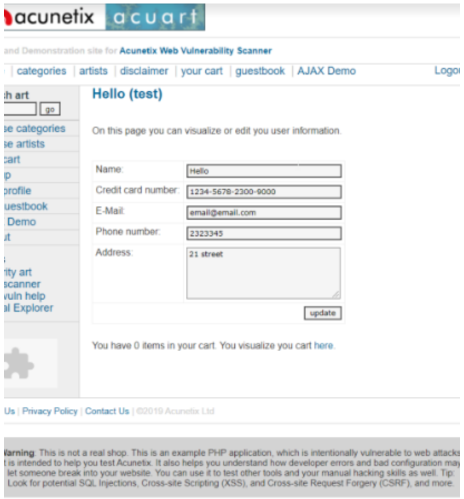
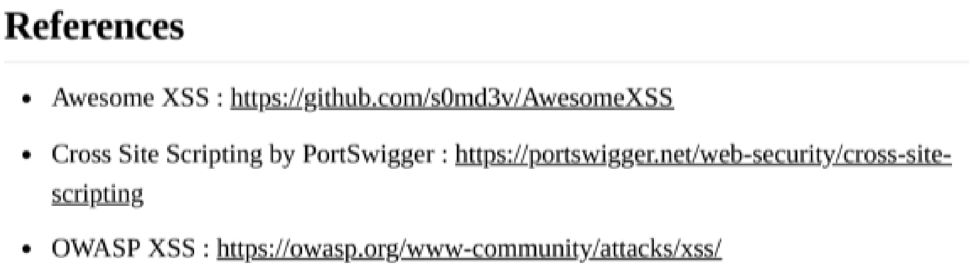
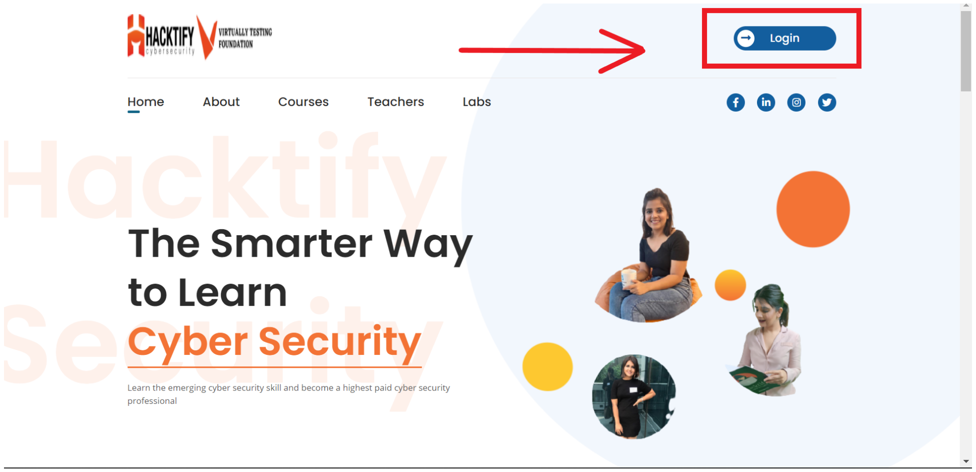
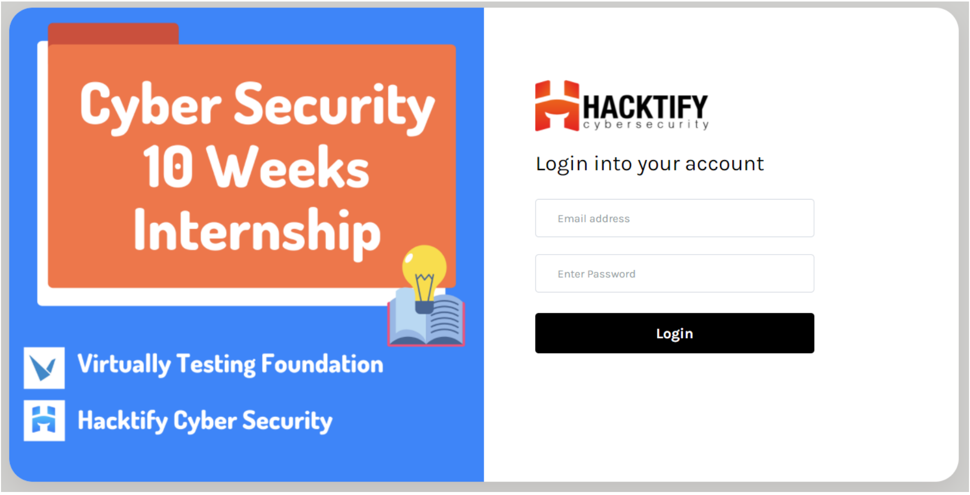
Week 3 Technical Guide

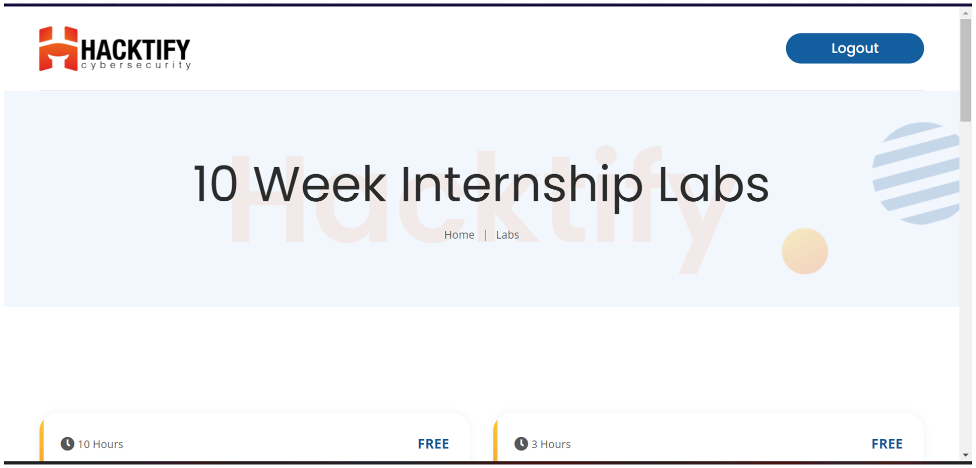
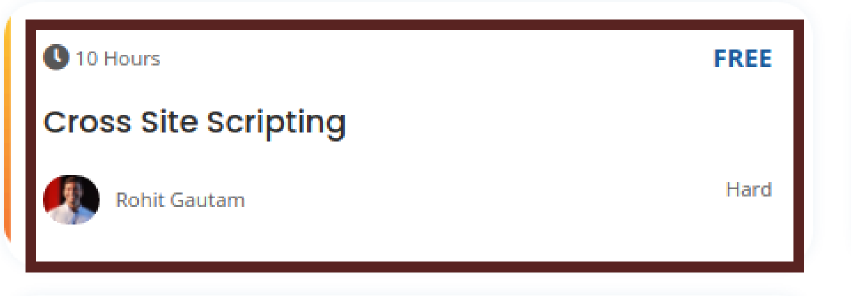
Task 1 - Weekly Labs [Mandatory]

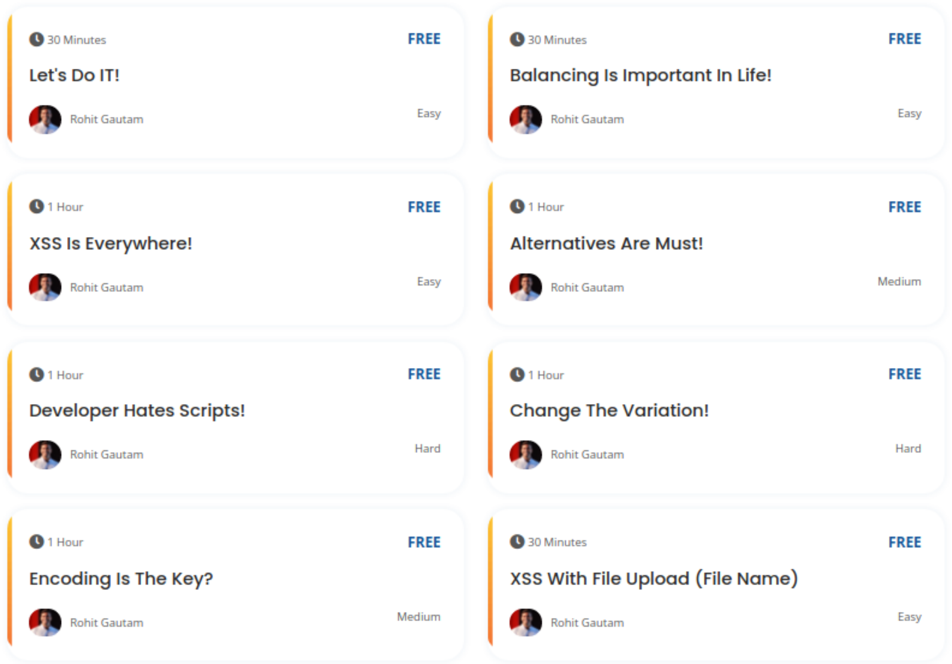
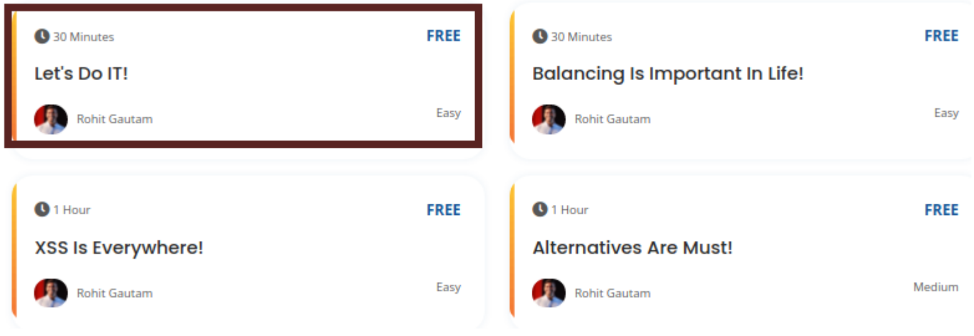
Cross-Site Scripting (XSS) Lab

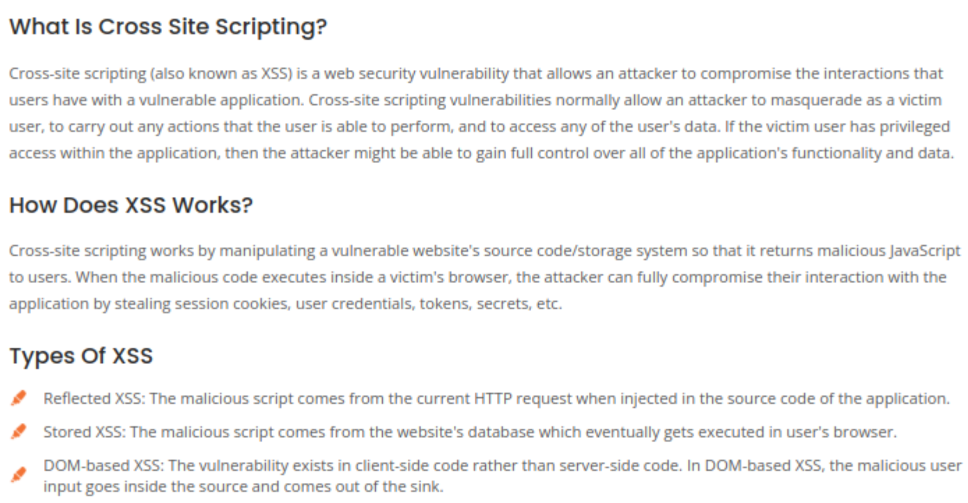
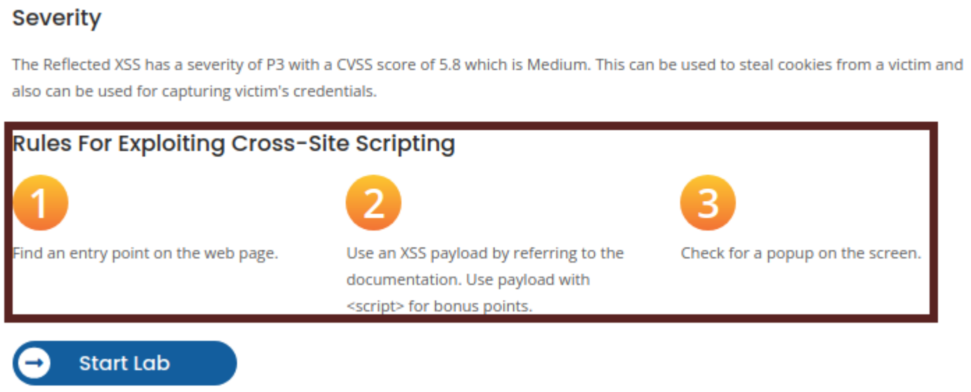
Important:	Make sure to take **Notes** as you proceed with your labs. It can include ● The steps you have taken ● Tools you have used ● The payloads you have used, and so on And also do your research on that specific vulnerability as all of this will help you in the **Weekly Assessment Test** which will be provided to you.	
Step 1	Hope you all have gone through the study material on Cross-Site Scripting for this week.	Cross-Site Scripting (XSS)

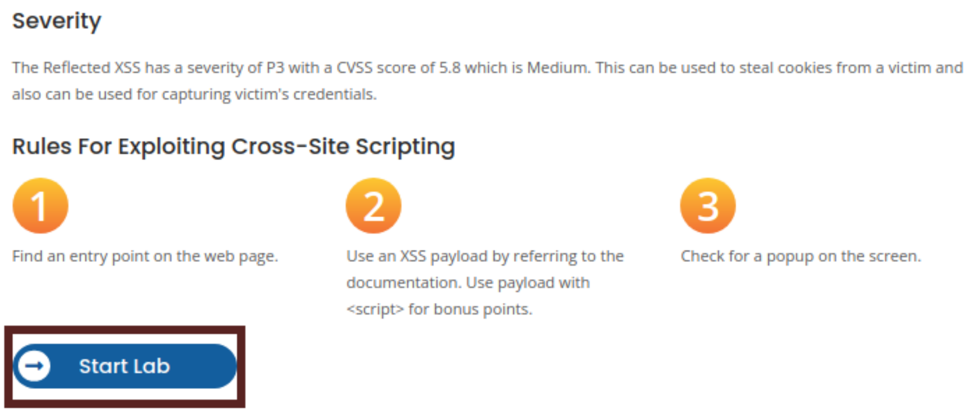
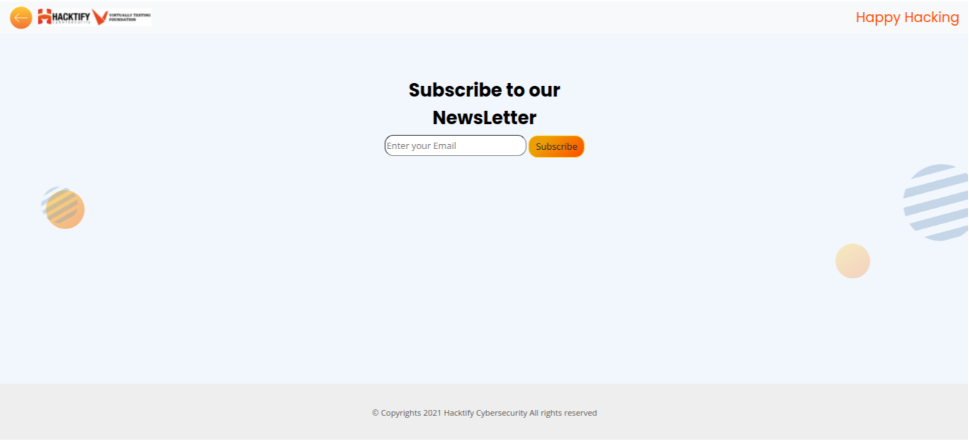
Step 2	Go through the links mentioned in the guide as they have examples of vulnerable websites as shown to the right, and you can practice that on your own to get a better understanding of vulnerabilities before accessing the labs.	 acunetix acuart and Demonstration site for Acunetix Web Vulnerability Scanner categories | artists | disclaimer | your cart | guestbook | AJAX Demo Logo h art go se categories se artists cart p profile uestbook Demo t ity art scanner vuln help l Explorer **Hello (test)** On this page you can visualize or edit you user information. Name: Hello Credit card number: 1234-5678-2300-9000 E-Mail: email@email.com Phone number: 2323345 Address: 21 street update You have 0 items in your cart. You visualize you cart here. Us | Privacy Policy | Contact Us | ©2019 Acunetix Ltd **arning**: This is not a real shop. This is an example PHP application, which is intentionally vulnerable to web attacks t is intended to help you test Acunetix. It also helps you understand how developer errors and bad configuration may let someone break into your website. You can use it to test other tools and your manual hacking skills as well. Tip: Look for potential SQL Injections, Cross-site Scripting (XSS), and Cross-site Request Forgery (CSRF), and more.
Step 3	Also make sure to check out the **references** mentioned at the end of the guide. They are very helpful.	 **References** • Awesome XSS : https://github.com/s0md3v/AwesomeXSS • Cross Site Scripting by PortSwigger : https://portswigger.net/web-security/cross-site-scripting • OWASP XSS : https://owasp.org/www-community/attacks/xss/
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]()

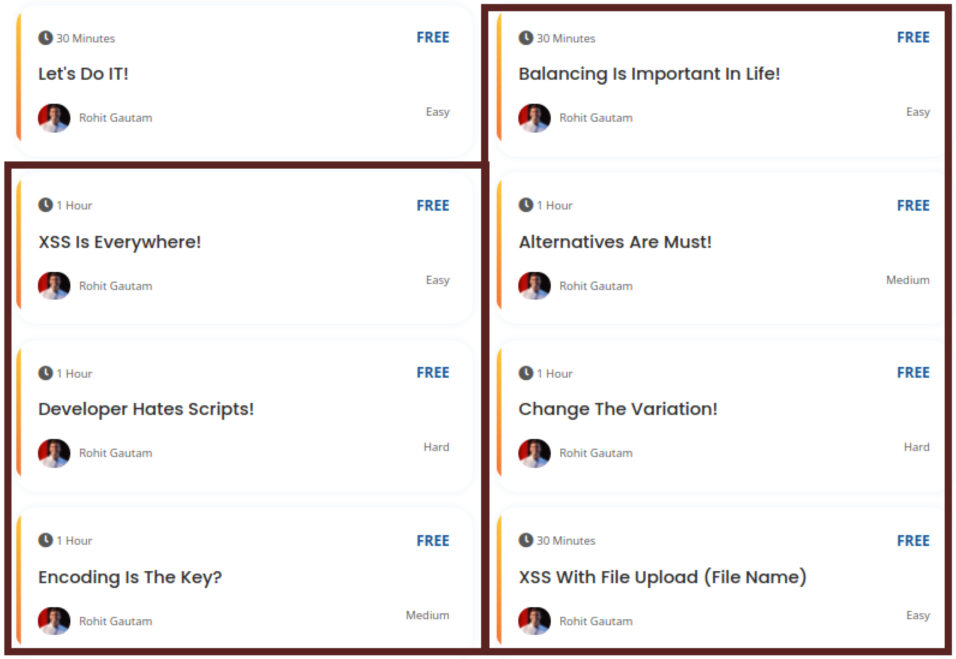
Step 5	Once you successfully open the portal link. Click on **Login**.	 HACKTIFY cybersecurity VIRTUALLY TESTING FOUNDATION Login Home About Courses Teachers Labs Hacktify Security The Smarter Way to Learn Cyber Security Learn the emerging cyber security skill and become a highest paid cyber security professional
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.	 Cyber Security 10 Weeks Internship Virtually Testing Foundation Hacktify Cyber Security HACKTIFY cybersecurity Email address Enter Password Login Login into your account

Step 7	Once you successfully logged in, you will see the **homepage** listed with labs.	 HACKTIFY cybersecurity Logout 10 Week Internship Labs Home | Labs 10 Hours FREE 3 Hours FREE
Step 8	From the list of labs, open the **Cross Site Scripting Lab**.	 10 Hours FREE Cross Site Scripting Rohit Gautam Hard

Step 9	Once you open the **Cross Site Scripting Labs,** you will be assigned with sub-labs as shown. **NOTE:** Here there are 11 sub-labs assigned to you. There might be multiple sub-labs in each of the main labs.	 30 Minutes FREE Let's Do IT! Rohit Gautam Easy 30 Minutes FREE Balancing Is Important In Life! Rohit Gautam Easy 1 Hour FREE XSS Is Everywhere! Rohit Gautam Easy 1 Hour FREE Alternatives Are Must! Rohit Gautam Medium 1 Hour FREE Developer Hates Scripts! Rohit Gautam Hard 1 Hour FREE Change The Variation! Rohit Gautam Hard 1 Hour FREE Encoding Is The Key? Rohit Gautam Medium 30 Minutes FREE XSS With File Upload (File Name) Rohit Gautam Easy
Step 10	Now open **Let's DO IT!,** Cross Site Scripting sub-lab 1 will open up.	 30 Minutes FREE Let's Do IT! Rohit Gautam Easy 30 Minutes FREE Balancing Is Important In Life! Rohit Gautam Easy 1 Hour FREE XSS Is Everywhere! Rohit Gautam Easy 1 Hour FREE Alternatives Are Must! Rohit Gautam Medium

Step 11	After opening the sub-lab, first go through the given details in the lab.	 **What Is Cross Site Scripting?** Cross-site scripting (also known as XSS) is a web security vulnerability that allows an attacker to compromise the interactions that users have with a vulnerable application. Cross-site scripting vulnerabilities normally allow an attacker to masquerade as a victim user, to carry out any actions that the user is able to perform, and to access any of the user's data. If the victim user has privileged access within the application, then the attacker might be able to gain full control over all of the application's functionality and data. **How Does XSS Works?** Cross-site scripting works by manipulating a vulnerable website's source code/storage system so that it returns malicious JavaScript to users. When the malicious code executes inside a victim's browser, the attacker can fully compromise their interaction with the application by stealing session cookies, user credentials, tokens, secrets, etc. **Types Of XSS** ✎ Reflected XSS: The malicious script comes from the current HTTP request when injected in the source code of the application. ✎ Stored XSS: The malicious script comes from the website's database which eventually gets executed in user's browser. ✎ DOM-based XSS: The vulnerability exists in client-side code rather than server-side code. In DOM-based XSS, the malicious user input goes inside the source and comes out of the sink.
Step 12	The highlighted portion are the **goals** that you have to accomplish for this lab.	 **Severity** The Reflected XSS has a severity of P3 with a CVSS score of 5.8 which is Medium. This can be used to steal cookies from a victim and also can be used for capturing victim's credentials. **Rules For Exploiting Cross-Site Scripting** 1 Find an entry point on the web page. 2 Use an XSS payload by referring to the documentation. Use payload with <script> for bonus points. 3 Check for a popup on the screen. Start Lab

Step 13	Once you are clear with **goals,** click on **Start Lab.**	 Severity The Reflected XSS has a severity of P3 with a CVSS score of 5.8 which is Medium. This can be used to steal cookies from a victim and also can be used for capturing victim's credentials. Rules For Exploiting Cross-Site Scripting 1 Find an entry point on the web page. 2 Use an XSS payload by referring to the documentation. Use payload with <script> for bonus points. 3 Check for a popup on the screen.
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.	 Subscribe to our NewsLetter Enter your Email Subscribe © Copyrights 2021 Hacktify Cybersecurity All rights reserved

Step 15	After completion of sub-lab 1 **Let's DO IT!**, move on to the next sub-lab and repeat the process from step 12. You have to follow the same procedure for every sub-lab available in the list.	

30 Minutes FREE
Let's Do IT!
Rohit Gautam Easy

30 Minutes FREE
Balancing Is Important In Life!
Rohit Gautam Easy

1 Hour FREE
XSS Is Everywhere!
Rohit Gautam Easy

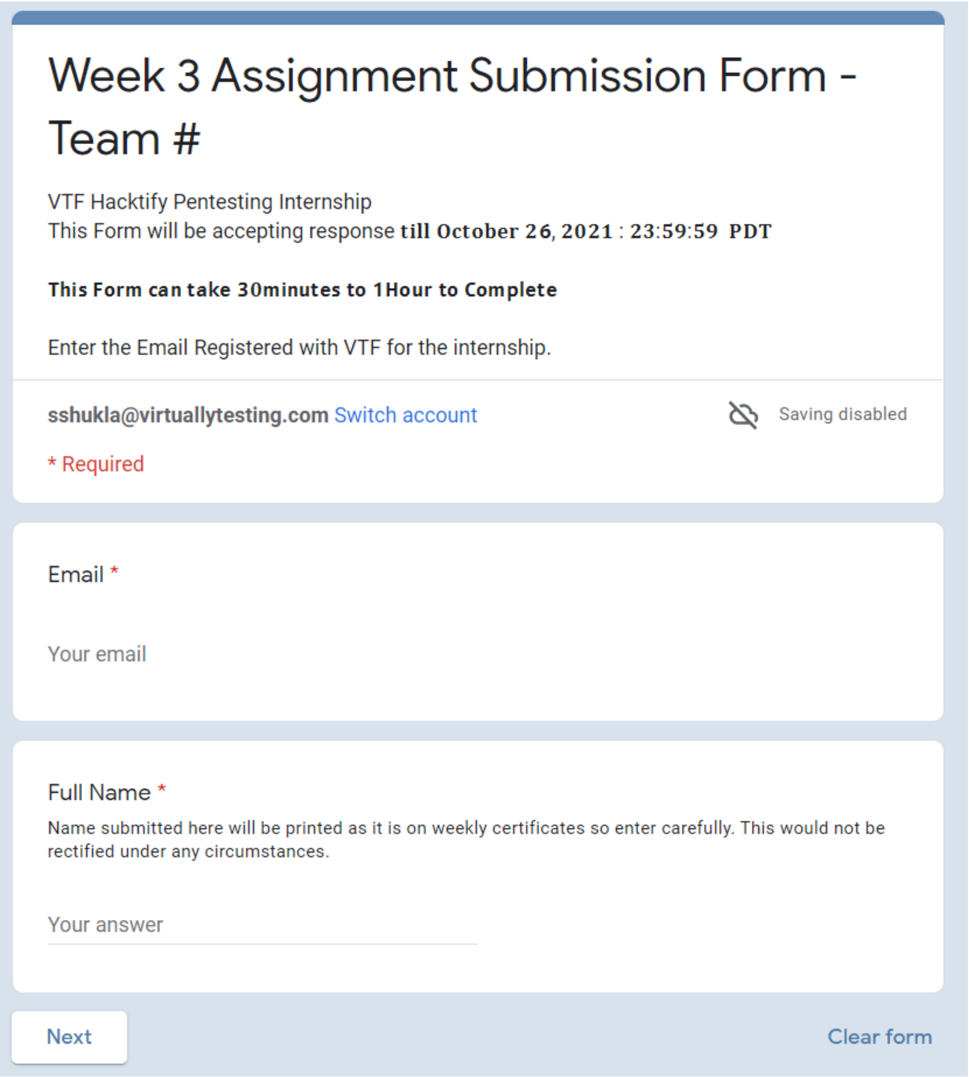
1 Hour FREE
Alternatives Are Must!
Rohit Gautam Medium

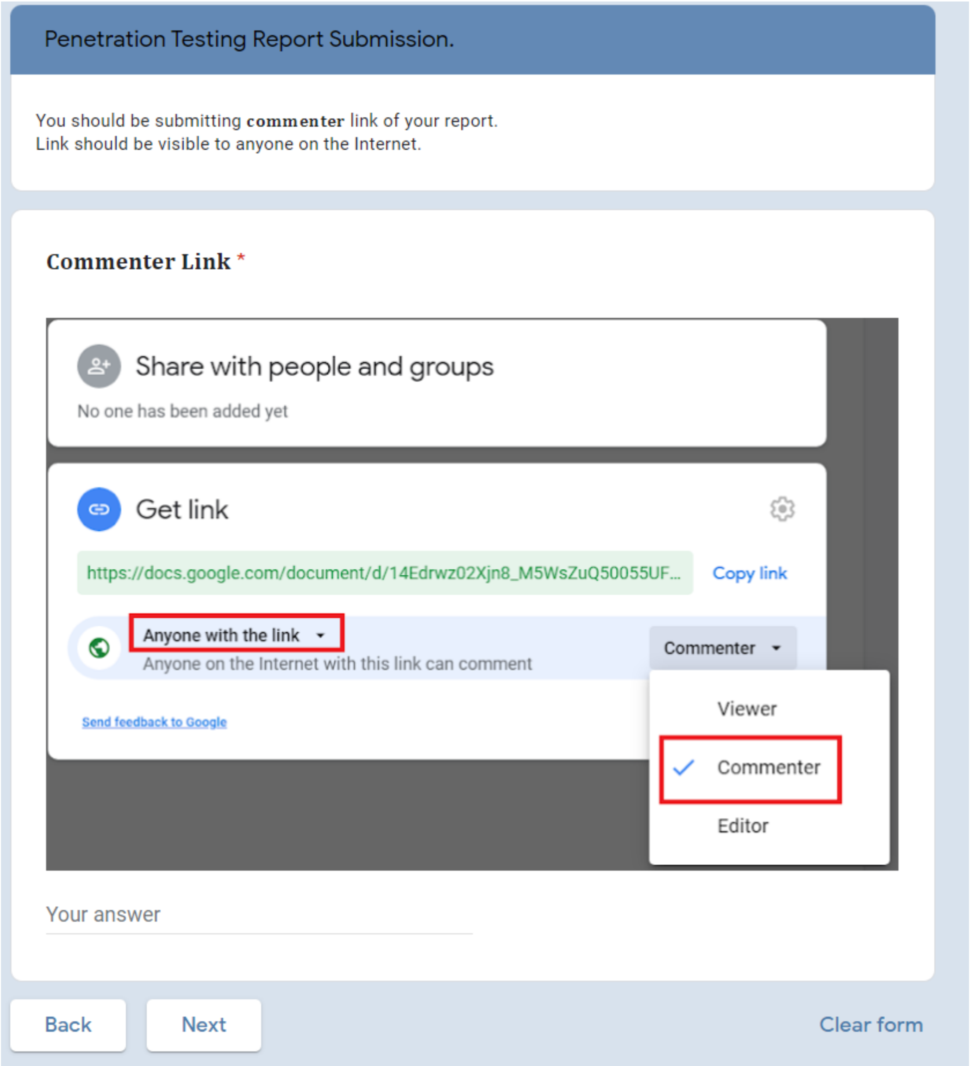
1 Hour FREE
Developer Hates Scripts!
Rohit Gautam Hard

1 Hour FREE
Change The Variation!
Rohit Gautam Hard

1 Hour FREE
Encoding Is The Key?
Rohit Gautam Medium

30 Minutes FREE
XSS With File Upload (File Name)
Rohit Gautam Easy

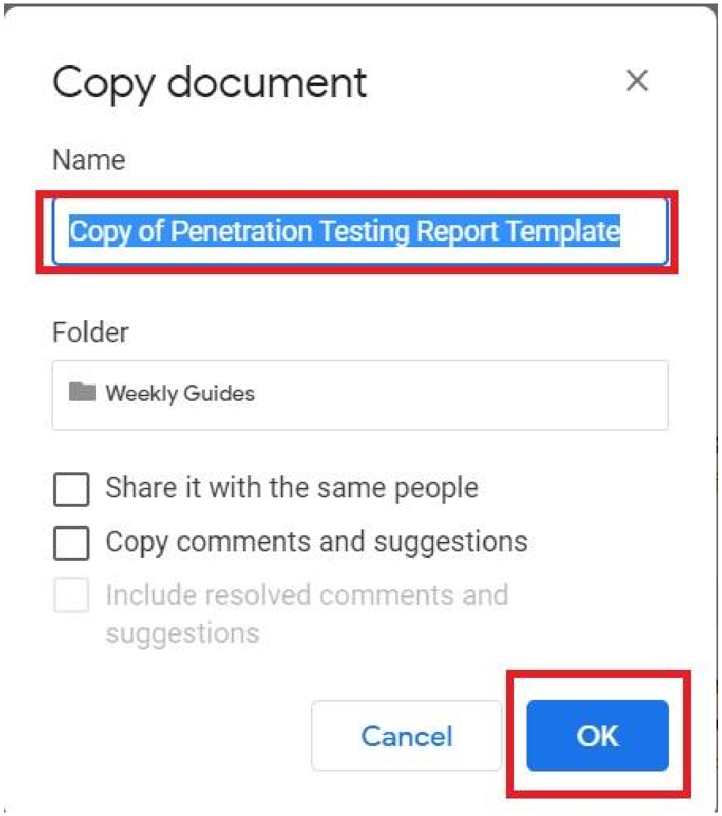
Step 16	Make sure to take **Notes** as you proceed with your labs. It can include ● The steps you have taken ● Tools you have used ● The payloads you have used, and so on. And also do your research on that specific vulnerability as all of this will help you in the **Weekly Assessment Test** which will be provided to you.	 Week 3 Assignment Submission Form - Team # VTF Hacktify Pentesting Internship This Form will be accepting response **till October 26, 2021 : 23:59:59 PDT** **This Form can take 30minutes to 1Hour to Complete** Enter the Email Registered with VTF for the internship. **sshukla@virtuallytesting.com** Switch account Saving disabled * Required Email * Your email Full Name * Name submitted here will be printed as it is on weekly certificates so enter carefully. This would not be rectified under any circumstances. Your answer Next Clear form

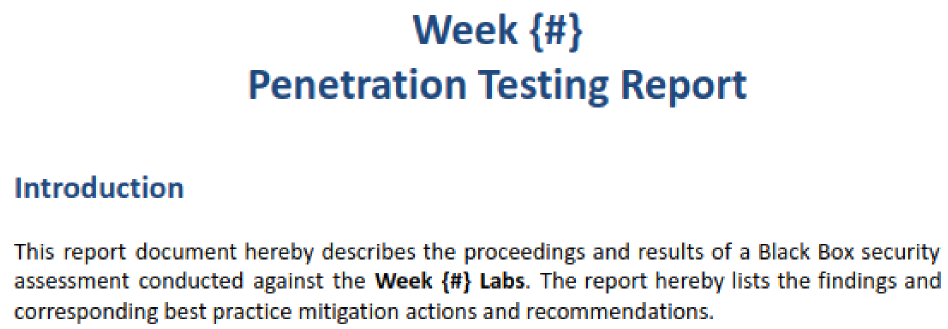
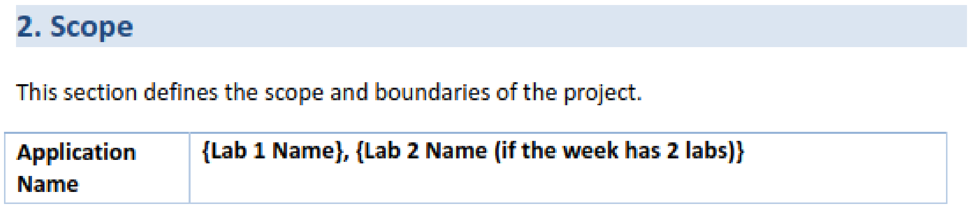
Step 17	Make sure to take a **Pentesting Report** as you proceed with your labs. ● You are required to submit your Report in the assessment form in the section shown in the image.	 Penetration Testing Report Submission. You should be submitting **commenter** link of your report. Link should be visible to anyone on the Internet. **Commenter Link** * Share with people and groups No one has been added yet Get link https://docs.google.com/document/d/14Edrwz02Xjn8_M5WsZuQ50055UF... Copy link Anyone with the link ▾ Anyone on the Internet with this link can comment Commenter ▾ Viewer ✓ Commenter Editor Send feedback to Google Your answer Back Next Clear form

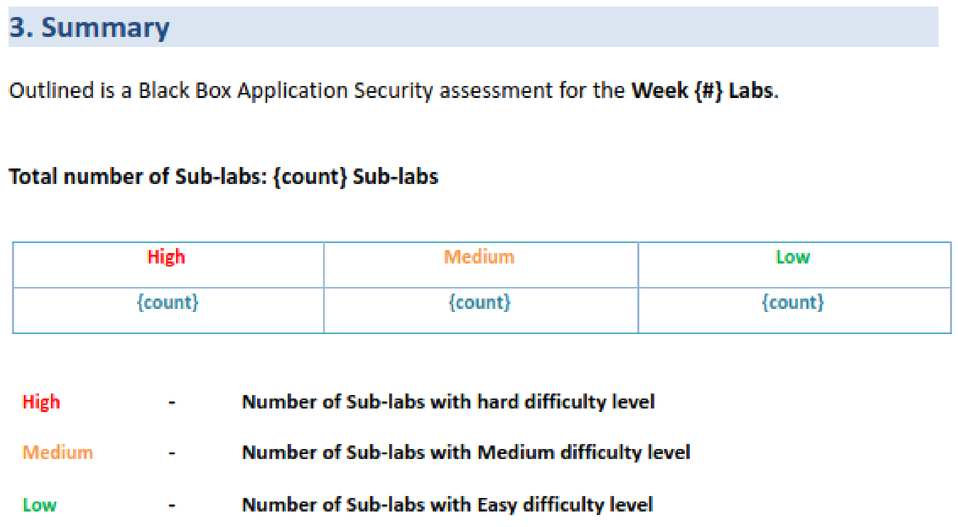
Task 2 - Penetration Testing Report

[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.	 Copy document 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	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 3** **Note:** **Everything mentioned inside the {} has to be changed.**	 **Week {#}** **Penetration Testing Report** **Introduction** 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.
Step 5	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.**	 **2. Scope** This section defines the scope and boundaries of the project. **Application Name** **{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

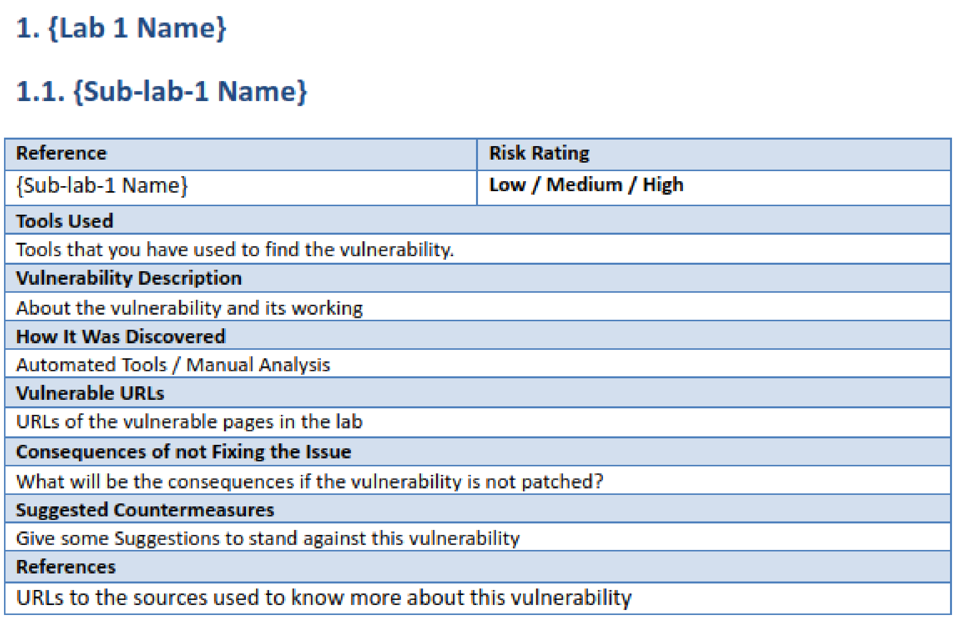
High	Medium	Low
{count}	{count}	{count}

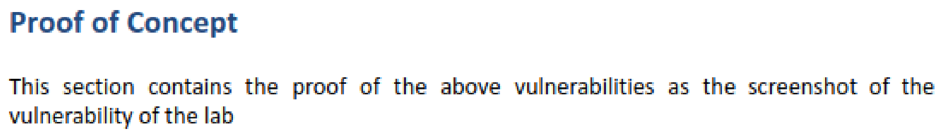
High - **Number of Sub-labs with hard difficulty level**

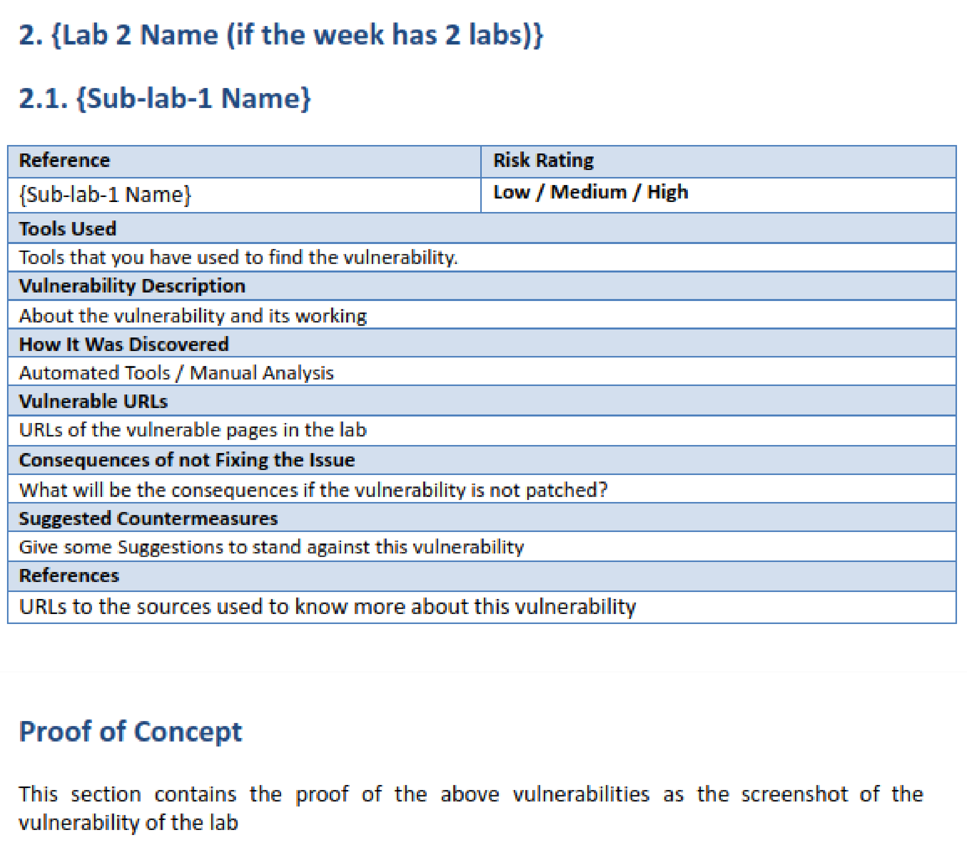
Medium - **Number of Sub-labs with Medium difficulty level**

Low - **Number of Sub-labs with Easy difficulty level**

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

<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></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><b>Low / Medium / High</b></td></tr>
<tr><td colspan="2"><b>Tools Used</b></td></tr>
<tr><td colspan="2">Tools that you have used to find the vulnerability.</td></tr>
<tr><td colspan="2"><b>Vulnerability Description</b></td></tr>
<tr><td colspan="2">About the vulnerability and its working</td></tr>
<tr><td colspan="2"><b>How It Was Discovered</b></td></tr>
<tr><td colspan="2">Automated Tools / Manual Analysis</td></tr>
<tr><td colspan="2"><b>Vulnerable URLs</b></td></tr>
<tr><td colspan="2">URLs of the vulnerable pages in the lab</td></tr>
<tr><td colspan="2"><b>Consequences of not Fixing the Issue</b></td></tr>
<tr><td colspan="2">What will be the consequences if the vulnerability is not patched?</td></tr>
<tr><td colspan="2"><b>Suggested Countermeasures</b></td></tr>
<tr><td colspan="2">Give some Suggestions to stand against this vulnerability</td></tr>
<tr><td colspan="2"><b>References</b></td></tr>
<tr><td colspan="2">URLs to the sources used to know more about this vulnerability</td></tr>
</table>
</td>
</tr>
<tr>
<td><b>Step 8</b></td>
<td>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.

<b>Note:</b>
<b>1 Screenshot is needed for each sub-labs and not more than that.</b></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>

<table>
<tr>
<td><b>Step 9</b></td>
<td><b>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.</b></td>
<td>


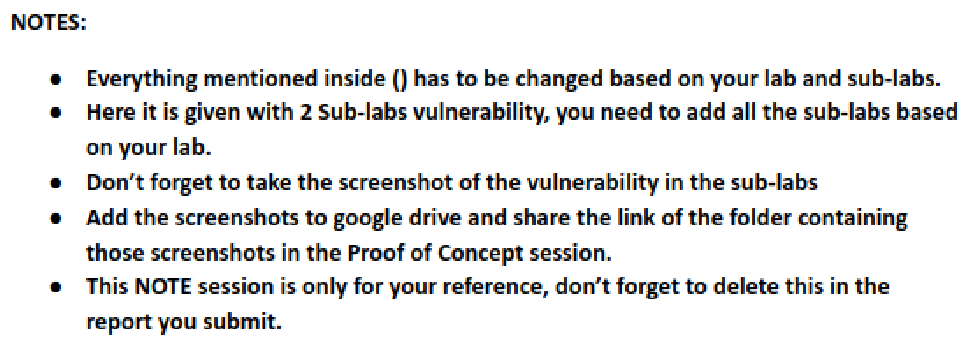
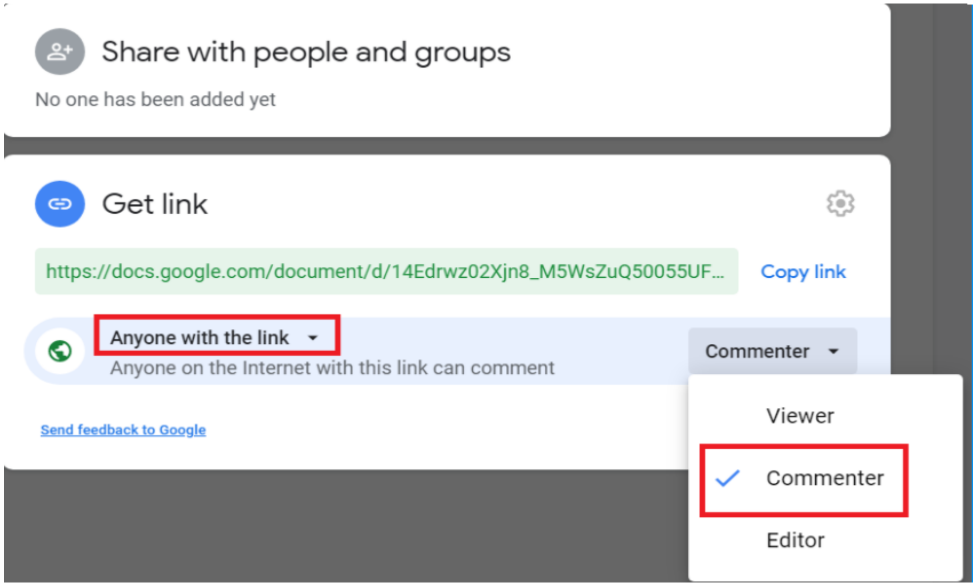
<h2>2. {Lab 2 Name (if the week has 2 labs)}</h2>

<h3>2.1. {Sub-lab-1 Name}</h3>

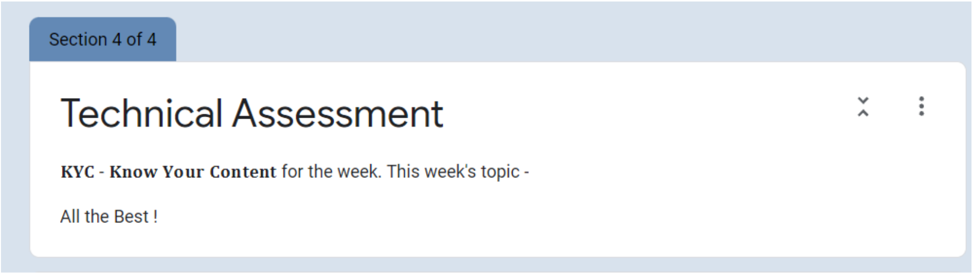
<table>
<tr><th>Reference</th><th>Risk Rating</th></tr>
<tr><td>{Sub-lab-1 Name}</td><td><b>Low / Medium / High</b></td></tr>
<tr><td colspan="2"><b>Tools Used</b></td></tr>
<tr><td colspan="2">Tools that you have used to find the vulnerability.</td></tr>
<tr><td colspan="2"><b>Vulnerability Description</b></td></tr>
<tr><td colspan="2">About the vulnerability and its working</td></tr>
<tr><td colspan="2"><b>How It Was Discovered</b></td></tr>
<tr><td colspan="2">Automated Tools / Manual Analysis</td></tr>
<tr><td colspan="2"><b>Vulnerable URLs</b></td></tr>
<tr><td colspan="2">URLs of the vulnerable pages in the lab</td></tr>
<tr><td colspan="2"><b>Consequences of not Fixing the Issue</b></td></tr>
<tr><td colspan="2">What will be the consequences if the vulnerability is not patched?</td></tr>
<tr><td colspan="2"><b>Suggested Countermeasures</b></td></tr>
<tr><td colspan="2">Give some Suggestions to stand against this vulnerability</td></tr>
<tr><td colspan="2"><b>References</b></td></tr>
<tr><td colspan="2">URLs to the sources used to know more about this vulnerability</td></tr>
</table>

<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 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.	 Share with people and groups No one has been added yet Get link https://docs.google.com/document/d/14Edrwz02Xjn8_M5WsZuQ50055UF... Copy link Anyone with the link Anyone on the Internet with this link can comment Commenter Viewer ✓ Commenter Editor Send feedback to Google
Important	You are required to submit the link to your Report in the **weekly assessment form**.	

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 (aka week 3) in order to proceed with the internship.**	 Section 4 of 4 Technical Assessment **KYC** - **Know Your Content** for the week. This week's topic - All the Best !
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.	

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