



## Week 6 Technical Guide

### Task 1 - Weekly Labs [Mandatory]

#### Cross-Site Request Forgery Lab

<b>Important:</b>	<p>Make sure to take <b>Notes</b> as you proceed with your labs. It can include:</p> <ul style="list-style-type: none"><li>• The steps you have taken.</li><li>• Tools you have used.</li><li>• The payloads you have used, and so on.</li></ul> <p>And also do your research on that specific vulnerability as all of this will help you in the <b>Weekly Assessment Test</b> which will be provided to you.</p>	
<b>Step 1</b>	Hope you all have gone through the study material on Cross-Site Request Forgery for this week.	<a href="#"><u>Cross-Site Request Forgery</u></a>

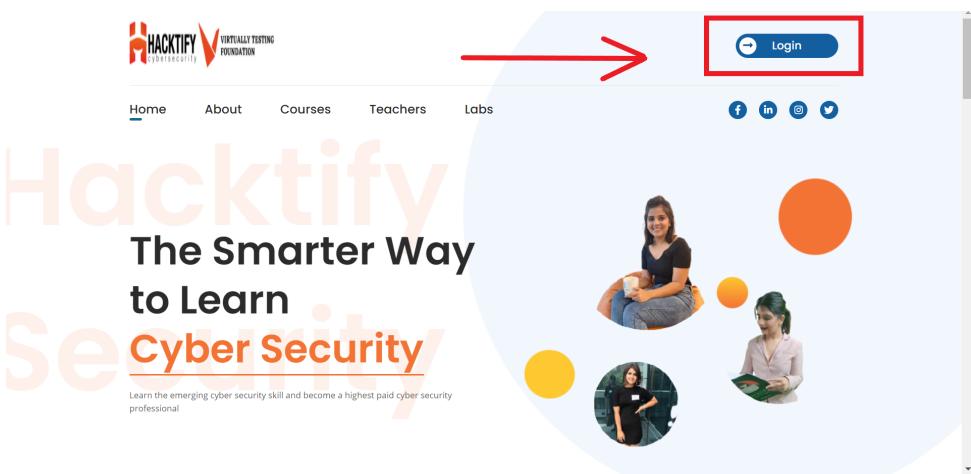


Learn, Test, and Share!

Step 2	<p>Go through the links mentioned in the guide as they have examples of vulnerable websites as shown to the right, and you can practice that on your own to get a better understanding of vulnerabilities before accessing the labs.</p>	
Step 3	<p>Also make sure to check out the references mentioned at the end of the guide. They are very helpful.</p>	



Learn, Test, and Share!

Step 4	Follow the <b>link</b> in the mail to open the Hacktify portal.	<a href="#"><u>Hacktify Labs</u></a>
Step 5	The portal will look like this. Once you successfully open the portal link. Click on <b>Login</b> .	
Step 6	Enter the <b>credentials</b> you received on your registered email on the following page.  Enter the <b>Email ID</b> you used to register for the internship.  And enter the password: <b>inter@oct#123</b>  And you should be logged in	



Learn, Test, and Share!

Step 7	The following <b>home page</b> of your portal will open up.	
Step 8	Open your <b>Weekly assigned course</b> and start accessing your labs.	



Learn, Test, and Share!

**Step 9**

Open the **Cross Site Request Forgery Lab.**

<p>10 Hours</p> <p>Cross-Origin Resource Sharing</p> <p>Rohit Gautam</p>	<p>FREE</p> <p>Hard</p>	<p>9 Hours</p> <p>Open Redirect</p> <p>Rohit Gautam</p>	<p>FREE</p> <p>Hard</p>
<p>7 Hours</p> <p>HTML Injection</p> <p>Rohit Gautam</p>	<p>FREE</p> <p>Medium</p>	<p>1 Hour</p> <p>Exchangeable Image File Format</p> <p>Rohit Gautam</p>	<p>FREE</p> <p>Easy</p>
<p>10 Hours</p> <p>Cross-Site Request Forgery</p> <p>Rohit Gautam</p>	<p>FREE</p> <p>Medium</p>		



Learn, Test, and Share!

#### Step 10

Once you open that, the **Cross Site Request Forgery Labs Page** will open up as shown.

**NOTE:**

Here is only 1 sub-lab assigned to you.

There might be multiple sub-labs in each of the main labs.

## Cross-Site Request Forgery Labs

Home | Labs

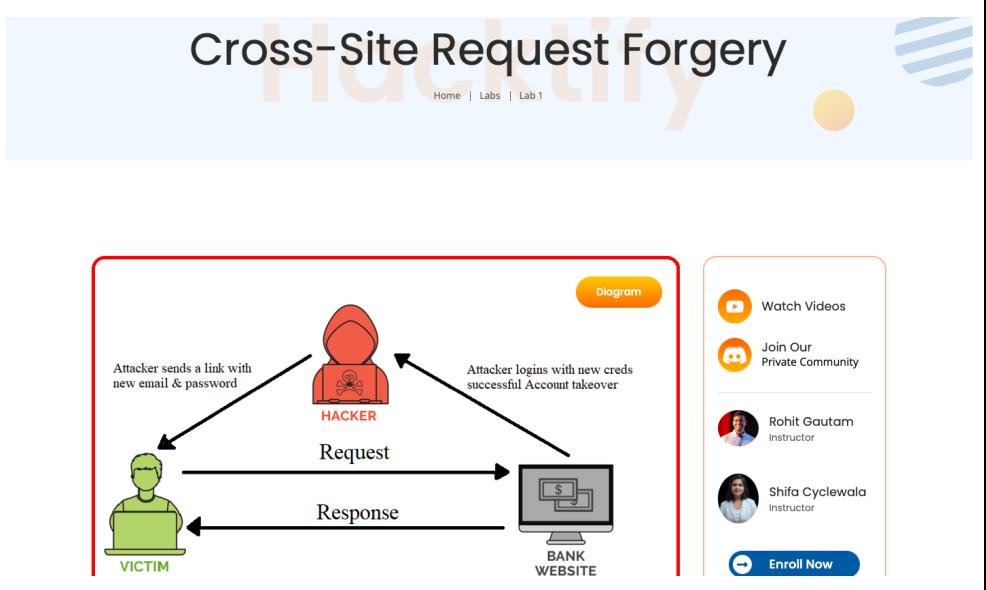
<p>1 Hour</p> <p>Eassy CSRF</p> <p>Rohit Gautam</p>	<p>FREE</p> <p>Easy</p>
<p>1 Hour 30 Minutes</p> <p>Always Validate Tokens</p> <p>Rohit Gautam</p>	<p>FREE</p> <p>Medium</p>
<p>1 Hour 30 Minutes</p> <p>I Hate When Someone Uses My Tokens!</p> <p>Rohit Gautam</p>	<p>FREE</p> <p>Medium</p>
<p>1 Hour</p> <p>GET Me Or POST ME</p> <p>Rohit Gautam</p>	<p>FREE</p> <p>Easy</p>



Learn, Test, and Share!

**Step 11**

Now, if you open **Eassy CSRF**, Cross Site Request Forgery sub-lab 1 will open up.





<b>Step 12</b>	<p>Go through the details given in the lab. The highlighted portion are the <b>goals</b> you have to reach for this lab.</p>	<p><b>Severity</b> The severity of CSRF varies from P3 to P2 depending on what action is being performed. In cases where there is an account takeover the severity will be P2.</p> <p><b>Exploiting CSRF</b></p> <div style="border: 2px solid red; padding: 10px;"><ol style="list-style-type: none"><li data-bbox="1072 414 1136 463">1</li><li data-bbox="1402 414 1465 463">2</li><li data-bbox="1729 414 1793 463">3</li><li data-bbox="1072 577 1136 626">4</li><li data-bbox="1402 577 1465 626">5</li></ol><p>Make 2 accounts, one is of victim and another of attacker</p><p>Sign In with attacker account and generate a malicious link also called as CSRF POC</p><p>Send the PoC to the victim.</p><p>Sign in with the victim's account and open the link.</p><p>If successful i.e. data changes, BOOM you proved the web application vulnerable to CSRF.</p></div>
----------------	--	---



Learn, Test, and Share!

Step 13	<p>Then click on <b>Start Lab</b> at the bottom of the page for successfully starting your lab.</p>	<p><b>Severity</b> The severity of CSRF varies from P3 to P2 depending on what action is being performed. In cases where there is an account takeover the severity will be P2.</p> <p><b>Exploiting CSRF</b></p> <p>1 Make 2 accounts, one is of victim and another of attacker</p> <p>2 Sign in with attacker account and generate a malicious link also called as CSRF POC</p> <p>3 Send the PoC to the victim.</p> <p>4 Sign in with the victim's account and open the link.</p> <p>5 If successful i.e. data changes, BOOM you proved the web application vulnerable to CSRF.</p> <p><b>Start Lab</b></p>
---------	---	---



Learn, Test, and Share!

**Step 14**

The lab will be started and you can continue doing the tasks assigned to you.

## User Login

Email

Password  

**Login**

**Register**



Learn, Test, and Share!

### Step 15

After completion of Sub-Lab 1 **Eassy CSRF !**, move on to do the second sub-lab **Always Validate Tokens!** And so on for all the labs in the section.  
You have to follow the same procedure from step 11 as mentioned above for this lab too.

<p>1 Hour</p> <p><b>Eassy CSRF</b></p> <p>Rohit Gautam</p>	<b>FREE</b>	Easy
<p>1 Hour 30 Minutes</p> <p><b>I Hate When Someone Uses My Tokens!</b></p> <p>Rohit Gautam</p>	<b>FREE</b>	Medium
<p>2 Hours</p> <p><b>XSS The Saviour</b></p> <p>Rohit Gautam</p>	<b>FREE</b>	Hard
<p>1 Hour 30 Minutes</p> <p><b>Always Validate Tokens</b></p> <p>Rohit Gautam</p>	<b>FREE</b>	Medium
<p>1 Hour</p> <p><b>GET Me Or POST ME</b></p> <p>Rohit Gautam</p>	<b>FREE</b>	Easy
<p>2 Hours</p> <p><b>Rm -Rf Token</b></p> <p>Rohit Gautam</p>	<b>FREE</b>	Hard



Learn, Test, and Share!

**Step 16**

Make sure to take **Notes** as you proceed with your labs.

It can include:

- The steps you have taken
- Tools you have used
- The payloads you have used, and so on.

And also do your research on that specific vulnerability as all of this will help you in the **Weekly Assessment Test** which will be provided to you.

## Week 6 - Assignment Submission Form

VTF Hackify Pentesting Internship

This Form will be accepting response till November 17, 2021 : 23:59:59 PST

**This Form can take 30minutes to 1Hour to Complete**

Enter the Email Registered with VTF for the internship.

sshukla@virtuallytesting.com [Switch account](#) 

\* Required

Email \*

Your email

Name \*

Your answer

[Next](#)

[Clear form](#)

Never submit passwords through Google Forms.

This form was created inside of VT. [Report Abuse](#)



Learn, Test, and Share!

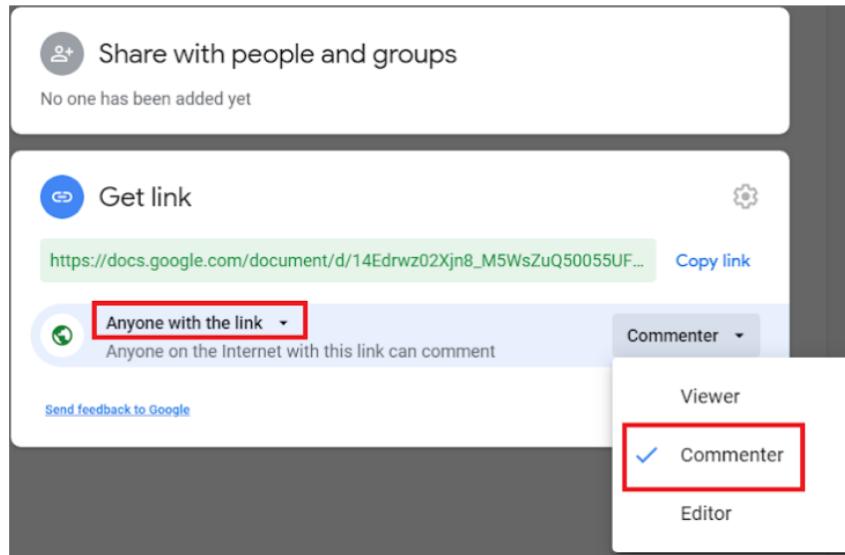
**Step 17**

- Make sure to take a **Pentesting Report** as you proceed with your labs.
- You are required to submit your Report in the assessment form in the section shown in the image.

Penetration Testing Report Submission.

You should be submitting **commenter** link of your report.  
Link should be visible to anyone on the Internet.

**Commenter Link \***

A screenshot of a Google Form interface. At the top, it says "Commenter Link \*". Below that is a "Share with people and groups" section showing "No one has been added yet". Underneath is a "Get link" section with a link "https://docs.google.com/document/d/14Edrwz02Xjn8\_M5WsZuQ50055UF...". A "Copy link" button is next to it. Below the link are two dropdown menus: "Anyone with the link" (set to "Anyone on the Internet with this link can comment") and "Commenter" (set to "Viewer"). A red box highlights the "Commenter" dropdown menu. A modal window is open over the form, also showing the "Commenter" dropdown with "Commenter" selected and checked. At the bottom of the form are "Back", "Next", and "Clear form" buttons.

Your answer

Back    Next    Clear form



## Task 2 - Penetration Testing Report

### [Mandatory]

<b>Important</b>	<p>1. Go through the steps more than once because you are requested to submit a Penetration Testing Report every week.</p> <p>2. Make sure to take notes as you proceed with your labs. It can include</p> <ul style="list-style-type: none"><li>• The steps you have taken</li><li>• Tools you have used</li><li>• The payloads you have used, and so on</li></ul> <p>And also do your research on that specific vulnerability as all of this will help you in the <b>Weekly Assessment Test</b> which will be provided to you.</p>	
<b>Step 1</b>	<p>If you have not copied the provided template in week 1 copy the model template provided for Penetration Testing Report in your Google Drive.</p>	<a href="#">Penetration Testing Report Template</a>



Learn, Test, and Share!

Step 3

Rename the copy to  
**Week\_{#}\_Penetration\_Testing\_Report** where # is the week number.

Copy document X

Name

**Copy of Penetration Testing Report Template**

Folder

Weekly Guides

Share it with the same people

Copy comments and suggestions

Include resolved comments and suggestions

Cancel

OK



Step 4	<p>Open the renamed copy of the template and start editing. Firstly edit the <b>Week {#}</b> of the template with the week number.</p> <p><b>e.g) From Week {#} to Week 6</b></p> <p><b>Note:</b> <b>Everything mentioned with the {} has to be changed.</b></p>	<p style="text-align: center;"><b>Week {#}</b> <b>Penetration Testing Report</b></p> <p><b>Introduction</b></p> <p>This report document hereby describes the proceedings and results of a Black Box security assessment conducted against the <b>Week {#} Labs</b>. The report hereby lists the findings and corresponding best practice mitigation actions and recommendations.</p>		
Step 5	<p>In section 2, edit the <b>Application Name</b> with the lab names.</p> <p><b>Note:</b> <b>Some weeks have 2 labs so you are required to provide both names in such cases, if not 1 is enough.</b></p>	<p><b>2. Scope</b></p> <p>This section defines the scope and boundaries of the project.</p> <table border="1" data-bbox="1066 796 2016 873"><tr><td data-bbox="1066 796 1235 873"><b>Application Name</b></td><td data-bbox="1235 796 2016 873">{Lab 1 Name}, {Lab 2 Name (if the week has 2 labs)}</td></tr></table>	<b>Application Name</b>	{Lab 1 Name}, {Lab 2 Name (if the week has 2 labs)}
<b>Application Name</b>	{Lab 1 Name}, {Lab 2 Name (if the week has 2 labs)}			



#### Step 6

In section 3, change **week {#}** and **{count}** with the number of the sub-labs present.  
Change the **{count}** inside the **table** with the number of easy sub-labs for low, medium sub-labs for medium and hard sub-labs for hard.

**Note:**

**{count} is the sum of both labs if 2 labs are present.**

#### 3. Summary

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

**Total number of Sub-labs: {count} Sub-labs**

High	Medium	Low
{count}	{count}	{count}

**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

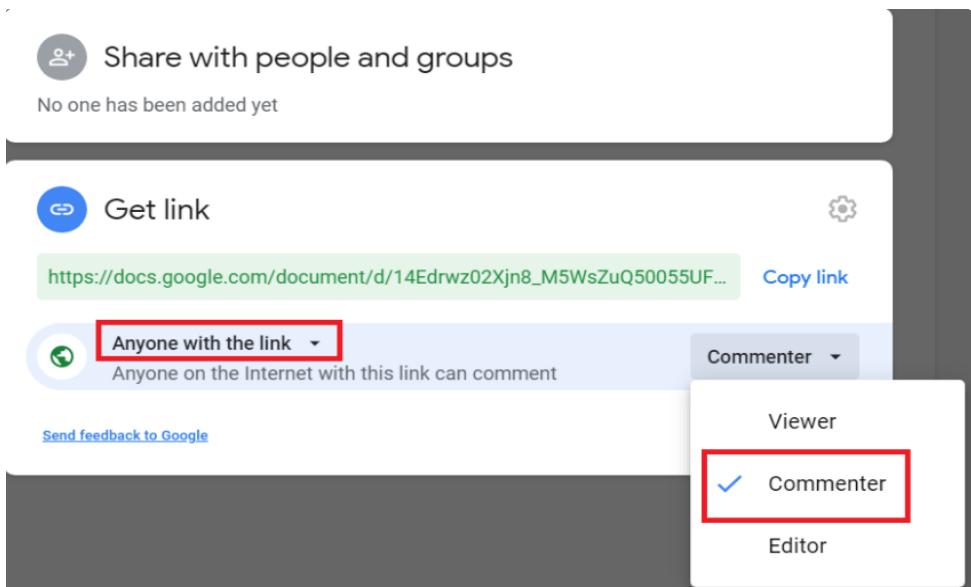


Step 7	<p>Now it's time to update the vulnerability for lab 1. Change {Lab 1 Name} to the lab assigned for the week and Change {Sub-lab-1 Name} to the name of the first sub-lab you worked. Update the table given with the information on the vulnerability.</p> <p><b>Note:</b> <b>Do the same for all the sub-labs.</b> <b>The template provides a table for 2 sub-labs, if more is needed copy-paste the same.</b></p>	<p><b>1. {Lab 1 Name}</b></p> <p><b>1.1. {Sub-lab-1 Name}</b></p> <table border="1" data-bbox="1062 372 2023 853"><tr><td data-bbox="1062 372 1558 412"><b>Reference</b></td><td data-bbox="1558 372 2023 412"><b>Risk Rating</b></td></tr><tr><td data-bbox="1062 412 1558 453">{Sub-lab-1 Name}</td><td data-bbox="1558 412 2023 453">Low / Medium / High</td></tr><tr><td colspan="2" data-bbox="1062 453 2023 494"><b>Tools Used</b></td></tr><tr><td colspan="2" data-bbox="1062 494 2023 535">Tools that you have used to find the vulnerability.</td></tr><tr><td colspan="2" data-bbox="1062 535 2023 576"><b>Vulnerability Description</b></td></tr><tr><td colspan="2" data-bbox="1062 576 2023 616">About the vulnerability and its working</td></tr><tr><td colspan="2" data-bbox="1062 616 2023 657"><b>How It Was Discovered</b></td></tr><tr><td colspan="2" data-bbox="1062 657 2023 698">Automated Tools / Manual Analysis</td></tr><tr><td colspan="2" data-bbox="1062 698 2023 739"><b>Vulnerable URLs</b></td></tr><tr><td colspan="2" data-bbox="1062 739 2023 780">URLs of the vulnerable pages in the lab</td></tr><tr><td colspan="2" data-bbox="1062 780 2023 820"><b>Consequences of not Fixing the Issue</b></td></tr><tr><td colspan="2" data-bbox="1062 820 2023 853">What will be the consequences if the vulnerability is not patched?</td></tr><tr><td colspan="2" data-bbox="1062 853 2023 886"><b>Suggested Countermeasures</b></td></tr><tr><td colspan="2" data-bbox="1062 886 2023 918">Give some Suggestions to stand against this vulnerability</td></tr><tr><td colspan="2" data-bbox="1062 918 2023 951"><b>References</b></td></tr><tr><td colspan="2" data-bbox="1062 951 2023 967">URLs to the sources used to know more about this vulnerability</td></tr></table>	<b>Reference</b>	<b>Risk Rating</b>	{Sub-lab-1 Name}	Low / Medium / High	<b>Tools Used</b>		Tools that you have used to find the vulnerability.		<b>Vulnerability Description</b>		About the vulnerability and its working		<b>How It Was Discovered</b>		Automated Tools / Manual Analysis		<b>Vulnerable URLs</b>		URLs of the vulnerable pages in the lab		<b>Consequences of not Fixing the Issue</b>		What will be the consequences if the vulnerability is not patched?		<b>Suggested Countermeasures</b>		Give some Suggestions to stand against this vulnerability		<b>References</b>		URLs to the sources used to know more about this vulnerability	
<b>Reference</b>	<b>Risk Rating</b>																																	
{Sub-lab-1 Name}	Low / Medium / High																																	
<b>Tools Used</b>																																		
Tools that you have used to find the vulnerability.																																		
<b>Vulnerability Description</b>																																		
About the vulnerability and its working																																		
<b>How It Was Discovered</b>																																		
Automated Tools / Manual Analysis																																		
<b>Vulnerable URLs</b>																																		
URLs of the vulnerable pages in the lab																																		
<b>Consequences of not Fixing the Issue</b>																																		
What will be the consequences if the vulnerability is not patched?																																		
<b>Suggested Countermeasures</b>																																		
Give some Suggestions to stand against this vulnerability																																		
<b>References</b>																																		
URLs to the sources used to know more about this vulnerability																																		
Step 8	<p>For the <b>Proof of Concept</b> you are required to attach the <b>screenshot</b> of the <b>vulnerability</b> you found in the sub-labs.</p> <p><b>Note:</b> <b>1 Screenshot is needed for each sub-labs and not more than that.</b></p>	<p><b>Proof of Concept</b></p> <p>This section contains the proof of the above vulnerabilities as the screenshot of the vulnerability of the lab</p>																																



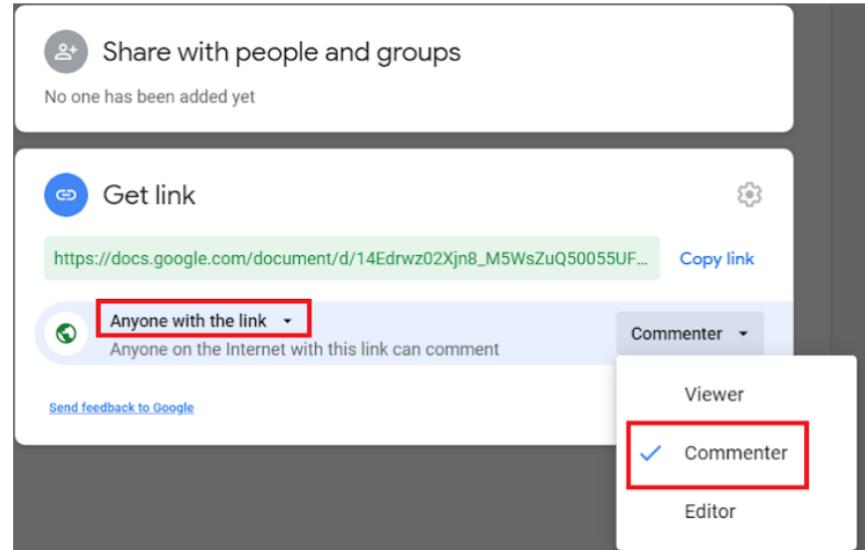
Step 9	<p>If you have worked on 2 labs, do the same step 8 and step 9 for the second lab, if not remove those things that are related to the 2nd lab.</p>	<p><b>2. {Lab 2 Name (if the week has 2 labs)}</b></p> <p><b>2.1. {Sub-lab-1 Name}</b></p> <table border="1" data-bbox="1072 376 2023 855"><thead><tr><th data-bbox="1072 376 1537 421">Reference</th><th data-bbox="1537 376 2023 421">Risk Rating</th></tr></thead><tbody><tr><td data-bbox="1072 421 1537 448">{Sub-lab-1 Name}</td><td data-bbox="1537 421 2023 448">Low / Medium / High</td></tr><tr><td colspan="2" data-bbox="1072 448 2023 476"><b>Tools Used</b></td></tr><tr><td colspan="2" data-bbox="1072 476 2023 504">Tools that you have used to find the vulnerability.</td></tr><tr><td colspan="2" data-bbox="1072 504 2023 532"><b>Vulnerability Description</b></td></tr><tr><td colspan="2" data-bbox="1072 532 2023 559">About the vulnerability and its working</td></tr><tr><td colspan="2" data-bbox="1072 559 2023 587"><b>How It Was Discovered</b></td></tr><tr><td colspan="2" data-bbox="1072 587 2023 615">Automated Tools / Manual Analysis</td></tr><tr><td colspan="2" data-bbox="1072 615 2023 643"><b>Vulnerable URLs</b></td></tr><tr><td colspan="2" data-bbox="1072 643 2023 670">URLs of the vulnerable pages in the lab</td></tr><tr><td colspan="2" data-bbox="1072 670 2023 698"><b>Consequences of not Fixing the Issue</b></td></tr><tr><td colspan="2" data-bbox="1072 698 2023 726">What will be the consequences if the vulnerability is not patched?</td></tr><tr><td colspan="2" data-bbox="1072 726 2023 753"><b>Suggested Countermeasures</b></td></tr><tr><td colspan="2" data-bbox="1072 753 2023 781">Give some Suggestions to stand against this vulnerability</td></tr><tr><td colspan="2" data-bbox="1072 781 2023 809"><b>References</b></td></tr><tr><td colspan="2" data-bbox="1072 809 2023 837">URLs to the sources used to know more about this vulnerability</td></tr></tbody></table> <p><b>Proof of Concept</b></p> <p>This section contains the proof of the above vulnerabilities as the screenshot of the vulnerability of the lab</p>	Reference	Risk Rating	{Sub-lab-1 Name}	Low / Medium / High	<b>Tools Used</b>		Tools that you have used to find the vulnerability.		<b>Vulnerability Description</b>		About the vulnerability and its working		<b>How It Was Discovered</b>		Automated Tools / Manual Analysis		<b>Vulnerable URLs</b>		URLs of the vulnerable pages in the lab		<b>Consequences of not Fixing the Issue</b>		What will be the consequences if the vulnerability is not patched?		<b>Suggested Countermeasures</b>		Give some Suggestions to stand against this vulnerability		<b>References</b>		URLs to the sources used to know more about this vulnerability	
Reference	Risk Rating																																	
{Sub-lab-1 Name}	Low / Medium / High																																	
<b>Tools Used</b>																																		
Tools that you have used to find the vulnerability.																																		
<b>Vulnerability Description</b>																																		
About the vulnerability and its working																																		
<b>How It Was Discovered</b>																																		
Automated Tools / Manual Analysis																																		
<b>Vulnerable URLs</b>																																		
URLs of the vulnerable pages in the lab																																		
<b>Consequences of not Fixing the Issue</b>																																		
What will be the consequences if the vulnerability is not patched?																																		
<b>Suggested Countermeasures</b>																																		
Give some Suggestions to stand against this vulnerability																																		
<b>References</b>																																		
URLs to the sources used to know more about this vulnerability																																		



Step 10	Don't forget to remove the <b>NOTES</b> given in the template. It is just for your reference.	<p><b>NOTES:</b></p> <ul style="list-style-type: none"><li>• Everything mentioned inside () has to be changed based on your lab and sub-labs.</li><li>• Here it is given with 2 Sub-labs vulnerability, you need to add all the sub-labs based on your lab.</li><li>• Don't forget to take the screenshot of the vulnerability in the sub-labs</li><li>• Add the screenshots to google drive and share the link of the folder containing those screenshots in the Proof of Concept session.</li><li>• This NOTE session is only for your reference, don't forget to delete this in the report you submit.</li></ul>
Step 11	After completing the work, now click on the <b>share</b> button and create a share link with the <b>Commenter</b> permission.	 <p>The screenshot shows the sharing settings for a Google Doc. At the top, there's a 'Share with people and groups' section with a note 'No one has been added yet'. Below it is a 'Get link' section with a generated URL and a 'Copy link' button. A dropdown menu for permissions is open, showing three options: 'Viewer' (unchecked), 'Commenter' (checked with a blue checkmark), and 'Editor' (unchecked). The 'Commenter' option is highlighted with a red box.</p>



Learn, Test, and Share!

<p><b>Important</b></p> <p>You are required to submit the link to your Report in the <b>weekly assessment form</b>.</p>	<p>Penetration Testing Report Submission.</p> <p>You should be submitting <b>commenter</b> link of your report. Link should be visible to anyone on the Internet.</p> <p><b>Commenter Link *</b></p> <p></p> <p>Your answer</p> <p>Back    Next    Clear form</p>
---	---



## Task 3 - Assessment Test [Mandatory]

Important	<p>There will be an assessment test at the end of each week in the weekly submission form in which you will have to answer a certain amount of questions related to this week's topic.</p> <p><b>You need to score 70% in this specific Week's Technical Assessment in order to proceed with the internship.</b></p>	<p>Section 4 of 4</p> <h3>Technical Assessment</h3> <p>KYC - Know Your Content for the week. This week's topic -</p> <p>All the Best !</p>
Note:	<ul style="list-style-type: none"><li>Number of questions could vary from 30 to 50 per week.</li><li>Make sure to take <b>Notes</b> on what you do. It is recommended to do research as all of this will help you in the <b>Weekly Assessment Test</b> which will be provided to you in the submission form.</li></ul>	



## Reminder

All Interns are required to participate in our Technical Skills Assignment. We will be using <https://www.bugbountyhunter.org>. If you do not participate you will be removed from the internship and your access to our content will be revoked.

When on [Hacktify Labs](#) you may notice that it takes a while for the labs to load in. If this is the case try reloading the page or closing your tab, and going back to the page. Once you have it open we suggest not closing this page as you can just go back to this tab to access other labs after you complete the currently deployed one.

**You must take Mandatory Weekly Assessment which is available on #weekly-submissions-📋 in discord:**

**Make sure to take Notes as you proceed with your labs**