Name:Ahmed Almass

Lab 5: Attacking Access Controls

Web Application Security

Table of Contents

[Lab Outcome 2](#_Toc524601657)

[Background Reading 2](#_Toc524601658)

[Required Hardware/Software 2](#_Toc524601659)

[Introduction 2](#_Toc524601660)

[1.0 Access Control Matrix 2](#_Toc524601661)

[2.0 Path-Based Access Control 2](#_Toc524601662)

[3.0 Role-Based Access Control 2](#_Toc524601663)

[4.0 Sign-Off – Lab 5: Attacking Access Controls 3](#_Toc524601664)

Web Application Security

Lab 5: Attacking Access Controls

# Lab Outcome

Exploit various access controls.

Background Reading

Read the textbook sections listed in the Course Schedule.

Required Hardware/Software

* WebGoat v7.1
* Burp

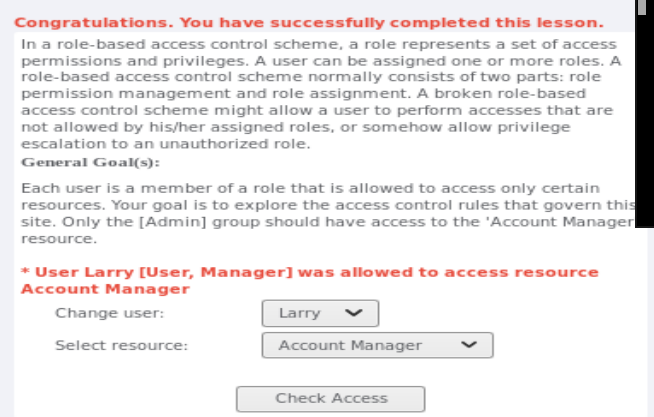
# Introduction

Access controls are built on top of authentication and session management. They control what users are allowed to see and do in the web application.

# 1.0 Access Control Matrix

In WebGoat, complete the **Access Control Flaws > Using an Access Control Matrix** lesson.

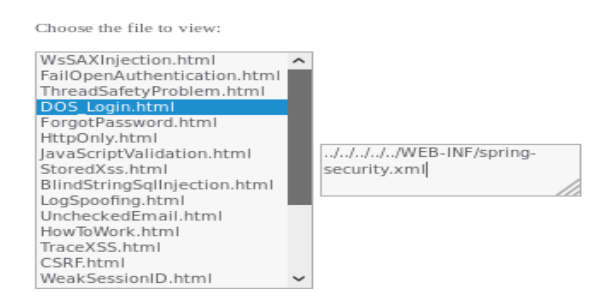
The objective is to find the specific user to access prevlidges for account manager.

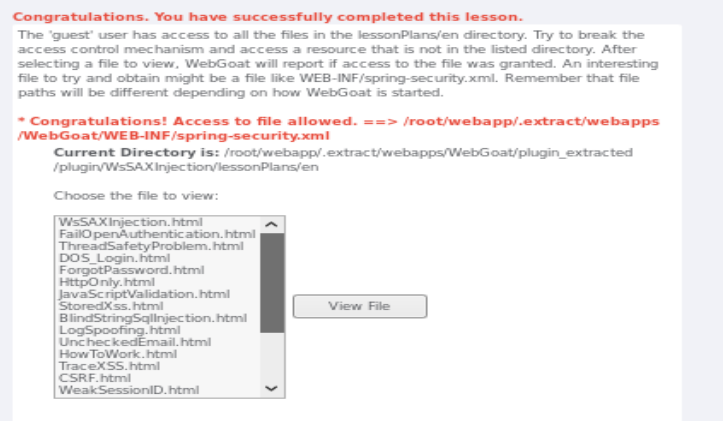


# 2.0 Path-Based Access Control

In WebGoat, complete the **Access Control Flaws > Bypass a Path Based Access Control Scheme** lesson.

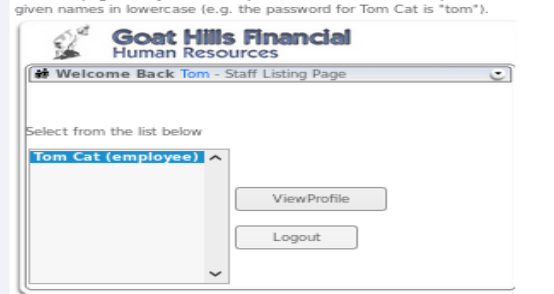
I used Web Developer tool in firefox called convert select element to text inputs to bypass a path to find unauthorized directoy or file.



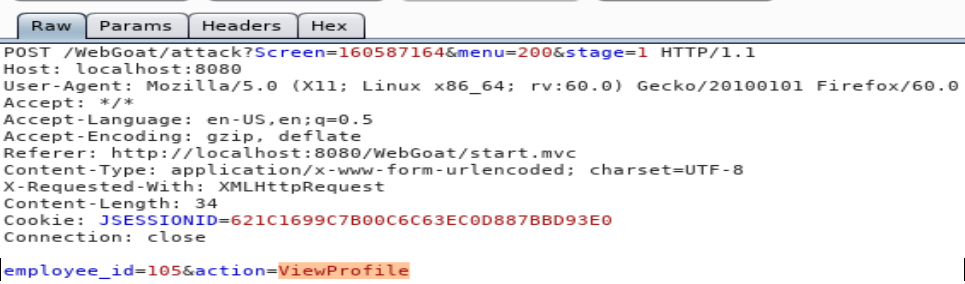


# 3.0 Role-Based Access Control

1. In WebGoat, complete the **Access Control Flaws > Role Based Access Control > Stage 1** lesson.

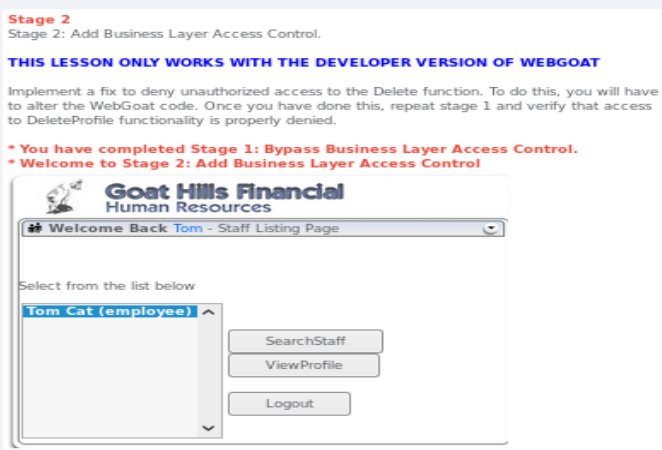


I intercepted the view profile request with burp.



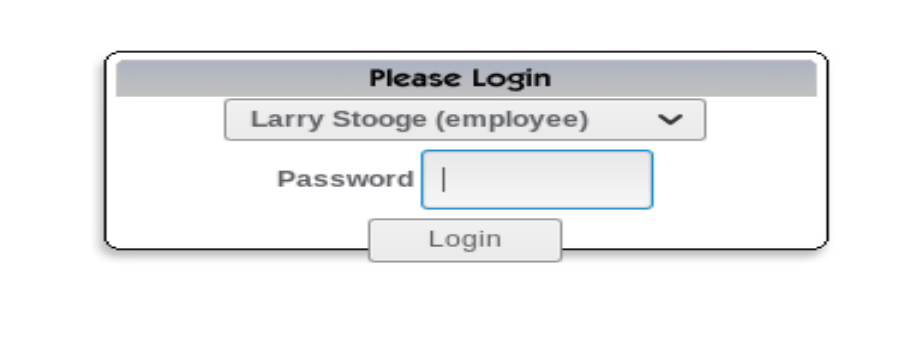
I than change the action from viewprofile to deleteprofile to do the action.



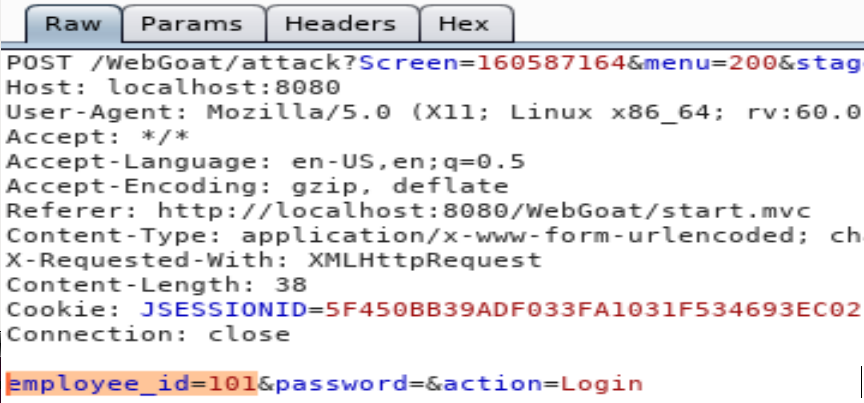


1. In WebGoat, complete the **Access Control Flaws > Role Based Access Control > Stage 2** lesson.
2. In WebGoat, complete the **Access Control Flaws >** **Role Based Access Control > Stage 3** lesson.

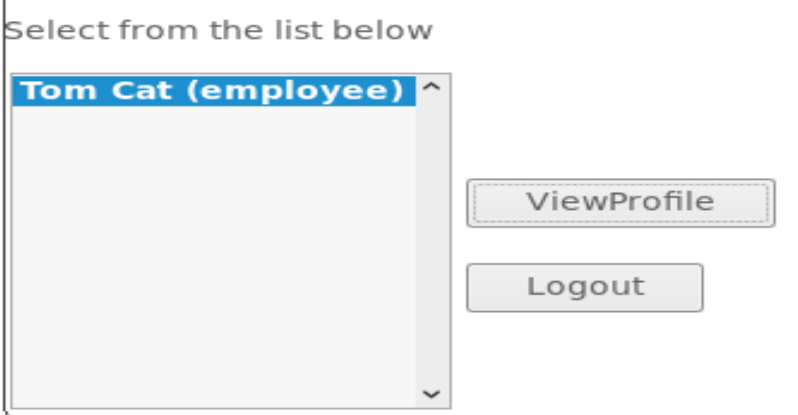
Tried login in with larry without password, intercepted with burp.



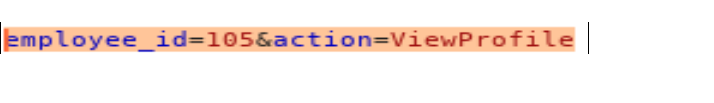
When trying to login burp showed that there was an employee\_id which was 101.



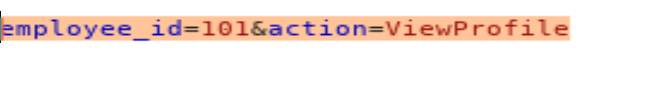
I than login was Tom with a password. I intercepted the ViewProfile command.



Tom had its own employee id which was 105



I changed the value of 105 to 101 to check the profile larry.





1. In WebGoat, complete the **Access Control Flaws > Role Based Access Control > Stage 4** lesson.

# 4.0 Sign-Off – Lab 5: Attacking Access Controls

Detach this page and submit it to your instructor to indicate you have completed all sections.

Name:

Student ID:

|  |  |
| --- | --- |
| **Section** | **Instructor Initials** |
| 1.0 Access Control Matrix |  |
| 2.0 Path-Based Access Control |  |
| 3.0 Role-Based Access Control – 1 |  |
| 3.0 Role-Based Access Control – 2 |  |
| 3.0 Role-Based Access Control – 3 |  |
| 3.0 Role-Based Access Control – 4 |  |