

Week 5 Penetration Testing Report

Introduction

This report document hereby describes the proceedings and results of a Black Box security assessment conducted against the **Week 5 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 5 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-Origin Resource Sharing Labs}
------------------	--------------------------------------

3. Summary

Outlined is a Black Box Application Security assessment for the **Week 5 Labs**.

Total number of Sub-labs: 7 Sub-labs

High	Medium	Low
3	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-Origin Resource Sharing Labs}

1.1. {CORS with Arbitrary Origin}

Reference	Risk Rating
CORS with Arbitrary Origin	Low
Tools Used	
Google Chrome Browser, CORS tool, Burp Suite	
Vulnerability Description	
I found this vulnerability by intercepting a login request into burp suite and adding origin header to the interception and forwarding it and successfully getting expected output.	
How It Was Discovered	
Manual Analysis	
Vulnerable URLs	
https://www.bugbountyhunter.org/internship_labs/HTML/cors_lab/lab_1/login.php	
Consequences of not Fixing the Issue	
Attackers would treat many victims to visit the attacker's website, if the victim is logged in, then his personal information is recorded in the attacker's server. Attackers can perform any action in the user's account, by bypassing CSRF tokens.	
Suggested Countermeasures	
Only Allow trusted sites.	
References	
https://portswigger.net/web-security/cors	

Proof of Concept

Request	Response
<pre>1 GET /internship_labs/HTML/cors_lab/lab_1/cors_1.php HTTP/1.1 2 Host: www.bugbountyhunter.org 3 Connection: close 4 sec-ch-ua: "Not A Brand";v="99", "Chromium";v="88" 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/88.0.4324.150 Safari/537.36 8 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 9 Origin: attacker.com 10 Sec-Fetch-Site: same-origin 11 Sec-Fetch-Mode: navigate 12 Sec-Fetch-User: ?1 13 Sec-Fetch-Dest: document 14 Referer: https://www.bugbountyhunter.org/internship_labs/HTML/cors_lab/lab_1/ 15 Accept-Encoding: gzip, deflate 16 Accept-Language: en-US,en-US;q=0.9,en;q=0.8 17 Cookie: PHPSESSID=suirtu74kshod8bptv6gmenml 18 19</pre>	<pre>1 HTTP/1.1 200 OK 2 Date: Mon, 08 Nov 2021 12:31:03 GMT 3 Content-Type: text/html; charset=UTF-8 4 Connection: close 5 expires: Thu, 19 Nov 1981 08:52:00 GMT 6 cache-control: no-store, no-cache, must-revalidate 7 pragma: no-cache 8 set-cookie: PHPSESSID=ms6j7z5203ncr805sonvne80fu; path=/ 9 access-control-allow-credentials: true 10 access-control-allow-origin: attacker.com 11 vary: Accept-Encoding 12 CF-Cache-Status: DYNAMIC 13 Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" 14 Report-To: ({"endpoints":[{"url":"https://a.nel.cloudflare.com/report/v3?s=Gd1Z5KyMlar5JQA:" 15 NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} 16 Server: cloudflare 17 CF-RAY: 6aaed0ecd7b70db0-BOM 18 alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400 19 Content-Length: 2573 20 21 <html> 22 <head> 23 <meta charset="UTF-8" /> 24 <meta name="viewport" content="width=device-width, initial-scale=1.0" /> 25 <meta name="keywords" content="" /> 26 <link rel="icon" href="../../assets/img/favicon.png" /> 27 <link rel="stylesheet" type="text/css" href="../../assets/css/animate.css" /> 28 <link rel="stylesheet" type="text/css" href="../../assets/css/bootstrap.min.css" /> 29 <link rel="stylesheet" type="text/css" href="../../assets/css/font-awesome.min.css" /> 30 <link rel="stylesheet" type="text/css" href="../../assets/css/main.css" /> 31 <link rel="stylesheet" type="text/css" href="../../assets/css/responsive.css" /> 32 <title> 33 <style> 34 .containers{</pre>

1.2. { CORS with null origin }

Reference	Risk Rating
CORS with null origin	Low
Tools Used	
Google Chrome Browser, CORS tool, Burp Suite	
Vulnerability Description	
I found this vulnerability by intercepting a login request into burp suite and adding origin header to the interception and forwarding it and successfully getting expected output.	
How It Was Discovered	
Manual Analysis	
Vulnerable URLs	
https://www.bugbountyhunter.org/internship_labs/HTML/cors_lab/lab_2/login.php	
Consequences of not Fixing the Issue	
Attackers would treat many victims to visit the attacker's website, if the victim is logged in, then his personal information is recorded in the attacker's server. Attackers can perform any action in the user's account, by bypassing CSRF tokens.	
Suggested Countermeasures	
Avoid whitelisting null.	
References	
https://owasp.org/www-community/attacks/CORS_OriginHeaderScrutiny	

Proof of Concept

Request	Response
<pre>1 GET /internship_labs/HTML/cors_lab/lab_2/cors_2.php HTTP/1.1 2 Host: www.bugbountyhunter.org 3 Connection: close 4 sec-ch-ua: "Not A Brand";v="99", "Chromium";v="88" 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/88.0.4324.150 Safari/537.36 8 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 9 Origin: attacker.com 10 Sec-Fetch-Site: same-origin 11 Sec-Fetch-Mode: navigate 12 Sec-Fetch-User: ?1 13 Sec-Fetch-Dest: document 14 Referer: https://www.bugbountyhunter.org/internship_labs/HTML/cors_lab/lab_2/index.php 15 Accept-Encoding: gzip, deflate 16 Accept-Language: en-US,en-US;q=0.9,en;q=0.8 17 Cookie: PHPSESSID=0S2hs615aa3u8hfd9shar2u56b 18 19</pre>	<pre>1 HTTP/1.1 200 OK 2 Date: Mon, 08 Nov 2021 13:31:54 GMT 3 Content-Type: text/html; charset=UTF-8 4 Connection: close 5 expires: Thu, 19 Nov 1981 08:52:00 GMT 6 cache-control: no-store, no-cache, must-revalidate 7 pragma: no-cache 8 set-cookie: PHPSESSID=hw7spu1l07hbo0etj3j1b2h4mr; path=/ 9 access-control-allow-origin: null 10 access-control-allow-credentials: true 11 vary: Accept-Encoding 12 CF-Cache-Status: DYNAMIC 13 Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" 14 Report-To: {"endpoints":[{"url":"https://a.nel.cloudflare.com/report/v3?s=Tg9KRA2F5fyQ"}]} 15 NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} 16 Server: cloudflare 17 CF-RAY: 6aaf2a12e3d31cf-BOM 18 alt-svc: h3="443"; ma=86400, h3-29="443"; ma=86400, h3-28="443"; ma=86400, h3-27="443" 19 Content-Length: 2572 20 21 <html> 22 <head> 23 <meta charset="UTF-8" /> 24 <meta name="viewport" content="width=device-width, initial-scale=1.0" /> 25 <meta name="keywords" content="" /> 26 <link rel="icon" href="../../../assets/img/favicon.png" /> 27 <link rel="stylesheet" type="text/css" href="../../../assets/css/animate.css" /> 28 <link rel="stylesheet" type="text/css" href="../../../assets/css/bootstrap.min.css" /> 29 <link rel="stylesheet" type="text/css" href="../../../assets/css/font-awesome.min.css" /> 30 <link rel="stylesheet" type="text/css" href="../../../assets/css/main.css" /> 31 <link rel="stylesheet" type="text/css" href="../../../assets/css/responsive.css" /> 32 </head> 33 <title> 34 .containers{</pre>

1.3. { CORS with Prefix Match }

Reference	Risk Rating
CORS with Prefix Match	Medium
Tools Used	
Google Chrome Browser, CORS tool, Burp Suite	
Vulnerability Description	
I found this vulnerability by intercepting a login request into burp suite and adding origin header to the interception and forwarding it and successfully getting expected output.	
How It Was Discovered	
Manual Analysis	
Vulnerable URLs	
https://www.bugbountyhunter.org/internship_labs/HTML/cors_lab/lab_3/cors_3.php	
Consequences of not Fixing the Issue	
Attackers would treat many victims to visit the attacker's website, if the victim is logged in, then his personal information is recorded in the attacker's server. Attackers can perform any action in the user's account, by bypassing CSRF tokens.	
Suggested Countermeasures	
Proper configuration of cross-domains requests.	
References	
https://portswigger.net/web-security/cors	

Proof of Concept

The screenshot displays a network capture in Burp Suite, showing a successful CORS request and response. The request is a GET to `/internship_labs/HTML/cors_lab/lab_3/cors_3.php` with an `Origin` header set to `hacktify.in.evil.com`. The response is a 200 OK from `www.bugbountyhunter.org` with an `Access-Control-Allow-Origin` header set to `hacktify.in.evil.com`.

Request:

```
1 GET /internship_labs/HTML/cors_lab/lab_3/cors_3.php HTTP/1.1
2 Host: www.bugbountyhunter.org
3 Origin: hacktify.in.evil.com
4 Connection: close
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 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
10 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
11 Sec-Fetch-Site: none
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-User: ?1
14 Sec-Fetch-Dest: document
15 Accept-Encoding: gzip, deflate
16 Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
17 Cookie: PHPSESSID=hs2n7qa4ge6uk4c03kvt8gmx9v
18
19
```

Response:

```
1 HTTP/1.1 200 OK
2 Date: Wed, 10 Nov 2021 06:37:57 GMT
3 Content-Type: text/html; charset=UTF-8
4 Connection: close
5 expires: Thu, 19 Nov 1981 08:52:00 GMT
6 cache-control: no-store, no-cache, must-revalidate
7 pragma: no-cache
8 set-cookie: PHPSESSID=4su5b8030ac5a9d31dg9aih9u5; path=/
9 access-control-allow-credentials: true
10 access-control-allow-origin: hacktify.in.evil.com
11 vary: Accept-Encoding
12 CF-Cache-Status: DYNAMIC
13 Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct"
14 Report-To: {"endpoints":[{"url":"https://a.nel.cloudflare.com/report/v3?s=9Cz2m42BBpYH"}]}
15 NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
16 Server: cloudflare
17 CF-RAY: 6abd466cea210ead-BOM
18 alt-svc: h3="443", ma=86400, h3-29="443", ma=86400, h3-28="443", ma=86400, h3-27="443"
19 Content-Length: 2572
20
21 <html>
22 <head>
23 <meta charset="UTF-8" />
24 <meta name="viewport" content="width=device-width, initial-scale=1.0" />
25 <meta name="keywords" content="" />
26 <link rel="icon" href="..." />
27 <link rel="stylesheet" type="text/css" href="..." />
28 <link rel="stylesheet" type="text/css" href="..." />
29 <link rel="stylesheet" type="text/css" href="..." />
30 <link rel="stylesheet" type="text/css" href="..." />
31 <link rel="stylesheet" type="text/css" href="..." />
32 <title>
33 </title>
34 <style>
35 .containers{

```

1.4. { CORS with Suffix Match }

Reference	Risk Rating
CORS with Suffix Match	Medium
Tools Used	
Google Chrome Browser, CORS tool, Burp Suite	
Vulnerability Description	
I found this vulnerability by intercepting a login request into burp suite and adding origin header to the interception and forwarding it and successfully getting expected output.	
How It Was Discovered	
Manual Analysis	
Vulnerable URLs	
https://www.bugbountyhunter.org/internship_labs/HTML/cors_lab/lab_4/cors_4.php	
Consequences of not Fixing the Issue	
Attackers would treat many victims to visit the attacker's website, if the victim is logged in, then his personal information is recorded in the attacker's server. Attackers can perform any action in the user's account, by bypassing CSRF tokens.	
Suggested Countermeasures	
Only Allow trusted sites.	
References	
https://owasp.org/www-community/attacks/CORS-OriginHeaderScrutiny	

Proof of Concept

The screenshot displays the Burp Suite interface with a Request and Response view. The Request tab is active, showing a GET request to `/internship_labs/HTML/cors_lab/lab_4/cors_4.php` with a `Host: www.bugbountyhunter.org` and `Origin: evilhacktify.in`. The Response tab is also visible, showing an HTTP/1.1 200 OK response with a `Content-Type: text/html; charset=UTF-8` and a `Server: cloudflare`. The response body contains HTML code, including a `<head>` section with `<meta>` tags for charset, viewport, and keywords, and a `<link>` tag for a stylesheet.

```
Request
1 GET /internship_labs/HTML/cors_lab/lab_4/cors_4.php HTTP/1.1
2 Host: www.bugbountyhunter.org
3 Connection: close
4 Origin: evilhacktify.in
5 sec-ch-ua: "Not A Brand";v="99", "Chromium";v="88"
6 sec-ch-ua-mobile: ?0
7 Upgrade-Insecure-Requests: 1
8 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
9 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
10 Sec-Fetch-Site: none
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-User: ?1
13 Sec-Fetch-Dest: document
14 Accept-Encoding: gzip, deflate
15 Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
16 Cookie: PHPSESSID=dp3vh6Edma5C8ra85oldikib8k
17
18

Response
1 HTTP/1.1 200 OK
2 Date: Wed, 10 Nov 2021 06:36:15 GMT
3 Content-Type: text/html; charset=UTF-8
4 Connection: close
5 expires: Thu, 19 Nov 1991 08:52:00 GMT
6 cache-control: no-store, no-cache, must-revalidate
7 pragma: no-cache
8 set-cookie: PHPSESSID=qjlik2drsoedqsj5ropgdrjpv; path=/
9 access-control-allow-credentials: true
10 access-control-allow-origin: evilhacktify.in
11 vary: Accept-Encoding
12 CF-Cache-Status: DYNAMIC
13 Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct"
14 Report-To: {"endpoints":[{"url":"https://a.nel.cloudflare.com/report/v3?s=GRT32PAlDCoP:"
15 NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
16 Server: cloudflare
17 CF-RAY: 6abdd43efcb250e60-BOM
18 alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"
19 Content-Length: 2572
20
21 <html>
22 <head>
23 <meta charset="UTF-8" />
24 <meta name="viewport" content="width=device-width, initial-scale=1.0" />
25 <meta name="keywords" content="" />
26 <link rel="icon" href="..." />
27 <link rel="stylesheet" type="text/css" href="..." />
28 <link rel="stylesheet" type="text/css" href="..." />
29 <link rel="stylesheet" type="text/css" href="..." />
30 <link rel="stylesheet" type="text/css" href="..." />
31 <link rel="stylesheet" type="text/css" href="..." />
32 </head>
33 <body>
34 <div>
```

1.5. { CORS with Escape Dot }

Reference	Risk Rating
CORS with Escape Dot	Hard
Tools Used	
Google Chrome Browser, CORS tool, Burp Suite	
Vulnerability Description	
I found this vulnerability by intercepting a login request into burp suite and adding origin header to the interception and forwarding it and successfully getting expected output.	
How It Was Discovered	
Manual Analysis	
Vulnerable URLs	
https://www.bugbountyhunter.org/internship_labs/HTML/cors_lab/lab_5/cors_5.php	
Consequences of not Fixing the Issue	
Attackers would treat many victims to visit the attacker's website, if the victim is logged in, then his personal information is recorded in the attacker's server. Attackers can perform any action in the user's account, by bypassing CSRF tokens.	
Suggested Countermeasures	
Avoid wildcards in internal networks.	
References	
https://portswigger.net/web-security/cors	

Proof of Concept

Request

PrettyRawInActions

```
1 GET /internship_labs/HTML/cors_lab/lab_5/cors_5.php HTTP/1.1
2 Host: www.bugbountyhunter.org
3 Origin: wwwhacktify.in
4 Connection: close
5 sec-ch-ua: "Not A Brand";v="99", "Chromium";v="89"
6 sec-ch-ua-mobile: ?0
7 Upgrade-Insecure-Requests: 1
8 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
9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
10 Sec-Fetch-Site: none
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-User: ?1
13 Sec-Fetch-Dest: document
14 Accept-Encoding: gzip, deflate
15 Accept-Language: en-GB,en-US;q=0.5,en;q=0.8
16 Cookie: PHPSESSID=1d4jcttd6lrr4entrels0e1gph
17
18
```

Response

PrettyRawRenderInActions

```
1 HTTP/1.1 200 OK
2 Date: Wed, 10 Nov 2021 14:17:25 GMT
3 Content-Type: text/html; charset=UTF-8
4 Connection: close
5 expires: Thu, 19 Nov 1991 08:52:00 GMT
6 cache-control: no-store, no-cache, must-revalidate
7 pragma: no-cache
8 set-cookie: PHPSESSID=aukjl7mpa6a7asmpoph3shikfe; path=/
9 access-control-allow-credentials: true
10 access-control-allow-origin: wwwhacktify.in
11 vary: Accept-Encoding
12 CF-Cache-Status: DYNAMIC
13 Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct/"
14 Report-To: {"endpoints":[{"url":"https://a.nel.cloudflare.com/report/v3?s=ic6942FXPU2Fn8vqKtT"}, {"url":"https://a.nel.cloudflare.com/report/v3?s=ic6942FXPU2Fn8vqKtT"}]}
15 URL: ("success_fraction":0,"report_to":"cf-nel","max_age":604800)
16 Server: cloudflare
17 CF-RAY: 6abfe77df8c70f0c-BOM
18 alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400
19 Content-Length: 2564
20
21 <html>
22 <head>
23 <meta charset="UTF-8" />
24 <meta name="viewport" content="width=device-width, initial-scale=1.0" />
25 <meta name="keywords" content="" />
26 <link rel="icon" href="../../assets/img/favicon.png" />
27 <link rel="stylesheet" type="text/css" href="../../assets/css/animate.css" />
28 <link rel="stylesheet" type="text/css" href="../../assets/css/bootstrap.min.css" />
29 <link rel="stylesheet" type="text/css" href="../../assets/css/font-awesome.min.css" />
30 <link rel="stylesheet" type="text/css" href="../../assets/css/main.css" />
31 <link rel="stylesheet" type="text/css" href="../../assets/css/responsive.css" />
32 <title>
33 </title>
34 <style>
35 .containers{
```

1.6. { CORS with Substring Match }

Reference	Risk Rating
CORS with Substring Match	Hard
Tools Used	
Google Chrome Browser, CORS tool, Burp Suite	
Vulnerability Description	
I found this vulnerability by intercepting a login request into burp suite and adding origin header to the interception and forwarding it and successfully getting expected output.	
How It Was Discovered	
Manual Analysis	
Vulnerable URLs	
https://www.bugbountyhunter.org/internship_labs/HTML/cors_lab/lab_6/cors_6.php	
Consequences of not Fixing the Issue	
Attackers would treat many victims to visit the attacker's website, if the victim is logged in, then his personal information is recorded in the attacker's server. Attackers can perform any action in the user's account, by bypassing CSRF tokens.	
Suggested Countermeasures	
Proper configuration of cross-domains requests.	
References	
https://owasp.org/www-community/attacks/CORS-OriginHeaderScrutiny	

Proof of Concept

Request	Response
<pre>1 GET /internship_labs/HTML/cors_lab/lab_6/cors_6.php HTTP/1.1 2 Host: www.bugbountyhunter.org 3 Connection: close 4 sec-ch-ua: "Not A Brand";v="99", "Chromium";v="80" 5 sec-ch-ua-mobile: ?0 6 Origin: hacktify.co 7 Upgrade-Insecure-Requests: 1 8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.4324.150 Safari/537.36 9 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 10 Sec-Fetch-Site: none 11 Sec-Fetch-Mode: navigate 12 Sec-Fetch-User: ?1 13 Sec-Fetch-Dest: document 14 Accept-Encoding: gzip, deflate 15 Accept-Language: en-US,en-US;q=0.9,en;q=0.8 16 Cookie: PHPSESSID=h6g96sm4qqqsq13hu5nfnchbaf 17 18</pre>	<pre>1 HTTP/1.1 302 Found 2 Date: Wed, 10 Nov 2021 06:46:34 GMT 3 Content-Type: text/html; charset=UTF-8 4 Connection: close 5 expires: Thu, 19 Nov 1981 08:52:00 GMT 6 cache-control: no-store, no-cache, must-revalidate 7 pragma: no-cache 8 set-cookie: PHPSESSID=5ohhmc32ahp67amulir92l7pce; path=/ 9 location: ../../Login/index.php 10 access-control-allow-credentials: true 11 access-control-allow-origin: hacktify.co 12 CF-Cache-Status: DYNAMIC 13 Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/eq 14 Report-To: {"endpoints":[{"url":"https://a.nel.cloudflare.com/report/v3?s=gupVAtu5qp42 15 NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} 16 Server: cloudflare 17 CF-RAY: 6abd530c0abc6e8e-BOM 18 alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443" 19 Content-Length: 2610 20 21 <html> 22 <head> 23 <meta charset="UTF-8" /> 24 <meta name="viewport" content="width=device-width, initial-scale=1.0" /> 25 <meta name="keywords" content="" /> 26 <link rel="icon" href="../../assets/img/favicon.png" /> 27 <link rel="stylesheet" type="text/css" href="assets/css/animate.css" /> 28 <link rel="stylesheet" type="text/css" href="../../assets/css/bootstrap.min.css" /> 29 <link rel="stylesheet" type="text/css" href="../../assets/css/font-awesome.min.css" /> 30 <link rel="stylesheet" type="text/css" href="../../assets/css/main.css" /> 31 <link rel="stylesheet" type="text/css" href="../../assets/css/responsive.css" /> 32 </head> 33 <body> 34 <div class="container"></pre>

1.7. { CORS with Arbitrary Subdomain }

Reference	Risk Rating
CORS with Arbitrary Subdomain	Hard
Tools Used	
Google Chrome Browser, CORS tool, Burp Suite	
Vulnerability Description	
I found this vulnerability by intercepting a login request into burp suite and adding origin header to the interception and forwarding it and successfully getting expected output.	
How It Was Discovered	
Manual Analysis	
Vulnerable URLs	
https://www.bugbountyhunter.org/internship_labs/HTML/cors_lab/lab_7/login.php	
Consequences of not Fixing the Issue	
Attackers would treat many victims to visit the attacker's website, if the victim is logged in, then his personal information is recorded in the attacker's server. Attackers can perform any action in the user's account, by bypassing CSRF tokens.	
Suggested Countermeasures	
Avoid wildcards in internal networks.	
References	
https://developer.mozilla.org/en-US/docs/Web/HTTP/CORS	

Proof of Concept

Request

```
1 GET /internship_labs/HTML/cors_lab/lab_7/cors_7.php HTTP/1.1
2 Host: www.bugbountyhunter.org
3 Connection: close
4 Cache-Control: max-age=0
5 Origin: evil.hacktify.in
6 sec-ch-ua: "Not A Brand";v="99", "Chromium";v="80"
7 sec-ch-ua-mobile: ?0
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.4324.150 Safari/537.36
10 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
11 Sec-Fetch-Site: none
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-User: ?1
14 Sec-Fetch-Dest: document
15 Accept-Encoding: gzip, deflate
16 Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
17 Cookie: PHPSESSID=r3u7fwcc5oqatd12hpefsphg9e
18
19
```

Response

```
1 HTTP/1.1 200 OK
2 Date: Wed, 10 Nov 2021 14:21:13 GMT
3 Content-Type: text/html; charset=UTF-8
4 Connection: close
5 expires: Thu, 19 Nov 1981 08:52:00 GMT
6 cache-control: no-store, no-cache, must-revalidate
7 pragma: no-cache
8 set-cookie: PHPSESSID=4idp8c19n712hdq6fqas8ur8f; path=/
9 access-control-allow-credentials: true
10 access-control-allow-origin: evil.hacktify.in
11 vary: Accept-Encoding
12 CF-Cache-Status: DYNAMIC
13 Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct";
14 Report-To: {"endpoints":[{"url":"https://a.nel.cloudflare.com/report/v3?s=53dipCEyx16:
15 NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800)
16 Server: cloudflare
17 CF-RAY: 6abfe0dfc4c0db0-BOM
18 alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"
19 Content-Length: 2563
20
21 <html>
22 <head>
23 <meta charset="UTF-8" />
24 <meta name="viewport" content="width=device-width, initial-scale=1.0" />
25 <meta name="keywords" content="" />
26 <link rel="icon" href=".../assets/img/favicon.png" />
27 <link rel="stylesheet" type="text/css" href=".../assets/css/animate.css" />
28 <link rel="stylesheet" type="text/css" href=".../assets/css/bootstrap.min.css" />
29 <link rel="stylesheet" type="text/css" href=".../assets/css/font-awesome.min.css" />
30 <link rel="stylesheet" type="text/css" href=".../assets/css/main.css" />
31 <link rel="stylesheet" type="text/css" href=".../assets/css/responsive.css" />
32 <title>
33 </title>
34 <style>
35 .containers{
```