Name: Jun Wang 000791814

Marks: \_\_\_\_\_/4\_\_\_

Lab 5: Attacking Access Controls

Web Application Security

Bonus:\_\_\_\_\_\_/6, 3 marks for each source code\_

Table of Contents

[Lab Outcome 2](#_Toc22496694)

[Background Reading 2](#_Toc22496695)

[Architecture Diagram 2](#_Toc22496696)

[Required Hardware/Software 2](#_Toc22496697)

[Introduction 3](#_Toc22496698)

[1.0 Access Control Matrix 3](#_Toc22496699)

[2.0 Path-Based Access Control 3](#_Toc22496700)

[3.0 Role-Based Access Control 3](#_Toc22496701)

[4.0 Sign-Off – Lab 5: Attacking Access Controls 4](#_Toc22496702)

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.

Architecture Diagram

|  |
| --- |
|  |

Required Hardware/Software

* VM Ubuntu 18.04 – 2 CPU, 4GB Ram, 20 GB hard disk
  + Docker
    - WebGoat v7.1
    - DVWA (Dawn Vulnerable Web App)
* VM Kali
  + Burp or other Web proxy (scanner)

# 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.

Refference:

<https://www.blackhillsinfosec.com/using-simple-burp-macros-to-automate-testing/>

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Users | Public Share | Time Card Entry | Performance Review | Time Card Approval | Site Manager | Account Manager |
| Moe | x |  |  |  |  |  |
| Larry |  | x | x | x |  | x |
| Curly | x |  | x | x |  |  |
| Shemp |  |  |  |  | x | x |

# Selection_004

# 2.0 Path-Based Access Control

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

Tool: ZAP

Step1> open zap, set proxy on firefox and zap , make sure the port match.

Step2> webgoat choose any file and click submit

Step3> find the POST request, right click on it, choose open/resend with request editor.

Step4>change the file name File=../../../../../WEB-INF/spring-security.xml and resend the post header.

|  |
| --- |
| Selection_005Insert evidence here. |
| Selection_006 |
| Selection_007 |
|  |

# 3.0 Role-Based Access Control

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

Tool: zap

Step1>login as Tom Cat passwd:tom

Step2> click view profile.

Step3>login as Jerry Mouse, found he has the access to DeleteProfile, click on DeleteProfile, on Zap we can see the POST packet, action= “DeleteProfile”.

Step4>on zap find the POST header, right click on the header, open/resend with request edit..

Step5> change the request to action=DeleteProfile and click on send.

Step6> reload the web page.

|  |
| --- |
| Selection_009Insert evidence here. |
| Selection_010 |
| Selection_014 |
| Selection_015 |
| Selection_011 |
| Selection_008 |

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

|  |
| --- |
|  |
|  |
|  |
|  |

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

Tool: ZAP

Step1>Same as stage1 login as Tom Cat.

Step2>find the POST request and open/resend request

Step3> change employee\_id from 105 to 109. Then send the request. Then I got the response from server, can view the profile of Sean Livingston.

|  |
| --- |
| Selection_011 |
| Selection_012 |
| Selection_013 |
| Insert evidence here. |

|  |
| --- |
| Insert evidence here. |

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

|  |
| --- |
|  |
|  |
|  |
| Insert evidence here. |

|  |
| --- |
| Insert evidence here. |

# 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 |  |