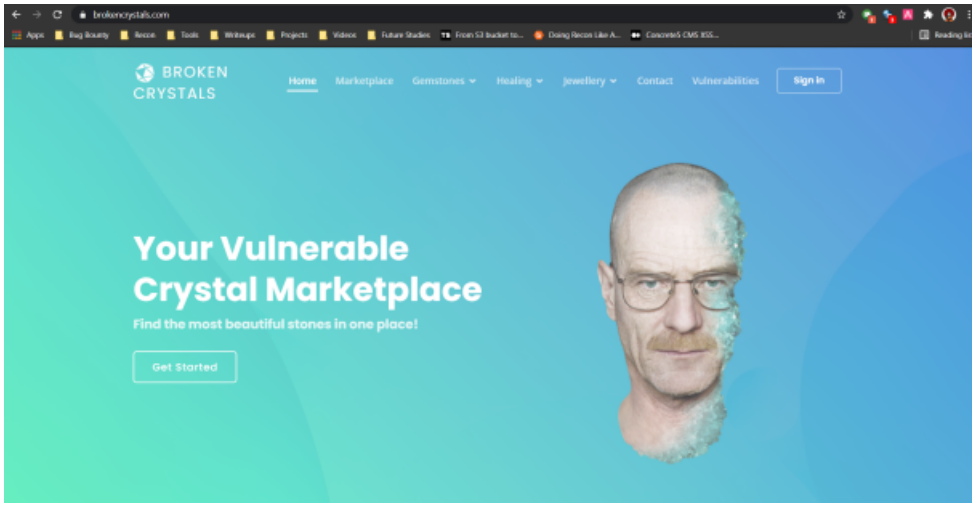
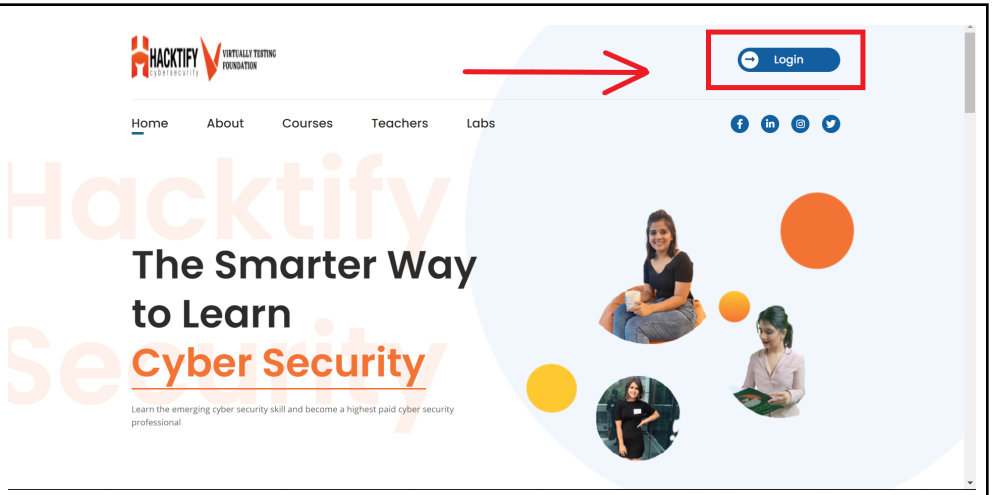
Week 4 Technical Guide

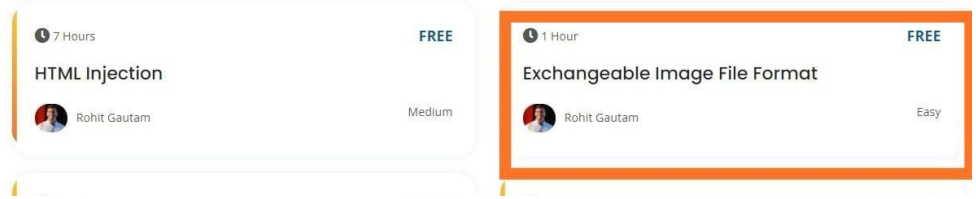
Task 1 - Weekly Labs [Mandatory]

Lab 1 - Exchangeable Image File Format

Important:	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.	
Step 1	Hope you all have gone through the study material on Cross-Site Scripting for this week.	EXIF

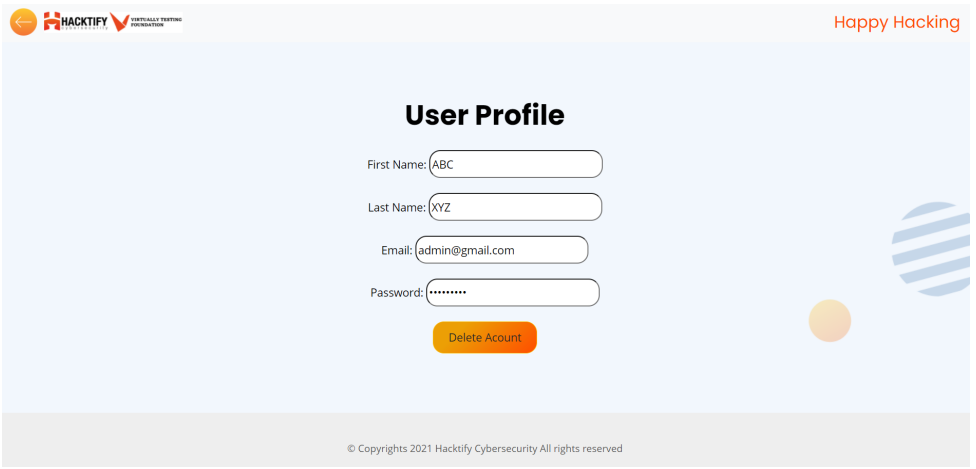
Step 2	Go through the links mentioned in the guide as they have examples of vulnerable websites as shown to the right, and you can practice that on your own to get a better understanding of vulnerabilities before accessing the labs.	
Step 3	Also make sure to check out the **references** mentioned at the end of the guide. They are very helpful.	**References** • EXIF Data : https://photographylife.com/what-is-exif-data • EXIF Data Information Leakage: https://beaglesecurity.com/blog/vulnerability/exif-data-information-leakage.html
Step 4	Follow the **link** to open the Hacktify portal.	Bug bounty hunter - Master web application vulnerabilities and kickstart your journey in bug bounty hunting | BugBountyHunter.org

Step 5	Once you successfully open the portal link. Click on **Login**.	
Step 6	Enter the **Email ID** you used to register for the internship. And enter the password: **inter@oct#123** And you should be logged in.	

Step 7	Once you successfully logged in, you will see the **homepage** listed with labs.	
Step 8	From the list of labs, open the **Exchangeable File Format Lab**.	

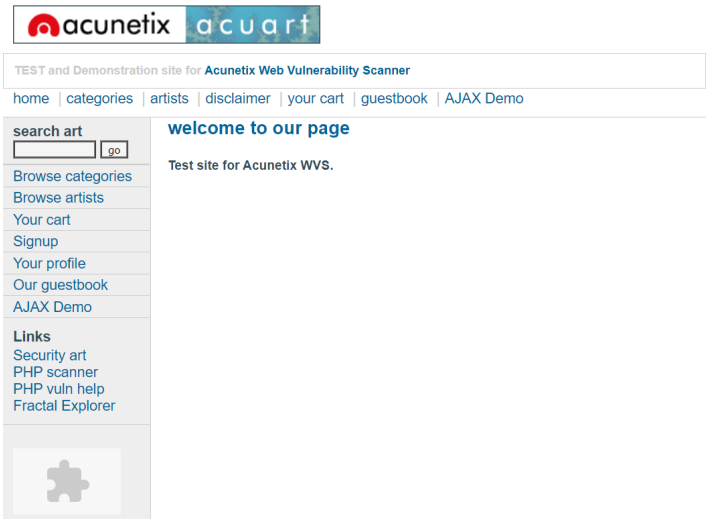
Step 9	Once you open the **Exchangeable File Format Lab,** you will be assigned with sub-labs as shown. **NOTE:** There might be multiple sub-labs in each of the main labs.	 
Step 10	Open **Let's PII!,** an Exchangeable File Format sub-lab will open up.	
Step 11	After opening the sub-lab, first go through the given details in the lab.	**What Is EXIF Metadata?** EXIF stands for Exchangeable Image File Format. It is a record which shows the digital SLR camera settings used to take a particular photograph. This data is recorded into the actual image file. Therefore each photograph has its own unique data. EXIF data shows photo information such as camera model, exposure, aperture, ISO, what camera mode was used and whether or not a flash fired. **What Is EXIF Exposure?** EXIF Data stores sensitive information like Geo-location, Date, Name of the camera, Modified date, Time, Sensing Method, File Source, Type of compression etc. in the photos you click. Now this data resides in the every photo you take using cameras. Whenever you upload a picture on a website and if the website does not strip these sensitive data then this could lead to sensitive data exposure like the Geo-location, Date of the photo, Time of the photo, Camera used etc.

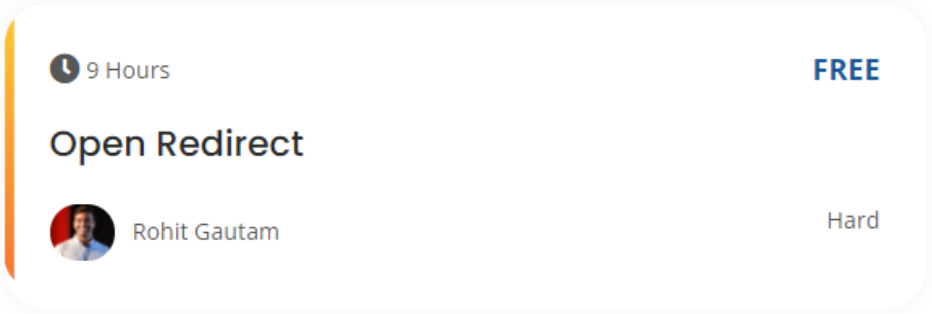
Step 12	The highlighted portion are the **goals** that you have to accomplish for this lab.	
Step 13	Once you are clear with **goals,** click on **Start Lab.**	

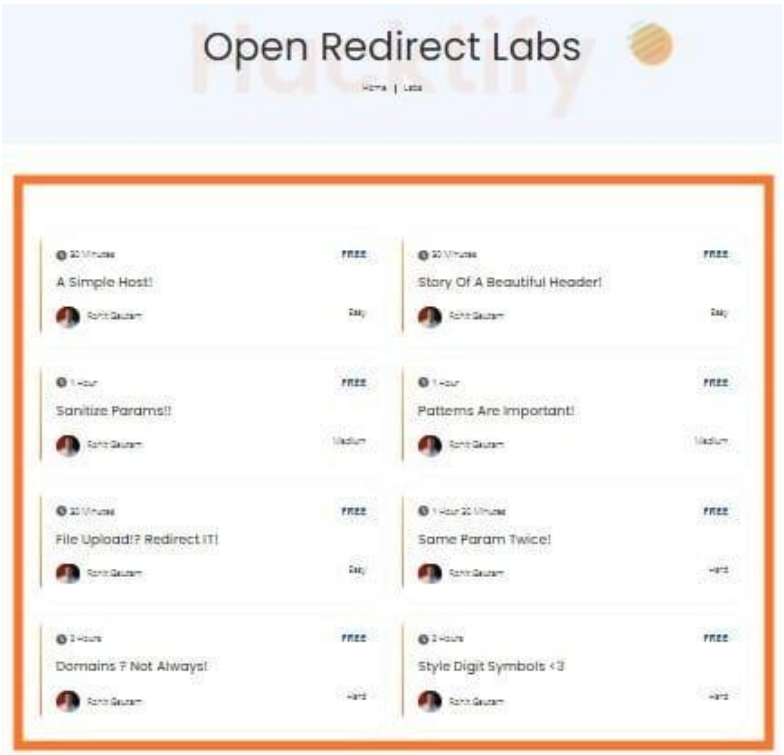
Step 14	Once the lab starts, hack through the goals that you need to accomplish. Happy Hacking. **NOTE:** Make sure to take **Notes** as you proceed with your labs.	

Lab 2 - Open Redirect

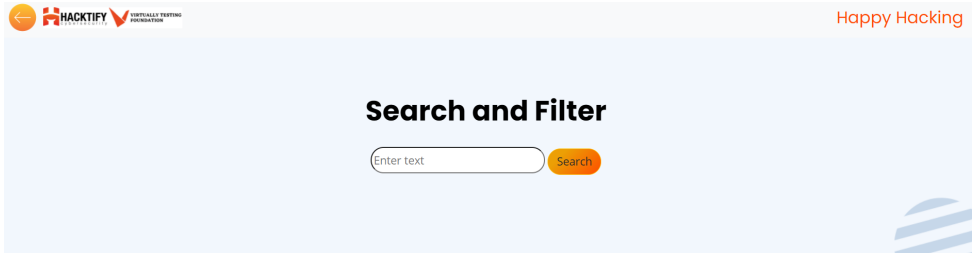
Important:	Make sure to take **Notes** as you proceed with your labs. It can include • The steps you have taken • Tools you have used • The payloads you have used, and so on. And also do your research on that specific vulnerability as all of this will help you in the **Weekly Assessment Test** which will be provided to you.	

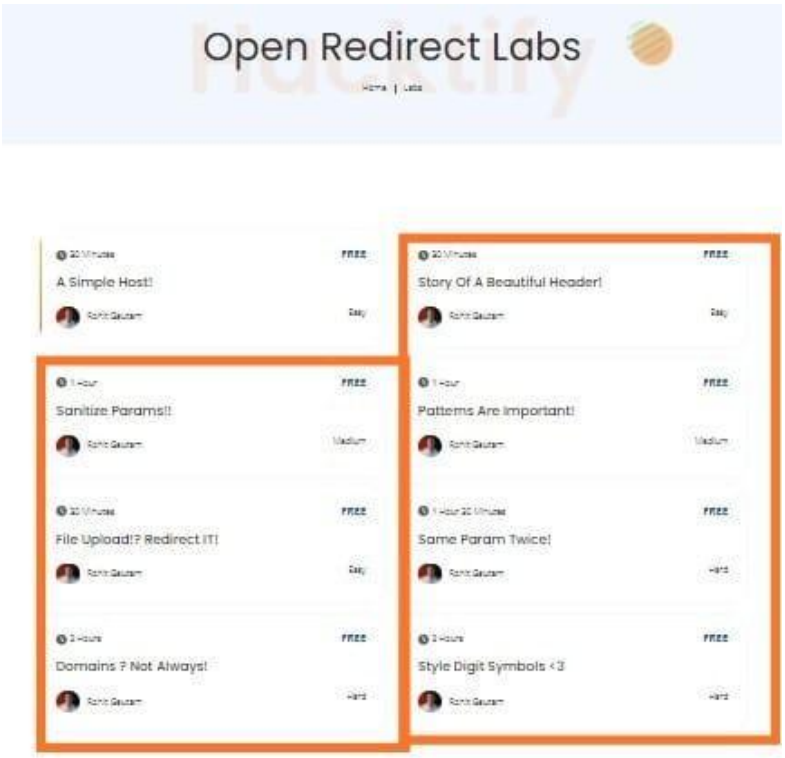
Step 1	Go through the study material given on Clickjacking lab.	Open_Redirect
Step 2	Go through the links mentioned in the guide as they have **examples** of vulnerable websites as shown to the right, and you can practice that on your own to get a better understanding of vulnerabilities before accessing the labs.	
Step 3	Also make sure to check out the references mentioned at the end of the guide. **Example** on the right.	**References** • Open Redirect by PortSwigger : https://portswigger.net/kb/issues/00500100_open-redirection-reflected • OWASP Open Redirect: https://cheatsheetseries.owasp.org/cheatsheets/Unvalidated_Redirects_and_Forwards_Cheat_Sheet.html • Open Redirect by Acunetix : https://www.acunetix.com/blog/web-security-zone/what-are-open-redirects/

Step 4	Follow the **link** to open the Hacktify portal.	Bug bounty hunter - Master web application vulnerabilities and kickstart your journey in bug bounty hunting | BugBountyHunter.org
Step 5	Open the **Open Redirect Lab**.	

Step 6	Once you open that, the **Open Redirect Labs Page** will open up as shown. **NOTE:** Here there are 8 sub-labs assigned to you. There might be multiple sub-labs in each of the main labs.	

Step 7	Now, if you open **A Simple Host!,** Open Redirect sub-lab 1 will open up.	
Step 8	Go through the details given in the lab. The highlighted portion is the steps you have to follow for this lab.	

Step 9	Then click on **Start Lab** at the bottom of the page for successfully starting your lab.	
Step 10	The lab will be started and you can continue doing the tasks assigned to you.	

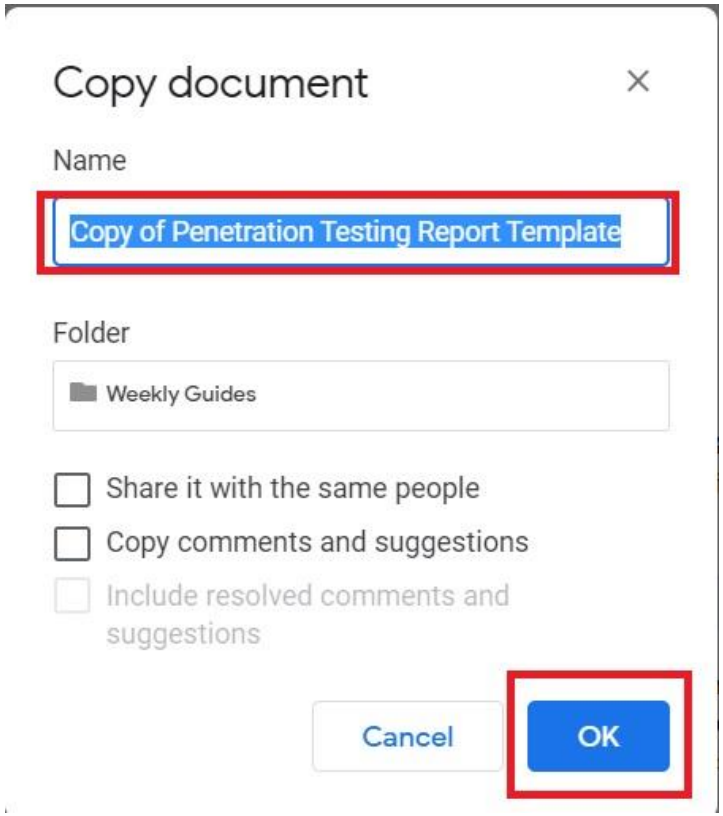
Step 11	After completion of Sub-Lab 1 **A Simple Host !**, move on to do the other sub-labs that are available. You have to follow the same procedure as mentioned above for this lab too.	

Step 12	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.	

Task 2 - Penetration Testing Report

[Mandatory]

Important	1. Go through the steps more than once because you are requested to submit a Penetration Testing Report every week. 2. 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.	
Step 1	If you have not copied the provided template in week 1 copy the model template provided for Penetration Testing Report in your Google Drive.	Penetration Testing Report Template

Step 3	Rename the copy to **Week_#_Penetration_Testing_Report** where # is the week number.	

<table>
<tr>
<td>Step 4</td>
<td>Open the renamed copy of the template and start editing. Firstly edit the Week {#} of the template with the week number.

e.g) From Week {#} to Week 4

Note:
Everything mentioned with the {} has to be changed.</td>
<td><h1>Week {#}
Penetration Testing Report</h1><h2>Introduction</h2>This report document hereby describes the proceedings and results of a Black Box security assessment conducted against the Week {#} Labs. The report hereby lists the findings and corresponding best practice mitigation actions and recommendations.</td>
</tr>
<tr>
<td>Step 5</td>
<td>In section 2, edit the Application Name with the lab names.

Note:
Some weeks have 2 labs so you are required to provide both names in such cases, if not 1 is enough.</td>
<td><h2>2. Scope</h2>This section defines the scope and boundaries of the project.<table><tr><td>Application Name</td><td>{Lab 1 Name}, {Lab 2 Name (if the week has 2 labs)}</td></tr></table></td>
</tr>
</table>

<table>
<tr>
<td>Step 6</td>
<td>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.</td>
<td>
<h3>3. Summary</h3>
Outlined is a Black Box Application Security assessment for the Week {#} Labs.

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

<table>
<tr><th>High</th><th>Medium</th><th>Low</th></tr>
<tr><td>{count}</td><td>{count}</td><td>{count}</td></tr>
</table>

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
</td>
</tr>
</table>

<table>
<tr>
<td>Step 7</td>
<td>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.

Note:
Do the same for all the sub-labs.
The template provides a table for 2 sub-labs, if more is needed copy-paste the same.</td>
<td>
<h3>1. {Lab 1 Name}</h3>
<h3>1.1. {Sub-lab-1 Name}</h3>
<table>
<tr><th>Reference</th><th>Risk Rating</th></tr>
<tr><td>{Sub-lab-1 Name}</td><td>Low / Medium / High</td></tr>
<tr><td colspan="2">Tools Used</td></tr>
<tr><td colspan="2">Tools that you have used to find the vulnerability.</td></tr>
<tr><td colspan="2">Vulnerability Description</td></tr>
<tr><td colspan="2">About the vulnerability and its working</td></tr>
<tr><td colspan="2">How It Was Discovered</td></tr>
<tr><td colspan="2">Automated Tools / Manual Analysis</td></tr>
<tr><td colspan="2">Vulnerable URLs</td></tr>
<tr><td colspan="2">URLs of the vulnerable pages in the lab</td></tr>
<tr><td colspan="2">Consequences of not Fixing the Issue</td></tr>
<tr><td colspan="2">What will be the consequences if the vulnerability is not patched?</td></tr>
<tr><td colspan="2">Suggested Countermeasures</td></tr>
<tr><td colspan="2">Give some Suggestions to stand against this vulnerability</td></tr>
<tr><td colspan="2">References</td></tr>
<tr><td colspan="2">URLs to the sources used to know more about this vulnerability</td></tr>
</table>
</td>
</tr>
<tr>
<td>Step 8</td>
<td>For the Proof of Concept you are required to attach the screenshot of the vulnerability you found in the sub-labs.

Note:
1 Screenshot is needed for each sub-labs and not more than that.</td>
<td>
<h3>Proof of Concept</h3>
This section contains the proof of the above vulnerabilities as the screenshot of the vulnerability of the lab
</td>
</tr>
</table>

Step 9	**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.**	

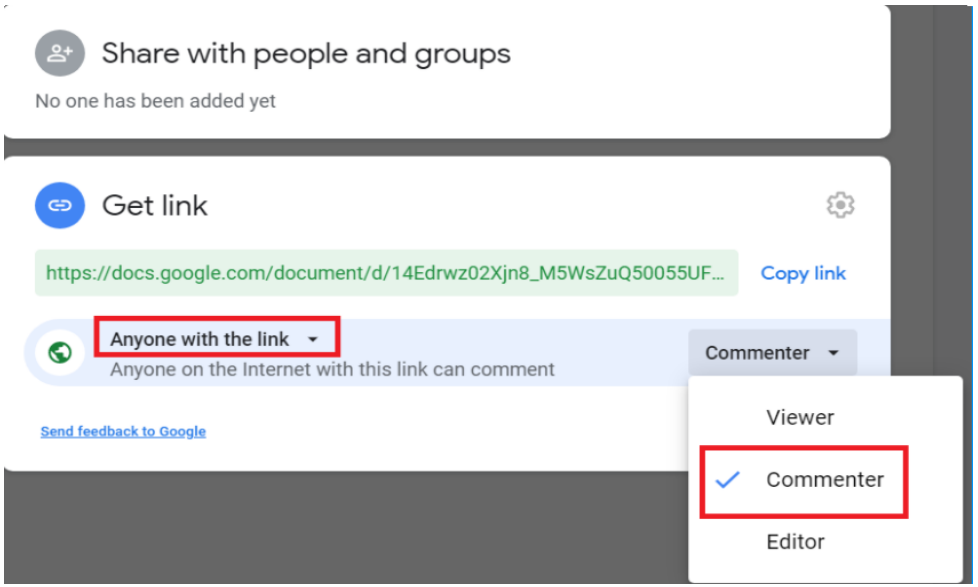
2. {Lab 2 Name (if the week has 2 labs)}

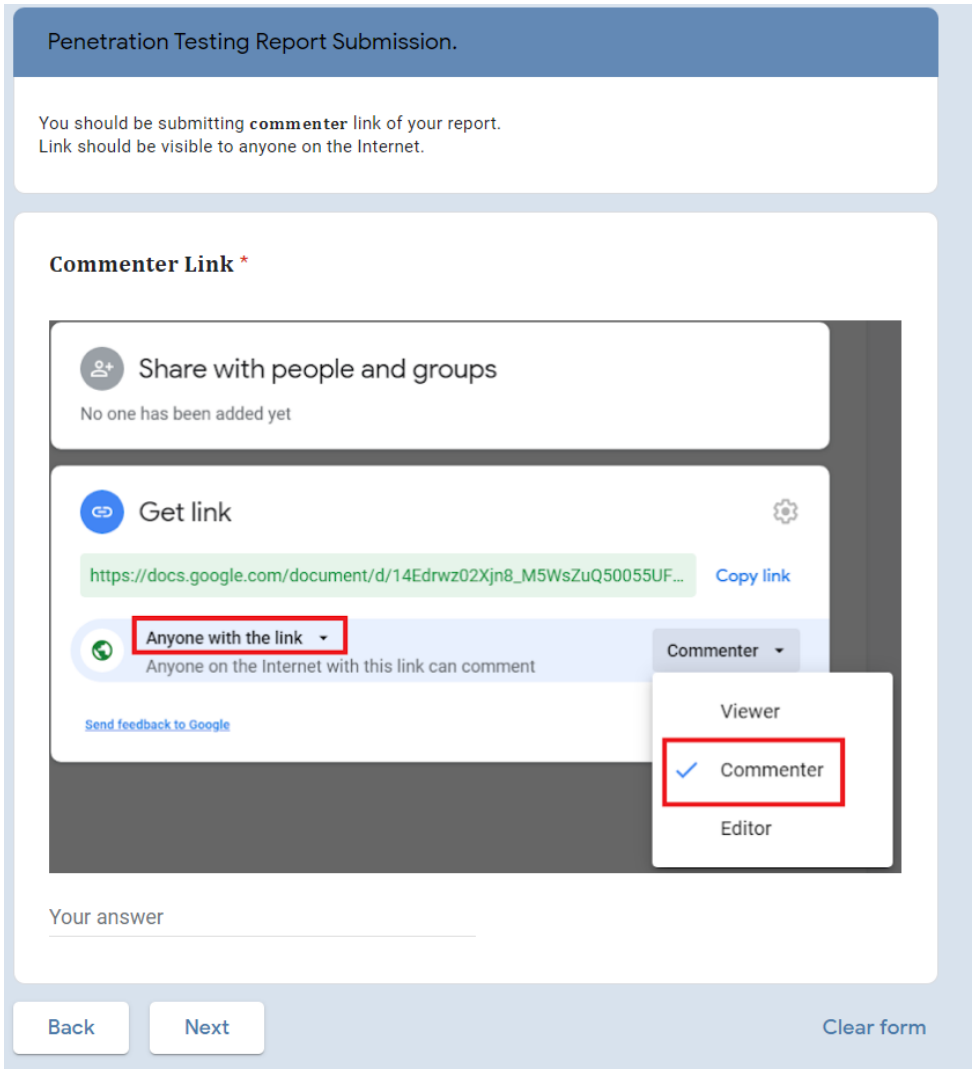
2.1. {Sub-lab-1 Name}

Reference	**Risk Rating**
{Sub-lab-1 Name}	**Low / Medium / High**
Tools Used	
Tools that you have used to find the vulnerability.	
Vulnerability Description	
About the vulnerability and its working	
How It Was Discovered	
Automated Tools / Manual Analysis	
Vulnerable URLs	
URLs of the vulnerable pages in the lab	
Consequences of not Fixing the Issue	
What will be the consequences if the vulnerability is not patched?	
Suggested Countermeasures	
Give some Suggestions to stand against this vulnerability	
References	
URLs to the sources used to know more about this vulnerability	

Proof of Concept

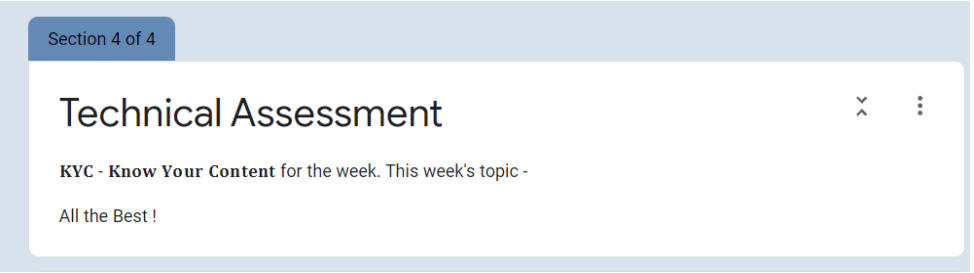
This section contains the proof of the above vulnerabilities as the screenshot of the vulnerability of the lab

Step 10	Don't forget to remove the **NOTES** given in the template. It is just for your reference.	**NOTES:** • **Everything mentioned inside () has to be changed based on your lab and sub-labs.** • **Here it is given with 2 Sub-labs vulnerability, you need to add all the sub-labs based on your lab.** • **Don't forget to take the screenshot of the vulnerability in the sub-labs** • **Add the screenshots to google drive and share the link of the folder containing those screenshots in the Proof of Concept session.** • **This NOTE session is only for your reference, don't forget to delete this in the report you submit.**
Step 11	After completing the work, now click on the **share** button and create a share link with the **Commenter** permission.	

Important	You are required to submit the link to your Report in the **weekly assessment form**.	

Learn, Test, and Share!

Task 3 - Assessment Test [Mandatory]

Important	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. **You need to score 70% in this specific Week's Technical Assessment in order to proceed with the internship.**	
Note:	• Number of questions could vary from 30 to 50 per week. • Make sure to take **Notes** on what you do. It is recommended to do research as all of this will help you in the **Weekly Assessment Test** which will be provided to you in the submission form.	

Learn, Test, and Share!

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