Name:Ahmed Almass

Lab 3: Attacking Authentication

Web Application Security

Table of Contents

[Lab Outcomes 2](#_Toc524601629)

[Background Reading 2](#_Toc524601630)

[Required Hardware/Software 2](#_Toc524601631)

[Introduction 2](#_Toc524601632)

[1.0 Sniffing Login 2](#_Toc524601633)

[2.0 Improper Error Handling 2](#_Toc524601634)

[3.0 Password Strength 2](#_Toc524601635)

[4.0 Forgot Password 2](#_Toc524601636)

[5.0 Multi-level Logins 2](#_Toc524601637)

[6.0 Sign-Off – Lab 3: Attacking Authentication 3](#_Toc524601638)

Web Application Security

Lab 3: Attacking Authentication

# Lab Outcomes

* Exploit the login process.
* Exploit passwords and related functionalities.

Background Reading

Read the textbook sections listed in the Course Schedule.

Required Hardware/Software

* WebGoat v7.1
* Burp

# Introduction

Authentication is essential to an application’s protection. It is the first line of defence against attackers seeking to gain unauthorized access and full control of a system.

# 1.0 Sniffing Login

In WebGoat, complete the **Insecure Communication > Insecure Login** lesson.

Stage 1:

Sniffing a HTTP connection with wireshark spits out HTTP Post in plain text. When sigining in password and user were shown pcture below.



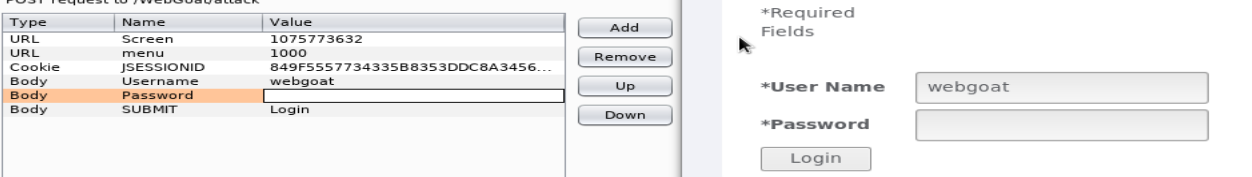
Stage2: (note: when doing stage 2 on webgoat it wouldnt go to https connection, so i was capable to get a screenshot).

When sniffing HTTPS, a secure connection the HTTP Post is encrypted by SHA-1 and MD5.

# 2.0 Improper Error Handling

In WebGoat, complete the **Improper Error Handling > Fail Open Authentication Scheme** lesson.

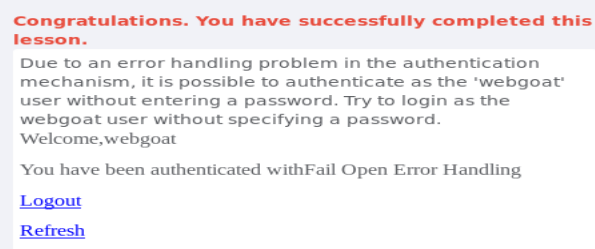
When loging in to webgoat i was cabable to intercept it with burp.



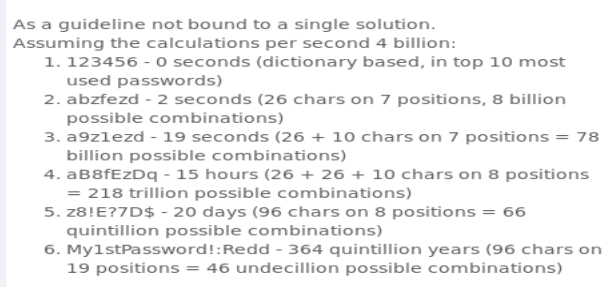
I than deleted the Password body.

# 

Aferwards i was capable to login.



# 3.0 Password Strength

In WebGoat, complete the **Authentication Flaws > Password Strength** lesson.

# 4.0 Forgot Password

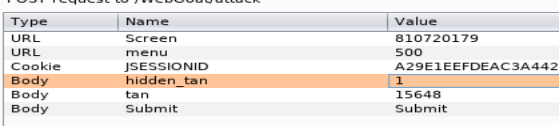
In WebGoat, complete the **Authentication Flaws > Forgot Password** lesson.

This method to get in is when a website doesnt have the security mechanisim for a forgot password. So its capable to forget password for admin or other users without getting locked out.

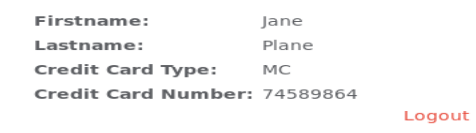
# 5.0 Multi-level Logins

1. In WebGoat, complete the **Authentication Flaws > Multi Level Login 1** lesson.

When phishing a person even havingd a username or password you’d sosmetimes need a transaction authentication number but the one is already been used, there a method when you intercept the request and change the hidden\_ tan to value 1.

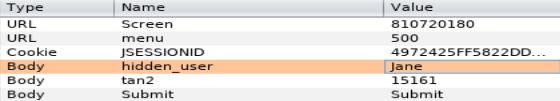


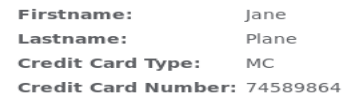
Than success your login.



1. In WebGoat, complete the **Authentication Flaws > Multi Level Login 2** lesson.

With this, its almost the same method as the first but you are signing in as Joe but having the second TAN. You intercept it with burp and change the user to Jane instead of Joe.





# 6.0 Sign-Off – Lab 3: Attacking Authentication

Detach this page and submit it to your instructor to indicate you have completed each section.

Name:

Student ID:

|  |  |
| --- | --- |
| **Section** | **Instructor Initials** |
| 1.0 Sniffing Login |  |
| 2.0 Improper Error Handling |  |
| 3.0 Password Strength |  |
| 4.0 Forgot Password |  |
| 5.0 Multi-level Login – 1 |  |
| 5.0 Multi-level Login – 2 |  |