Week 6
Penetration Testing Report

Introduction

This report document hereby describes the proceedings and results of a Black Box security assessment conducted against the **Week 6 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 6 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	**Cross-Site Request Forgery**

3. Summary

Outlined is a Black Box Application Security assessment for the **Week 6 Labs**.

Total number of Sub-labs: 6 Sub-labs

High	Medium	Low
2	2	2

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. Cross-Site Request Forgery

1.1. Easy CSRF

Reference	Risk Rating
Easy CSRF	**Low**
Tools Used	
Browser, Burp Suite	
Vulnerability Description	
The vulnerability is Cross-Site Request Forgery that makes victims load or execute unwanted things on web applications.	
How It Was Discovered	
Manual Analysis - Change password of victim using attacker CSRF poc generator.	
Vulnerable URLs	
https://www.bugbountyhunter.org/internship_labs/HTML/csrf_lab/lab_1/login.php	
Consequences of not Fixing the Issue	
It is based on attacker intension, the attacker can possibly take full control of access to the system.	
Suggested Countermeasures	
Using CSRF Tokens.	
References	
https://owasp.org/www-community/attacks/csrf	

Proof of Concept

The proof of the above vulnerability.

```
<html>
  <!-- CSRF PoC - generated by Burp Suite Professional -->
  <body>
  <script>history.pushState('', '', '/')</script>
    <form action="https://www.bugbountyhunter.org/internship_labs/HTML/csrf_lab/lab_1/passwordChange.php" method="POST">
      <input type="hidden" name="newPassword" value="attacker1" />
      <input type="hidden" name="newPassword2" value="attacker1" />
      <input type="submit" value="Submit request" />
    </form>
  </body>
</html>
```

1.2. Always Validate Tokens

Reference	Risk Rating
Always Validate Tokens	**Low**
Tools Used	
Browser, Burp Suite	
Vulnerability Description	
The vulnerability is Cross-Site Request Forgery that makes victims load or execute unwanted things on web applications.	
How It Was Discovered	
Manual Analysis - Change password of victim using attacker CSRF poc generator and clear the token.	
Vulnerable URLs	
https://www.bugbountyhunter.org/internship_labs/HTML/csrf_lab/lab_2/index.php	
Consequences of not Fixing the Issue	
It is based on attacker intension, the attacker can possibly take full control of access to the system.	
Suggested Countermeasures	
Using CSRF Tokens.	
References	
https://owasp.org/www-community/attacks/csrf	

Proof of Concept

The proof of the above vulnerability.

1.3. I Hate When Someone Uses My Tokens!

Reference	Risk Rating
I Hate When Someone Uses My Tokens!	**Medium**
Tools Used	
Browser, Burp Suite	
Vulnerability Description	
The vulnerability is Cross-Site Request Forgery that makes victims load or execute unwanted things on web applications.	
How It Was Discovered	
Manual Analysis - Change the tokens of users.	
Vulnerable URLs	
https://www.bugbountyhunter.org/internship_labs/HTML/csrf_lab/lab_4/login.php	
Consequences of not Fixing the Issue	
It is based on attacker intension, the attacker can possibly take full control of access to the system.	
Suggested Countermeasures	
Using CSRF Tokens.	
References	
https://owasp.org/www-community/attacks/csrf	

Proof of Concept

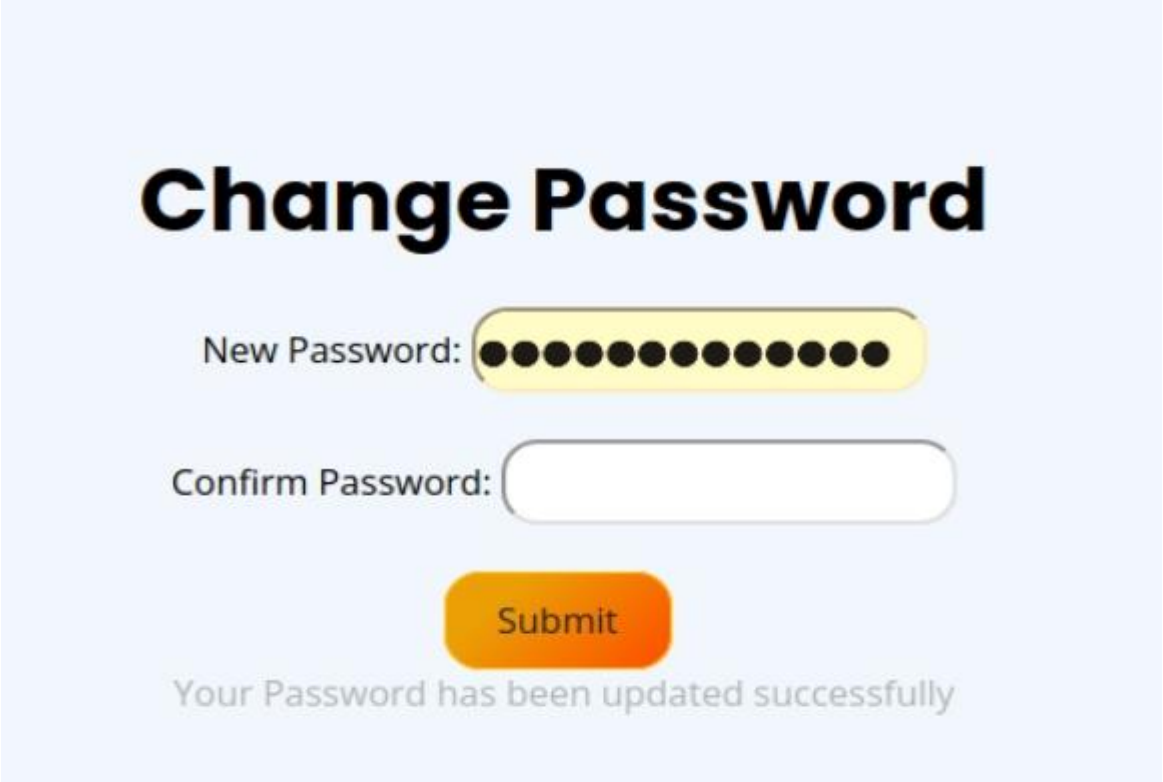
The proof of the above vulnerability.

1.4. GET Me Or POST ME

Reference	Risk Rating
GET Me Or POST ME	**Medium**
Tools Used	
Browser, Burp Suite	
Vulnerability Description	
The vulnerability is Cross-Site Request Forgery that makes victims load or execute unwanted things on web applications.	
How It Was Discovered	
Manual Analysis - Change the request method from POST to GET.	
Vulnerable URLs	
https://www.bugbountyhunter.org/internship_labs/HTML/csrf_lab/lab_6/login.php	
Consequences of not Fixing the Issue	
It is based on attacker intension, the attacker can possibly take full control of access to the system.	
Suggested Countermeasures	
Using CSRF Tokens.	
References	
https://owasp.org/www-community/attacks/csrf	

Proof of Concept

The proof of the above vulnerability.



1.5. XSS The Saviour

Reference	Risk Rating
XSS The Saviour	**High**
Tools Used	
Browser, Burp Suite	
Vulnerability Description	
The vulnerability is Cross-Site Request Forgery that makes victims load or execute unwanted things on web applications.	
How It Was Discovered	
Manual Analysis - Inject XSS script on attacker and generate CSRF poc then use it on victim account.	
Vulnerable URLs	
https://www.bugbountyhunter.org/internship_labs/HTML/csrf_lab/lab_7/login.php	
Consequences of not Fixing the Issue	
It is based on attacker intension, the attacker can possibly take full control of access to the system.	
Suggested Countermeasures	
Using CSRF Tokens.	
References	
https://owasp.org/www-community/attacks/csrf	

Proof of Concept

The proof of the above vulnerability.

```
<html>
  <!-- CSRF PoC - generated by Burp Suite Professional -->
  <body>
  <script>history.pushState('', '', '/')</script>
    <form action="https://www.bugbountyhunter.org/internship_labs/HTML/csrf_lab/lab_7/lab_7.php">
      <input type="hidden" name="name" value="
&lt;script&gt;alert&#40;document&#46;cookie&#41;&lt;&#47;script&gt;" />
      <input type="hidden" name="show" value="Save" />
      <input type="submit" value="Submit request" />
    </form>
  </body>
</html>
```

1.6. Rm -Rf Token

Reference	Risk Rating
Rm -Rf Token	**High**
Tools Used	
Browser, Burp Suite	
Vulnerability Description	
The vulnerability is Cross-Site Request Forgery that makes victims load or execute unwanted things on web applications.	
How It Was Discovered	
Manual Analysis - Remove the CSRF token and send the request.	
Vulnerable URLs	
https://www.bugbountyhunter.org/internship_labs/HTML/csrf_lab/lab_8/login.php	
Consequences of not Fixing the Issue	
It is based on attacker intension, the attacker can possibly take full control of access to the system.	
Suggested Countermeasures	
Using CSRF Tokens.	
References	
https://owasp.org/www-community/attacks/csrf	

Proof of Concept

The proof of the above vulnerability.