Name:Ahmed almass

Lab 8: Attacking the Servers

Web Application Security

Table of Contents

[Lab Outcome 2](#_Toc524601731)

[Background Reading 2](#_Toc524601732)

[Required Hardware/Software 2](#_Toc524601733)

[Introduction 2](#_Toc524601734)

[1.0 Buffer Overflows 2](#_Toc524601735)

[2.0 Sign-Off – Lab 8: Attacking the Servers 3](#_Toc524601736)

Web Application Security

Lab 8: Attacking the Servers

# Lab Outcome

Exploit natively compiled applications.

Background Reading

Read the textbook sections listed in the Course Schedule.

Required Hardware/Software

* WebGoat v7.1
* Burp

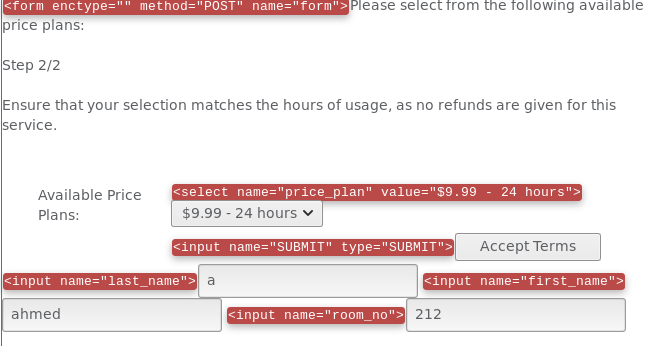
# Introduction

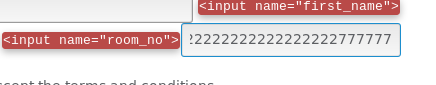
Web applications written in native languages, like C and C++, suffer from vulnerabilities such as buffer overflows and format string errors.

# 1.0 Buffer Overflows

In WebGoat, complete the **Buffer Overflows > Off-by-One Overflows** lesson.

In this lesson, I did a buffer overflow using over 4097 digits, when doing this it creates a data leakage.



Inserting 4097 digits

# The leakage

# 

# 2.0 Sign-Off – Lab 8: Attacking the Servers

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

Name:

Student ID:

|  |  |
| --- | --- |
| **Section** | **Instructor Initials** |
| 1.0 Buffer Overflows |  |