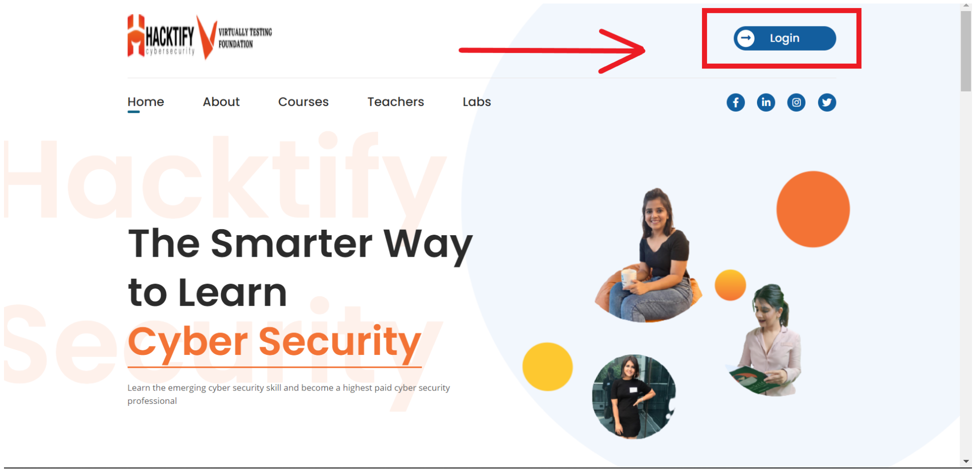
Learn, Test, and Share!

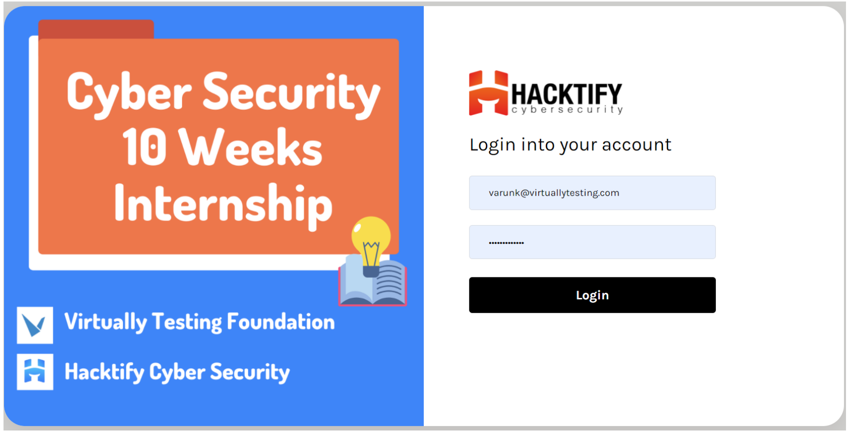
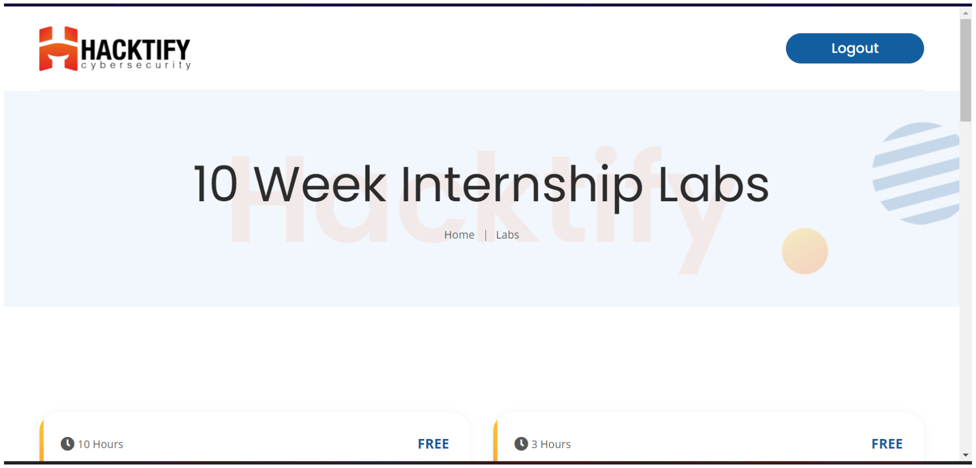
Week 10 Technical Guide

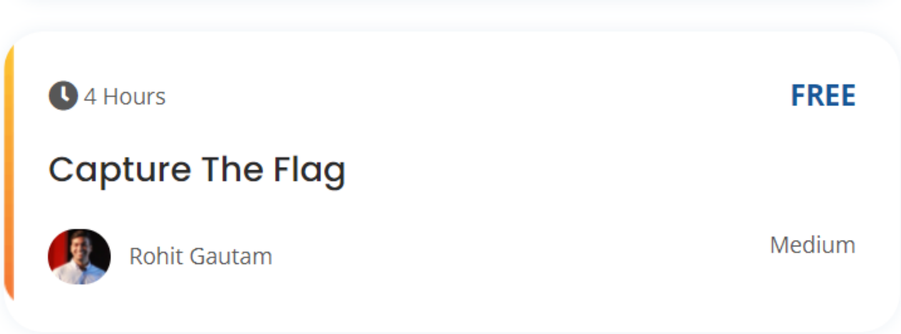
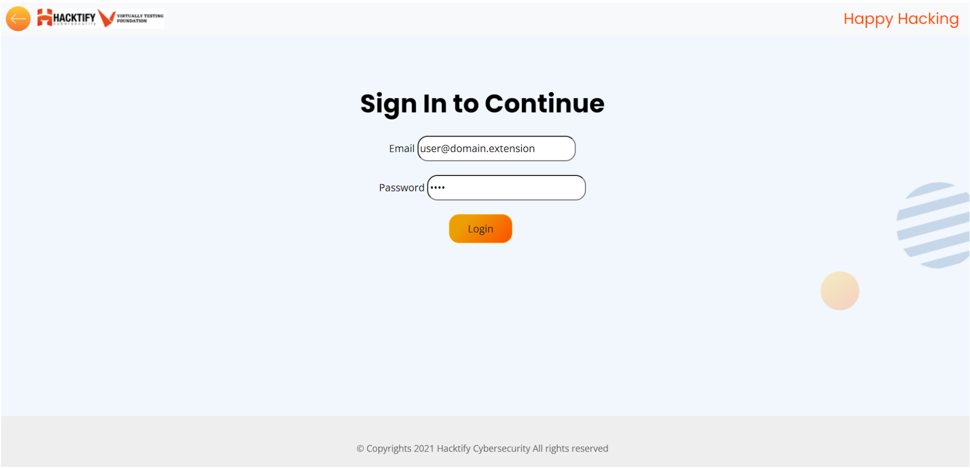
Task 1 - Weekly Labs [Mandatory]

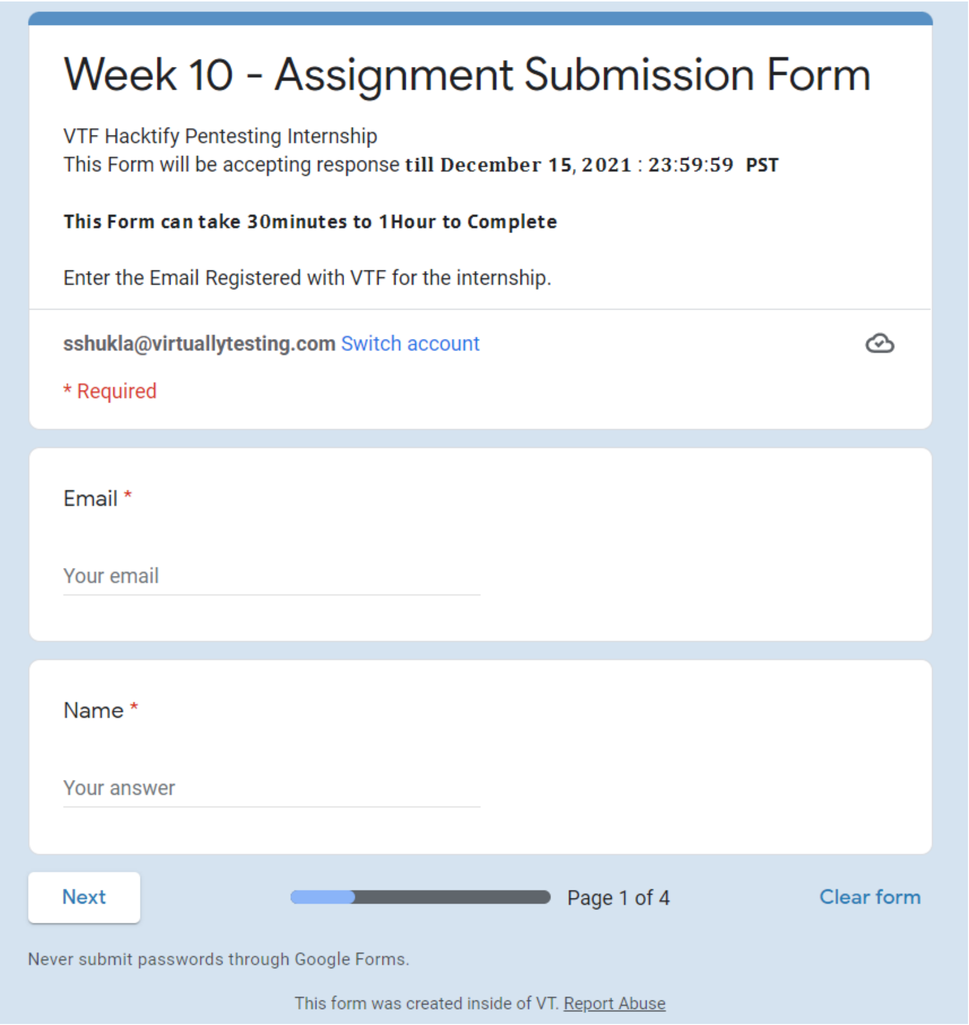
Capture The Flag

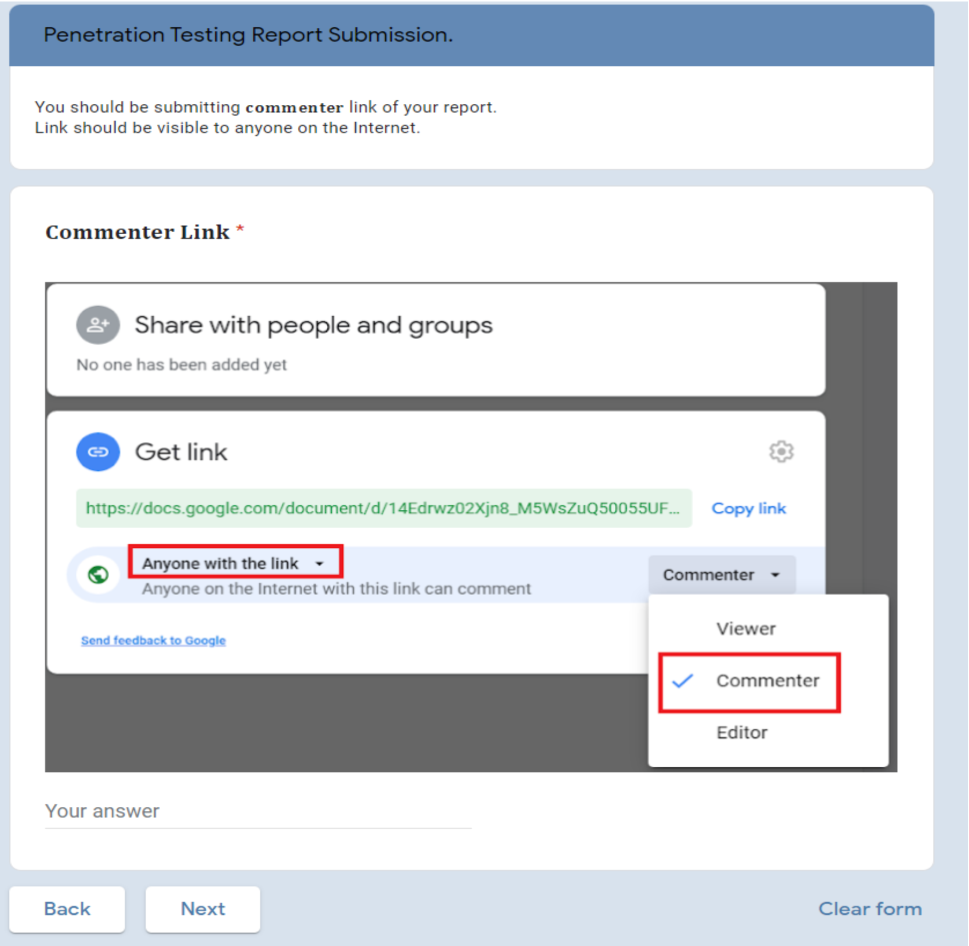
Important:	Make sure to take **Notes** as you proceed with your labs. It can include ● The steps you have taken ● Tools you have used ● The payloads you have used, and so on And also do your research on that specific vulnerability as all of this will help you in the **Weekly Assessment Test** which will be provided to you.	
Important	**Week 10 does not have any study material. You are required to play CTF by incorporating previous weeks learning.**	

Step 1	Open your registered **email** containing the Hacktify portal **credentials**.	
Step 2	Follow the **link** in the mail to open the Hacktify portal.	Hacktify Labs
Step 3	The portal will look like this. Once you successfully open the portal link. Click on **Login**.	 The Smarter Way to Learn Cyber Security Learn the emerging cyber security skill and become a highest paid cyber security professional HACKTIFY cybersecurity VIRTUALLY TESTING FOUNDATION Login Home About Courses Teachers Labs Hacktify Security

Step 4	Enter the **credentials** you received on your registered email on the following page. 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 Login Login into your account varunk@virtuallytesting.com
Step 5	The following **home page** of your portal will open up.	 HACKTIFY cybersecurity Logout Hacktify Home | Labs 10 Week Internship Labs 10 Hours FREE 3 Hours FREE
Step 6	Open your **Weekly assigned course** and start accessing your labs.	

Step 7	Open the **Capture The Flag Lab**.	
Step 8	Once you open that, the **Capture The Flag Lab Page** will open up as shown.	 4 Hours FREE Capture The Flag Rohit Gautam Medium
Step 9	Now, if you open **Capture The Flag Lab,** You will be presented with a Login page - The lab has started. **Goal**: *Try to find the Flag* **Note:** *Only one final flag has to be found.*	 HACKTIFY VIRTUALLY TESTING FOUNDATION Happy Hacking Sign In to Continue Email user@domain.extension Password •••• Login © Copyrights 2021 Hacktify Cybersecurity All rights reserved

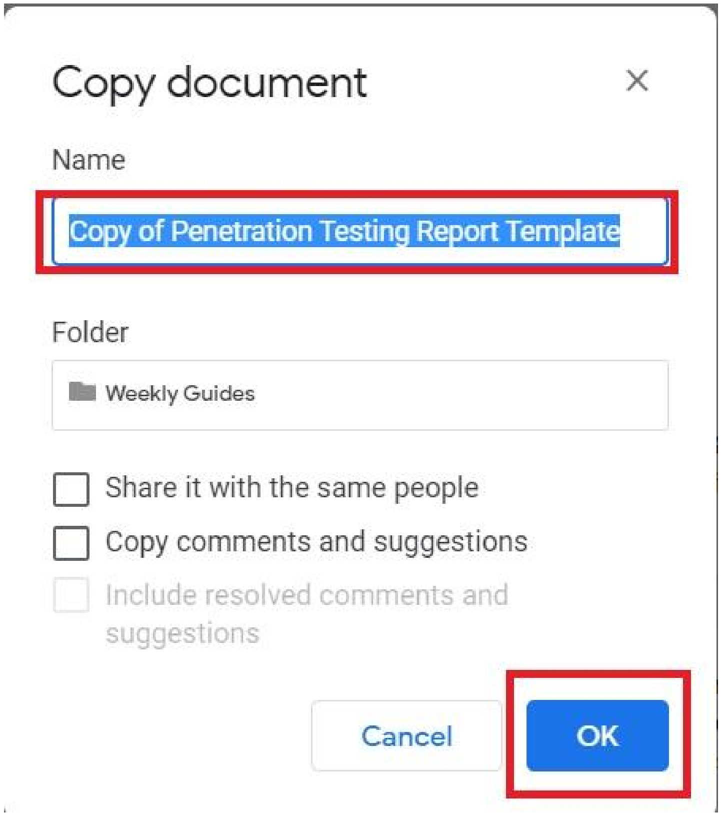
Step 10	Make sure to take **Notes** as you proceed with your labs. It can include ● The steps you have taken ● Tools you have used ● The payloads you have used, and so on. And also do your research on that specific vulnerability as all of this will help you in the **Weekly Assessment Test** which will be provided to you.	Week 10 - Assignment Submission Form VTF Hacktify Pentesting Internship This Form will be accepting response **till December 15, 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 Page 1 of 4 Clear form Never submit passwords through Google Forms. This form was created inside of VT. Report Abuse

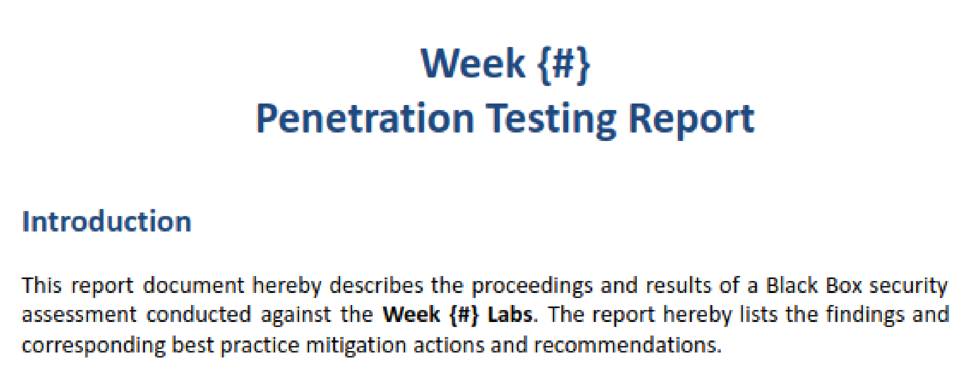
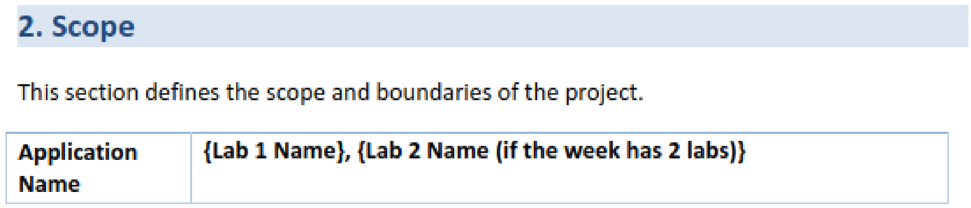
Step 11	Make sure to take a **Pentesting Report** as you proceed with your labs. ● You are required to submit your Report in the assessment form in the section shown in the image.	 Penetration Testing Report Submission. You should be submitting **commenter** link of your report. Link should be visible 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... Anyone with the link Anyone on the Internet with this link can comment Commenter Viewer ✓ Commenter Editor Your answer Copy link Send feedback to Google Back Next Clear form

Task 2 - Penetration Testing Report

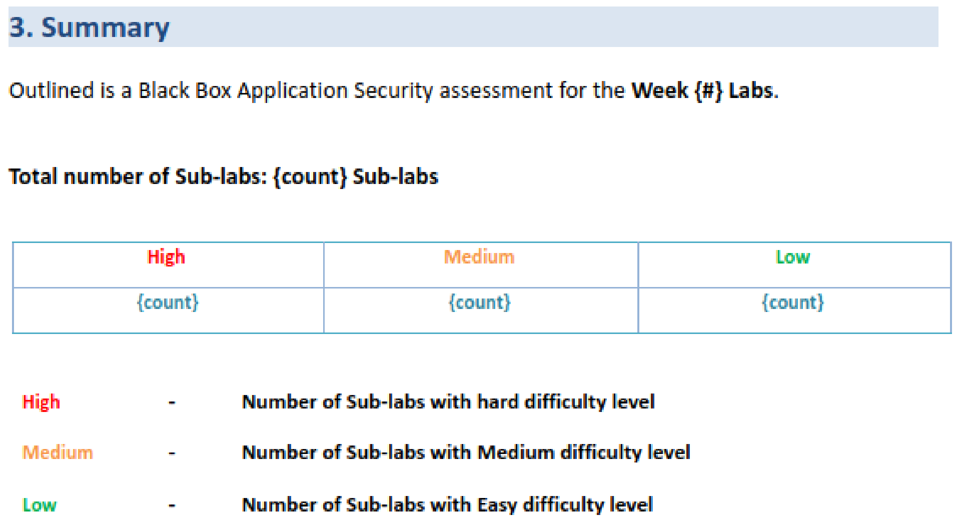
[Mandatory]

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

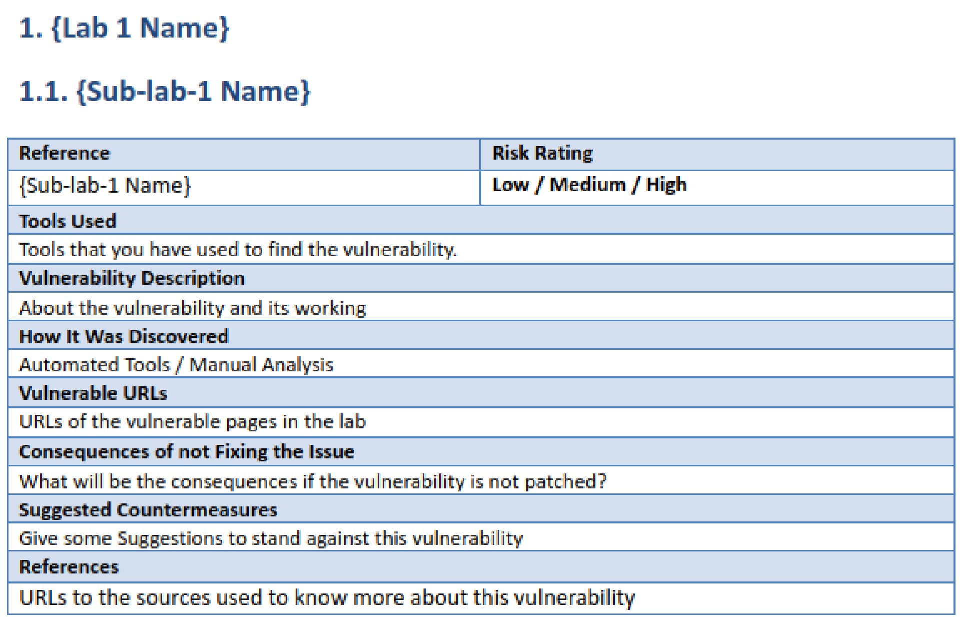
Step 2	Rename the copy to **Week_#_Penetration_Testing_Report** where # is the week number.	 Copy document Name Copy of Penetration Testing Report Template Folder Weekly Guides □ Share it with the same people □ Copy comments and suggestions □ Include resolved comments and suggestions Cancel OK

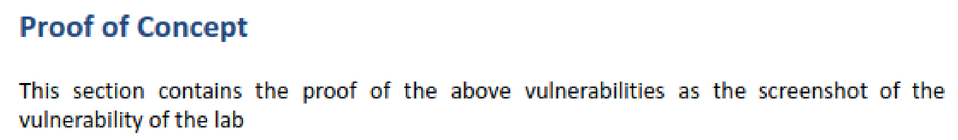
Step 3	Open the renamed copy of the template and start editing. Firstly edit the **Week {#}** of the template with the week number. **e.g) From Week {#} to Week 10** **Note:** **Everything mentioned with the {} has to be changed.**	 **Week {#}** **Penetration Testing Report** **Introduction** This report 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 4	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)}**

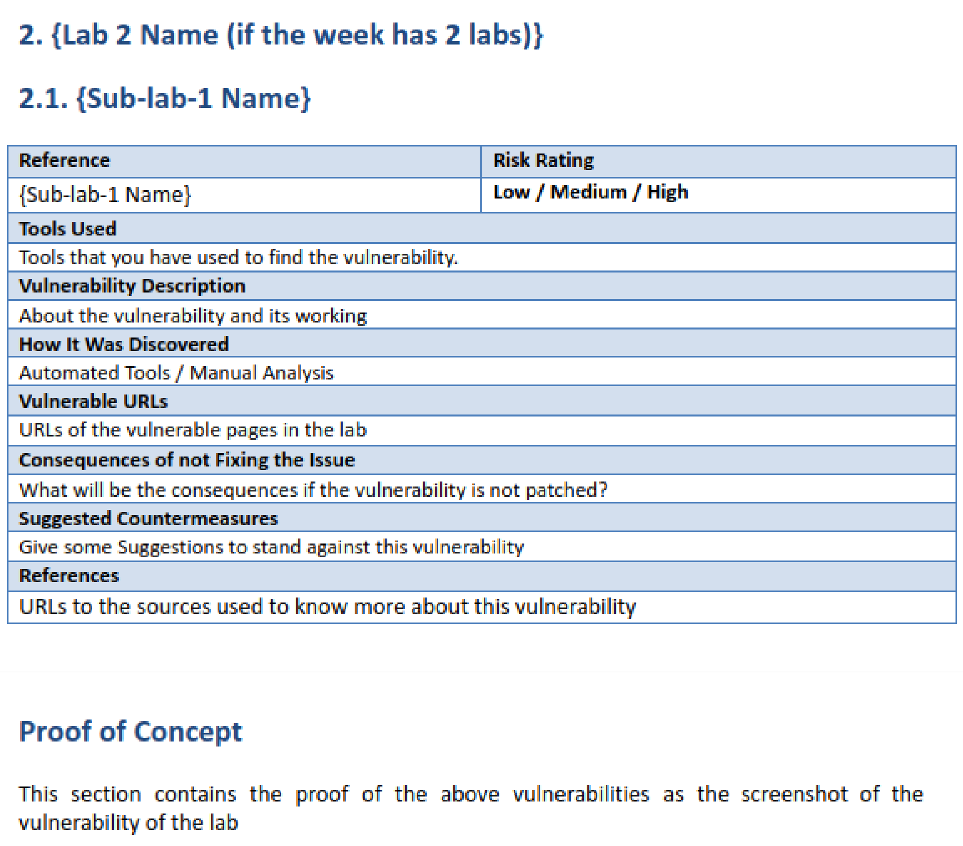
<table>
<tr>
<td><b>Step 5</b></td>
<td>In section 3, change <b>week {#}</b> and <b>{count}</b> with the number of the sub-labs present.
Change the <b>{count} inside the table</b> with the number of easy sub-labs for low, medium sub-labs for medium and hard sub-labs for hard.

<b>Note:</b>
<b>{count} is the sum of both labs if 2 labs are present.</b></td>
<td>
<h3>3. Summary</h3>
<p>Outlined is a Black Box Application Security assessment for the <b>Week {#} Labs</b>.</p>
<p><b>Total number of Sub-labs: {count} Sub-labs</b></p>
<table>
<tr><th>High</th><th>Medium</th><th>Low</th></tr>
<tr><td>{count}</td><td>{count}</td><td>{count}</td></tr>
</table>
<table>
<tr><td>High</td><td>-</td><td><b>Number of Sub-labs with hard difficulty level</b></td></tr>
<tr><td>Medium</td><td>-</td><td><b>Number of Sub-labs with Medium difficulty level</b></td></tr>
<tr><td>Low</td><td>-</td><td><b>Number of Sub-labs with Easy difficulty level</b></td></tr>
</table>
</td>
</tr>
</table>

<table>
<tr>
<td><strong>Step 6</strong></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.

<strong>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.</strong></td>
<td>
<h3>1. {Lab 1 Name}</h3>
<h4>1.1. {Sub-lab-1 Name}</h4>
<table>
<tr><th>Reference</th><th>Risk Rating</th></tr>
<tr><td>{Sub-lab-1 Name}</td><td><strong>Low / Medium / High</strong></td></tr>
<tr><td colspan="2"><strong>Tools Used</strong></td></tr>
<tr><td colspan="2">Tools that you have used to find the vulnerability.</td></tr>
<tr><td colspan="2"><strong>Vulnerability Description</strong></td></tr>
<tr><td colspan="2">About the vulnerability and its working</td></tr>
<tr><td colspan="2"><strong>How It Was Discovered</strong></td></tr>
<tr><td colspan="2">Automated Tools / Manual Analysis</td></tr>
<tr><td colspan="2"><strong>Vulnerable URLs</strong></td></tr>
<tr><td colspan="2">URLs of the vulnerable pages in the lab</td></tr>
<tr><td colspan="2"><strong>Consequences of not Fixing the Issue</strong></td></tr>
<tr><td colspan="2">What will be the consequences if the vulnerability is not patched?</td></tr>
<tr><td colspan="2"><strong>Suggested Countermeasures</strong></td></tr>
<tr><td colspan="2">Give some Suggestions to stand against this vulnerability</td></tr>
<tr><td colspan="2"><strong>References</strong></td></tr>
<tr><td colspan="2">URLs to the sources used to know more about this vulnerability</td></tr>
</table>
</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>For the <strong>Proof of Concept</strong> you are required to attach the <strong>screenshot</strong> of the <strong>vulnerability</strong> you found in the sub-labs.

<strong>Note:
1 Screenshot is needed for each sub-labs and not more than that.</strong></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 8	**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.**	

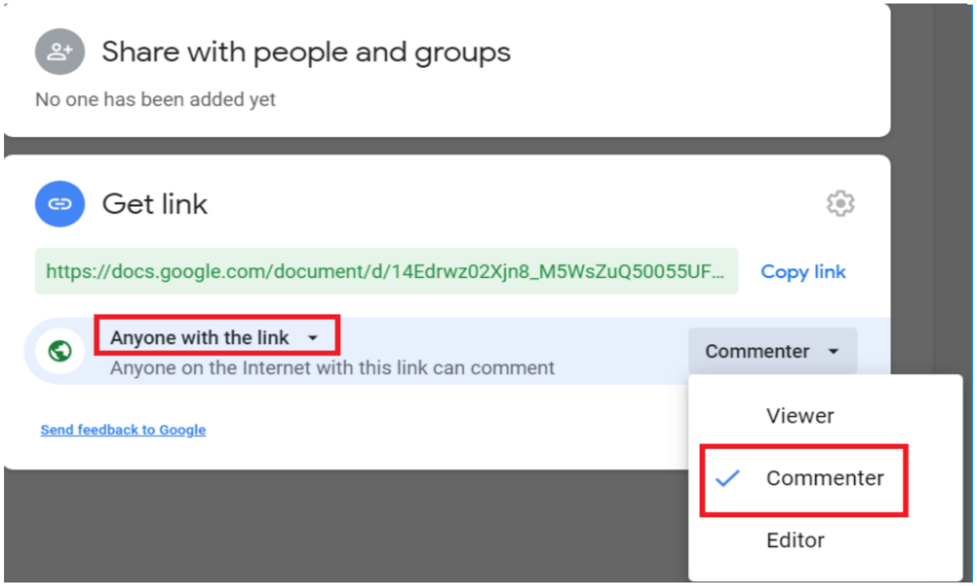
2. {Lab 2 Name (if the week has 2 labs)}

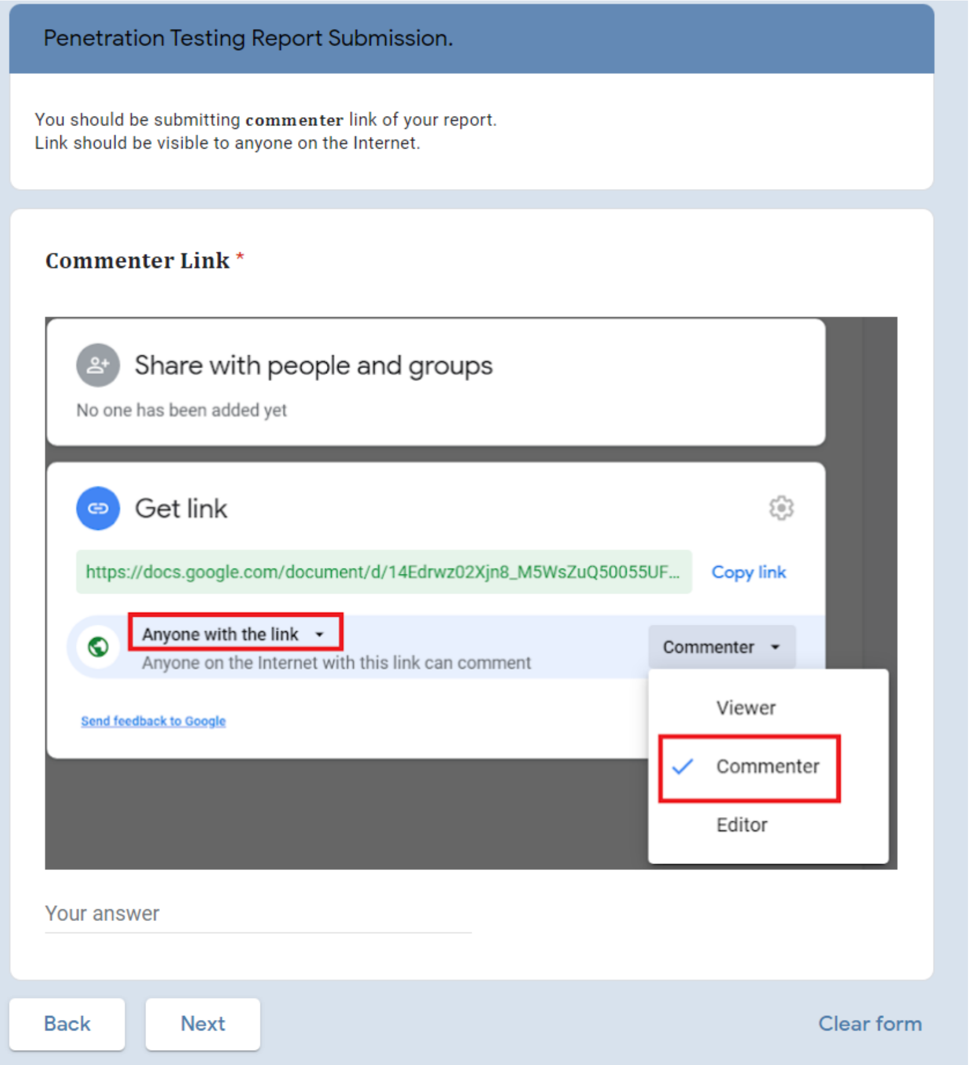
2.1. {Sub-lab-1 Name}

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	

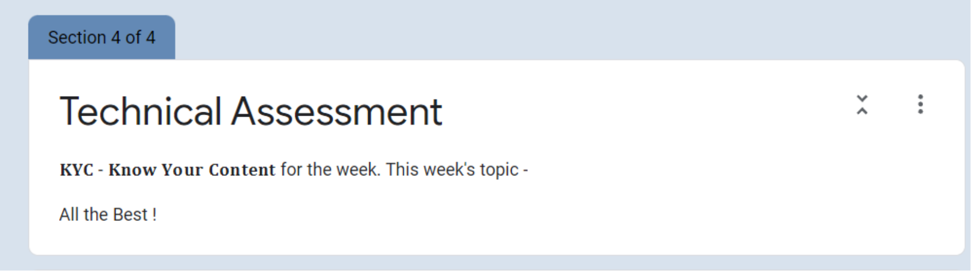
Proof of Concept

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

Step 9	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 10	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... Anyone with the link Anyone on the Internet with this link can comment Commenter Copy link Viewer Commenter Editor Send feedback to Google

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

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