Learn, Test, and Share!

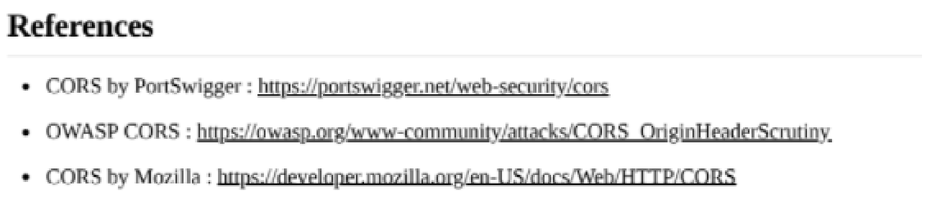
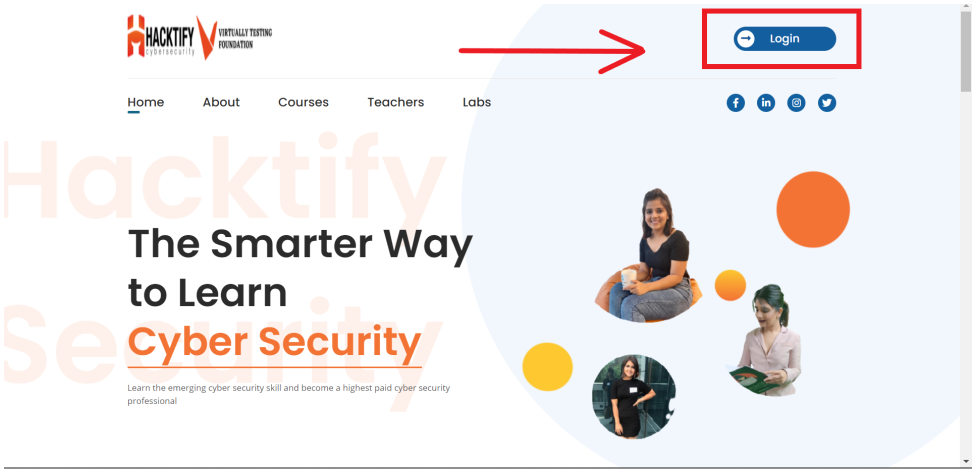
Week 5 Technical Guide

Task 1 - Weekly Labs

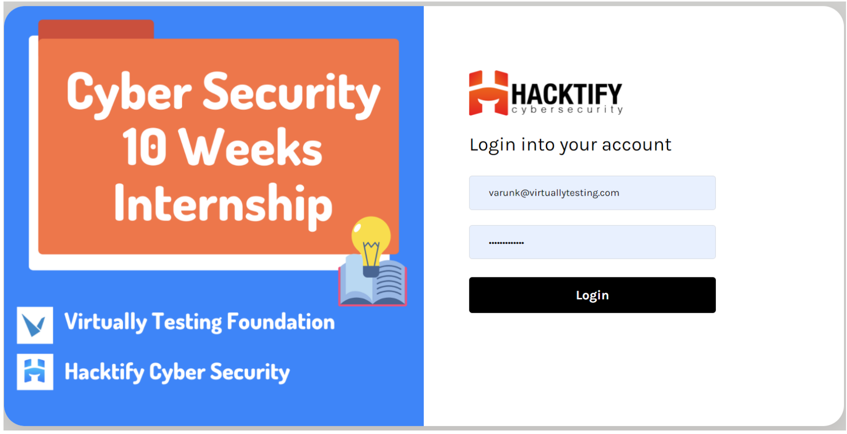
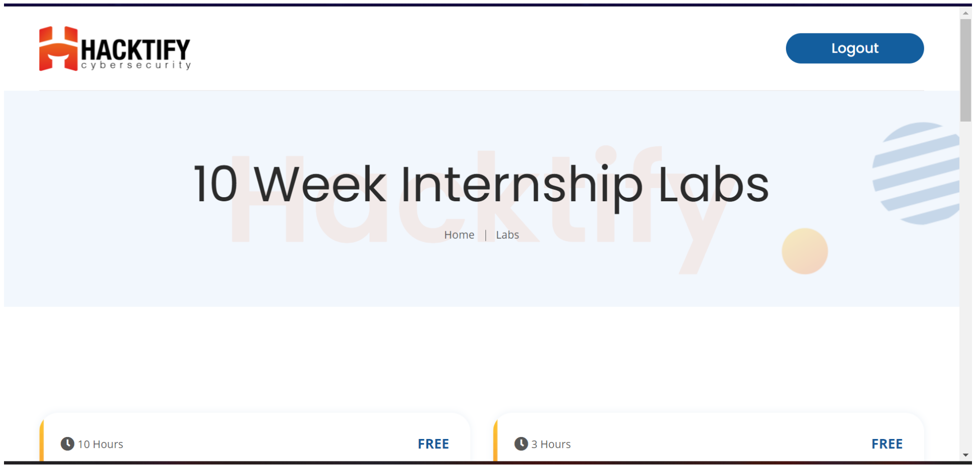
Cross Origin Resource Sharing (CORS)

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 Origin Resource Sharing (CORS)** for this week.	Cross Origin Resource Sharing (CORS)

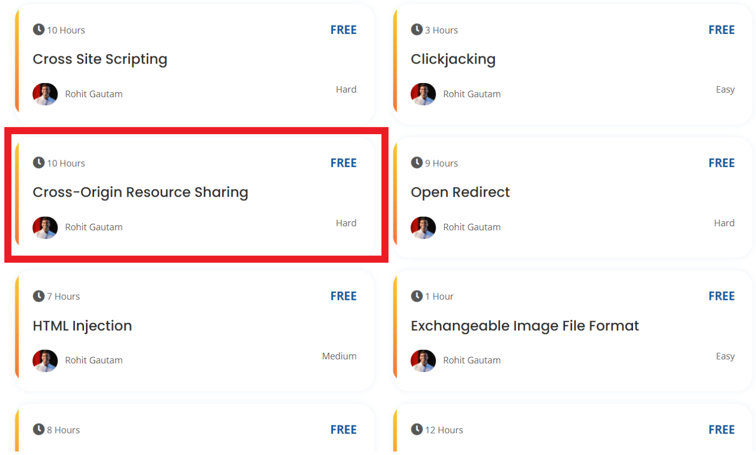
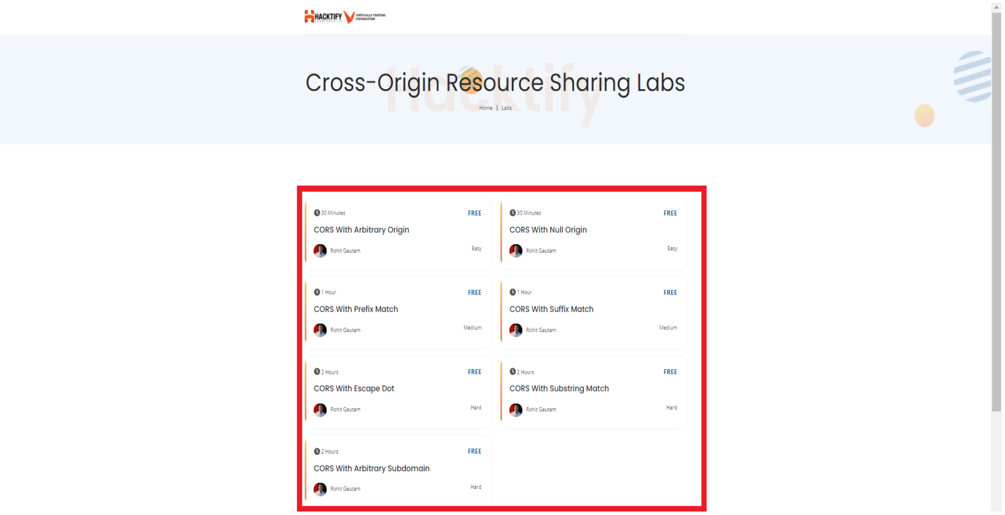
©2021 VIRTUALLY TESTING. All rights reserved.

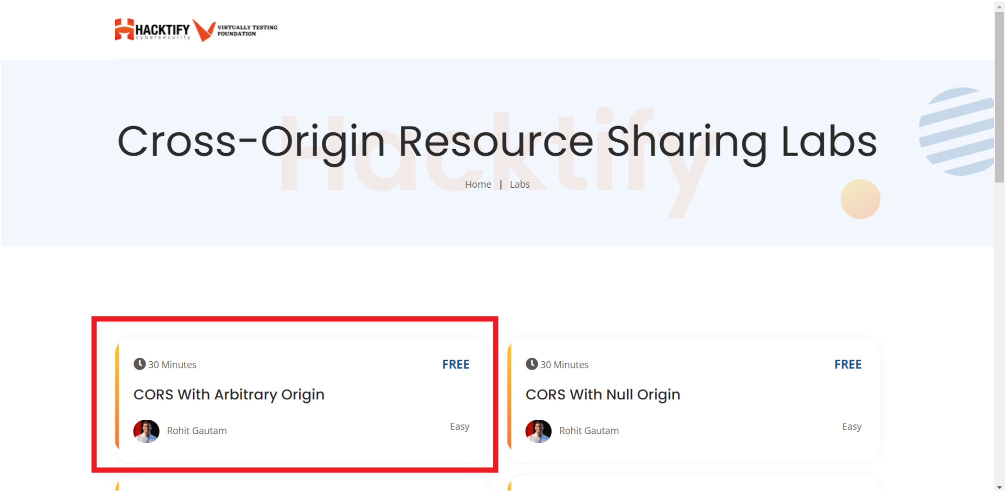
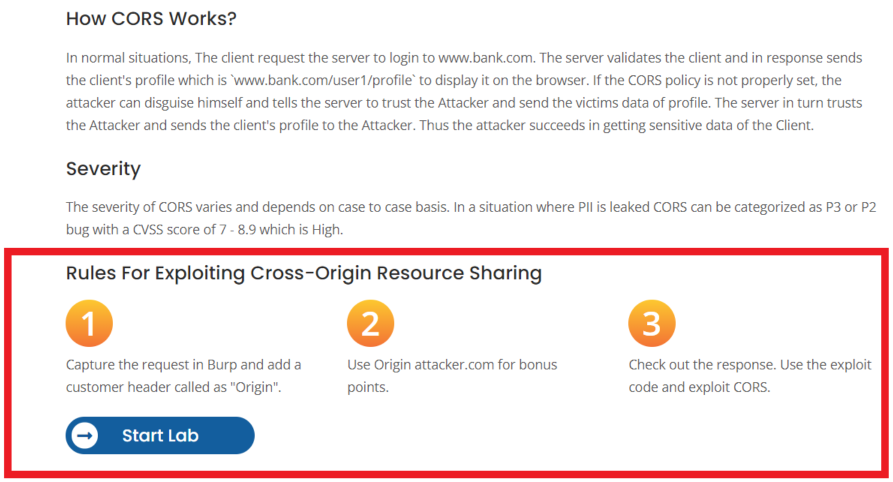
Step 2	Also make sure to check out the references mentioned at the end of the guide. They are very helpful.	 **References** - CORS by PortSwigger : https://portswigger.net/web-security/cors - OWASP CORS : https://owasp.org/www-community/attacks/CORS_OriginHeaderScrutiny - CORS by Mozilla : https://developer.mozilla.org/en-US/docs/Web/HTTP/CORS
Step 3	Open your registered **email** containing the Hacktify portal **credentials**.	
Step 4	Follow the **link** in the mail to open the Hacktify portal.	[Hacktify Labs]
Step 5	The portal will look like this. 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

©2021 VIRTUALLY TESTING. All rights reserved.

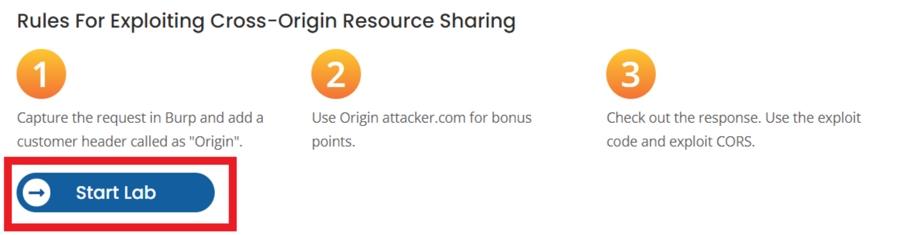
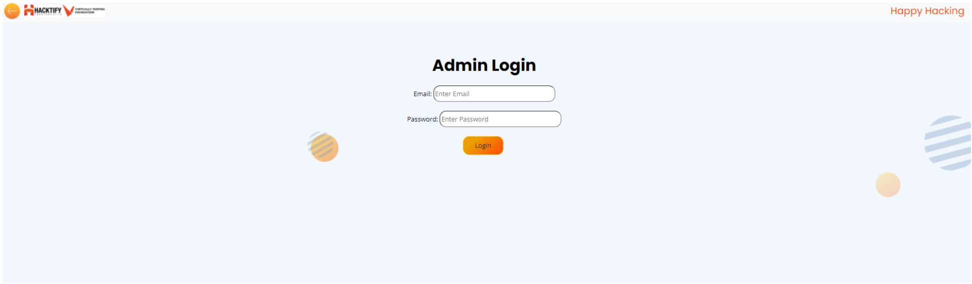
Step 6	**Enter the Email ID you used to register for the internship.** And enter the password: **inter@oct#123** And you should be logged in.	 Cyber Security 10 Weeks Internship Virtually Testing Foundation Hacktify Cyber Security HACKTIFY cybersecurity Login into your account varunk@virtuallytesting.com Login
Step 7	The following **home page** of your portal will open up.	 HACKTIFY cybersecurity Logout 10 Week Internship Labs Home | Labs 10 Hours FREE 3 Hours FREE
Step 8	Open your **Weekly assigned course** and start accessing your labs.	

©2021 VIRTUALLY TESTING. All rights reserved.

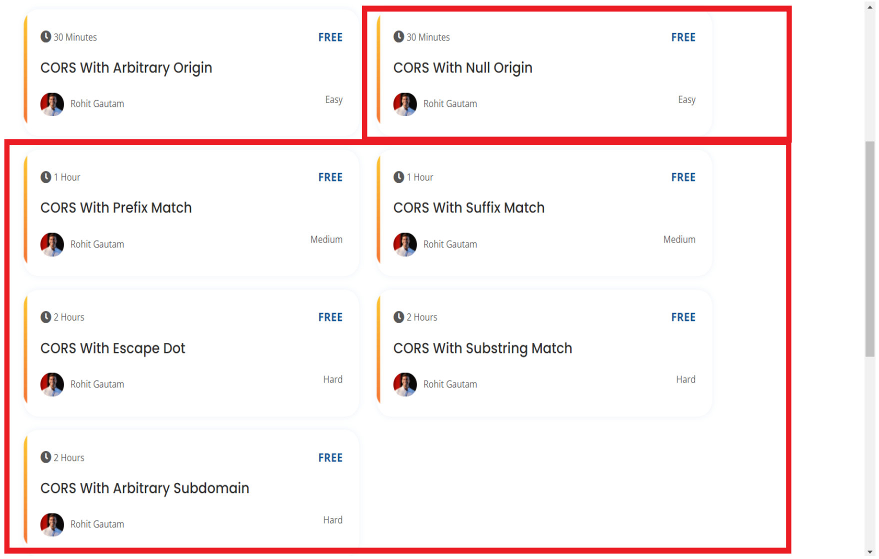
Step 9	Open the **Cross Origin Resource Sharing (CORS) Lab.**	 10 Hours FREE Cross Site Scripting Rohit Gautam Hard 3 Hours FREE Clickjacking Rohit Gautam Easy 10 Hours FREE Cross-Origin Resource Sharing Rohit Gautam Hard 9 Hours FREE Open Redirect Rohit Gautam Hard 7 Hours FREE HTML Injection Rohit Gautam Medium 1 Hour FREE Exchangeable Image File Format Rohit Gautam Easy 8 Hours FREE 12 Hours FREE
Step 10	Once you open that, the **Cross Origin Resource Sharing (CORS) Labs Page** will open up as shown. **NOTE:** Here there are 7 sub-labs assigned to you. There might be multiple sub-labs in each of the main labs.	 Cross-Origin Resource Sharing Labs Home | Labs 30 Minutes FREE CORS With Arbitrary Origin Rohit Gautam Easy 30 Minutes FREE CORS With Null Origin Rohit Gautam Easy 1 Hour FREE CORS With Prefix Match Rohit Gautam Medium 1 Hour FREE CORS With Suffix Match Rohit Gautam Medium 2 Hours FREE CORS With Escape Dot Rohit Gautam Hard 2 Hours FREE CORS With Substring Match Rohit Gautam Hard 2 Hours FREE CORS With Arbitrary Subdomain Rohit Gautam Hard

Step 11	Now, open **CORS With Arbitrary Origin!,** Cross Origin Resource Sharing (CORS) sub-lab 1 will open up.	 HACKTIFY cybersecurity VIRTUALLY TESTING FOUNDATION Cross-Origin Resource Sharing Labs Home | Labs 30 Minutes FREE CORS With Arbitrary Origin Rohit Gautam Easy 30 Minutes FREE CORS With Null Origin Rohit Gautam Easy
Step 12	Go through the details given in the lab. The highlighted portion are the **goals** you have to reach for this lab.	 How CORS Works? In normal situations, The client request the server to login to www.bank.com. The server validates the client and in response sends the client's profile which is `www.bank.com/user1/profile` to display it on the browser. If the CORS policy is not properly set, the attacker can disguise himself and tells the server to trust the Attacker and send the victims data of profile. The server in turn trusts the Attacker and sends the client's profile to the Attacker. Thus the attacker succeeds in getting sensitive data of the Client. Severity The severity of CORS varies and depends on case to case basis. In a situation where PII is leaked CORS can be categorized as P3 or P2 bug with a CVSS score of 7 - 8.9 which is High. Rules For Exploiting Cross-Origin Resource Sharing 1 Capture the request in Burp and add a customer header called as "Origin". 2 Use Origin attacker.com for bonus points. 3 Check out the response. Use the exploit code and exploit CORS. Start Lab

©2021 VIRTUALLY TESTING. All rights reserved.

Step 13	Then click on **Start Lab** at the bottom of the page for successfully starting your lab.	 Rules For Exploiting Cross-Origin Resource Sharing 1 Capture the request in Burp and add a customer header called as "Origin". 2 Use Origin attacker.com for bonus points. 3 Check out the response. Use the exploit code and exploit CORS.
Step 14	The lab will be started and you can continue doing the tasks assigned to you. **NOTE:** Make sure to take **Notes** as you proceed with your labs.	 Happy Hacking Admin Login Email: Enter Email Password: Enter Password Login

©2021 VIRTUALLY TESTING. All rights reserved.

Step 15	After completion of Sub-Lab 1 **CORS With Arbitrary Origin!**, move on to do the second sub-lab **CORS With Null Origin!**. **NOTE:** You have to follow the same procedure for every sub-lab available in the list.	 30 Minutes FREE CORS With Arbitrary Origin Rohit Gautam Easy 30 Minutes FREE CORS With Null Origin Rohit Gautam Easy 1 Hour FREE CORS With Prefix Match Rohit Gautam Medium 1 Hour FREE CORS With Suffix Match Rohit Gautam Medium 2 Hours FREE CORS With Escape Dot Rohit Gautam Hard 2 Hours FREE CORS With Substring Match Rohit Gautam Hard 2 Hours FREE CORS With Arbitrary Subdomain Rohit Gautam Hard

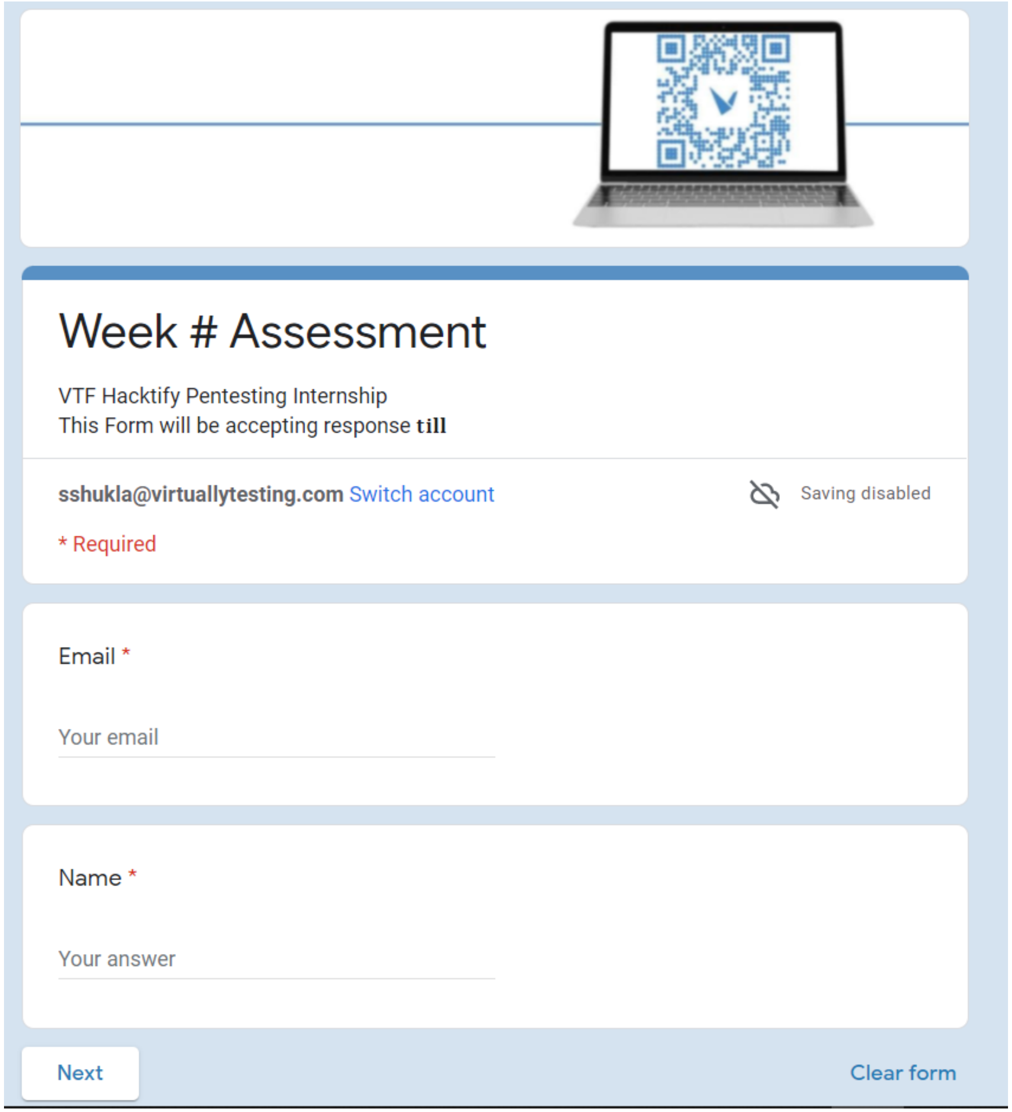
©2021 VIRTUALLY TESTING. All rights reserved.

NOTE:

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 # Assessment

VTF Hacktify Pentesting Internship
This Form will be accepting response till

sshukla@virtuallytesting.com Switch account

Saving disabled

* Required

Email *

Your email

Name *

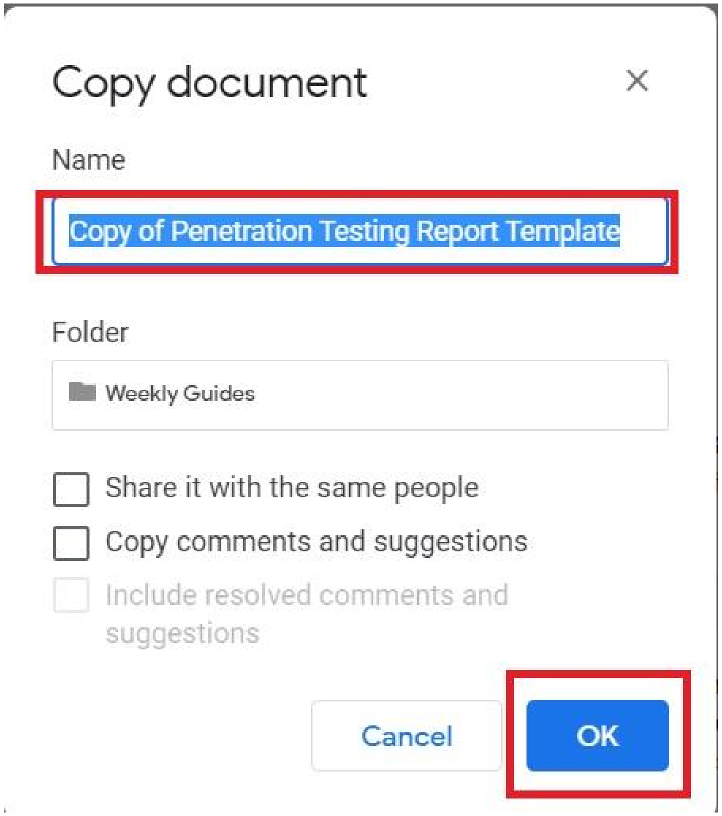
Your answer

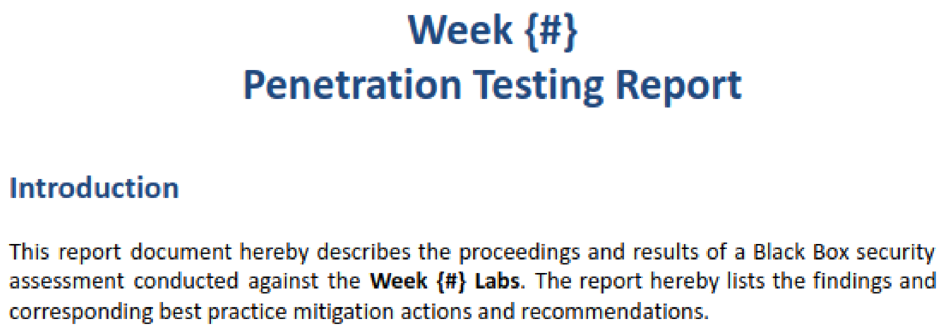
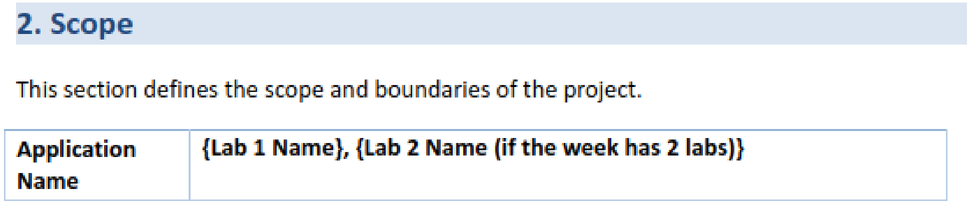
©2021 VIRTUALLY TESTING. All rights reserved.

Task 2 - Penetration Testing Report

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

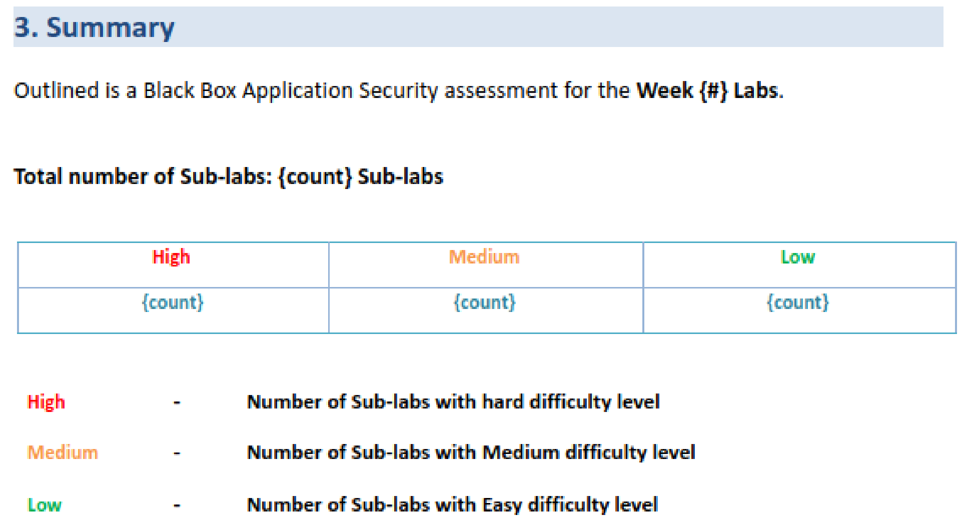
©2021 VIRTUALLY TESTING. All rights reserved.

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 5** **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)}**

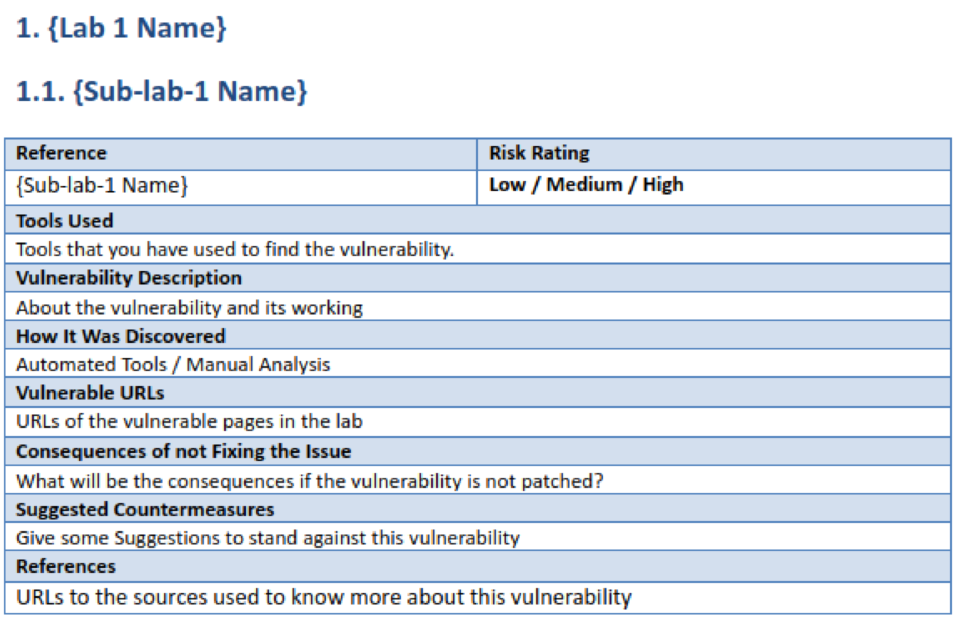
©2021 VIRTUALLY TESTING. All rights reserved.

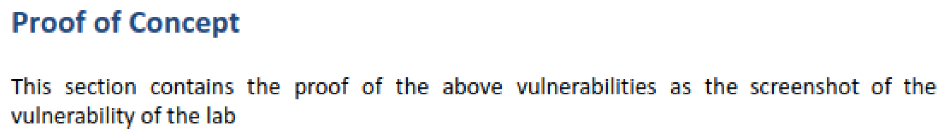
<table>
<tr>
<td><b>Step 6</b></td>
<td>In section 3, change <b>week {#}</b> and <b>{count}</b> with the number of the sub-labs present.
Change the <b>{count} inside the table</b> with the number of easy sub-labs for low, medium sub-labs for medium and hard sub-labs for hard.

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

©2021 VIRTUALLY TESTING. All rights reserved.

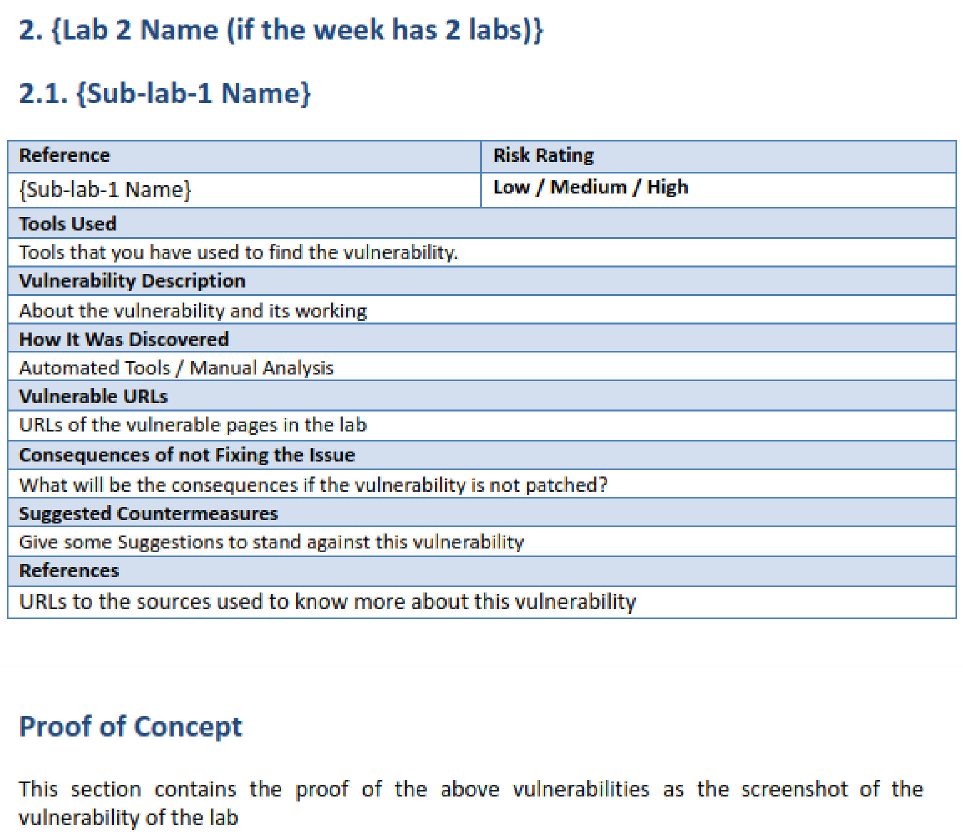
<table>
<tr>
<td><b>Step 7</b></td>
<td>Now it’s time to update the vulnerability for lab 1. Change {Lab 1 Name} to the lab assigned for the week and Change {Sub-lab-1 Name} to the name of the first sub-lab you worked. Update the table given with the information on the vulnerability.

<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>
1. {Lab 1 Name}
1.1. {Sub-lab-1 Name}
<table>
<tr><td><b>Reference</b></td><td><b>Risk Rating</b></td></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>
Proof of Concept

This section contains the proof of the above vulnerabilities as the screenshot of the vulnerability of the lab</td>
</tr>
</table>

©2021 VIRTUALLY TESTING. All rights reserved.

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.**	

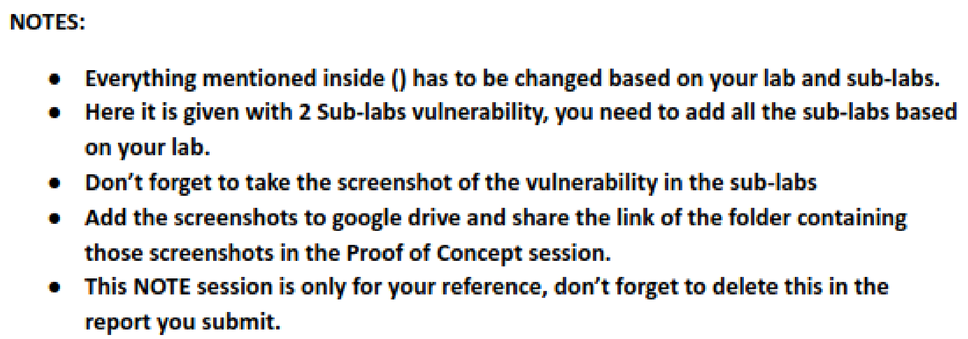
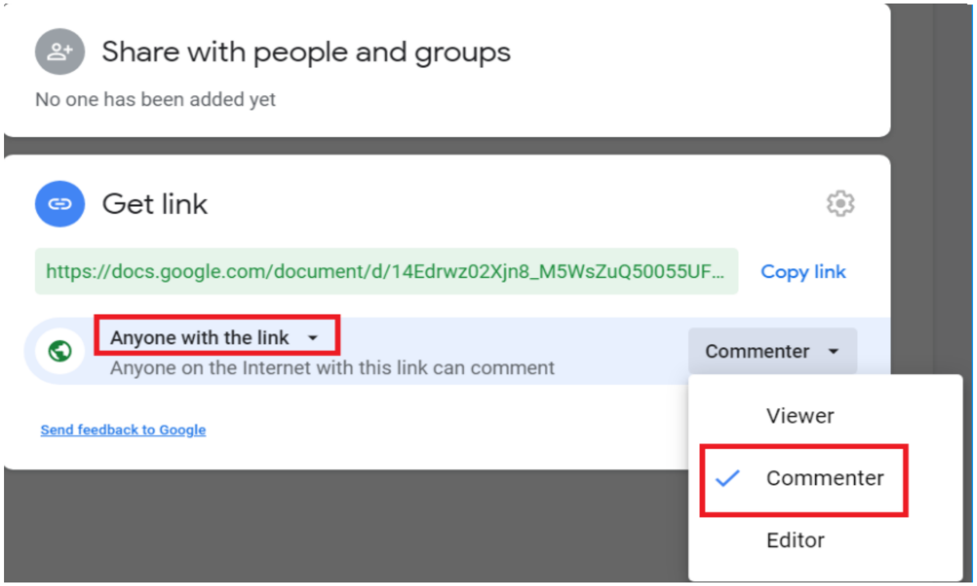
2. {Lab 2 Name (if the week has 2 labs)}

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	

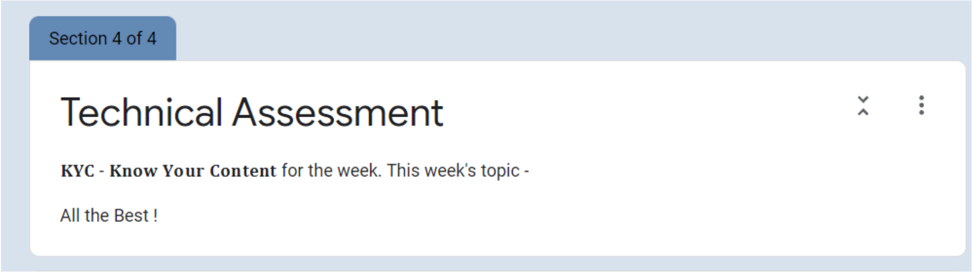
Proof of Concept

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.	 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 Send feedback to Google Viewer ✓ Commenter Editor
Important	You are required to submit the link to your Report in the **weekly assessment form**.	

©2021 VIRTUALLY TESTING. All rights reserved.

Task 3 - Assessment Test

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.	 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.	

©2021 VIRTUALLY TESTING. All rights reserved.

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

©2021 VIRTUALLY TESTING. All rights reserved.