Week 4
Penetration Testing Report

Introduction

This report document hereby describes the proceedings and results of a Black Box security assessment conducted against the **Week 4 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 4 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	**Exchangeable Image File Format and Open Redirect**

3. Summary

Outlined is a Black Box Application Security assessment for the **Week 4 Labs**.

Total number of Sub-labs: 9 Sub-labs

High	Medium	Low
3	2	4

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**

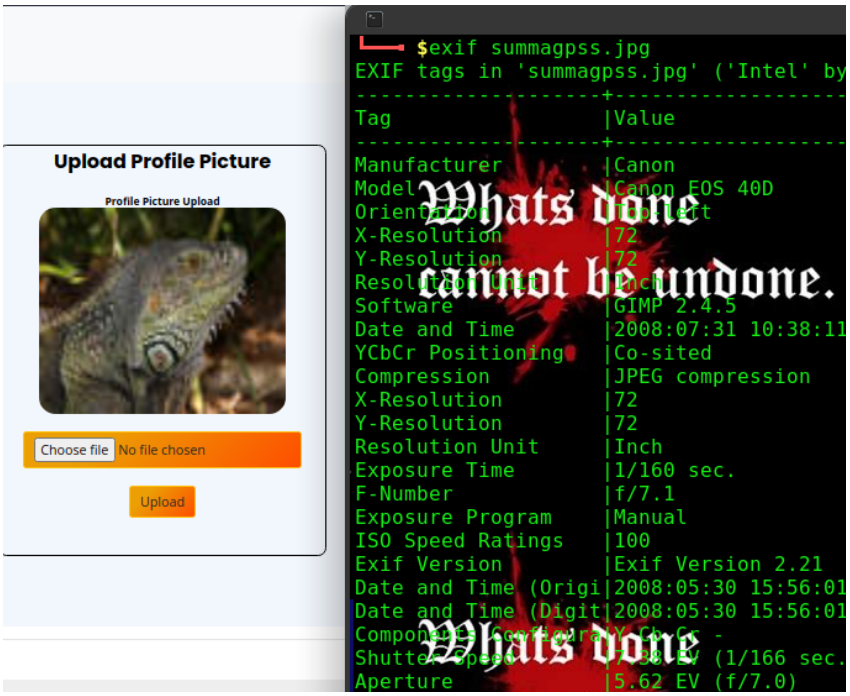
1. Exchangeable Image File Format

1.1. Let's PII!

Reference	Risk Rating
Let's PII!	**Low**
Tools Used	
Browser, EXIF Tool	
Vulnerability Description	
EXIF is a vulnerability where we can get sensitive information from the picture.	
How It Was Discovered	
Manual Analysis - Copy the url of the image and analyse it with EXIF tool.	
Vulnerable URLs	
https://www.bugbountyhunter.org/internship_labs/HTML/exif_lab/lab_1/exif.php	
Consequences of not Fixing the Issue	
The attacker can gain sensitive information from the images.	
Suggested Countermeasures	
Strip the data from the image.	
References	
https://www.softwaretestinghelp.com/exif-tutorial/	

Proof of Concept

The proof of the above vulnerability.



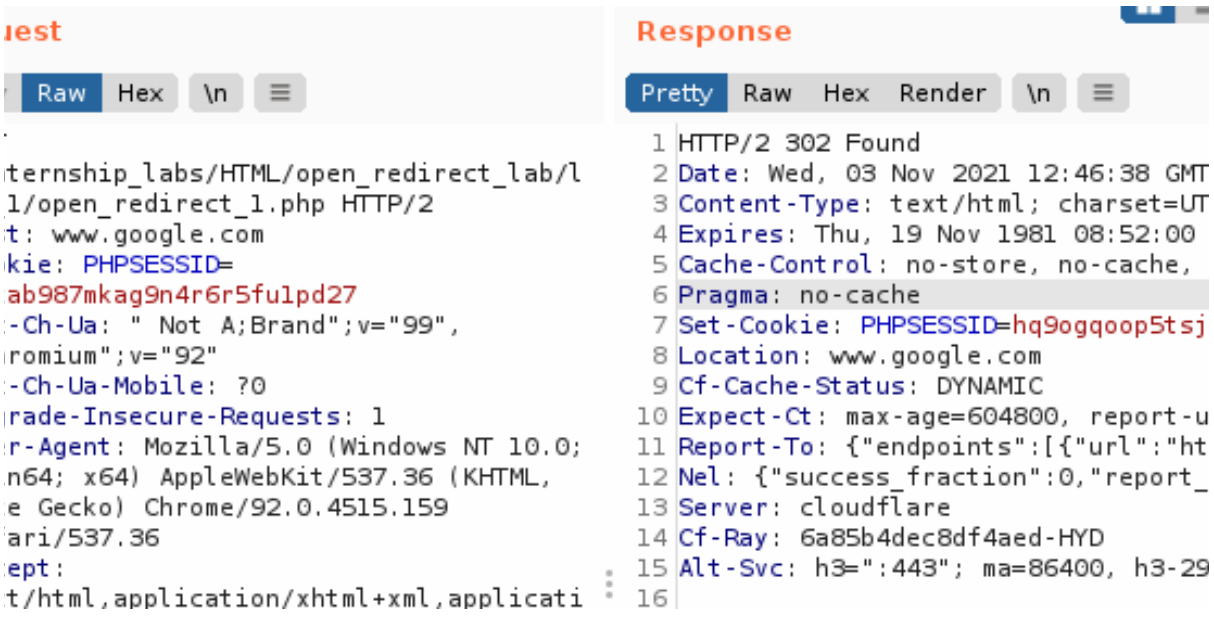
2. Open Redirect

2.1. A Simple Host!

Reference	Risk Rating
A Simple Host!	**Low**
Tools Used	
Browser, Burp Suite	
Vulnerability Description	
Open Redirect is a vulnerability that makes the user redirect to a malicious website without the knowledge.	
How It Was Discovered	
Manual Analysis- Change the host header with the malicious website.	
Vulnerable URLs	
https://www.bugbountyhunter.org/internship_labs/	
Consequences of not Fixing the Issue	
Phishing attack	
Suggested Countermeasures	
Input validation	
References	
https://cheatsheetseries.owasp.org/cheatsheets/Unvalidated_Redirects_and_Forwards_Cheat_Sheet.html	

Proof of Concept

The proof of the above vulnerability.

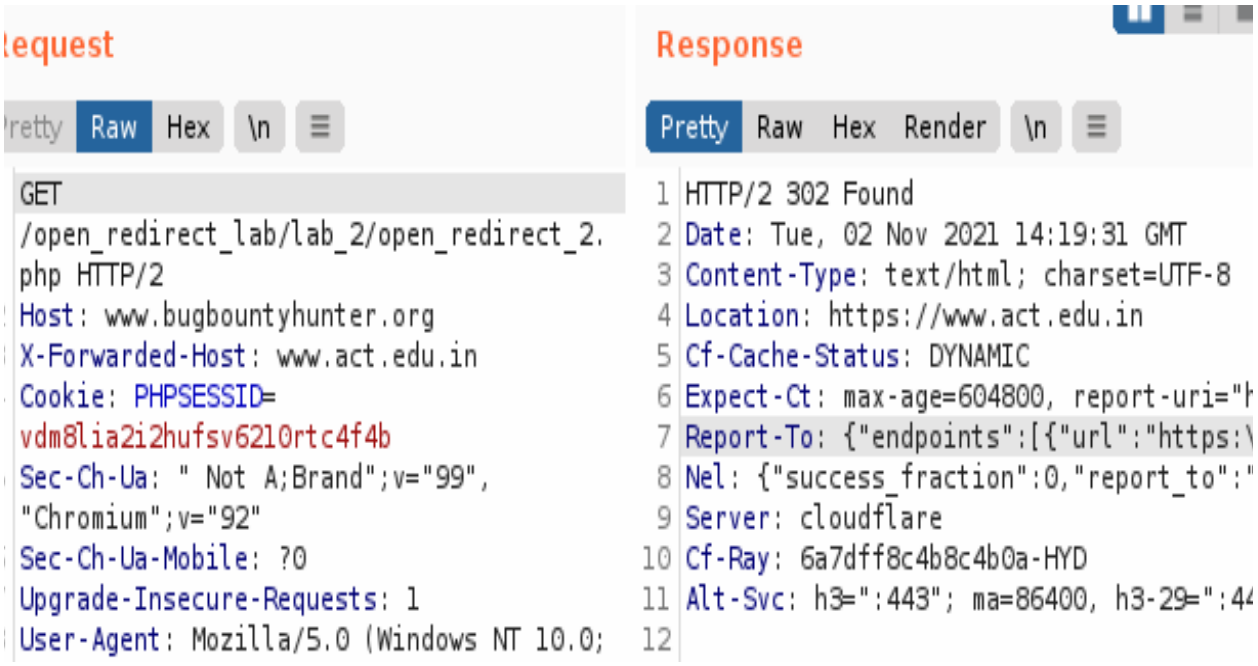


2.2. Story Of A Beautiful Header!

Reference	Risk Rating
Story Of A Beautiful Header!	**Low**
Tools Used	
Browser, Burp Suite	
Vulnerability Description	
Open Redirect is a vulnerability that makes the user redirect to a malicious website without the knowledge.	
How It Was Discovered	
Manual Analysis - Add http forward header and enter malicious site url.	
Vulnerable URLs	
https://www.bugbountyhunter.org/internship_labs/HTML/open_redirect_lab/lab_2/open_redirect_2.php	
Consequences of not Fixing the Issue	
Phishing attack	
Suggested Countermeasures	
Input Validation	
References	
https://cheatsheetseries.owasp.org/cheatsheets/Unvalidated_Redirects_and_Forwards_Cheat_Sheet.html	

Proof of Concept

The proof of the above vulnerability.

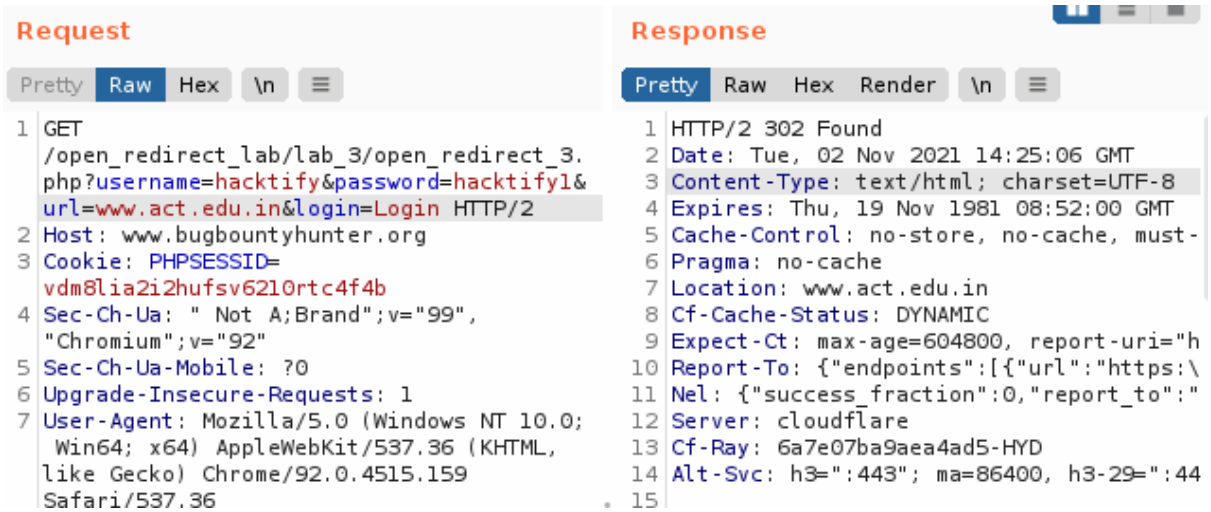


2.3. Sanitize Params!!

Reference	Risk Rating
Sanitize Params!!	**Medium**
Tools Used	
Browser, Burp Suite	
Vulnerability Description	
Open Redirect is a vulnerability that makes the user redirect to a malicious website without the knowledge.	
How It Was Discovered	
Manual Analysis - Edit the url param with malicious url.	
Vulnerable URLs	
https://www.bugbountyhunter.org/internship_labs/HTML/open_redirect_lab/lab_3/open_redirect_3.php	
Consequences of not Fixing the Issue	
Phishing attack	
Suggested Countermeasures	
Input Validation	
References	
https://cheatsheetseries.owasp.org/cheatsheets/Unvalidated_Redirects_and_Forwards_Cheat_Sheet.html	

Proof of Concept

The proof of the above vulnerability.

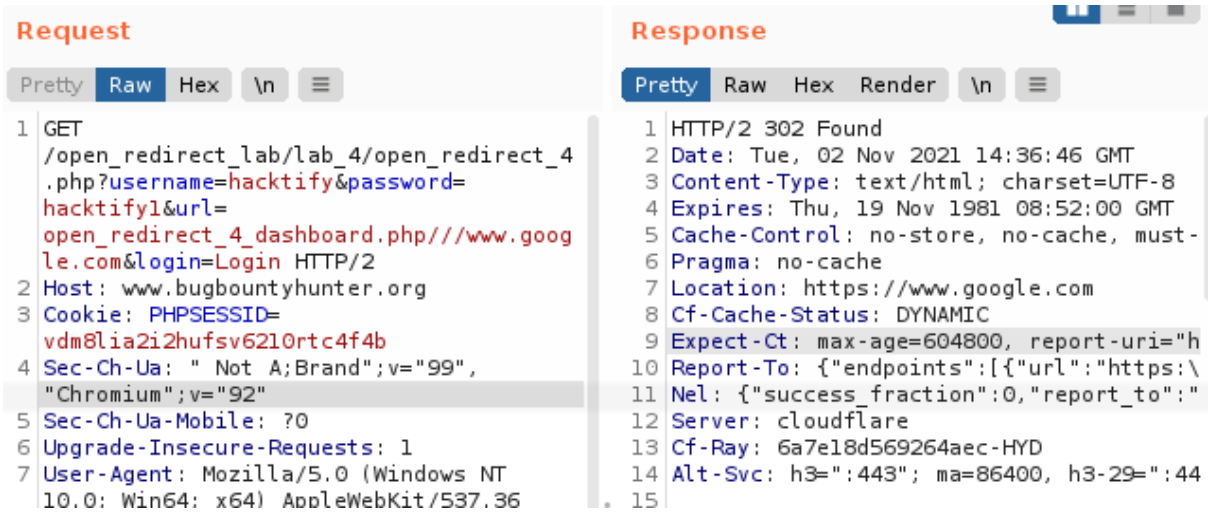


2.4. Patterns Are Important!

Reference	Risk Rating
Patterns Are Important!	**Medium**
Tools Used	
Browser, Burp Suite	
Vulnerability Description	
Open Redirect is a vulnerability that makes the user redirect to a malicious website without the knowledge.	
How It Was Discovered	
Manual Analysis - Edit the url param with /// and add the malicious site url.	
Vulnerable URLs	
https://www.bugbountyhunter.org/internship_labs/HTML/open_redirect_lab/lab_4/open_redirect_4.php	
Consequences of not Fixing the Issue	
Phishing attack	
Suggested Countermeasures	
Input Validation	
References	
https://cheatsheetseries.owasp.org/cheatsheets/Unvalidated_Redirects_and_Forwards_Cheat_Sheet.html	

Proof of Concept

The proof of the above vulnerability.

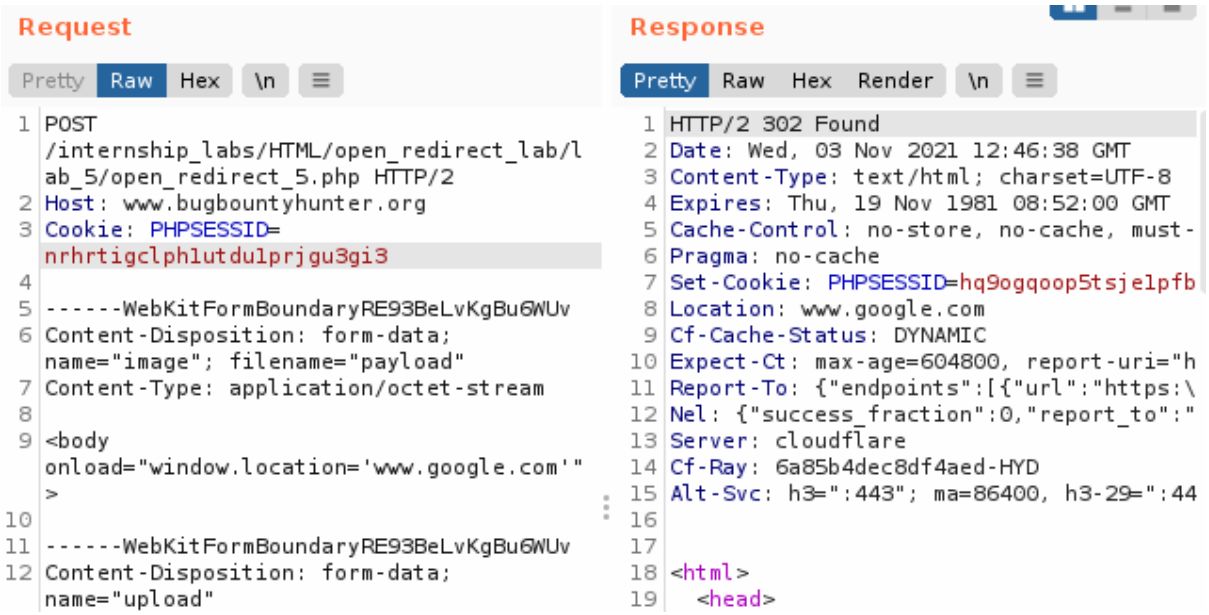


2.5. File Upload!? Redirect IT!

Reference	Risk Rating
File Upload!? Redirect IT!	**Low**
Tools Used	
Browser, Burp Suite	
Vulnerability Description	
Open Redirect is a vulnerability that makes the user redirect to a malicious website without the knowledge.	
How It Was Discovered	
Manual Analysis - Edit file with payload and upload it.	
Vulnerable URLs	
https://www.bugbountyhunter.org/internship_labs/HTML/open_redirect_lab/lab_5/open_redirect_5.php	
Consequences of not Fixing the Issue	
Phishing attack	
Suggested Countermeasures	
Input Validation	
References	
https://cheatsheetseries.owasp.org/cheatsheets/Unvalidated_Redirects_and_Forwards_Cheat_Sheet.html	

Proof of Concept

The proof of the above vulnerability.

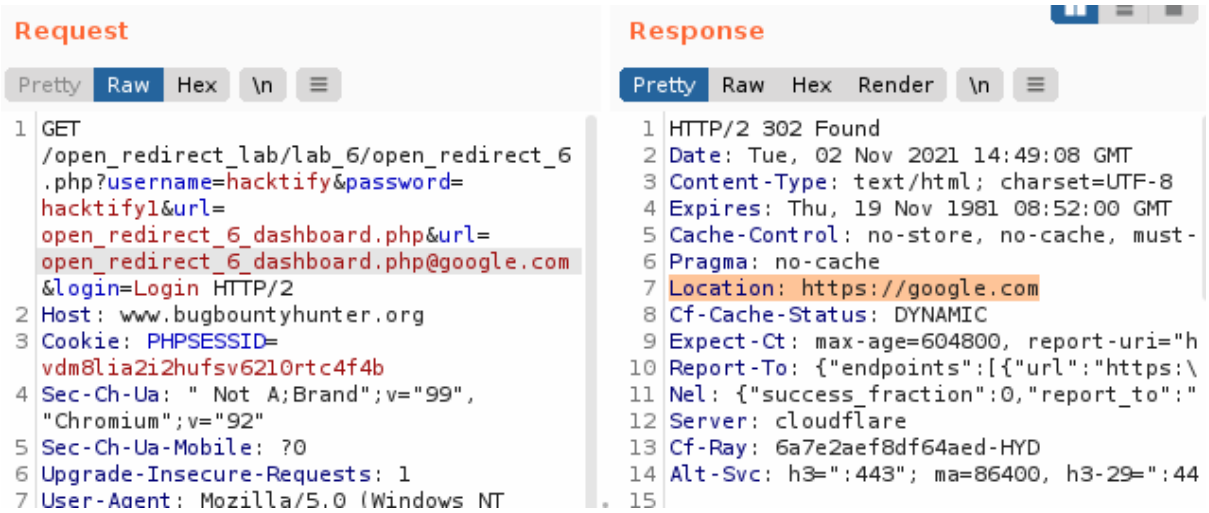


2.6. Same Param Twice!

Reference	Risk Rating
Same Param Twice!	**High**
Tools Used	
Browser, Burp Suite	
Vulnerability Description	
Open Redirect is a vulnerability that makes the user redirect to a malicious website without the knowledge.	
How It Was Discovered	
Manual Analysis - Add url param twice and edit the second with the malicious url.	
Vulnerable URLs	
https://www.bugbountyhunter.org/internship_labs/HTML/open_redirect_lab/lab_6/open_redirect_6.php	
Consequences of not Fixing the Issue	
Phishing attack	
Suggested Countermeasures	
Input Validation	
References	
https://cheatsheetseries.owasp.org/cheatsheets/Unvalidated_Redirects_and_Forwards_Cheat_Sheet.html	

Proof of Concept

The proof of the above vulnerability.

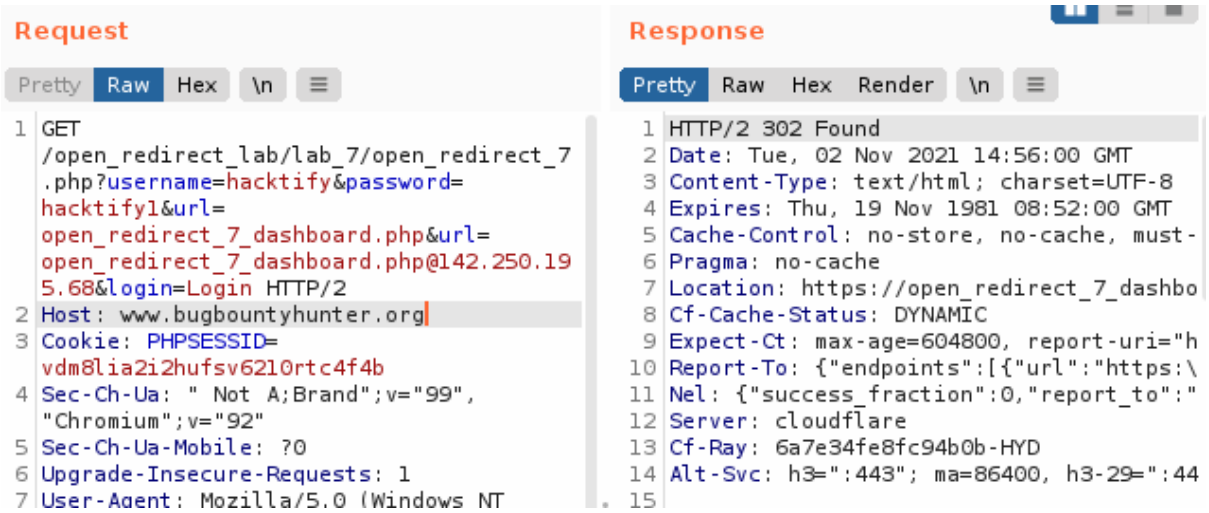


2.7. Domains? Not Always!

Reference	Risk Rating
Domains? Not Always!	**High**
Tools Used	
Browser, Burp Suite	
Vulnerability Description	
Open Redirect is a vulnerability that makes the user redirect to a malicious website without the knowledge.	
How It Was Discovered	
Manual Analysis - Add url param twice and edit the second with the ip address of a malicious website.	
Vulnerable URLs	
https://www.bugbountyhunter.org/internship_labs/HTML/open_redirect_lab/lab_7/open_redirect_7.php	
Consequences of not Fixing the Issue	
Phishing attack	
Suggested Countermeasures	
Input Validation	
References	
https://cheatsheetseries.owasp.org/cheatsheets/Unvalidated_Redirects_and_Forwards_Cheat_Sheet.html	

Proof of Concept

The proof of the above vulnerability.



2.8. Style Digit Symbols < 3

Reference	Risk Rating
Story Of A Beautiful Header!	**High**
Tools Used	
Browser, Burp Suite	
Vulnerability Description	
Open Redirect is a vulnerability that makes the user redirect to a malicious website without the knowledge.	
How It Was Discovered	
Manual Analysis - Edit the url param with the ip address of a malicious website.	
Vulnerable URLs	
https://www.bugbountyhunter.org/internship_labs/HTML/open_redirect_lab/lab_8/open_redirect_8.php	
Consequences of not Fixing the Issue	
Phishing attack	
Suggested Countermeasures	
Input Validation	
References	
https://cheatsheetseries.owasp.org/cheatsheets/Unvalidated_Redirects_and_Forwards_Cheat_Sheet.html	

Proof of Concept

The proof of the above vulnerability.