



Week 2 Technical Guide

Task 1 - Weekly Labs

Lab 1 - HTML Injection

NOTE:	<p>Make sure to take Notes as you proceed with your labs. It can include</p> <ul style="list-style-type: none">• The steps you have taken• Tools you have used• The payloads you have used, and so on. <p>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.</p>	
Step 1	Go through the study material on HTML Injection.	HTML Injection



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.</p>	<p>References</p> <ul style="list-style-type: none">HTML Injection by Acunetix : https://www.acunetix.com/vulnerabilities/web/html-injection/OWASP HTML Injection : https://owasp.org/www-project-web-security-testing-guide/latest/4-Web_Application_Security_Testing/11-Client-side_Testing/03-Testing_for_HTML_InjectionHTML Injection by Imperva : https://www.imperva.com/learn/application-security/html-injection/
Step 4	<p>Follow the link to open the Hackify portal.</p>	<p>Bug bounty hunter - Master web application vulnerabilities and kickstart your journey in bug bounty hunting BugBountyHunter.org</p>



Learn, Test, and Share!

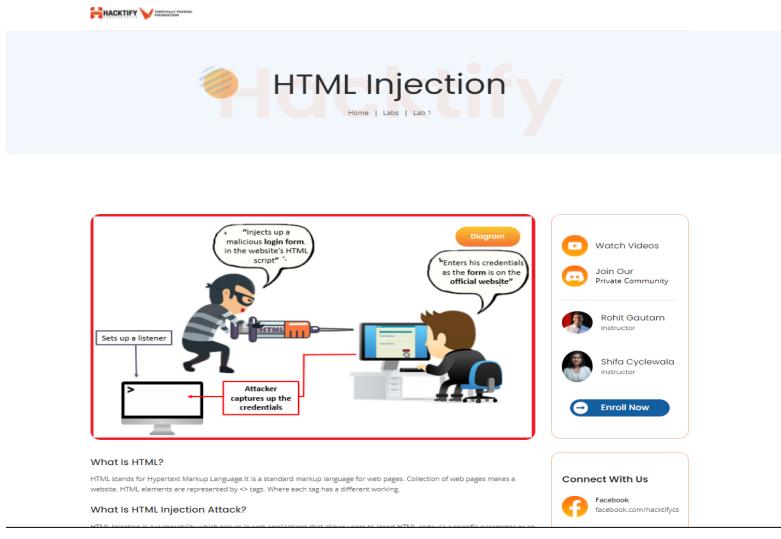
Step 5	<p>The portal will look like this. Once you successfully open the portal link. Click on Login.</p>	
Step 6	<p>Enter the Email ID you used to register for the internship. And enter the password: inter@oct#123 And you should be logged in.</p>	



Learn, Test, and Share!

Step 7	<p>Make sure you are logged into the Hackify portal. If you are not, please follow the steps mentioned above from Step 2 - Step 6.</p> <p>Open the HTML Injection Lab.</p>	<p>7 Hours HTML Injection Rohit Gautam Medium</p>						
Step 8	<p>Once you open that, the HTML Injection Labs page will open up as shown.</p> <p>NOTE: Here there are 6 sub-labs assigned to you. There might be multiple sub-labs in each of the main labs.</p>	<p>Home Labs</p> <p>HTML Injection Labs</p> <table border="1"><tbody><tr><td>30 Minutes HTML's Are Easy! Rohit Gautam FREE Easy</td><td>1 Hour Let Me Store Them! Rohit Gautam FREE Easy</td></tr><tr><td>1 Hour File Names Are Also Vulnerable! Rohit Gautam FREE Easy</td><td>1 Hour 30 Minutes File Content And HTML Injection A Perfect Pair! Rohit Gautam FREE Medium</td></tr><tr><td>1 Hour 30 Minutes Injecting HTML Using URL Rohit Gautam FREE Medium</td><td>1 Hour 30 Minutes Encode IT! Rohit Gautam FREE Hard</td></tr></tbody></table>	30 Minutes HTML's Are Easy! Rohit Gautam FREE Easy	1 Hour Let Me Store Them! Rohit Gautam FREE Easy	1 Hour File Names Are Also Vulnerable! Rohit Gautam FREE Easy	1 Hour 30 Minutes File Content And HTML Injection A Perfect Pair! Rohit Gautam FREE Medium	1 Hour 30 Minutes Injecting HTML Using URL Rohit Gautam FREE Medium	1 Hour 30 Minutes Encode IT! Rohit Gautam FREE Hard
30 Minutes HTML's Are Easy! Rohit Gautam FREE Easy	1 Hour Let Me Store Them! Rohit Gautam FREE Easy							
1 Hour File Names Are Also Vulnerable! Rohit Gautam FREE Easy	1 Hour 30 Minutes File Content And HTML Injection A Perfect Pair! Rohit Gautam FREE Medium							
1 Hour 30 Minutes Injecting HTML Using URL Rohit Gautam FREE Medium	1 Hour 30 Minutes Encode IT! Rohit Gautam FREE Hard							



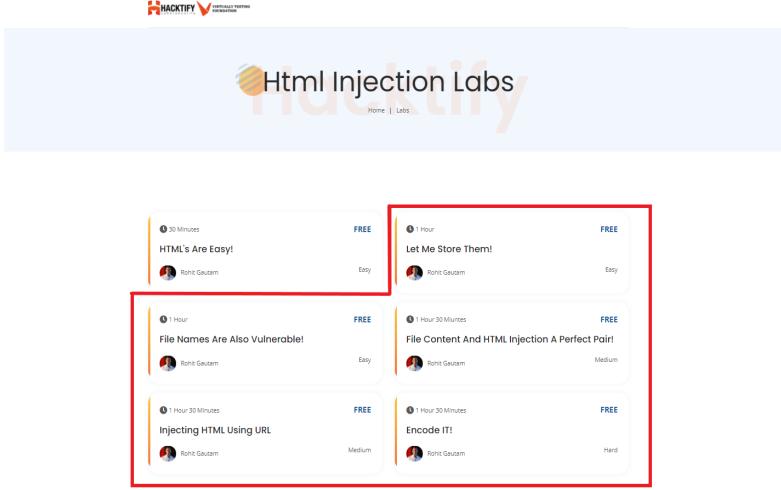
Step 9	<p>Now, if you open HTML's are Easy!, HTML Injection sub-lab 1 will open up.</p>	
Step 10	<p>Go through the details given in the lab. The highlighted portion is the steps you have to follow for this lab.</p>	<p>Severity The severity of HTML Injection can be categorized as P4 bug with a CVSS score of 0.1-3.9 which is Low. In case of an account takeover it can be categorized as P3.</p> <p>Exploiting HTML Injection</p> <div style="border: 2px solid red; padding: 10px; margin: 10px auto; width: fit-content;"><ol style="list-style-type: none"><li data-bbox="1056 946 1140 1044">1 Test every entry point on a target website.<li data-bbox="1140 946 1351 1044">2 Refer the HTML Injection Documentation.<li data-bbox="1351 946 1837 1044">3 Check for valid HTML Injection onto the screen.<p>Start Lab</p></div>



Learn, Test, and Share!

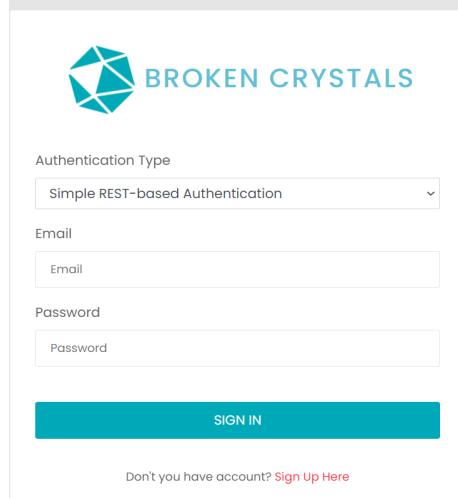
Step 11	<p>Then click on Start Lab at the bottom of the page for successfully starting your lab.</p>	<p>Severity The severity of HTML Injection can be categorized as P4 bug with a CVSS score of 0.1-3.9 which is Low. In case of an account takeover it can be categorized as P3.</p> <p>Exploiting HTML Injection</p> <ol style="list-style-type: none"><li data-bbox="1079 393 1121 425">1<li data-bbox="1079 442 1269 474">Test every entry point on a target website.<li data-bbox="1332 393 1374 425">2<li data-bbox="1332 442 1480 474">Refer the HTML Injection Documentation.<li data-bbox="1586 393 1628 425">3<li data-bbox="1586 442 1818 474">Check for valid HTML Injection onto the screen. <p>Start Lab</p>
Step 12	<p>The lab will be started and you can continue doing the tasks assigned to you.</p>	<p>HACKIFY VIRTUALLY TESTING SEARCH</p> <p>Happy Hacking</p> <p>Search and Filter</p> <p>Enter text <input type="text"/> Search</p> <p>Happy Hacking</p>



Step 13	<p>After completion of Sub-Lab 1 HTML's are Easy!, move on to do the other sub-labs that are available. You have to follow the same procedure from step 11 as mentioned above for this lab too.</p>	 <p>The screenshot shows the Hackify website interface. At the top, there's a navigation bar with the Hackify logo and links for Home and Labs. Below the navigation, the title "Html Injection Labs" is displayed. A grid of six lab cards is shown, each with a thumbnail, title, duration, author, difficulty level, and a "FREE" badge. The first two columns of the grid are highlighted with a red box.</p> <table border="1"><thead><tr><th>Lab Title</th><th>Duration</th><th>Author</th><th>Difficulty</th><th>Status</th></tr></thead><tbody><tr><td>HTML's Are Easy!</td><td>30 Minutes</td><td>Rohit Gezam</td><td>Easy</td><td>FREE</td></tr><tr><td>Let Me Store Them!</td><td>1 Hour</td><td>Rohit Gezam</td><td>Easy</td><td>FREE</td></tr><tr><td>File Names Are Also Vulnerable!</td><td>1 Hour</td><td>Rohit Gezam</td><td>Easy</td><td>FREE</td></tr><tr><td>File Content And HTML Injection A Perfect Pair!</td><td>1 Hour 30 Minutes</td><td>Rohit Gezam</td><td>Medium</td><td>FREE</td></tr><tr><td>Injecting HTML Using URL</td><td>1 Hour 30 Minutes</td><td>Rohit Gezam</td><td>Medium</td><td>FREE</td></tr><tr><td>Encode IT!</td><td>1 Hour 30 Minutes</td><td>Rohit Gezam</td><td>Hard</td><td>FREE</td></tr></tbody></table>	Lab Title	Duration	Author	Difficulty	Status	HTML's Are Easy!	30 Minutes	Rohit Gezam	Easy	FREE	Let Me Store Them!	1 Hour	Rohit Gezam	Easy	FREE	File Names Are Also Vulnerable!	1 Hour	Rohit Gezam	Easy	FREE	File Content And HTML Injection A Perfect Pair!	1 Hour 30 Minutes	Rohit Gezam	Medium	FREE	Injecting HTML Using URL	1 Hour 30 Minutes	Rohit Gezam	Medium	FREE	Encode IT!	1 Hour 30 Minutes	Rohit Gezam	Hard	FREE
Lab Title	Duration	Author	Difficulty	Status																																	
HTML's Are Easy!	30 Minutes	Rohit Gezam	Easy	FREE																																	
Let Me Store Them!	1 Hour	Rohit Gezam	Easy	FREE																																	
File Names Are Also Vulnerable!	1 Hour	Rohit Gezam	Easy	FREE																																	
File Content And HTML Injection A Perfect Pair!	1 Hour 30 Minutes	Rohit Gezam	Medium	FREE																																	
Injecting HTML Using URL	1 Hour 30 Minutes	Rohit Gezam	Medium	FREE																																	
Encode IT!	1 Hour 30 Minutes	Rohit Gezam	Hard	FREE																																	
Important:	<p>Make sure to take Notes as you proceed with your labs. It can include</p> <ul style="list-style-type: none">• The steps you have taken• Tools you have used• The payloads you have used, and so on <p>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.</p>																																				



Learn, Test, and Share!

Step 1	Go through the study material given on Clickjacking lab.	<u>Clickjacking</u>
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 <ul style="list-style-type: none">• Clickjacking by PortSwigger : https://portswigger.net/web-security/clickjacking• OWASP Clickjacking: https://owasp.org/www-community/attacks/Clickjacking
Step 4	Follow the link to open the Hackify portal.	<u>Bug bounty hunter - Master web application vulnerabilities and kickstart your journey in bug bounty hunting BugBountyHunter.org</u>

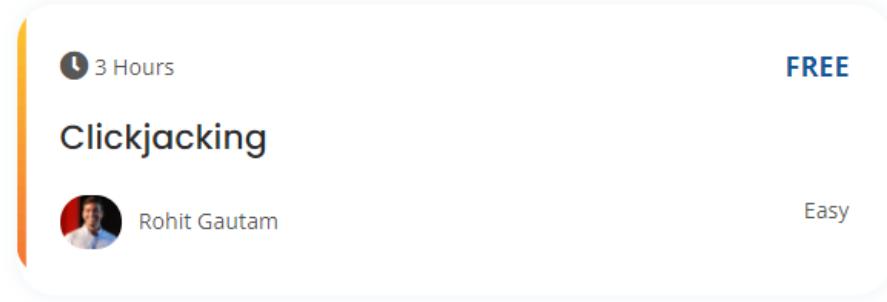


Learn, Test, and Share!

Step 5	<p>The portal will look like this. Once you successfully open the portal link. Click on Login.</p>	
Step 6	<p>Enter the Email ID you used to register for the internship. And enter the password: inter@oct#123 And you should be logged in.</p>	



Learn, Test, and Share!

Step 7	The following home page of your portal will open up.	
Step 8	Open the Clickjacking Lab .	



Learn, Test, and Share!

Step 9	<p>Once you open that, the Clickjacking Labs page will open up as shown.</p> <p>NOTE: Here there are 2 sub-labs assigned to you. There might be multiple sub-labs in each of the main labs.</p>	<p>HACKTIFY VIRTUALLY TESTING FOUNDATION</p> <h1>Clickjacking Labs</h1> <p>Home Labs</p> <div style="border: 1px solid red; padding: 10px; margin-top: 20px;"><p>1 Hour 30 Minutes FREE 1 Hour 30 Minutes FREE</p><p>Let's Hijack! Re-Hijack!</p><p>Easy Medium</p><p>Rohit Gautam Rohit Gautam</p></div>
Step 10	<p>Now, if you open Let's Hijack!, Clickjacking sub-lab 1 will open up.</p>	<p>HACKTIFY VIRTUALLY TESTING FOUNDATION</p> <h1>Clickjacking</h1> <p>Home Labs Lab 1</p> <div style="margin-top: 20px;"><p>Let's Hijack!</p><p>Diagram</p></div>



Step 11	<p>Go through the details given in the lab. The highlighted portion are the goals you have to reach for this lab.</p>	<p>Severity</p> <p>Clickjacking based vulnerabilities are one of the simple bugs to find and are classified into two types:</p> <ul style="list-style-type: none">📌 Clickjacking on Non-Sensitive Pages📌 Clickjacking on Sensitive Pages <p>Clickjacking on Non-Sensitive Pages are generally considered as Informational and categorized as P5 vulnerability where-as Clickjacking on Sensitive Pages are categorized as P4. Clickjacking on sensitive pages can also increase the impact of account takeover and hence can sometimes go up to P3 category.</p> <p>Exploiting Clickjacking</p> <div style="border: 2px solid red; padding: 10px; display: inline-block;"><ol style="list-style-type: none">1 Find a target.2 Refer clickjacking documentation.3 Check if the target is loaded into iframe.<p>Start Lab</p></div>
Step 12	<p>Then click on Start Lab at the bottom of the page for successfully starting your lab.</p>	<p>Severity</p> <p>Clickjacking based vulnerabilities are one of the simple bugs to find and are classified into two types:</p> <ul style="list-style-type: none">📌 Clickjacking on Non-Sensitive Pages📌 Clickjacking on Sensitive Pages <p>Clickjacking on Non-Sensitive Pages are generally considered as Informational and categorized as P5 vulnerability where-as Clickjacking on Sensitive Pages are categorized as P4. Clickjacking on sensitive pages can also increase the impact of account takeover and hence can sometimes go up to P3 category.</p> <p>Exploiting Clickjacking</p> <div style="border: 2px solid red; padding: 10px; display: inline-block;"><ol style="list-style-type: none">1 Find a target.2 Refer clickjacking documentation.3 Check if the target is loaded into iframe.<p>Start Lab</p></div>



Learn, Test, and Share!

Step 13	<p>The lab will be started and you can continue doing the tasks assigned to you.</p>	<p>Happy Hacking</p>				
Step 14	<p>After completion of Sub-Lab 1 Let's Hijack!, move on to do the second sub-lab Re-Hijack!. You have to follow the same procedure from step 11 as mentioned above for this lab too.</p> <p>Note: After completing the labs take a screenshot of the vulnerability exploited. It will be useful in the pentest report writing.</p>	<p>Clickjacking Labs</p> <p>Home Labs</p> <table border="1"><tr><td> 1 Hour 30 Minutes Let's Hijack! Rohit Gautam</td><td>FREE</td></tr><tr><td> 1 Hour 30 Minutes Re-Hijack! Rohit Gautam</td><td>FREE</td></tr></table>	1 Hour 30 Minutes Let's Hijack! Rohit Gautam	FREE	1 Hour 30 Minutes Re-Hijack! Rohit Gautam	FREE
1 Hour 30 Minutes Let's Hijack! Rohit Gautam	FREE					
1 Hour 30 Minutes Re-Hijack! Rohit Gautam	FREE					



Task 2 - Penetration Testing Report

[Mandatory]

Important	<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">• The steps you have taken• Tools you have used• The payloads you have used, and so on <p>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.</p>	
Step 1	<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>	Penetration Testing Report Template



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 Week {#} of the template with the week number.</p> <p>e.g) From Week {#} to Week 2</p> <p>Note: Everything mentioned inside the {} has to be changed.</p>	<p style="text-align: center;">Week {#} Penetration Testing Report</p> <p>Introduction</p> <p>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.</p>		
Step 5	<p>In section 2, edit the Application Name with the lab names.</p> <p>Note: Some weeks have 2 labs so you are required to provide both names in such cases, if not 1 is enough.</p>	<p>2. Scope</p> <p>This section defines the scope and boundaries of the project.</p> <table border="1" data-bbox="1062 796 2012 869"><tr><td data-bbox="1062 796 1241 869">Application Name</td><td data-bbox="1241 796 2012 869">{Lab 1 Name}, {Lab 2 Name (if the week has 2 labs)}</td></tr></table>	Application Name	{Lab 1 Name}, {Lab 2 Name (if the week has 2 labs)}
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

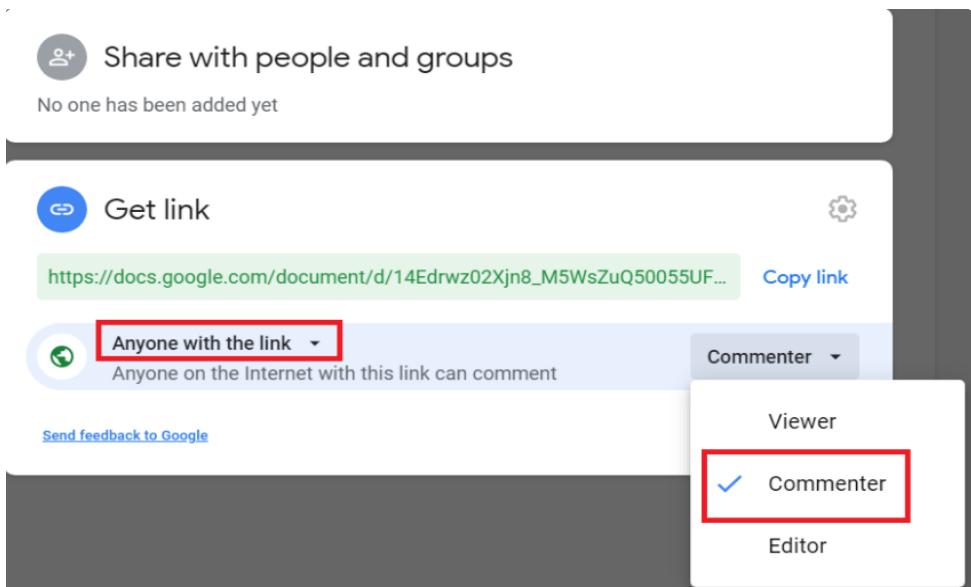


Step 7	<p>Now it's time to update the vulnerability for lab 1. Change {Lab 1 Name} to the lab assigned for the week and Change {Sub-lab-1 Name} to the name of the first sub-lab you worked. Update the table given with the information on the vulnerability.</p> <p>Note: Do the same for all the sub-labs. The template provides a table for 2 sub-labs, if more is needed copy-paste the same.</p>	<p>1. {Lab 1 Name}</p> <p>1.1. {Sub-lab-1 Name}</p> <table border="1" data-bbox="1062 372 2023 853"><thead><tr><th>Reference</th><th>Risk Rating</th></tr></thead><tbody><tr><td>{Sub-lab-1 Name}</td><td>Low / Medium / High</td></tr><tr><td>Tools Used</td><td>Tools that you have used to find the vulnerability.</td></tr><tr><td>Vulnerability Description</td><td>About the vulnerability and its working</td></tr><tr><td>How It Was Discovered</td><td>Automated Tools / Manual Analysis</td></tr><tr><td>Vulnerable URLs</td><td>URLs of the vulnerable pages in the lab</td></tr><tr><td>Consequences of not Fixing the Issue</td><td>What will be the consequences if the vulnerability is not patched?</td></tr><tr><td>Suggested Countermeasures</td><td>Give some Suggestions to stand against this vulnerability</td></tr><tr><td>References</td><td>URLs to the sources used to know more about this vulnerability</td></tr></tbody></table>	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
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																			
Step 8	<p>For the Proof of Concept you are required to attach the screenshot of the vulnerability you found in the sub-labs.</p> <p>Note: 1 Screenshot is needed for each sub-labs and not more than that.</p>	<p>Proof of Concept</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>2. {Lab 2 Name (if the week has 2 labs)}</p> <p>2.1. {Sub-lab-1 Name}</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">Tools Used</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">Vulnerability Description</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">How It Was Discovered</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">Vulnerable URLs</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">Consequences of not Fixing the Issue</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">Suggested Countermeasures</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">References</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>Proof of Concept</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	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	
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																																		



Step 10	Don't forget to remove the NOTES given in the template. It is just for your reference.	<p>NOTES:</p> <ul style="list-style-type: none">• 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.	 <p>The screenshot shows the Google Drive sharing interface. 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: https://docs.google.com/document/d/14Edrwz02Xjn8_M5WsZuQ50055UF.... A 'Copy link' button is next to it. Below the URL is a dropdown menu set to 'Anyone with the link'. A red box highlights this dropdown. To the right, there's a 'Commenter' dropdown with three options: 'Viewer', 'Commenter' (which is checked with a blue checkmark), and 'Editor'. A red box highlights the 'Commenter' option.</p>
Important	You are required to submit the link to your Report in the weekly assessment form .	



Task 3 - Assessment Test

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>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">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