Name: Jun Wang 000791814

Marks: /10

Lab 7: Attacking Users

Web Application Security

Bonus Marks: -/-

Table of Contents

[Lab Outcome 2](#_Toc530921007)

[Background Reading 2](#_Toc530921008)

[Required Hardware/Software 2](#_Toc530921009)

[Introduction 2](#_Toc530921010)

[1.0 Phishing with XSS 2](#_Toc530921011)

[2.0 Stored XSS Attacks 2](#_Toc530921012)

[3.0 Reflected XSS Attacks 2](#_Toc530921013)

[4.0 More Cross-Site Scripting 2](#_Toc530921014)

[5.0 DOM-Based XSS 3](#_Toc530921015)

[6.0 Cross-Site Request Forgery 3](#_Toc530921016)

[7.0 CSRF Prompt By-Pass 3](#_Toc530921017)

[8.0 CSRF Token By-Pass 3](#_Toc530921018)

[9.0 Sign-Off – Lab 7: Attacking Users 4](#_Toc530921019)

Web Application Security

Lab 7: Attacking Users

# Lab Outcome

Target users using cross-site scripting and other techniques.

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

You can gain access to data and functionalities without directly attacking the web application on the server. Targeting users of the application by leveraging different vulnerabilities can achieve the same results and more.

# 1.0 Phishing with XSS

In WebGoat, complete the **Cross-Site Scripting (XSS) > Phishing with XSS** lesson.

|  |
| --- |
|  |
| Selection_088 |
| Selection_085 |
| Selection_086 |
|  |
| Insert evidence here. |

# 2.0 Stored XSS Attacks

In WebGoat, complete the **Cross-Site Scripting (XSS) > Stored XSS Attacks** lesson.

Tool: Burp

Stage1:

Step1> login as Tom, password ‘tom’

Step2> clik on view profile. Turn on intercept on burp.

Step3> click on updateprofile.

Step4> change the post request that burp intercepted and then forward the post request. In field ddress 1 add the following script: <script> alter(“document.cookie”); </script>

Step5> login as Jerry, password ‘jerry’, view profile of Tom Cat.

|  |
| --- |
| Selection_091 |
| Selection_092 |
| Selection_093 |
| Selection_095 |
| Selection_097 |
|  |

# 3.0 Reflected XSS Attacks

In WebGoat, complete the **Cross-Site Scripting (XSS) > Reflected XSS Attacks** lesson.

Step1> login as any account

Step2> search staff

Step3> fill the form as <script> alter(“document.cookie”); </script>

Then click on FindProfile

|  |
| --- |
| Selection_102 |
| Selection_103 |
|  |
| Selection_104 |
| Selection_105 |

# 4.0 More Cross-Site Scripting

1. Start the DVWA VM and set it to Low security. (Try Medium and High as practice as well.) admin / password

|  |
| --- |
|  |
|  |

1. Exploit the section XSS (Reflected).

<script>alert(“what’s up!”)</script>

|  |
| --- |
| Security level: Low |
|  |
| Security level: Medium  Selection_111 |
| Security level: High  Selection_112 |

1. Exploit the section XSS (Stored).

|  |
| --- |
| Security level: Low  Selection_113 |
| Selection_114 |
| Selection_117 |
| Security level: Medium  Selection_118 |
| Security level: HighSelection_119  Selection_120 |

# 5.0 DOM-Based XSS

In WebGoat, complete the **AJAX Security > DOM-Based cross-site scripting** lesson.

|  |
| --- |
|  |
| Selection_145 |
| Selection_146 |
| Selection_147 |
| Selection_149 |
| Selection_152 |
| Selection_153 |

# 6.0 Cross-Site Request Forgery

In WebGoat, complete the **Cross-Site Scripting (XSS) > Cross Site Request Forgery (CSRF)** lesson.

|  |
| --- |
| Selection_156 |
| Selection_157 |
| Selection_158 |

# 7.0 CSRF Prompt By-Pass

In WebGoat, complete the **Cross-Site Scripting (XSS) > CSRF Prompt By-Pass** lesson.

|  |
| --- |
| Selection_161 |
| Selection_163 |
| Selection_164 |
| Selection_165 |

# 8.0 CSRF Token By-Pass

In WebGoat, complete the **Cross-Site Scripting (XSS) > CSRF Token By-Pass** lesson.

|  |
| --- |
| Selection_166 |
| Selection_169 |
| Selection_167 |
| Selection_168 |

9.0 Sign-Off – Lab 7: Attacking Users

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

Name:

Student ID:

|  |  |
| --- | --- |
| **Section** | **Instructor Initials** |
| 1.0 Phishing with XSS |  |
| 2.0 Stored XSS Attacks |  |
| 3.0 Reflected XSS Attacks |  |
| 4.0 More Cross-Site Scripting – 1 |  |
| 4.0 More Cross-Site Scripting – 2 |  |
| 5.0 DOM-Based XSS |  |
| 6.0 Cross-Site Request Forgery |  |
| 7.0 CSRF Prompt By-Pass |  |
| 8.0 CSRF Token By-Pass |  |