Week 10 Penetration Testing Report

Introduction

This report document hereby describes the proceedings and results of a Black Box security assessment conducted against the **Week 10 Labs**. The report hereby lists the findings and corresponding best practice mitigation actions and recommendations.

1. Objective

The objective of the assessment was to uncover vulnerabilities in the **Week 10 Labs** and provide a final security assessment report comprising vulnerabilities, remediation strategy and recommendation guidelines to help mitigate the identified vulnerabilities and risks during the activity.

2. Scope

This section defines the scope and boundaries of the project.

Application Name	**{Capture the Flag}**

3. Summary

Outlined is a Black Box Application Security assessment for the **Week 10 Labs**.

Total number of Sub-labs: 1 Sub-labs

High	Medium	Low
0	1	0

High - **Number of Sub-labs with hard difficulty level**

Medium - **Number of Sub-labs with Medium difficulty level**

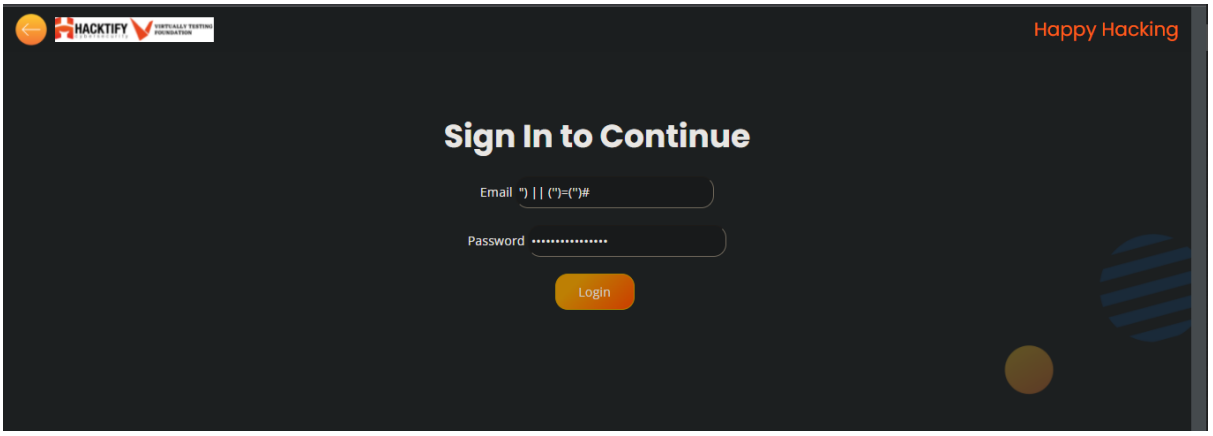
Low - **Number of Sub-labs with Easy difficulty level**

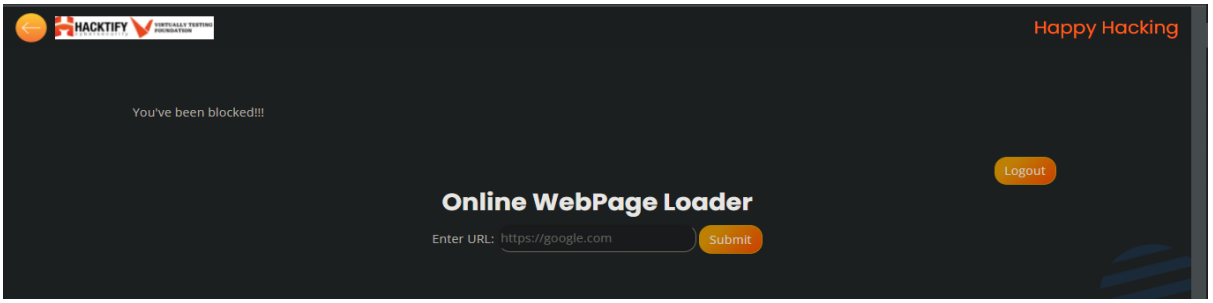
1. {Capture the Flag}

1.1. {Capture the Flag}

Reference	Risk Rating
Capture the Flag	**Medium**
Tools Used	
Google chrome, Burp suite, CTF tool	
Vulnerability Description	
I found this vulnerability by performing two security vulnerabilities as SQL Injection and Server Side Request Forgery (SSRF). Initially, I performed SQL Injection on login page where I got password as vulnerable field and with the help of successful payload input I got next page as URL loader where I performed SSRF and successfully captured the flag.	
How It Was Discovered	
Automated Tools and Manual Analysis	
Vulnerable URLs	
https://www.bugbountyhunter.org/internship_labs/HTML/ctf/index.php	
Consequences of not Fixing the Issue	
Stealing credentials, access to the database, altering or modifying data, access to the network. Taking over information of IP Address, Remote Code Execution, and IP address of servers running behind a reverse proxy.	
Suggested Countermeasures	
Using stored procedures instead of dynamic SQL, prepared statements, least privilege access and input validation, character escaping, vulnerability scanner, firewall, whitelist domains, enforcing URL Schemas, enable authentication and validation of all inputs.	
References	
https://ctfd.io/whats-a-ctf/ https://www.paloaltonetworks.com/blog/2016/06/unit-42-countdown-to-labyrenth-capture-the-flag-ctf-challenge/	

Proof of Concept




HACKTIFY
Happy Hacking
You've been blocked!!!
Logout
Online WebPage Loader
Enter URL:
https://google.com
Submit