Week {#}
Penetration Testing Report

Introduction

This report document hereby describes the proceedings and results of a Black Box security assessment conducted against the **Week {#} 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 {#} 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 Name}, {Lab 2 Name (if the week has 2 labs)}**

3. Summary

Outlined is a Black Box Application Security assessment for the **Week {#} Labs**.

Total number of Sub-labs: {count} Sub-labs

High	Medium	Low
{count}	{count}	{count}

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. {Lab 1 Name}

1.1. {Sub-lab-1 Name}

Reference	**Risk Rating**
{Sub-lab-1 Name}	**Low / Medium / High**
Tools Used	
Tools that you have used to find the vulnerability.	
Vulnerability Description	
About the vulnerability and its working	
How It Was Discovered	
Automated Tools / Manual Analysis	
Vulnerable URLs	
URLs of the vulnerable pages in the lab	
Consequences of not Fixing the Issue	
What will be the consequences if the vulnerability is not patched?	
Suggested Countermeasures	
Give some Suggestions to stand against this vulnerability	
References	
URLs to the sources used to know more about this vulnerability	

Proof of Concept

This section contains the proof of the above vulnerabilities as the screenshot of the vulnerability of the lab

1.2. {Sub-lab-2 Name}

Reference	**Risk Rating**
{Sub-lab-2 Name}	**Low / Medium / High**
Tools Used	
Tools that you have used to find the vulnerability.	
Vulnerability Description	
About the vulnerability and its working	
How It Was Discovered	
Automated Tools / Manual Analysis	
Vulnerable URLs	
URLs of the vulnerable pages in the lab	
Consequences of not Fixing the Issue	
What will be the consequences if the vulnerability is not patched?	
Suggested Countermeasures	
Give some Suggestions to stand against this vulnerability	
References	
URLs to the sources used to know more about this vulnerability	

Proof of Concept

This section contains the proof of the above vulnerabilities as the screenshot of the vulnerability of the lab

2. {Lab 2 Name (if the week has 2 labs)}

2.1. {Sub-lab-1 Name}

Reference	Risk Rating
{Sub-lab-1 Name}	**Low / Medium / High**
Tools Used	
Tools that you have used to find the vulnerability.	
Vulnerability Description	
About the vulnerability and its working	
How It Was Discovered	
Automated Tools / Manual Analysis	
Vulnerable URLs	
URLs of the vulnerable pages in the lab	
Consequences of not Fixing the Issue	
What will be the consequences if the vulnerability is not patched?	
Suggested Countermeasures	
Give some Suggestions to stand against this vulnerability	
References	
URLs to the sources used to know more about this vulnerability	

Proof of Concept

This section contains the proof of the above vulnerabilities as the screenshot of the vulnerability of the lab

2.2. {Sub-lab-2 Name}

Reference	**Risk Rating**
{Sub-lab-2 Name}	**Low / Medium / High**
Tools Used	
Tools that you have used to find the vulnerability.	
Vulnerability Description	
About the vulnerability and its working	
How It Was Discovered	
Automated Tools / Manual Analysis	
Vulnerable URLs	
URLs of the vulnerable pages in the lab	
Consequences of not Fixing the Issue	
What will be the consequences if the vulnerability is not patched?	
Suggested Countermeasures	
Give some Suggestions to stand against this vulnerability	
References	
URLs to the sources used to know more about this vulnerability	

Proof of Concept

This section contains the proof of the above vulnerabilities as the screenshot of the vulnerability of the lab

NOTES:

- **Everything mentioned inside {} has to be changed based on your week, labs and sub-labs.**
- **If you have 2 labs in same week you need to mention that, if not ignore those mentions for lab 2.**
- **Here it is given with 2 Sub-labs vulnerability, you need to add all the sub-labs based on your labs.**
- **Don’t forget to add the screenshot of the vulnerability in the proof of concept.**
- **Add only 1 screenshot in the Proof of Concept section.**
- **This NOTE session is only for your reference, don’t forget to delete this in the report you submit.**