

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

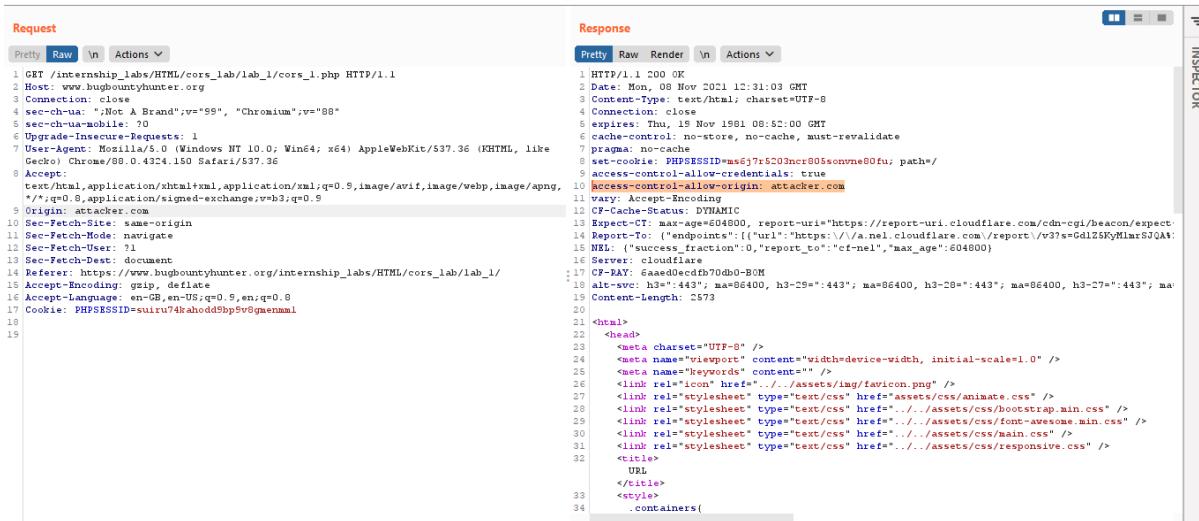
Low - Number of Sub-labs with Easy difficulty level

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



The screenshot shows the browser developer tools Network tab with two panels: Request and Response. The Request panel shows a POST request to 'https://www.bugbountyhunter.org/internship_labs/HTML/cors_lab/lab_1/login.php' with various headers including 'Origin: attacker.com'. The Response panel shows the server's response with a status of 200 OK, containing HTML code for a login page. The response body includes meta tags, links to CSS files like 'animate.css', and a title 'URL'. The 'INSPECTOR' tab is visible on the right side of the developer tools interface.

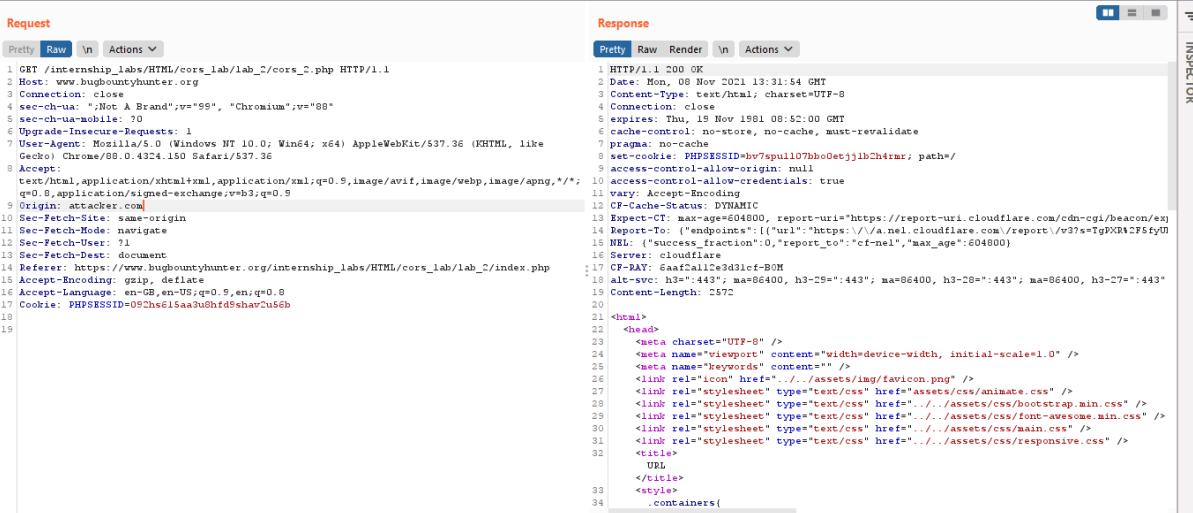
```
Request
Pretty Raw In Actions ▾
1 GET /internship_labs/HTML/cors_lab/lab_1/login.php HTTP/1.1
2 Host: www.bugbountyhunter.org
3 Connection: close
4 sec-ch-ua: "Not A Brand";v="99", "Chromium";v="98"
5 sec-ch-ua-mobile: ?0
6 Upgrade-Insecure-Requests: 1
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/98.0.4724.150 Safari/537.36
8 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8
9 Origin: attacker.com
10 Sec-Fetch-Site: same-origin
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-User: ?
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;q=0.9,fr;q=0.8
17 Cookie: PHPSESSID=euiru74kabd9sbp5v8gmenam1
18
19

Response
Pretty Raw Render In Actions ▾
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=euiru74kabd9sbp5v8gmenam1; path=/; secure; http-only; samesite=strict; domain=.bugbountyhunter.org; expires=Thu, 19 Nov 1981 08:52:00 GMT; max-age=0; access-control-allow-origin: attacker.com
9
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=GdIZSKyMlxrSJQAt"}]
15 NEL: {"success_fraction": 0, "report_to": "cf-nel", "max_age": 604800}
16 Server: cloudflare
17 CF-RAY: 6aaed0edfb70db0-B0M
18 alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400, h3-26=":443"; ma=86400, h3-25=":443"; ma=86400, h3-24=":443"; ma=86400, h3-23=":443"; ma=86400, h3-22=":443"; ma=86400, h3-21=":443"; ma=86400, h3-20=":443"; ma=86400, h3-19=":443"; ma=86400, h3-18=":443"; ma=86400, h3-17=":443"; ma=86400, h3-16=":443"; ma=86400, h3-15=":443"; ma=86400, h3-14=":443"; ma=86400, h3-13=":443"; ma=86400, h3-12=":443"; ma=86400, h3-11=":443"; ma=86400, h3-10=":443"; ma=86400, h3-9=":443"; ma=86400, h3-8=":443"; ma=86400, h3-7=":443"; ma=86400, h3-6=":443"; ma=86400, h3-5=":443"; ma=86400, h3-4=":443"; ma=86400, h3-3=":443"; ma=86400, h3-2=":443"; ma=86400, h3-1=":443"; ma=86400, h3=":443"
19 Content-Length: 2973
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     URL
34   </title>
35   <style>
36     .containers{
37       width: 100%;
```

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



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

Request:

```
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="98"
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/98.0.4724.150 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-User: -1
12 Sec-Fetch-Dest: document
13 Referer: https://www.bugbountyhunter.org/internship_labs/HTML/cors_lab/lab_2/index.php
14 Accept-Encoding: gzip, deflate
15 Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
16 Cookie: PHPSESSID=02hsel15aa3uhfd5shav2u56b
17
```

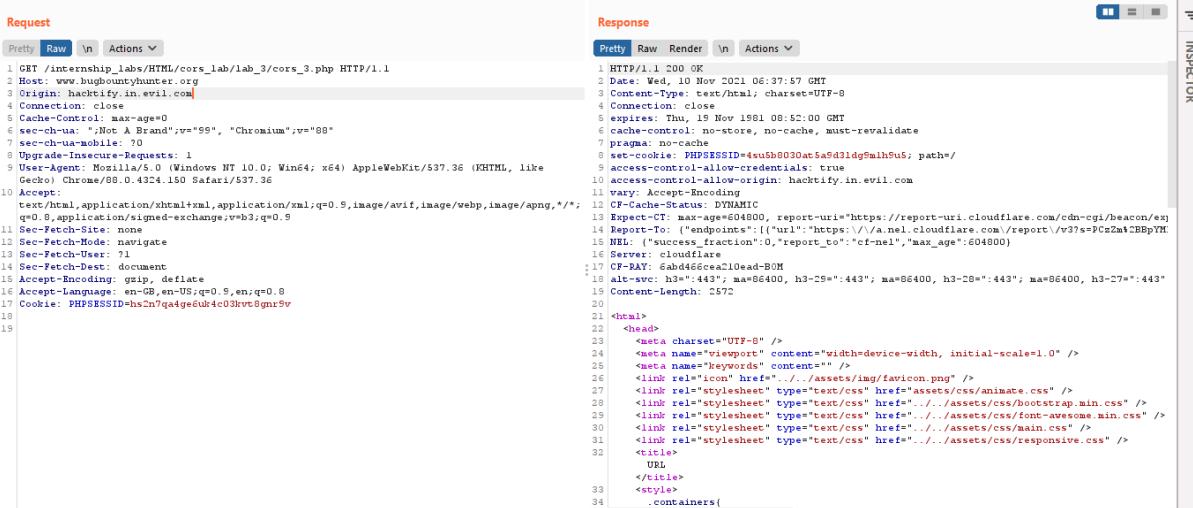
Response:

```
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, 15 Nov 1981 08:52:00 GMT
6 cache-control: no-store, no-cache, must-revalidate
7 pragma: no-cache
8 set-cookie: PHPSESSID=v7spul0Tbb0OetjjlbZh4rmr; 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/ex
14 Report-To: {"endpoints":[{"url": "https://v3.report.cloudflare.com/report/v3?r=TgPxRt2F5fyU
15 max_age": 604800, "section": 0, "report_to": "cf-nei", "max_age": 604800}
16 Server: cloudflare
17 CF-RAY: 6aaefallc2ed3bf-B0M
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   <URL
34     <title>
35     <style>
36       .containers{
```

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



```

Request
Pretty Raw ▾ Actions ▾
1 GET /internship_labs/HTML/cors_lab/lab_3/cors_3.php HTTP/1.1
2 Host: www.bugbountyhunter.org
3 Origin: hackify.in.evil.com
4 Connection: close
5 Cache-Control: max-age=0
6 Sec-Ch-Ua: "Not A Brand";v="99", "Chromium";v="98"
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/98.0.4324.150 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: sameorigin
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=hscn7q4dqe6u4c03hvc8gnr9v
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34

```

```

Response
Pretty Raw Render ▾ Actions ▾
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, 15 Nov 1961 08:52:00 GMT
6 cache-control: no-store, no-cache, must-revalidate
7 pragma: no-cache
8 set-cookie: PHPSESSID=hscn7q4dqe6u4c03hvc8gnr9v; path=/
9 access-control-allow-credentials: true
10 access-control-allow-origin: hackify.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/ex
14 Report-To: https://report-uri.cloudflare.com/route/1v3?e=9CzMa4BBpY
15 Strict-Transport-Security: ("max-age":604800, "report-to":"cf-nei","max_age":604800)
16 Server: cloudflare
17 CF-RAY: 6ab4d466ca1c0ead-B0M
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   <URL
34     </title>
      <style>
        .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

```

Request
Pretty Raw \n Actions ▾
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="98"
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/98.0.4324.150 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-User: ?1
12 Sec-Fetch-Dest: document
13 Accept-Encoding: gzip, deflate
14 Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
15 Cookie: PHPSESSID=dp3vh66dma528rm85o1di1kb8k
16
17
18

Response
Pretty Raw Render \n Actions ▾
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 1981 08:52:00 GMT
6 cache-control: no-store, no-cache, must-revalidate
7 pragma: no-cache
8 set-cookie: PHPSESSID=dp3vh66dma528rm85o1di1kb8k; path=/; access-control-allow-credentials: true
9
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: rpts://cloudflare.com/report?max_age=604800
15 HTTP {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
16 Server: cloudflare
17 CF-RAY: 6abd43e7cb290e60-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   <title>
33     URL
34   </title>
35   <style>
36     .containers{

```

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	

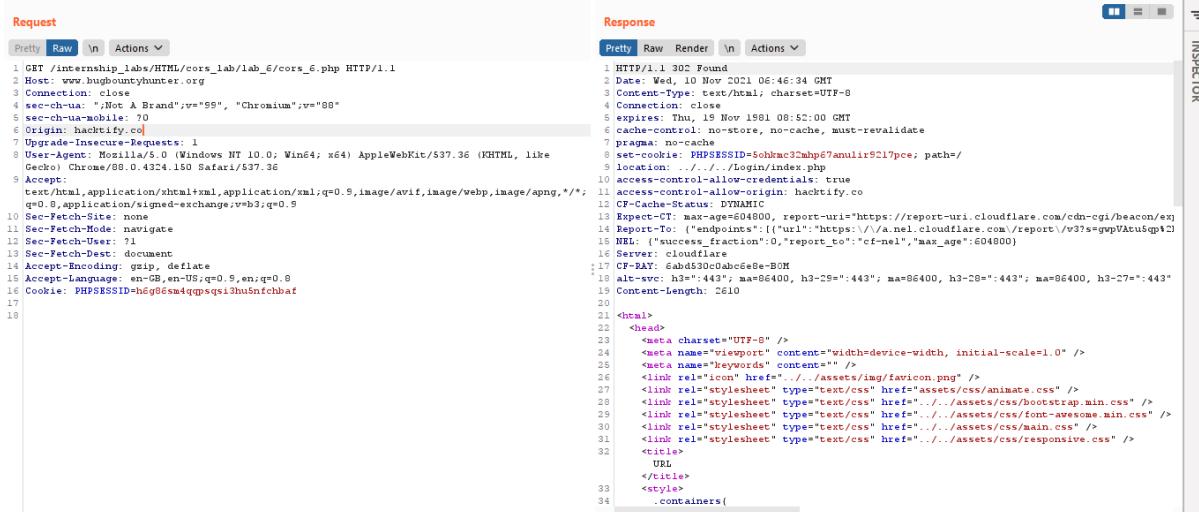
Proof of Concept

```
Request
Pretty Raw ▾ Actions ▾
1 GET /internship_labs/HTML/cors_lab/lab_5/cors_5.php HTTP/1.1
2 Host: www.bugbountyhunter.org
3 Origin: www.hackify.in
4 Connection: close
5 Sec-Fetch-Dest: document
6 Sec-Fetch-Mode: noCors
7 Sec-Fetch-Site: sameSite
8 Sec-Fetch-User: ?1
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-User: ?1
12 Sec-Fetch-Dest: document
13 Accept-Encoding: gzip, deflate
14 Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
15 Cookie: PHPSESSID=1d4jctfd6lrr4entr6ls0elggbh
16
17
18
Response
Pretty Raw Render ▾ Actions ▾
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, 01 Nov 1981 08:00:00 GMT
6 pragma: no-store, no-cache, must-revalidate
7 pragma: no-cache
8 set-cookie: PHPSESSID=1d4jctfd6lrr4entr6ls0elggbh; path=/; secure; HttpOnly
9 access-control-allow-credentials: true
10 access-control-allow-origin: www.hackify.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 Feature-Policy: ("cross-origin-isolated","("url": "https://a.nel.cloudflare.com/report/v3/slice/cfXPUt2FnbvqXit
15 HSTS: ("success_fraction":0, "report_to": "cf-nel", "max_age": 604800)
16 Server: cloudflare
17 CF-RAY: 6abf77d4fc7010c-BON
18 alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=864
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   </head>
33   <body>
34     .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



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

Request:

```
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="98"
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/98.0.4324.150 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=b6g6sm4qqpsqsi3husnfchbat
17
18
```

Response:

```
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=b6g6sm4qqpsqsi3husnfchbat
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/extra/00000000000000000000000000000000"
14 Report-To: {"endpoints":[{"url": "https://v.a.net.cloudflare.com/report/v3?sa=gwpVAtu5qp+CI"}]
15 100 forwarded-for-section":0,"report_to":"cf-nel","max_age":604800}
16 Server: cloudflare
17 CF-RAY: 6abd5d30aabc6e8-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     .containers{
```

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

The screenshot shows a browser developer tools window with two tabs: "Request" and "Response".

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="99"
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/99.0.4324.150 Safari/537.36
10 Accept:
11 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*
12 q=0.8,application/signed-exchange;v=b3;qu=0.9
13 Sec-Fetch-Site: none
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-User: ?1
16 Sec-Fetch-Dest: document
17 Accept-Encoding: gzip, deflate
18 Accept-Language: en-US,en;q=0.5,en;q=0.8
19 Cookie: PHPSESSID=43u7fvcc5ogutdi3hpefshkg8e
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
```

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=4idp8C19n713bdq6fqas8m@f; 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/ex
14 Report-To: {"endpoints": [{"url": "https://v.a.net.cloudflare.com/report/v3?sz=23dipCByx16
15 NEL: {"success_fraction":0,"report_to":"cf-ne1","max_age":604800}
16 Server: cloudflare
17 CF-RAY: 6abfed0acf4cd0b-B0M
18 alt-svc: h3=":443"; ma=64400, h3-28=:443; ma=64400, h3-29=:443; ma=64400, 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   </head>
33   <URL>
34   <style>
35     .containers{
```