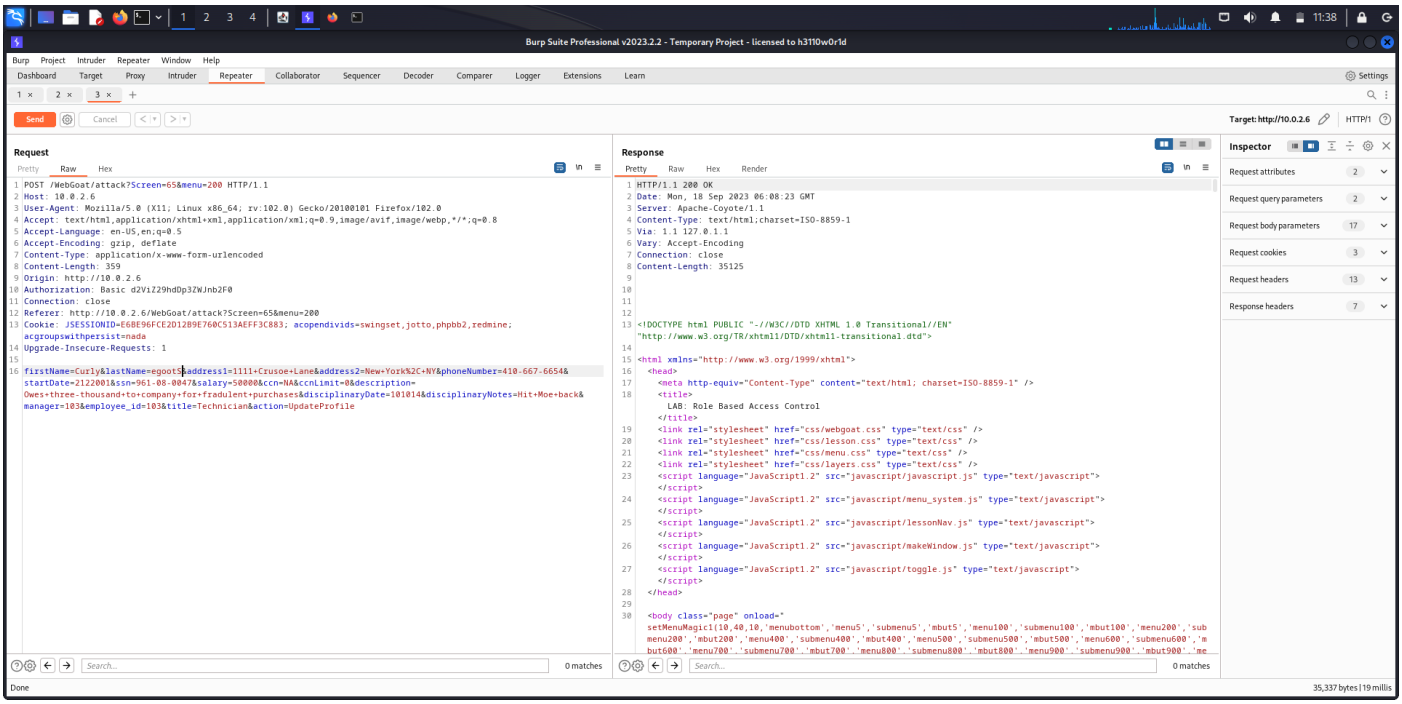
Before: lastName=Stooge

After: lastName=egootS

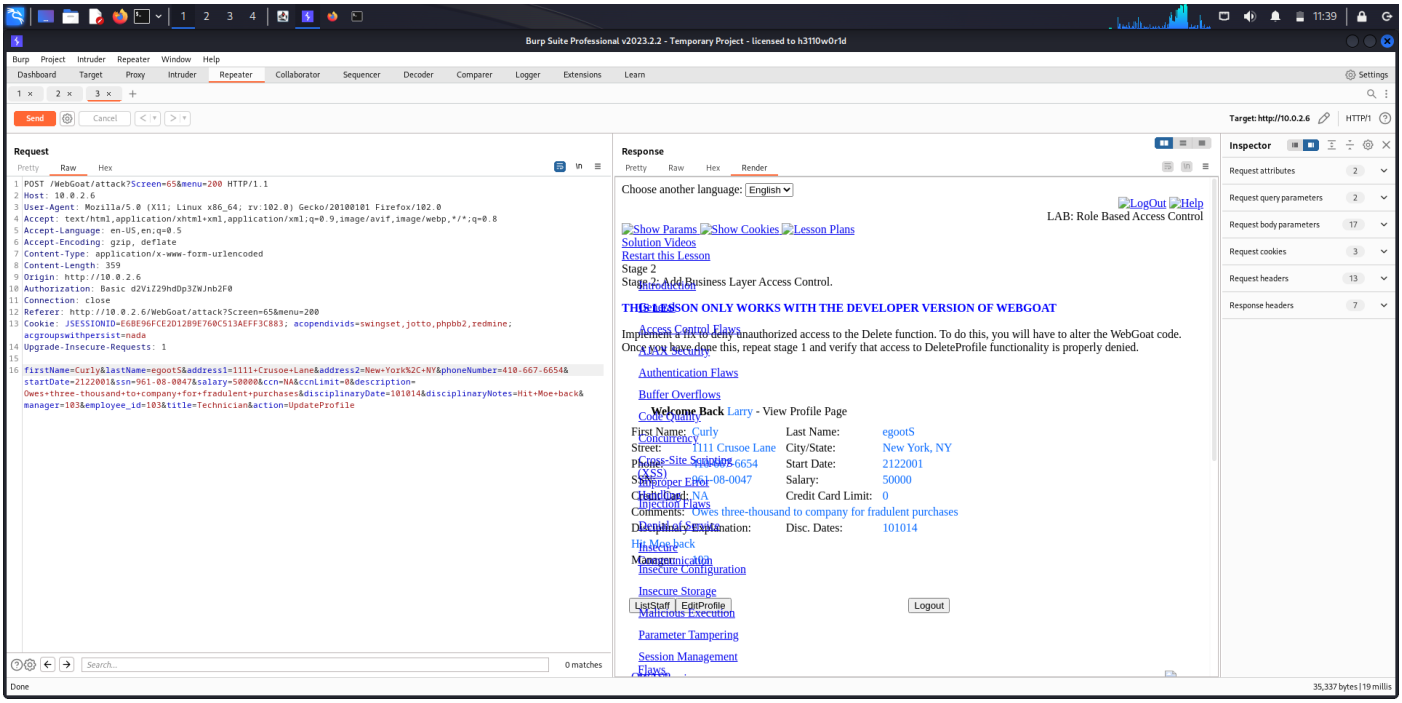
Send the HTTP Request message by clicking on the Send button on the top-left corner.



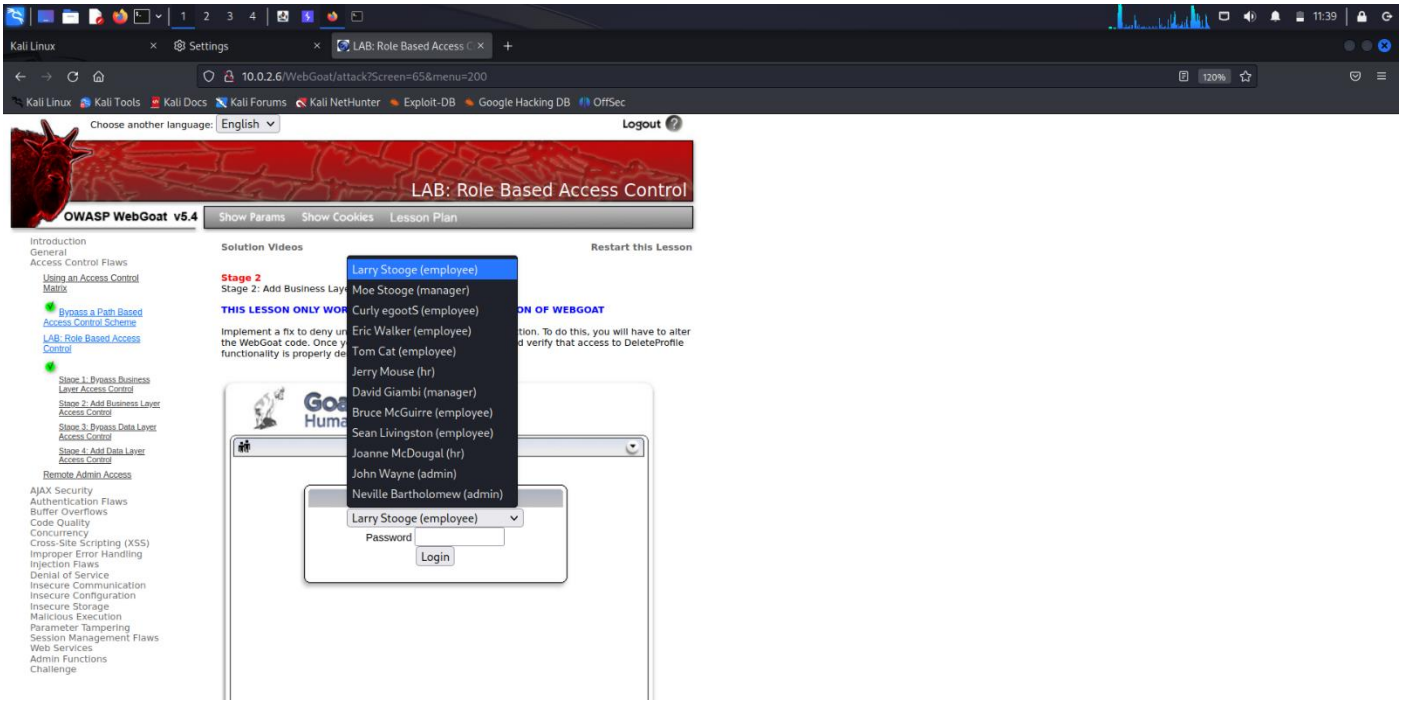
After sending the HTTP Request message, a HTTP Response message is received from the server.



By clicking on Render, we can roughly see the Response page.



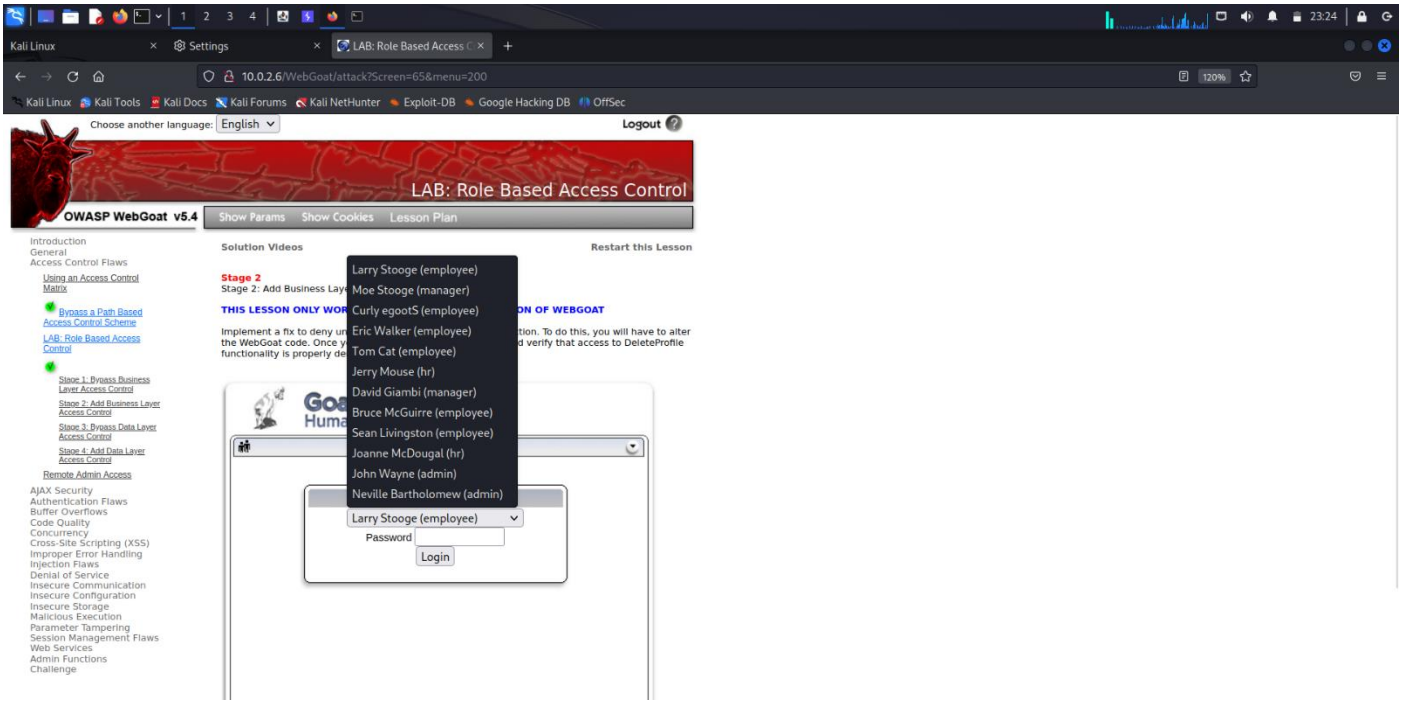
In the login page, we can see that the last name of Curly has been changed from Stooge to egootS which was not made by her.



Vertical Privilege Escalation

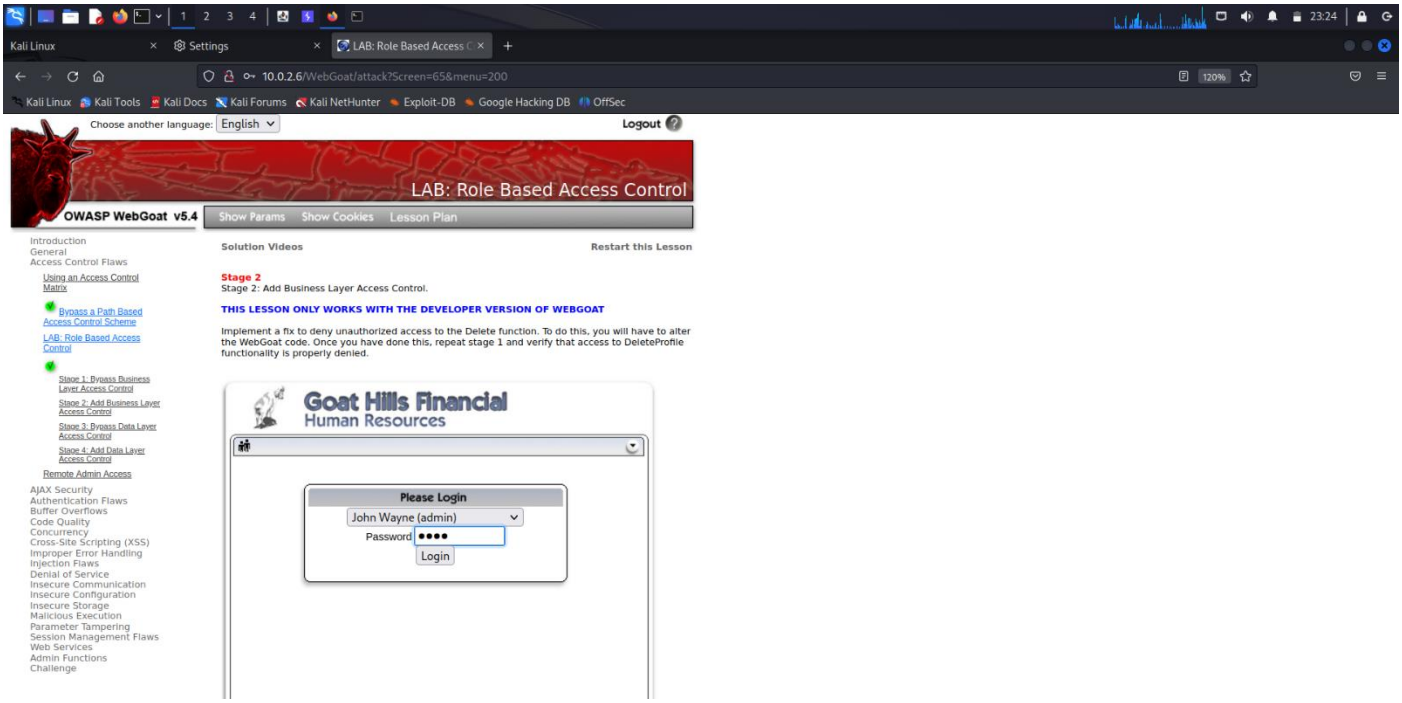
Description:

The drop-down list shows all the employees of the Goat Hills Financial corporation. Goat Hills Financial's Human Resources department contains employees with any one of employee/manager/hr/admin privilege. Consider yourself as the user Larry Stooge (employee). We are going to perform ***Vertical Privilege Escalation***. Here, there are two victims of privilege escalation. We delete an employee (Curly Stooge) from the database even though only admins are permissible to delete a Profile. Consider John Wayne is the admin.

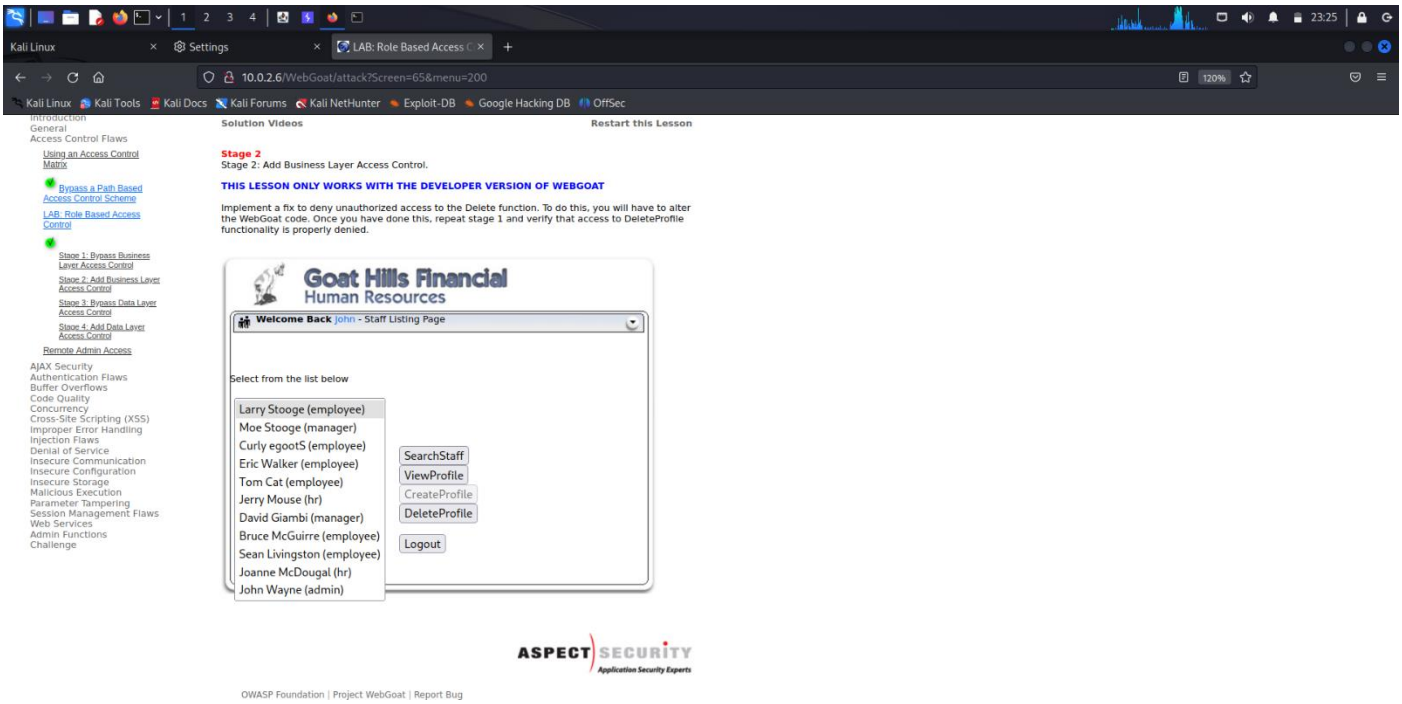


Admin John Wayne logs into his profile using his credentials.

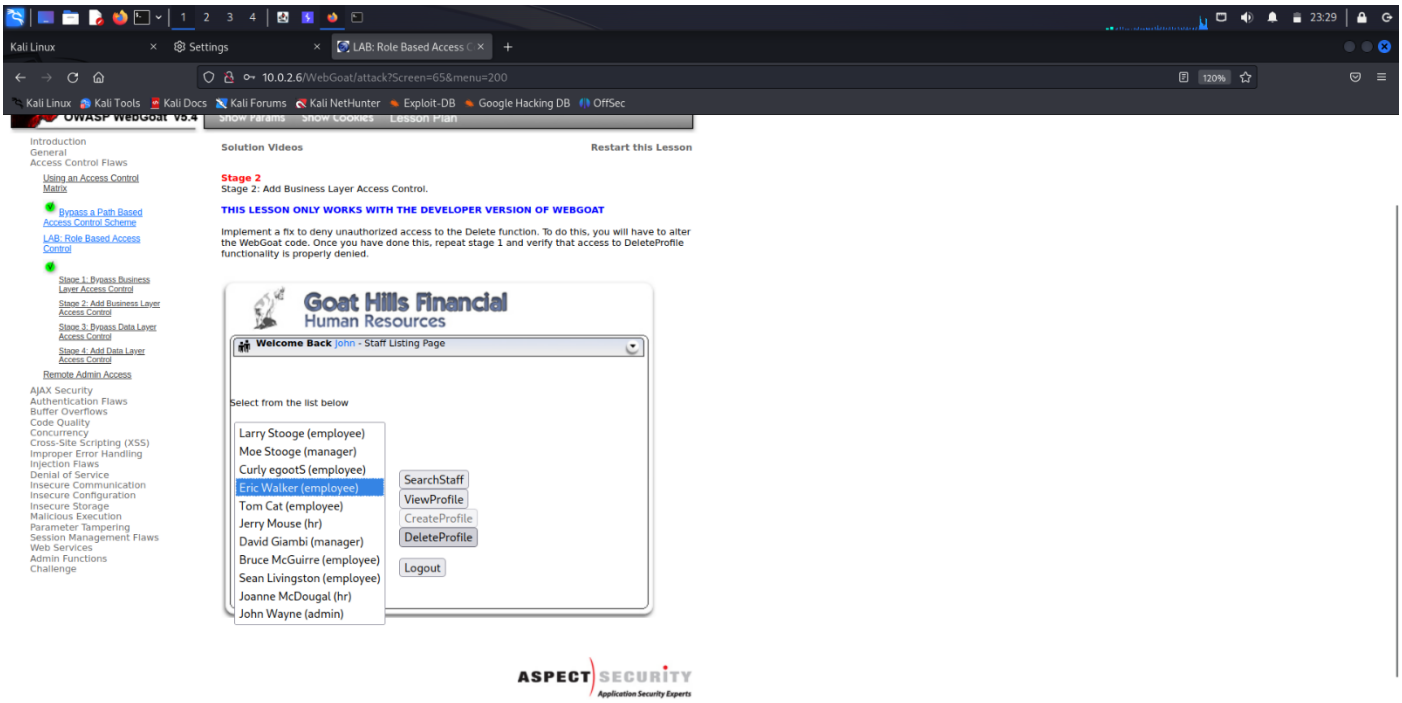
Password: john



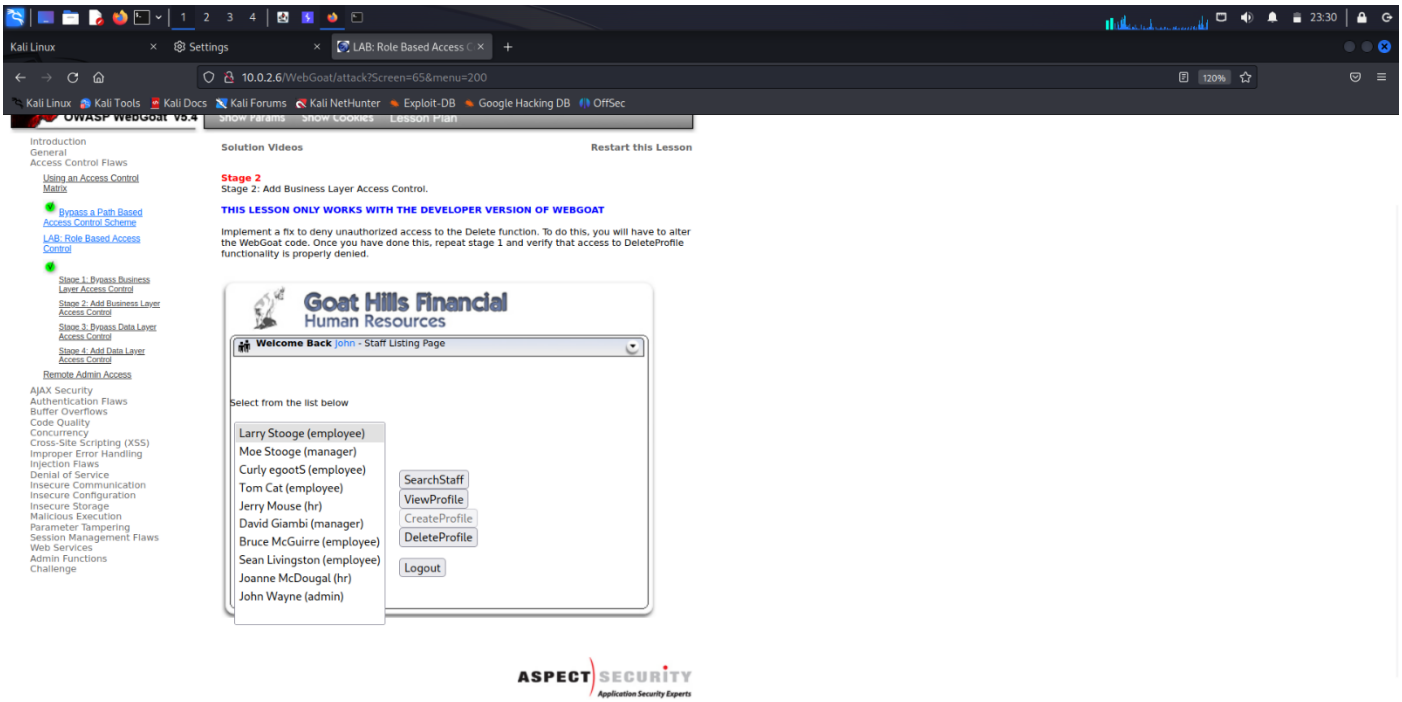
The admin has the privileges to view and delete profiles of all the users.



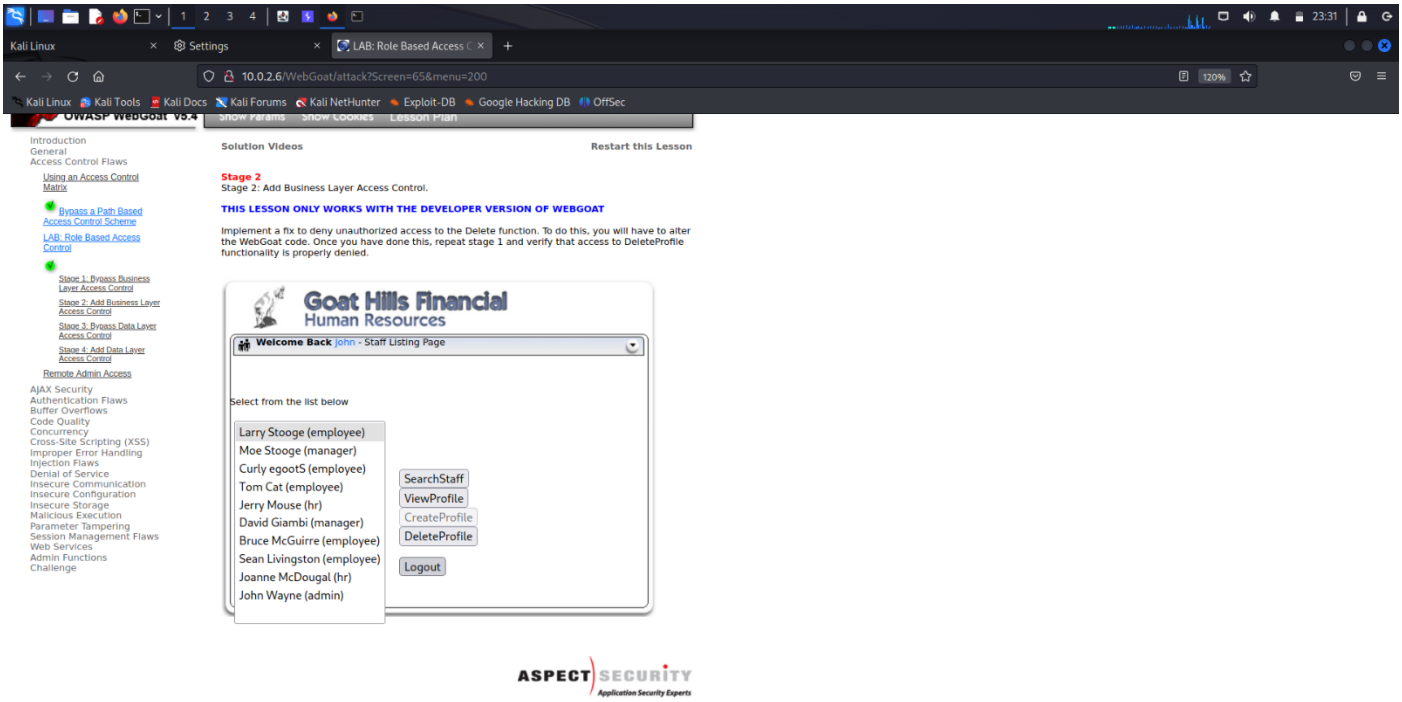
The admin wants to delete the employee Eric Walker. Select Eric Walker from the list and click on DeleteProfile button.



The employee Eric Walker has been deleted from the Goat Hills Financial Human Resources department.

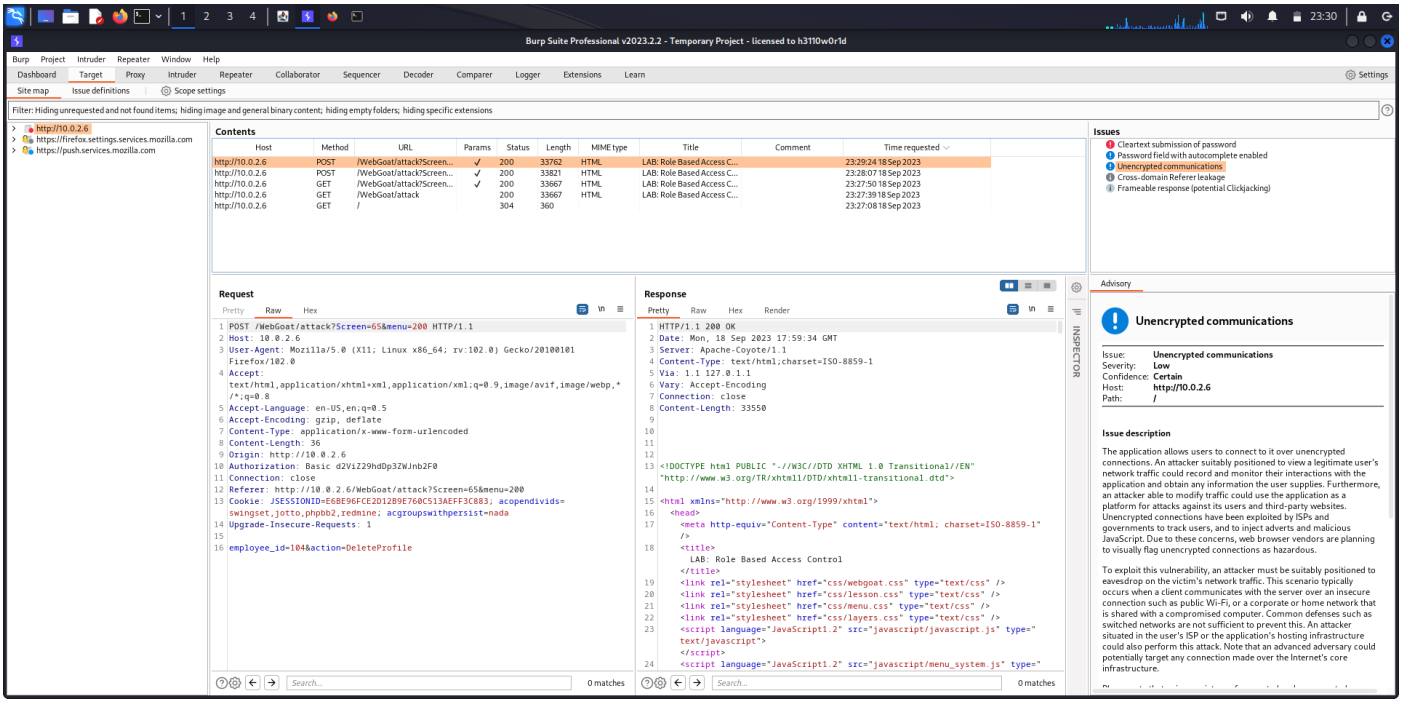


The admin logs out of the account.

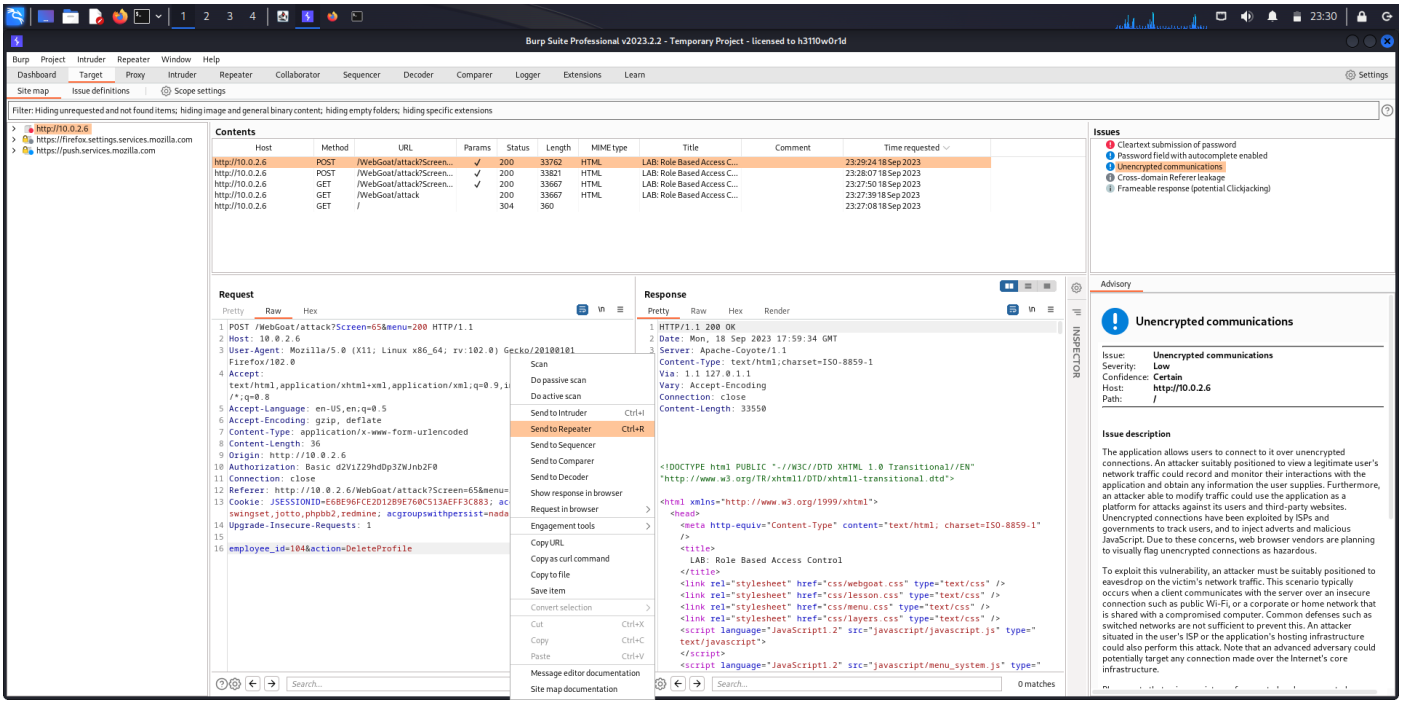


The action=DeleteProfile HTTP Request message is captured in the burpsuite.

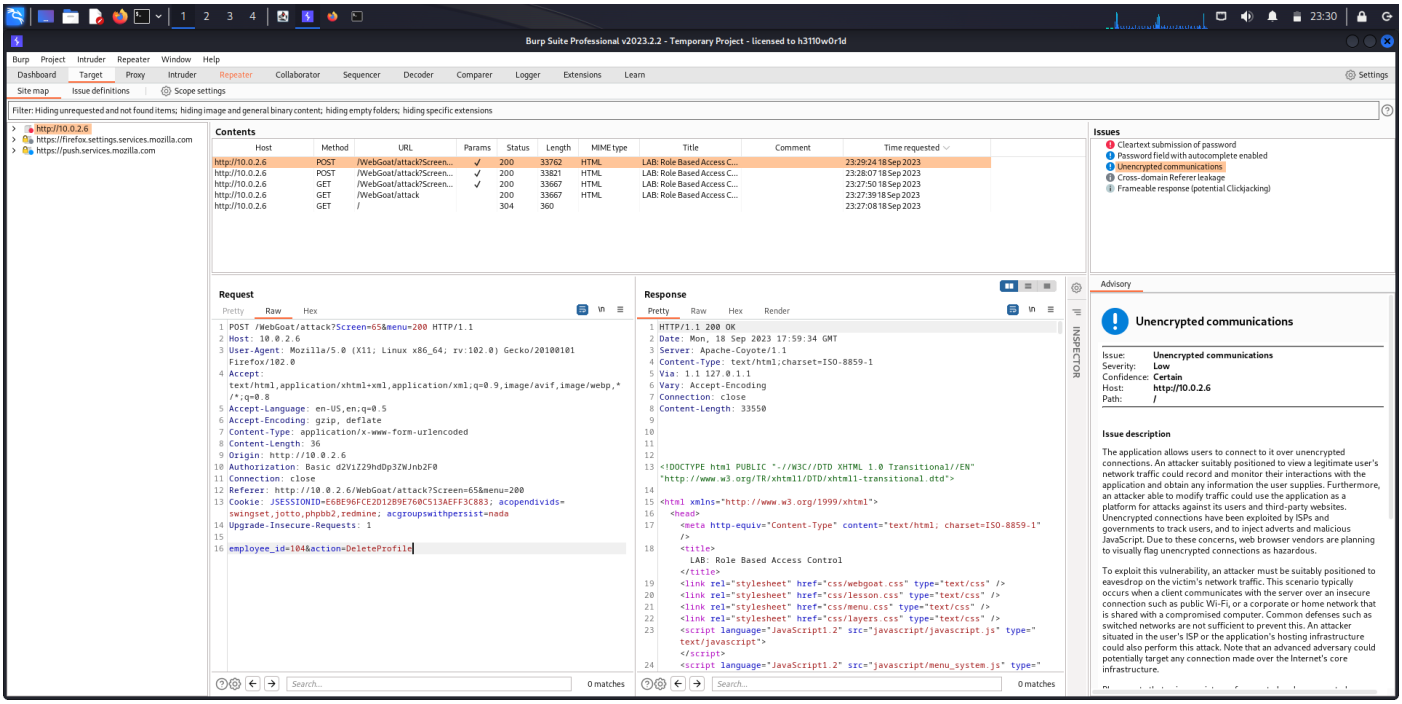
Eric Walker had the Employee-ID 104.



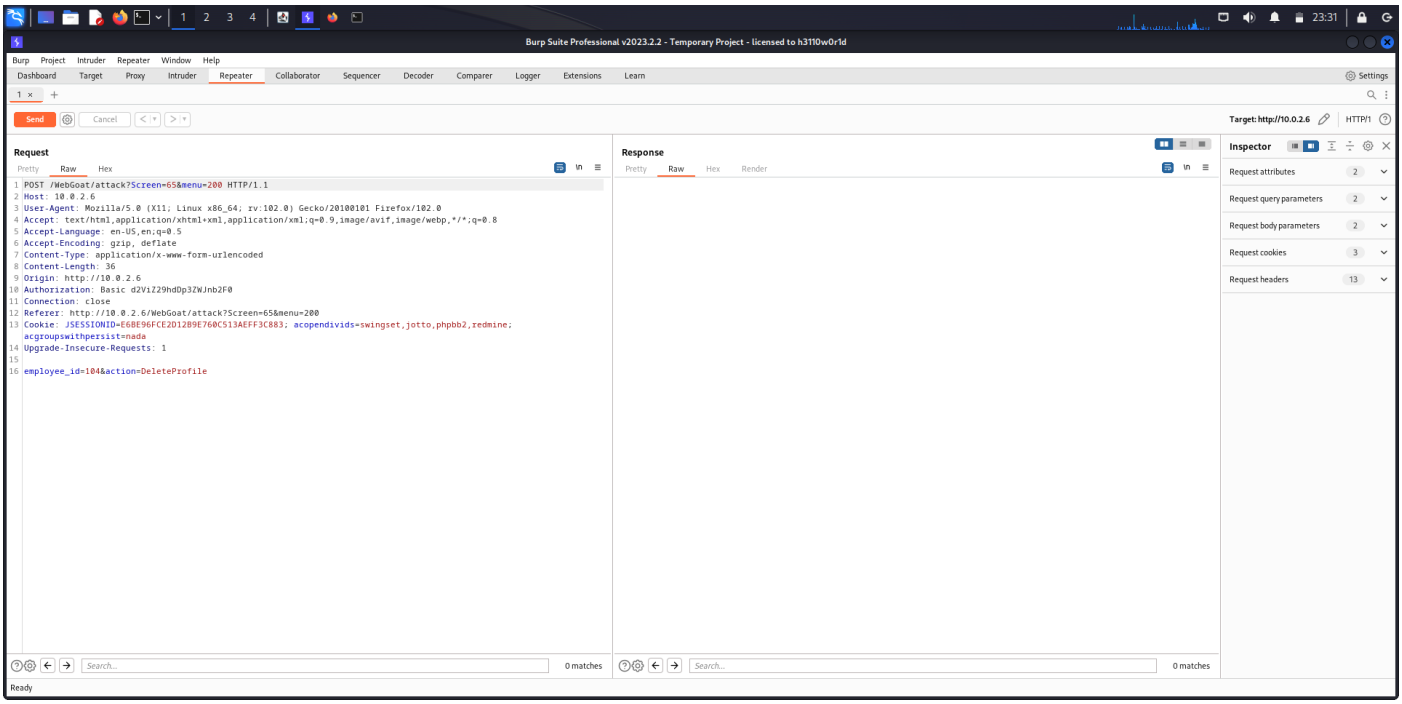
Right click on the HTTP Request message and click on Send to Repeater.



The HTTP Request message has been sent to the Repeater as it is indicated by highlighting the Repeater tab in red.

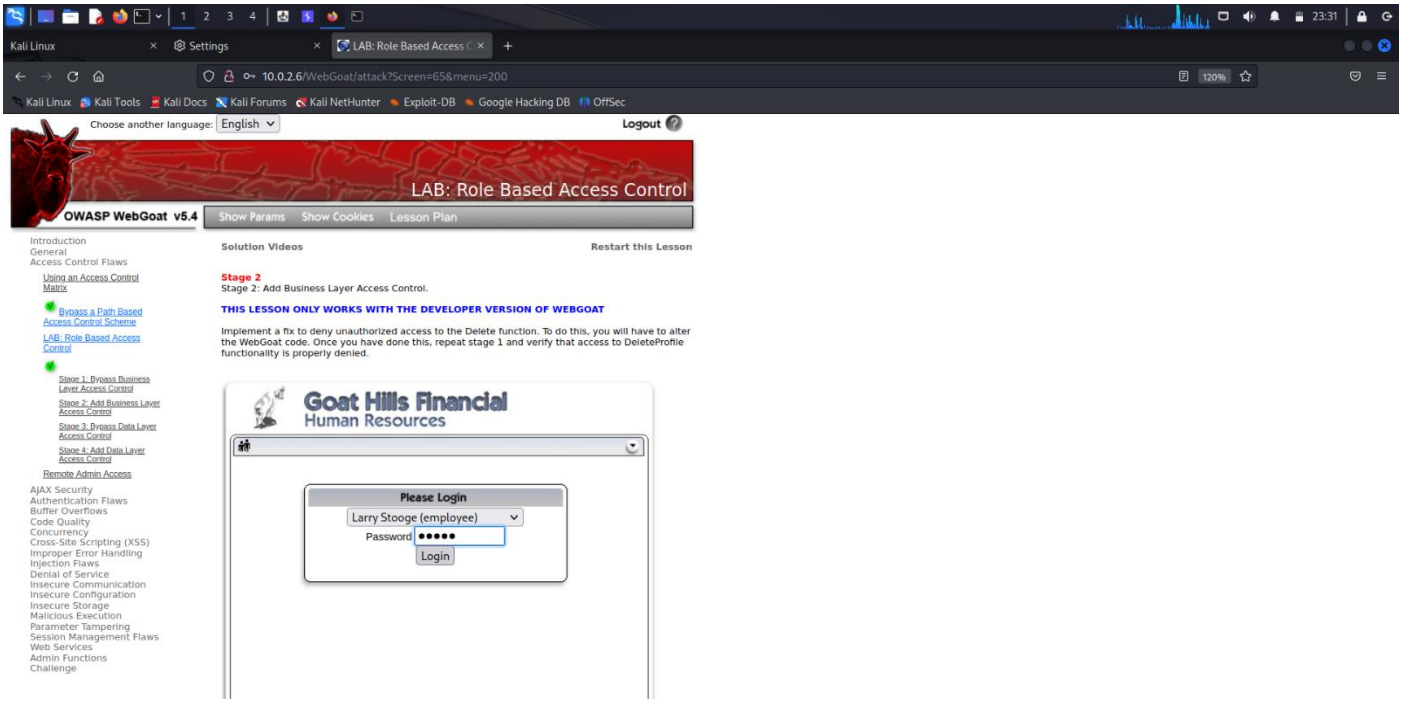


First payload has been received in the Repeater tab.

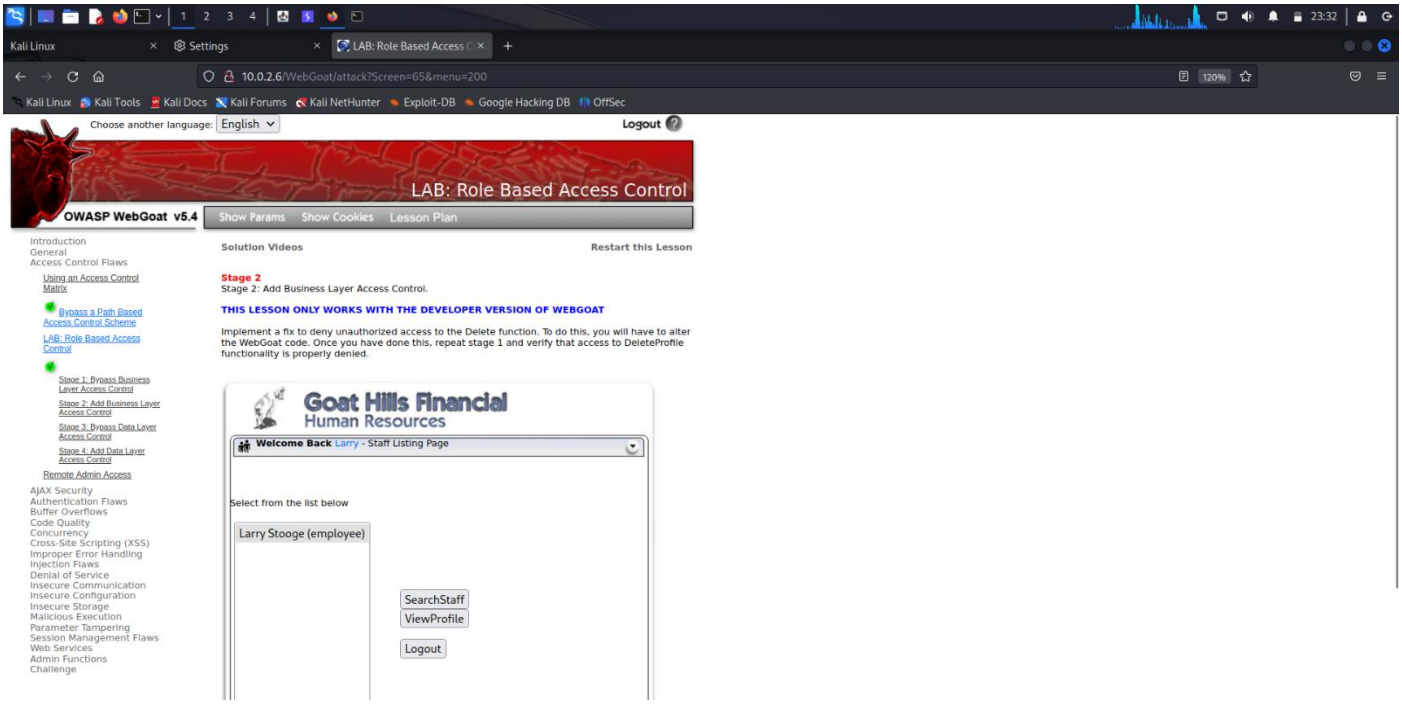


The attacker Larry logs into the Login Page using his credentials.

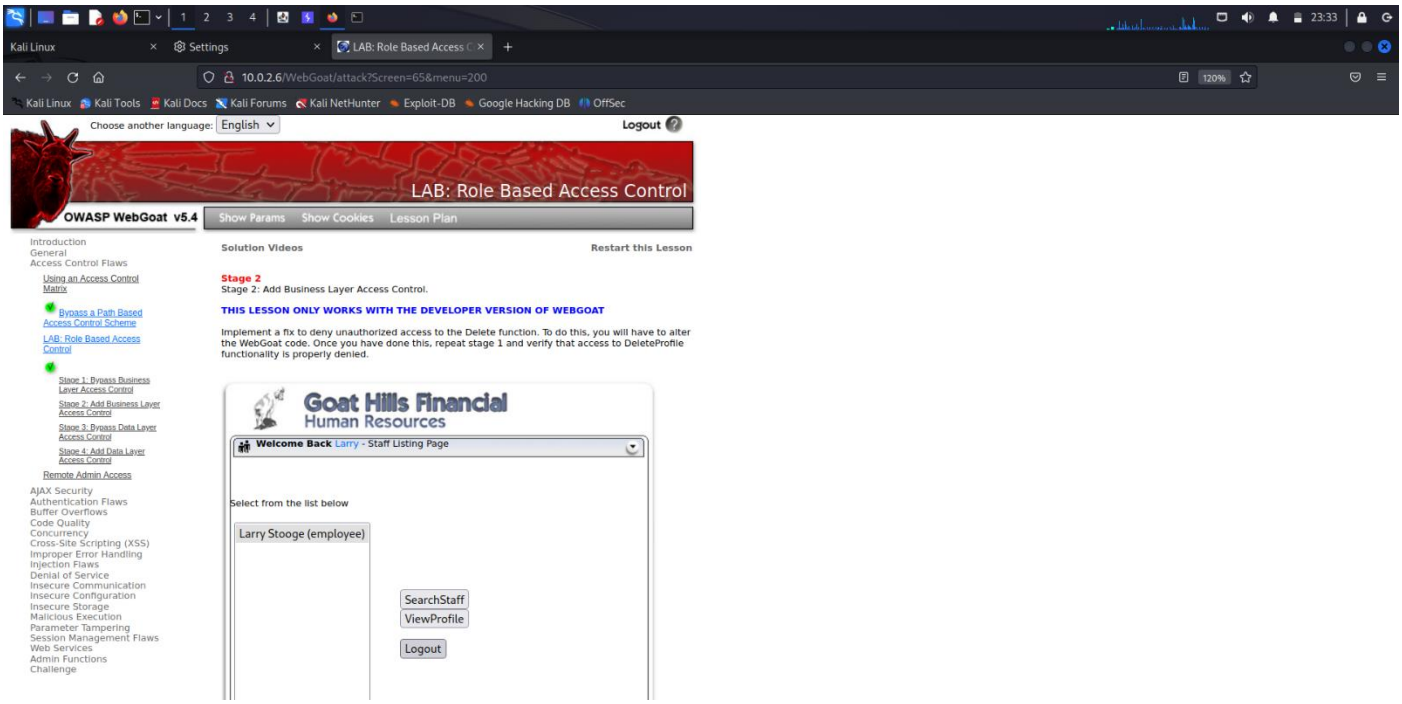
Password: larry



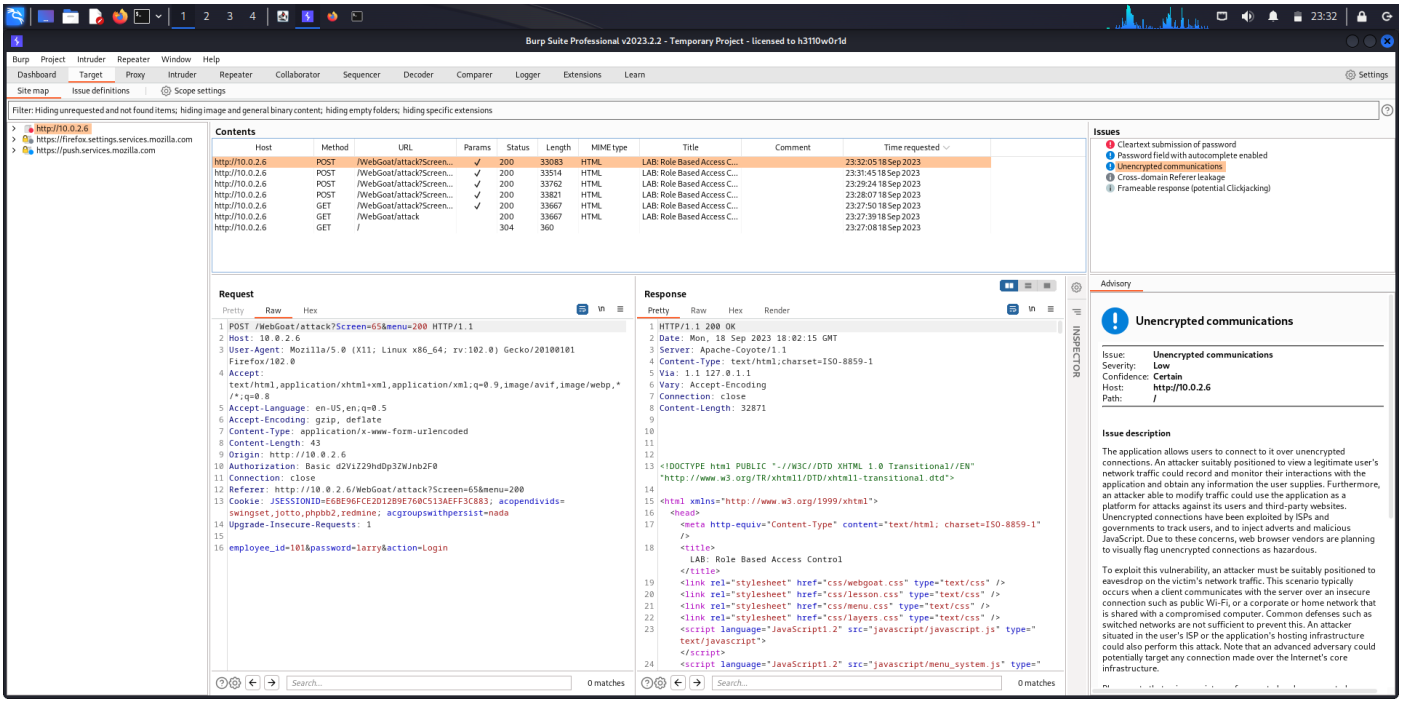
The employee Larry has been logged into his account.



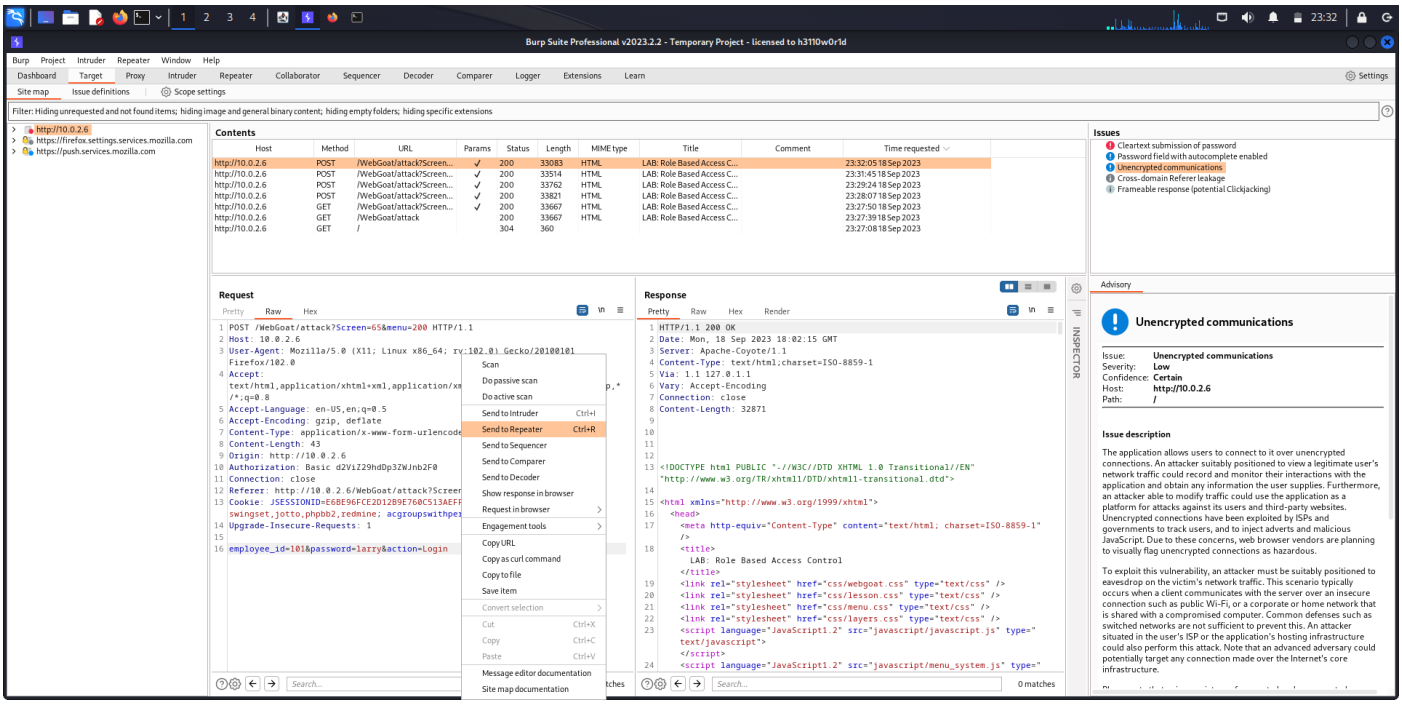
Larry logs out of his account.



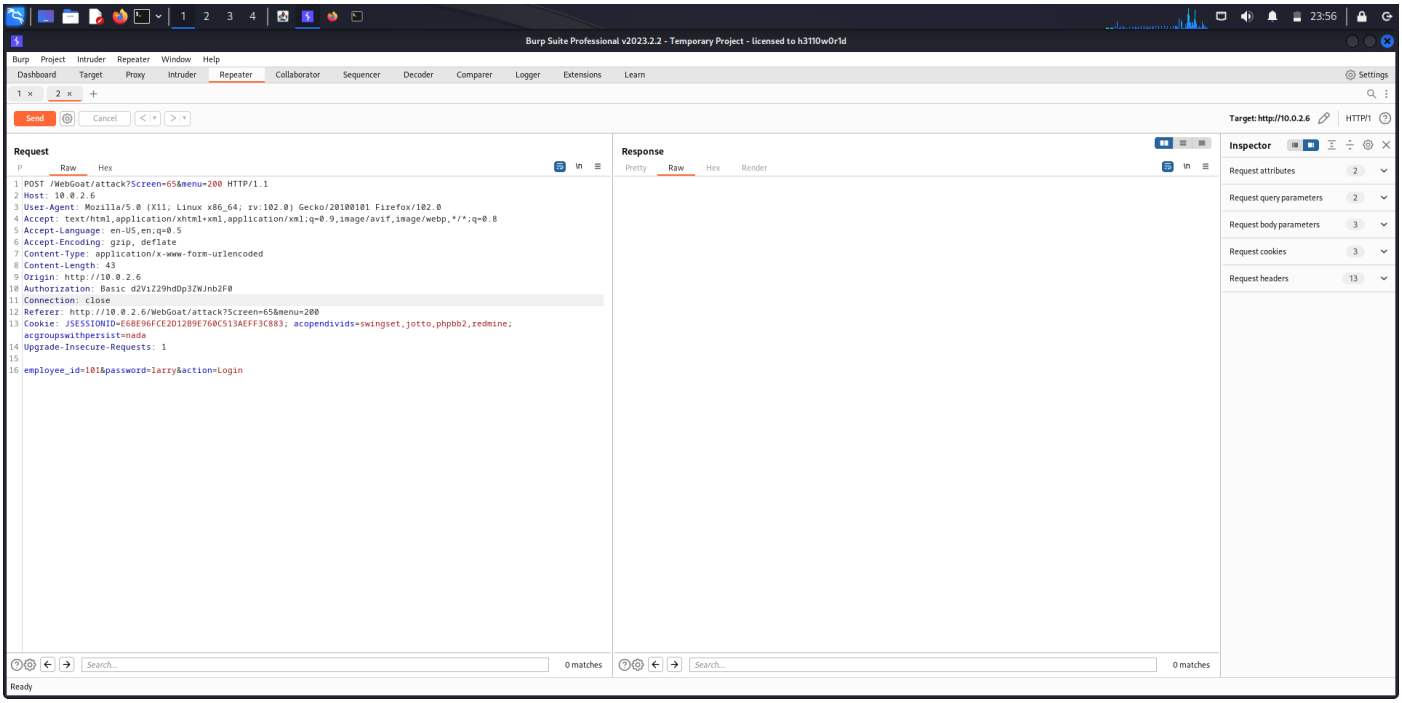
The action=Login HTTP Request message is captured in the burpsuite.



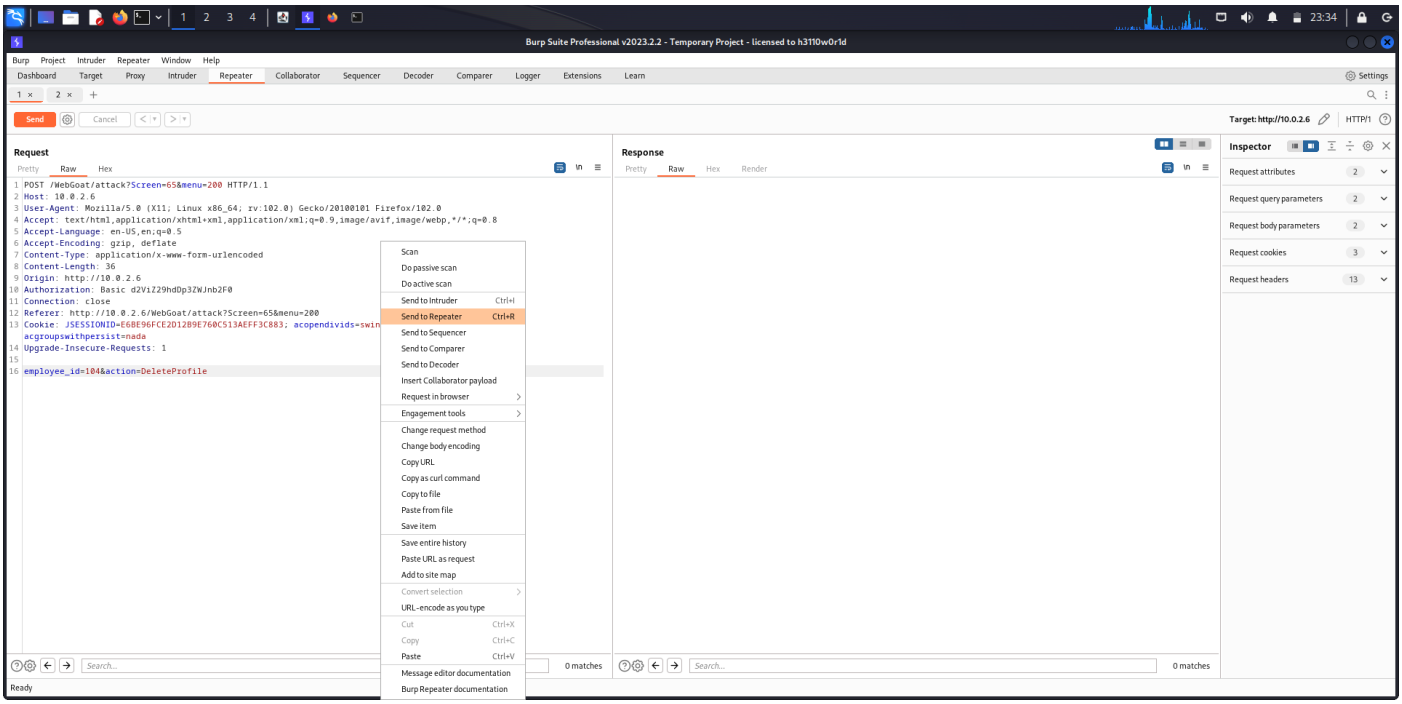
Right click on the HTTP Request message and click on Send to Repeater.



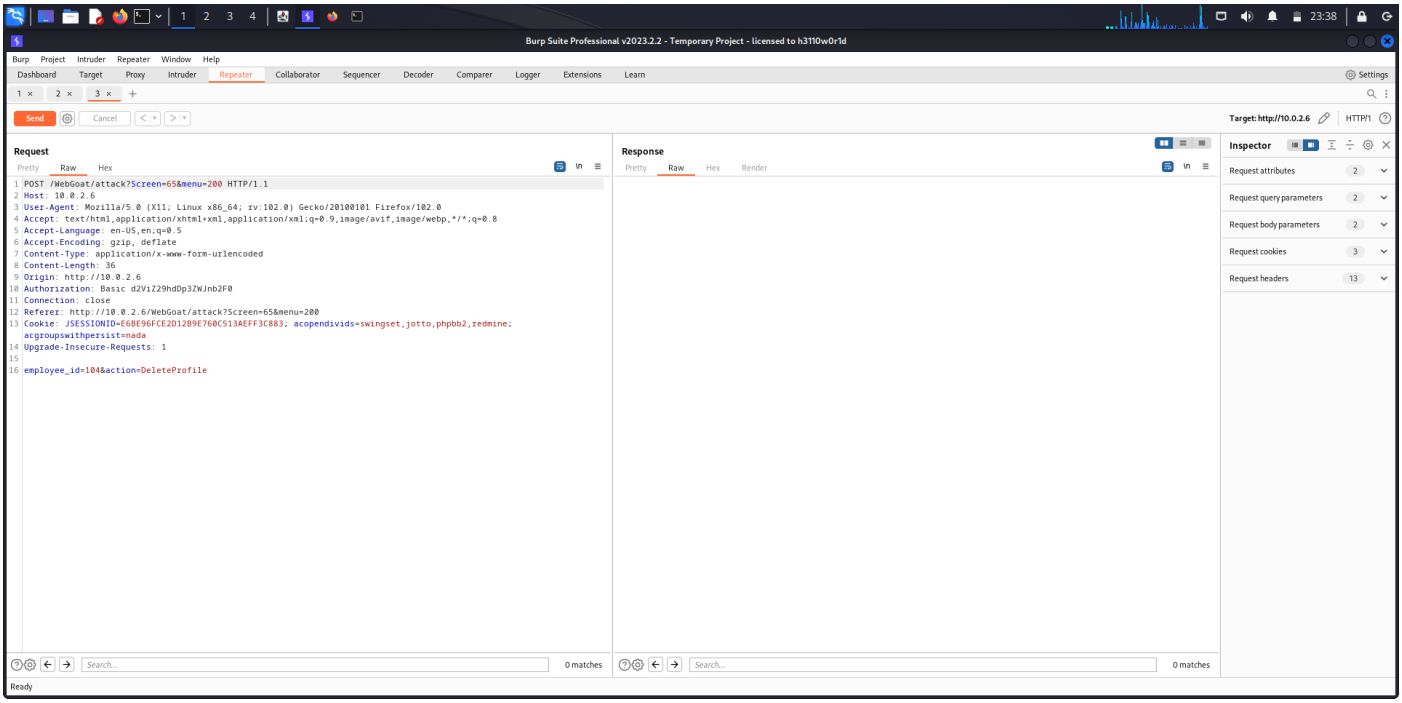
Second payload has been received in the Repeater tab.



Right click on the first payload and send it to Repeater again.



The HTTP Request message from the first payload has been sent to Repeater again.

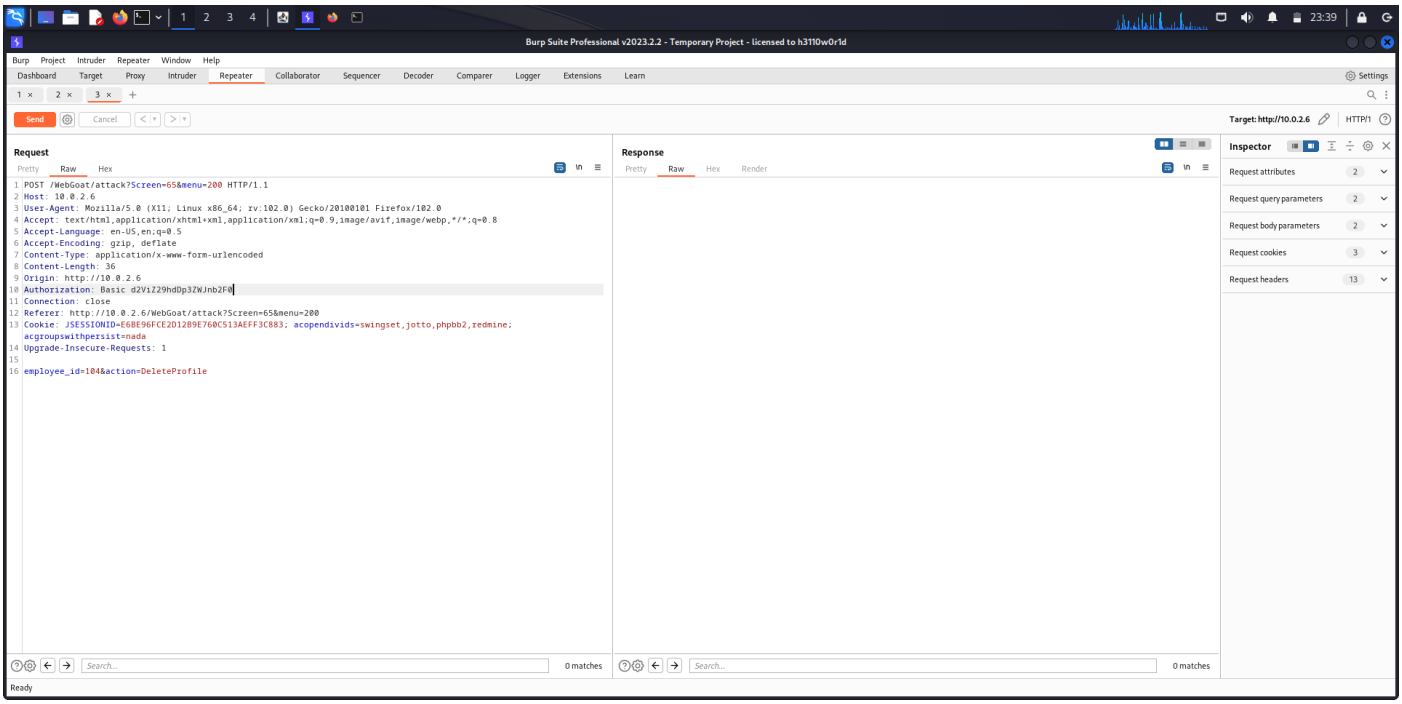


Copy the Authorization token and Cookie Session ID from second payload and paste it in the third payload.

Now, first payload contains John's DeleteProfile HTTP Request message

second payload contains Larry's Login HTTP Request message

third payload contains John's modified HTTP Request Message.

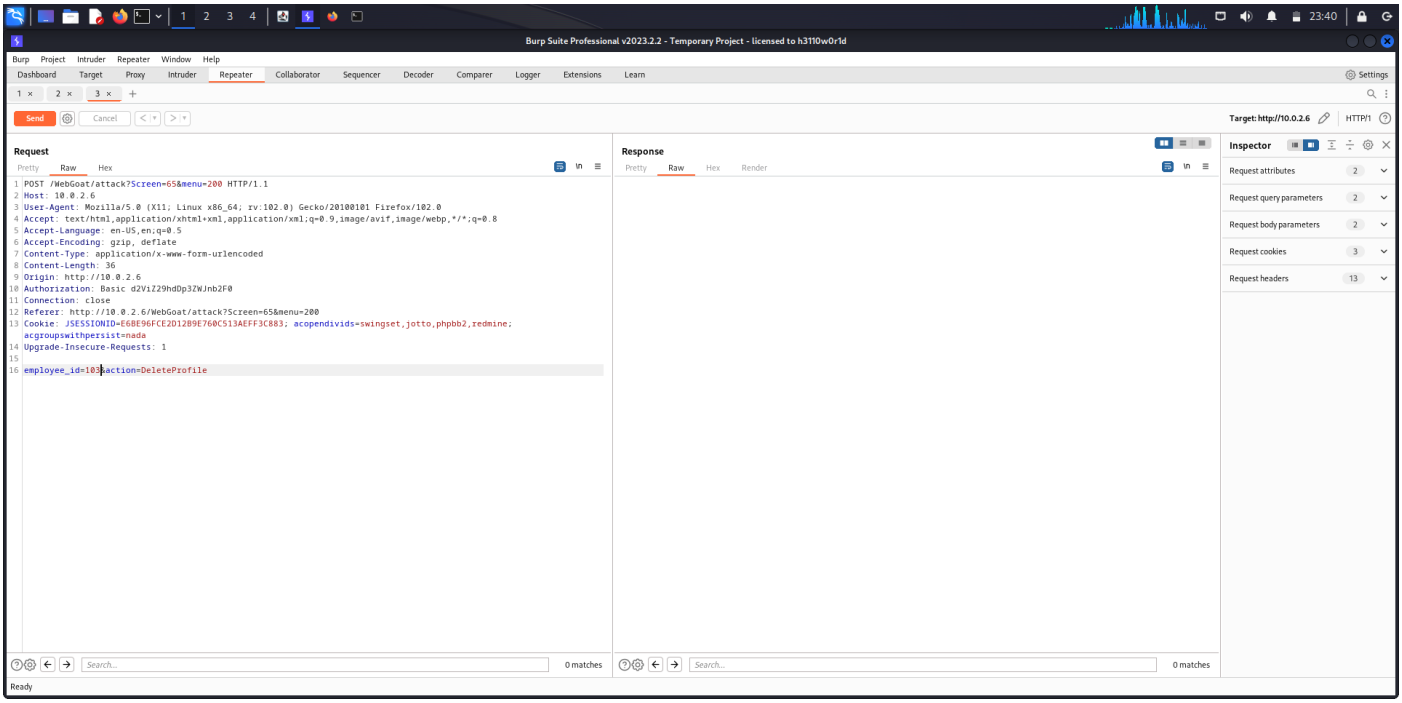


The E-ID of employee who is to be deleted has been replaced onto the E-ID of the employee who has been deleted.

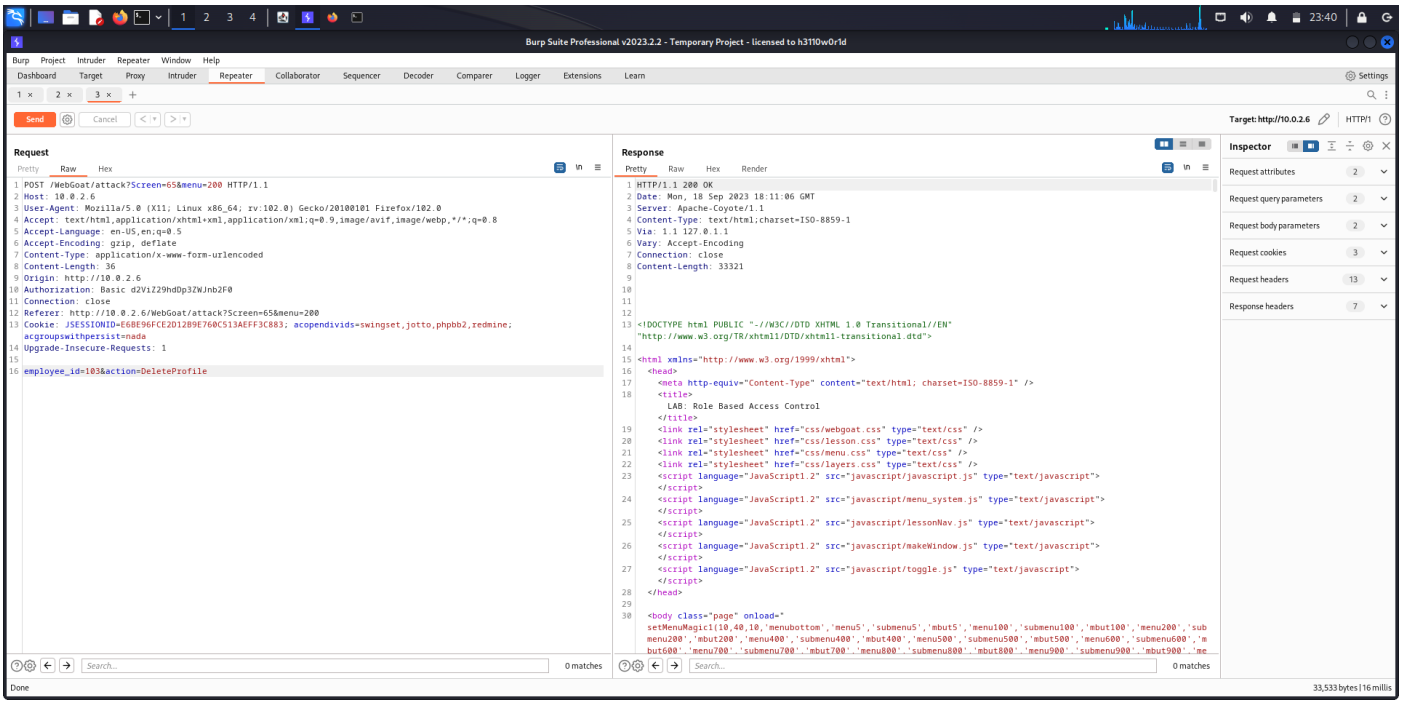
Before: employee_id: 104 //Emplpyee-ID of Eric Walker

After: employee_id: 103 //Employee-ID of Curly

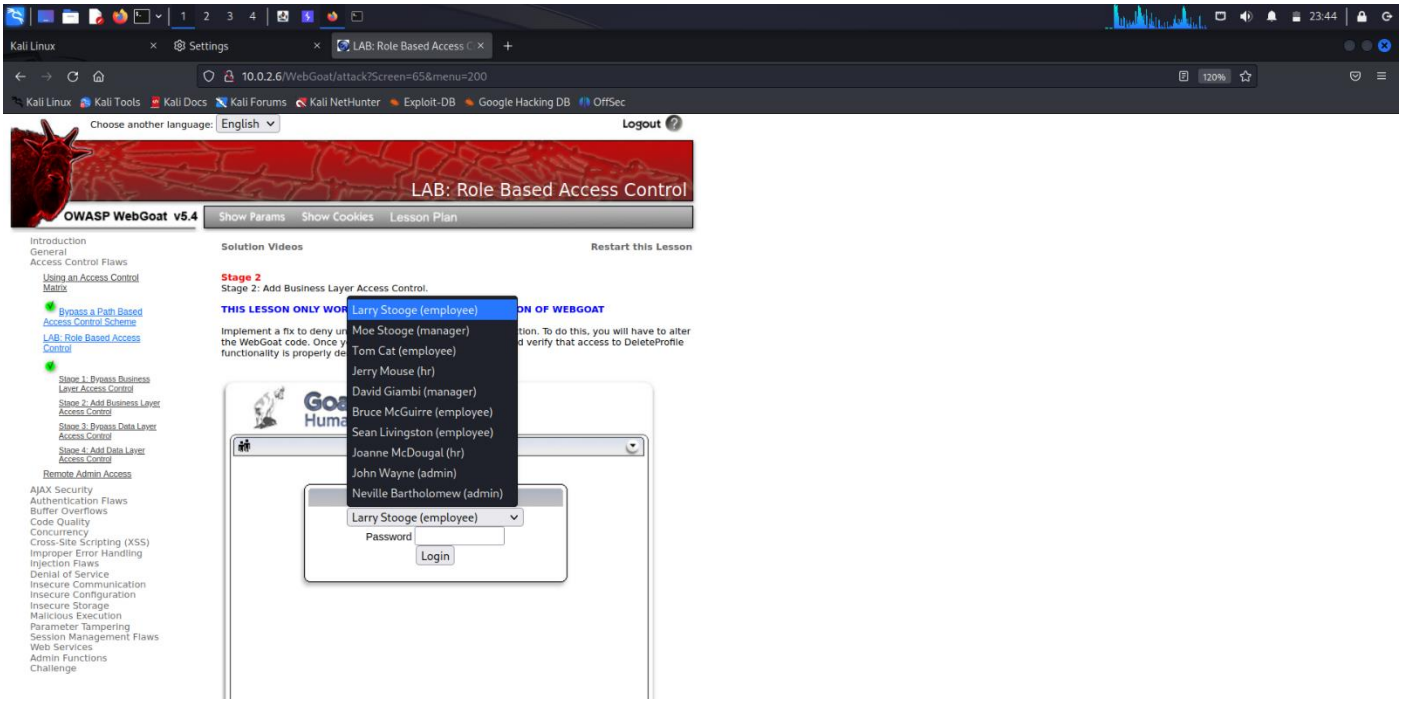
Send the HTTP Request message by clicking on the Send button on the top-left corner.



After sending the HTTP Request message, a HTTP Response message is received from the server.



In the Login page, we can see that Curly's profile has been deleted which was not done by the admin.



Analysis

The report on privilege escalation provides a comprehensive analysis of a critical cybersecurity issue that organizations face. It highlights the two primary forms of privilege escalation: horizontal and vertical, shedding light on the methods and implications of each. The report effectively underscores the significance of privilege escalation as a potential pathway for cyberattacks, emphasizing its role in data breaches and system compromises. It also stresses the importance of implementing robust security measures to mitigate the risk of privilege escalation, making it a valuable resource for organizations seeking to enhance their cybersecurity posture.

Conclusion

In conclusion, this report has delved into the complex and pressing issue of privilege escalation in cybersecurity. By examining both horizontal and vertical privilege escalation, it has illuminated the diverse avenues through which attackers can gain unauthorized access and elevate their privileges within a system or network. The report has underscored the paramount importance of proactive security measures, such as access controls, patch management, and vigilant monitoring, to thwart privilege escalation attempts. As organizations strive to safeguard their digital assets and sensitive data, the insights provided in this report serve as a valuable resource for strengthening their defence mechanisms against the ever-evolving landscape of cyber threats.