# 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** | **{Open Redirect Labs}, {Exchangeable Image File Format Labs}** |

## 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**

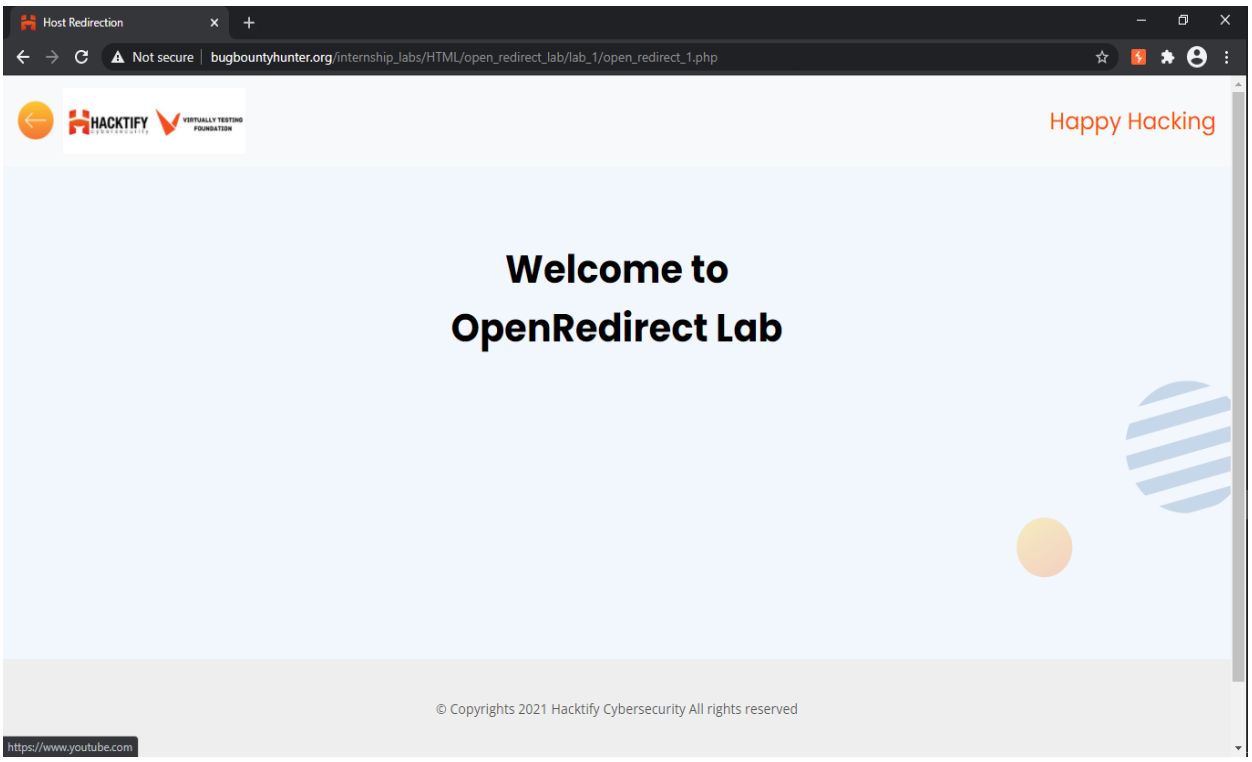
**Low** - **Number of Sub-labs with Easy difficulty level**

# 1. {Open Redirect Labs}

## 1.1. {A Simple Host!}

| Reference | Risk Rating |
|---|---|
| A Simple Host! | **Low** |
| **Tools Used** | |
| Google Chrome and Burp Suite | |
| **Vulnerability Description** | |
| I found this vulnerability using the burp suite tool by intercepting it. | |
| **How It Was Discovered** | |
| Manual Analysis and Automated Analysis | |
| **Vulnerable URLs** | |
| https://www.bugbountyhunter.org/internship_labs/HTML/open_redirect_lab/lab_1/open_redirect_1.php | |
| **Consequences of not Fixing the Issue** | |
| An attacker can use this vulnerability to redirect users to other malicious websites, which can lead to phishing or other similar attacks. | |
| **Suggested Countermeasures** | |
| Maintain a server-side list of all URLs that are permitted for redirection. Instead of passing the target URL as a parameter to a redirector, pass an index into the list. | |
| **References** | |
| https://cheatsheetseries.owasp.org/cheatsheets/Unvalidated_Redirects_and_Forwards_Cheat_Sheet.html | |

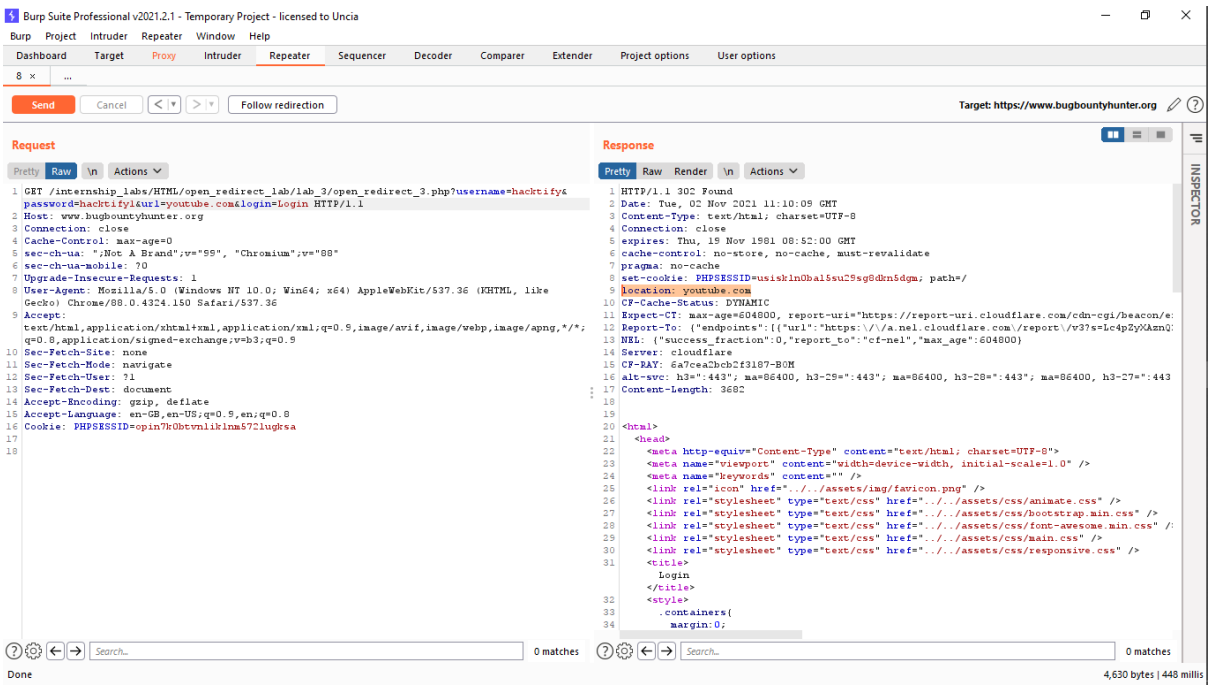
## Proof of Concept



## 1.2. {Story of a beautiful header!}

| Reference | Risk Rating |
|---|---|
| Story of a beautiful header | **Low** |
| **Tools Used** | |
| Google Chrome and Burp Suite | |
| **Vulnerability Description** | |
| I found this vulnerability by intercepting a redirect request into burp suite and inserting payload into it and then by forwarding through repeater by verifying the location of the payload result. | |
| **How It Was Discovered** | |
| Manual Analysis and Automated Analysis | |
| **Vulnerable URLs** | |
| https://www.bugbountyhunter.org/internship_labs/HTML/open_redirect_lab/lab_2/open_redirect_2.php | |
| **Consequences of not Fixing the Issue** | |
| An attacker can use this vulnerability to redirect users to other malicious websites, which can lead to phishing or other similar attacks. | |
| **Suggested Countermeasures** | |
| Remove the redirection function from the application, and replace links to it with direct links to the relevant target URLs. | |
| **References** | |
| https://cheatsheetseries.owasp.org/cheatsheets/Unvalidated_Redirects_and_Forwards_Cheat_Sheet.html | |

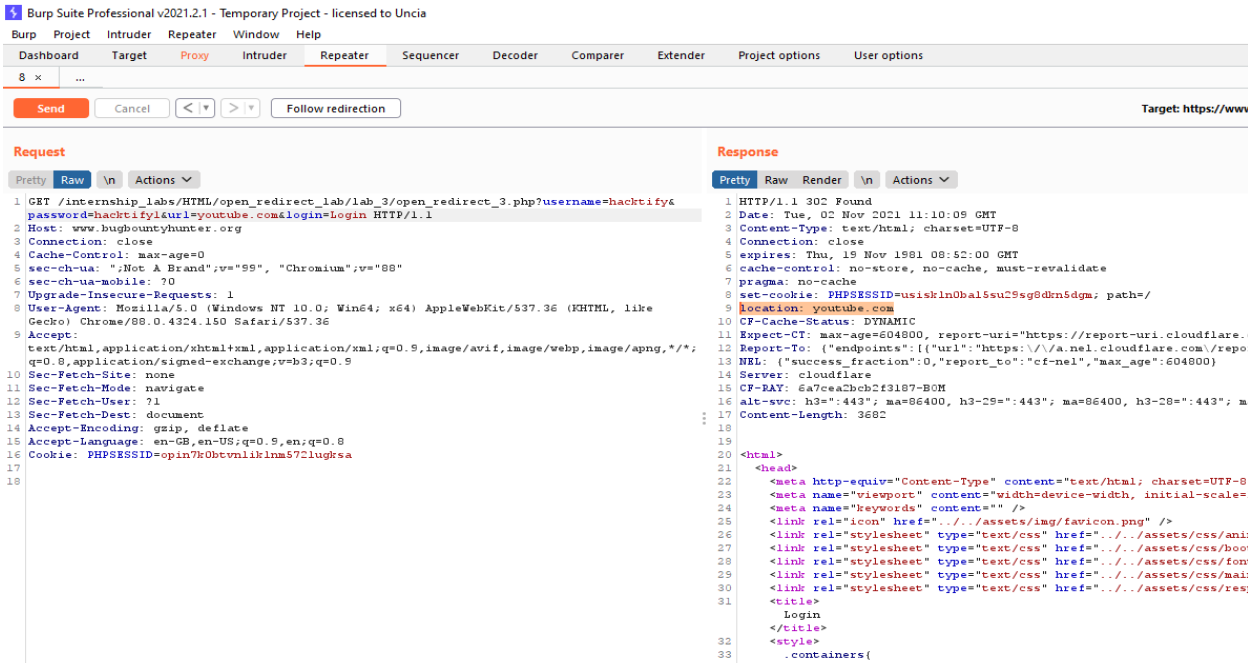
## Proof of Concept



## 1.3. {Sanitize Params!!}

| Reference | Risk Rating |
|---|---|
| Sanitize params!! | **Medium** |
| **Tools Used** | |
| Google Chrome and Burp Suite | |
| **Vulnerability Description** | |
| I found this vulnerability by intercepting a redirect request into burp suite and inserting payload into it and then by forwarding through repeater by verifying the location of the payload result. | |
| **How It Was Discovered** | |
| Manual Analysis and Automated Analysis | |
| **Vulnerable URLs** | |
| https://www.bugbountyhunter.org/internship_labs/HTML/open_redirect_lab/lab_3/open_redirect_3_dashboard.php | |
| **Consequences of not Fixing the Issue** | |
| An attacker can use this vulnerability to redirect users to other malicious websites, which can lead to phishing or other similar attacks. | |
| **Suggested Countermeasures** | |
| The application should use relative URLs in all of its redirects, and the redirection function should strictly validate that the URL received is a valid URL. | |
| **References** | |
| https://cheatsheetseries.owasp.org/cheatsheets/Unvalidated_Redirects_and_Forwards_Cheat_Sheet.html | |

## Proof of Concept



## 1.4. {Patterns are important!!}

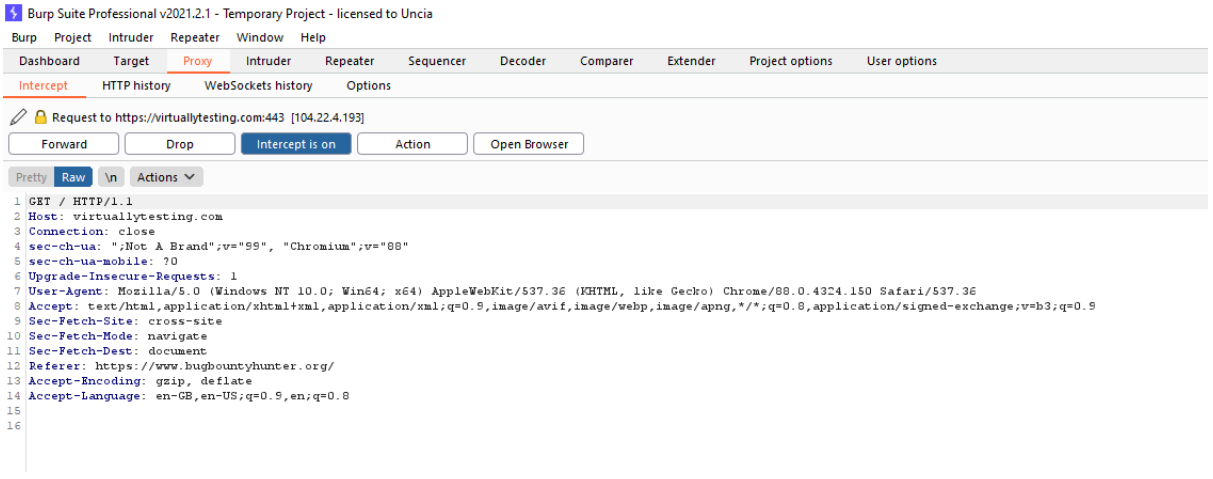
| Reference | Risk Rating |
|---|---|
| Patterns are important!! | **Medium** |
| **Tools Used** | |
| Google Chrome and Burp Suite | |
| **Vulnerability Description** | |
| I found this vulnerability by inserting payload at the end of link by adding “?” and then followed by a payload. | |
| **How It Was Discovered** | |
| Manual Analysis and Automated Analysis | |
| **Vulnerable URLs** | |
| https://www.bugbountyhunter.org/internship_labs/HTML/open_redirect_lab/lab_4/open_redirect_4.php///youtube.com | |
| **Consequences of not Fixing the Issue** | |
| An attacker can use this vulnerability to redirect users to other malicious websites, which can lead to phishing or other similar attacks. | |
| **Suggested Countermeasures** | |
| Maintain a server-side list of all URLs that are permitted for redirection. Instead of passing the target URL as a parameter to a redirector, pass an index into the list. | |
| **References** | |
| https://cheatsheetseries.owasp.org/cheatsheets/Unvalidated_Redirects_and_Forwards_Cheat_Sheet.html | |

## Proof of Concept

## 1.5. {File Upload? Redirect IT!}

| Reference | Risk Rating |
|---|---|
| File upload? Redirect IT! | **Low** |
| **Tools Used** | |
| Google Chrome and Burp Suite | |
| **Vulnerability Description** | |
| I found this vulnerability by intercepting a file upload request into burp suite and changing file name to make it vulnerable. | |
| **How It Was Discovered** | |
| Manual Analysis and Automated Analysis | |
| **Vulnerable URLs** | |
| https://virtuallytesting.com/ | |
| **Consequences of not Fixing the Issue** | |
| An attacker can use this vulnerability to redirect users to other malicious websites, which can lead to phishing or other similar attacks. | |
| **Suggested Countermeasures** | |
| Maintain a server-side list of all URLs that are permitted for redirection. Instead of passing the target URL as a parameter to a redirector, pass an index into the list. | |
| **References** | |
| https://cheatsheetseries.owasp.org/cheatsheets/Unvalidated_Redirects_and_Forwards_Cheat_Sheet.html | |

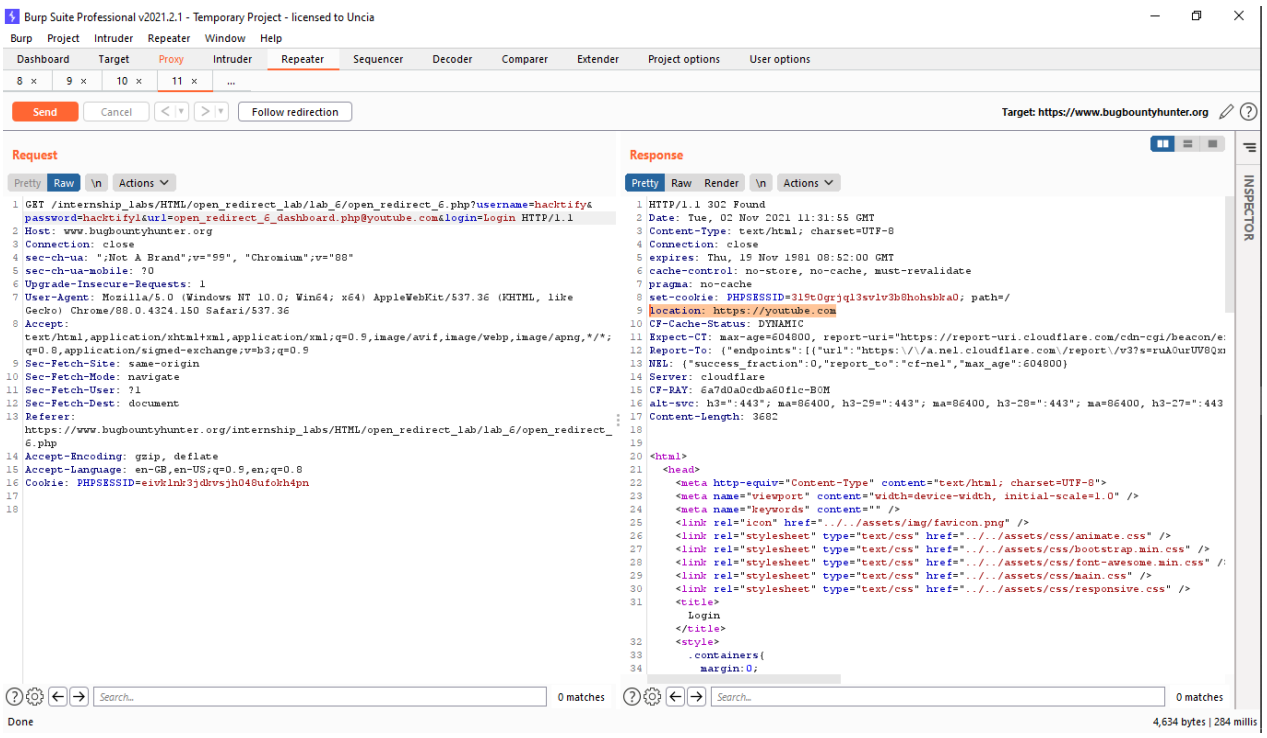
## Proof of Concept



## 1.6. {Same Param Twice!}

| Reference | Risk Rating |
|---|---|
| Same Param Twice! | **High** |
| **Tools Used** | |
| Google Chrome and Burp Suite | |
| **Vulnerability Description** | |
| I found this vulnerability by intercepting a redirect request into burp suite and inserting payload into it and then by forwarding through repeater by verifying the location of the payload result. | |
| **How It Was Discovered** | |
| Manual Analysis and Automated Analysis | |
| **Vulnerable URLs** | |
| https://www.bugbountyhunter.org/internship_labs/HTML/open_redirect_lab/lab_6/open_redirect_6_dashboard.php | |
| **Consequences of not Fixing the Issue** | |
| An attacker can use this vulnerability to redirect users to other malicious websites, which can lead to phishing or other similar attacks. | |
| **Suggested Countermeasures** | |
| Remove the redirection function from the application, and replace links to it with direct links to the relevant target URLs. | |
| **References** | |
| https://cheatsheetseries.owasp.org/cheatsheets/Unvalidated_Redirects_and_Forwards_Cheat_Sheet.html | |

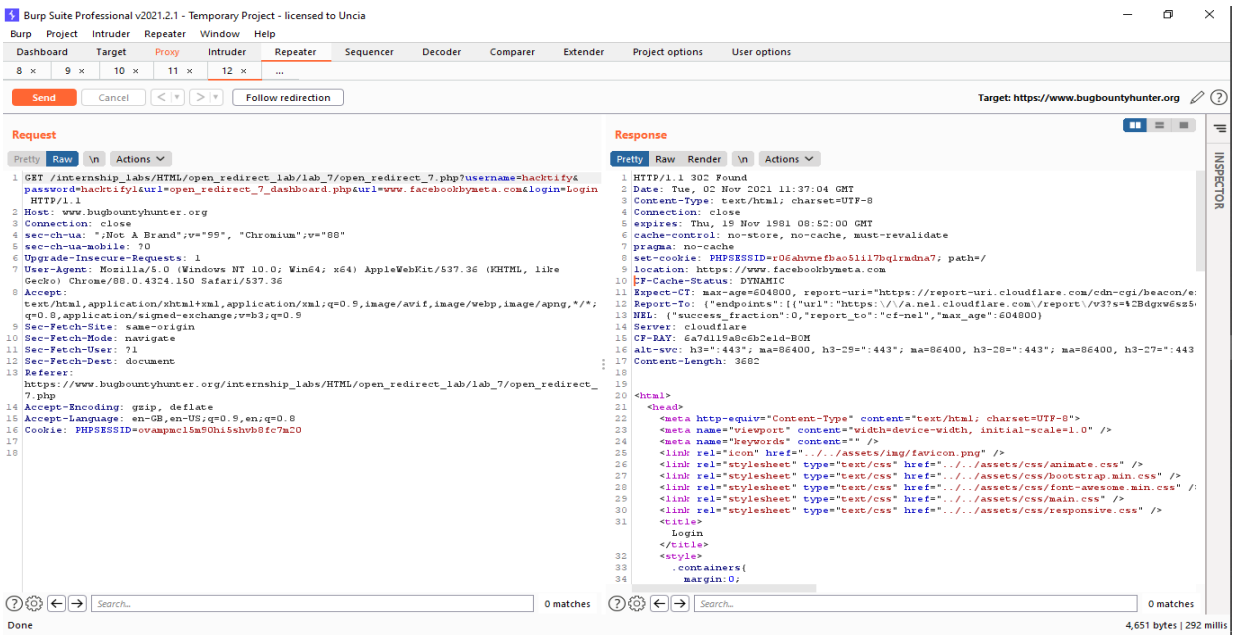
## Proof of Concept



## 1.7. {Domains? Not Always!}

| Reference | Risk Rating |
|---|---|
| Domains? Not Always! | **High** |
| **Tools Used** | |
| Google Chrome and Burp Suite | |
| **Vulnerability Description** | |
| I found this vulnerability by intercepting a redirect request into burp suite and inserting payload into it and then by forwarding through repeater by verifying the location of the payload result. | |
| **How It Was Discovered** | |
| Manual Analysis and Automated Analysis | |
| **Vulnerable URLs** | |
| https://www.bugbountyhunter.org/internship_labs/HTML/open_redirect_lab/lab_7/open_redirect_7_dashboard.php&url=google.co,m&login=Login | |
| **Consequences of not Fixing the Issue** | |
| An attacker can use this vulnerability to redirect users to other malicious websites, which can lead to phishing or other similar attacks. | |
| **Suggested Countermeasures** | |
| Maintain a server-side list of all URLs that are permitted for redirection. Instead of passing the target URL as a parameter to a redirector, pass an index into the list. | |
| **References** | |
| https://cheatsheetseries.owasp.org/cheatsheets/Unvalidated_Redirects_and_Forwards_Cheat_Sheet.html | |

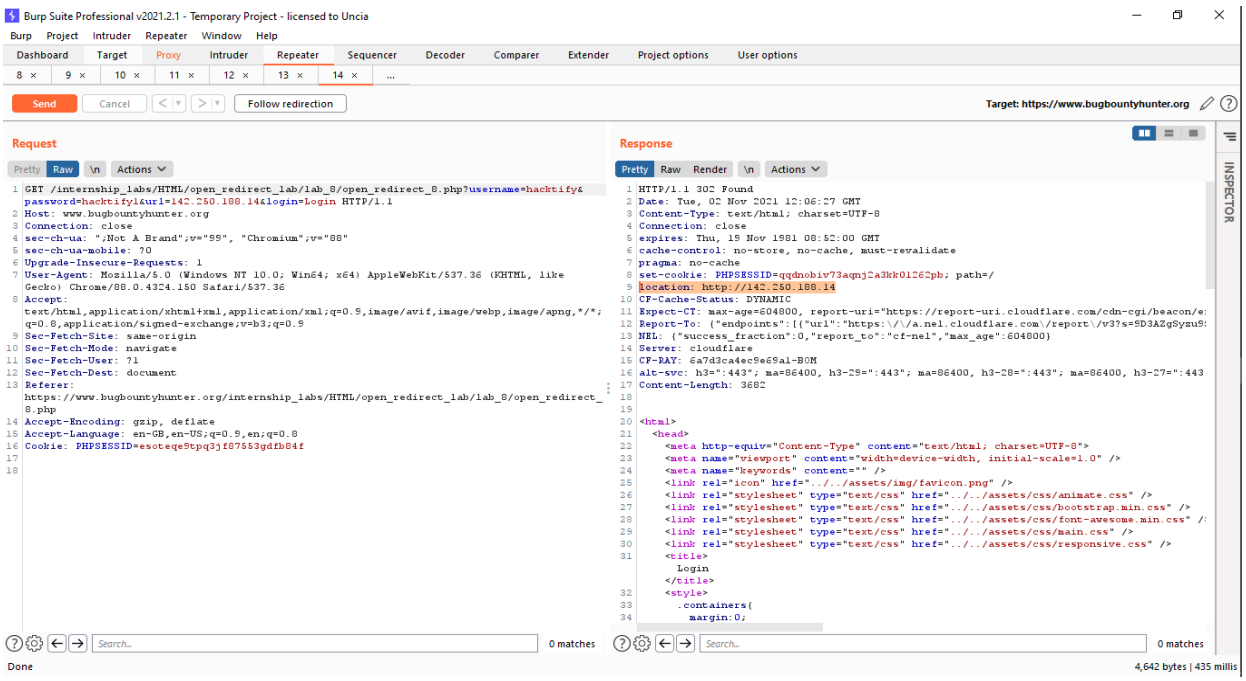
## Proof of Concept



## 1.8. {Style digit symbols < 3}

| Reference | Risk Rating |
|---|---|
| Style digit symbols < 3 | **High** |
| **Tools Used** | |
| Google Chrome and Burp Suite | |
| **Vulnerability Description** | |
| I found this vulnerability by intercepting a redirect request into burp suite and inserting IP Address as payload into it and then by forwarding through repeater by verifying the location of the payload result. | |
| **How It Was Discovered** | |
| Manual Analysis and Automated Analysis | |
| **Vulnerable URLs** | |
| https://www.bugbountyhunter.org/internship_labs/HTML/open_redirect_lab/lab_8/open_redirect_8.php<br>https://www.google.com/?gws_rd=ssl | |
| **Consequences of not Fixing the Issue** | |
| An attacker can use this vulnerability to redirect users to other malicious websites, which can lead to phishing or other similar attacks. | |
| **Suggested Countermeasures** | |
| Remove the redirection function from the application, and replace links to it with direct links to the relevant target URLs. | |
| **References** | |
| https://cheatsheetseries.owasp.org/cheatsheets/Unvalidated_Redirects_and_Forwards_Cheat_Sheet.html | |

## Proof of Concept



# 2. {Exchangeable Image File Format Labs}

## 2.1. Lets PII!

| Reference | Risk Rating |
|---|---|
| Lets PII! | **Low** |
| **Tools Used** | |
| Google Chrome | |
| **Vulnerability Description** | |
| I found this vulnerability by uploading an image into the profile photo section. I found the entry point for EXIF in the profile photo upload section. This allowed me to upload images containing sensitive data. | |
| **How It Was Discovered** | |
| Manual Analysis | |
| **Vulnerable URLs** | |
| https://www.bugbountyhunter.org/internship_labs/HTML/exif_lab/lab_1/exif.php | |
| **Consequences of not Fixing the Issue** | |
| This vulnerability violates the privacy of a user and shares sensitive information of the user who uploaded an image on the vulnerable websites. | |
| **Suggested Countermeasures** | |
| Disable geotagging on the digital device you use to take photographs. | |
| **References** | |
| https://photographylife.com/what-is-exif-data | |

## Proof of Concept