**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** | Lab 1-CAPTURE THE FLAG(CTF) |
| --- | --- |

**3. Summary**

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

**Total number of Sub-labs: 12 Sub-labs**

| **High** | **Medium** | **Low** |
| --- | --- | --- |
| **0** | **01** | **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** | |
| Web Browser,Burp Suite | |
| **Vulnerability Description** | |
|  | |
| **How It Was Discovered** | |
|  | |
| **Vulnerable URLs** | |
|  | |
| **Consequences of not Fixing the Issue** | |
|  | |
| **Suggested Countermeasures** | |
|  | |
| **References** | |
|  | |

# Proof of Concept

# 

# 