



Week 4 Technical Guide

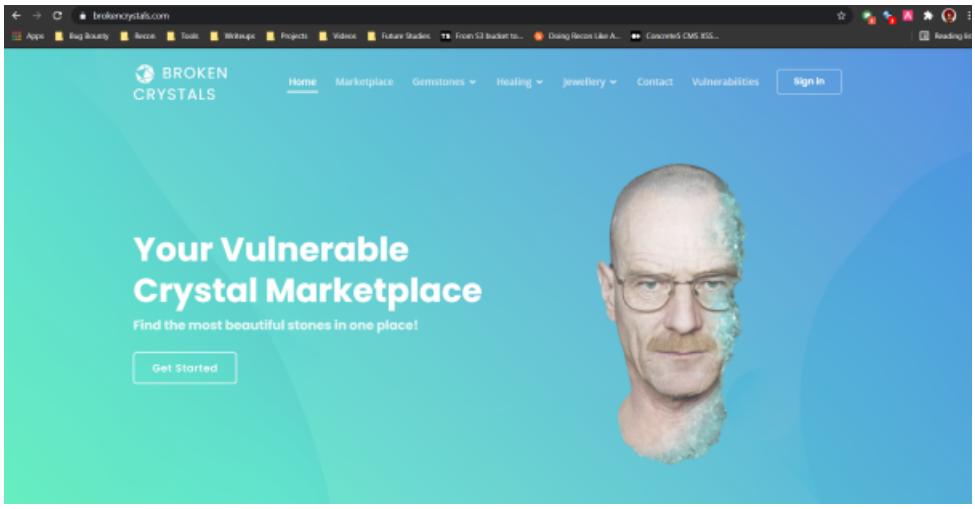
Task 1 - Weekly Labs [Mandatory]

Lab 1 - Exchangeable Image File Format

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>	
Step 1	Hope you all have gone through the study material on Cross-Site Scripting for this week.	<u>EXIF</u>



Learn, Test, and Share!

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. They are very helpful.</p>	<h2>References</h2> <ul style="list-style-type: none">• 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	<p>Follow the link to open the Hackify portal.</p>	Bug bounty hunter - Master web application vulnerabilities and kickstart your journey in bug bounty hunting BugBountyHunter.org



Learn, Test, and Share!

Step 5	<p>Once you successfully open the portal link. Click on Login.</p>	 <p>The screenshot shows the Hacktify homepage. At the top right, there is a blue 'Login' button with a white arrow icon. A thick red arrow points from the left towards this 'Login' button. The page features the Hacktify logo ('HACKTIFY V VIRTUALLY TESTING FOUNDATION'), a navigation bar with links for Home, About, Courses, Teachers, and Labs, and social media icons for Facebook, LinkedIn, Instagram, and Twitter. Below the navigation, the text 'Hacktify The Smarter Way to Learn Cyber Security' is displayed, along with a subtext 'Learn the emerging cyber security skill and become a highest paid cyber security professional'. There are also three circular profile pictures of people.</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>	 <p>The screenshot shows the Hacktify login page for the 'Cyber Security 10 Weeks Internship'. The page has a blue header with the text 'Cyber Security 10 Weeks Internship' in large orange letters. Below the header, there are two logos: 'Virtually Testing Foundation' with a checkmark icon and 'Hacktify Cyber Security' with a blue square icon. To the right, the Hacktify logo is shown again, followed by the text 'Login into your account' and two input fields for 'Email address' and 'Enter Password'. A black 'Login' button is at the bottom.</p>



Learn, Test, and Share!

Step 7	<p>Once you successfully logged in, you will see the homepage listed with labs.</p>	<p>The screenshot shows the Hacktify cybersecurity platform. At the top right is a blue 'Logout' button. Below it is a large, semi-transparent watermark-like graphic with the word 'Hacktify' in large orange letters. The main content area features a section titled '10 Week Internship Labs' with three lab cards. The first card, 'HTML Injection', is labeled 'FREE' and has a duration of '10 Hours'. The second card, 'Exchangeable Image File Format', is also labeled 'FREE' and has a duration of '1 Hour'. Both cards are attributed to 'Rohit Gautam' and are marked as 'Medium' difficulty. A vertical scrollbar is visible on the far right of the page.</p>
Step 8	<p>From the list of labs, open the Exchangeable File Format Lab.</p>	<p>The screenshot shows the Hacktify cybersecurity platform. The 'Exchangeable Image File Format' lab card from the previous row is now highlighted with a thick orange border. This card has a duration of '1 Hour', is attributed to 'Rohit Gautam', and is marked as 'Easy' difficulty. The other two cards in the list are no longer highlighted.</p>



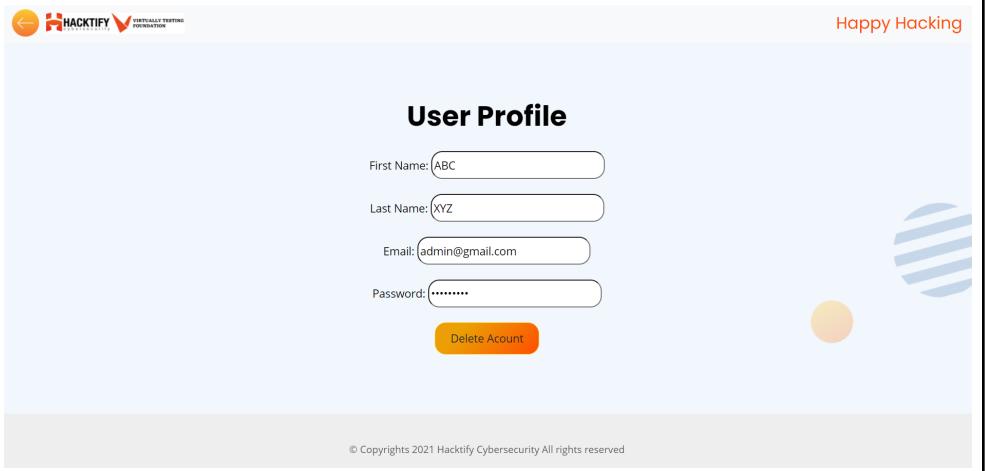
Step 9	<p>Once you open the Exchangeable File Format Lab, you will be assigned with sub-labs as shown.</p> <p>NOTE: There might be multiple sub-labs in each of the main labs.</p>	
Step 10	Open Let's PII! , an Exchangeable File Format sub-lab will open up.	
Step 11	After opening the sub-lab, first go through the given details in the lab.	<p>What Is EXIF Metadata?</p> <p>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.</p> <p>What Is EXIF Exposure?</p> <p>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.</p>



Step 12	<p>The highlighted portion are the goals that you have to accomplish for this lab.</p>	<p>Exploiting EXIF Data Exposure</p> <ol style="list-style-type: none"><li data-bbox="1142 323 1184 355">1<li data-bbox="1142 372 1374 421">Find an entry point for uploading an image<li data-bbox="1438 323 1480 355">2<li data-bbox="1438 372 1712 442">Upload image containing sensitive EXIF meta data. You can find such images on https://github.com/ianare/exif-samples<li data-bbox="1733 323 1776 355">3<li data-bbox="1733 372 1966 421">Once uploaded, either Copy Image Address or Save the Image<li data-bbox="1142 470 1184 502">4<li data-bbox="1142 518 1396 567">Go to http://exif.regex.info/exif.cgi and paste the link or upload the image.<li data-bbox="1438 470 1480 502">5<li data-bbox="1438 518 1712 589">Click on View Image Data and it will give you the EXIF metadata of that image (if the data is not stripped by the server).
Step 13	<p>Once you are clear with goals, click on Start Lab.</p>	<p>Exploiting EXIF Data Exposure</p> <ol style="list-style-type: none"><li data-bbox="1142 714 1184 747">1<li data-bbox="1142 763 1311 812">Find an entry point for uploading an image<li data-bbox="1374 714 1417 747">2<li data-bbox="1374 763 1628 833">Upload image containing sensitive EXIF meta data. You can find such images on https://github.com/ianare/exif-samples<li data-bbox="1649 714 1691 747">3<li data-bbox="1649 763 1881 812">Once uploaded, either Copy Image Address or Save the Image<li data-bbox="1142 861 1184 894">4<li data-bbox="1142 910 1311 959">Go to http://exif.regex.info/exif.cgi and paste the link or upload the image.<li data-bbox="1374 861 1417 894">5<li data-bbox="1374 910 1628 980">Click on View Image Data and it will give you the EXIF metadata of that image (if the data is not stripped by the server). <p>Start Lab</p>



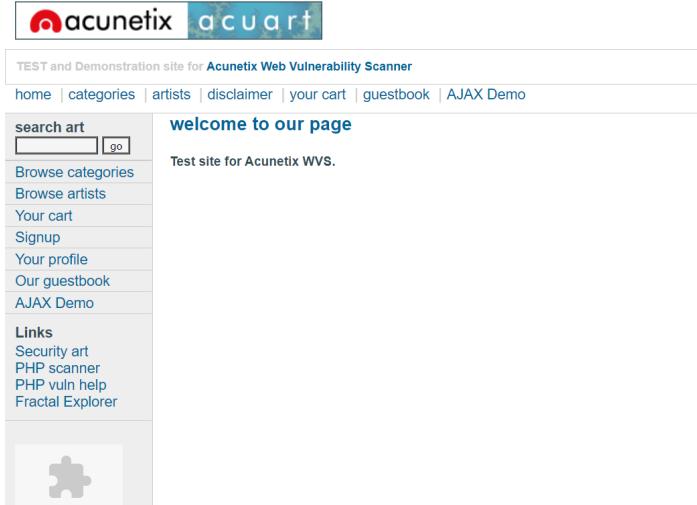
Learn, Test, and Share!

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

Lab 2 - Open Redirect

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>	
------------	--	--



Step 1	Go through the study material given on Clickjacking lab.	<u>Open Redirect</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">• 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/



Learn, Test, and Share!

Step 4	Follow the link to open the Hackify 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 .	<p>The screenshot shows a card for the 'Open Redirect' lab. It includes a timer icon indicating '9 Hours', the title 'Open Redirect', a profile picture of 'Rohit Gautam', and the difficulty level 'Hard'. A 'FREE' badge is also visible.</p>



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.

The screenshot shows a web page titled "Open Redirect Labs" with a subtitle "HACKING". The page displays a grid of 8 sub-labs, each with a thumbnail, title, duration, difficulty level, and a "View" button. The sub-labs are:

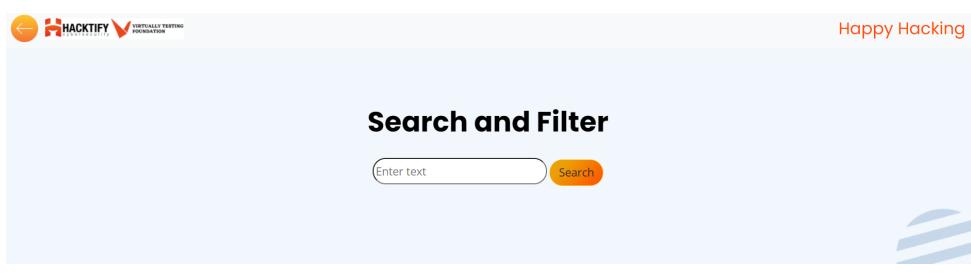
Thumbnail	Title	Duration	Difficulty	Action
	A Simple Host!	FREE	Easy	View
	Story Of A Beautiful Header!	FREE	Easy	View
	Sanitize Params!!	FREE	Medium	View
	Patterns Are Important!	FREE	Medium	View
	File Upload? Redirect IT!	FREE	Easy	View
	Some Param Twice!	FREE	Medium	View
	Domains ? Not Always!	FREE	Hard	View
	Style Digit Symbols <3	FREE	Hard	View



Step 7	<p>Now, if you open A Simple Host!, Open Redirect sub-lab 1 will open up.</p>	<p>The diagram shows the following sequence:</p> <ul style="list-style-type: none">User clicks a link to a trusted siteUser logs into site successfullyUser receives redirectUser redirected to malicious site <p>A red box highlights the "User receives redirect" and "User redirected to malicious site" steps. To the right of the diagram, there is a sidebar with links like "Watch Videos", "Join Our Private Community", and profiles for Rohit Gautam and Shifa Cyclewala, along with an "Enroll Now" button.</p>
Step 8	<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 Open Redirect Vulnerability can be categorized as P4 with a CVSS score of 3.9 which is Low.</p> <p>Exploiting Open Redirect:</p> <ol style="list-style-type: none">Find parameters using Auto-Suite. Broken Authentication parameters include ?-redirect-> ?url-> ?redirect_url-Add the malicious website name to the vulnerable parameter and hit enter!Add the malicious website name to the vulnerable parameter and hit enter!



Learn, Test, and Share!

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.	 <p>Happy Hacking</p>



Learn, Test, and Share!

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.

The screenshot shows a list of sub-labs under the heading "Open Redirect Labs". Each sub-lab entry includes a thumbnail, title, duration, difficulty level, and a "View" button. The first five sub-labs are highlighted with an orange border:

Thumbnail	Title	Duration	Difficulty	Action
	A Simple Host!	20 Minutes	FREE	View
	Sanitize Params!!	1 Hour	FREE	View
	File Upload? Redirect IT!	20 Minutes	FREE	View
	Domains ? Not Always!	2 Hours	FREE	View
	Story Of A Beautiful Header!	1 hour	FREE	View
	Patterns Are Important!	1 hour	FREE	View
	Some Param Twice!	1 Hour 30 Minutes	FREE	View
	Style Digit Symbols <3	2 Hours	FREE	View



Learn, Test, and Share!

Step 12	<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>	
---------	--	--



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 4</p> <p>Note: Everything mentioned with 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="1066 801 2008 866"><tr><td data-bbox="1066 801 1241 866">Application Name</td><td data-bbox="1241 801 2008 866">{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

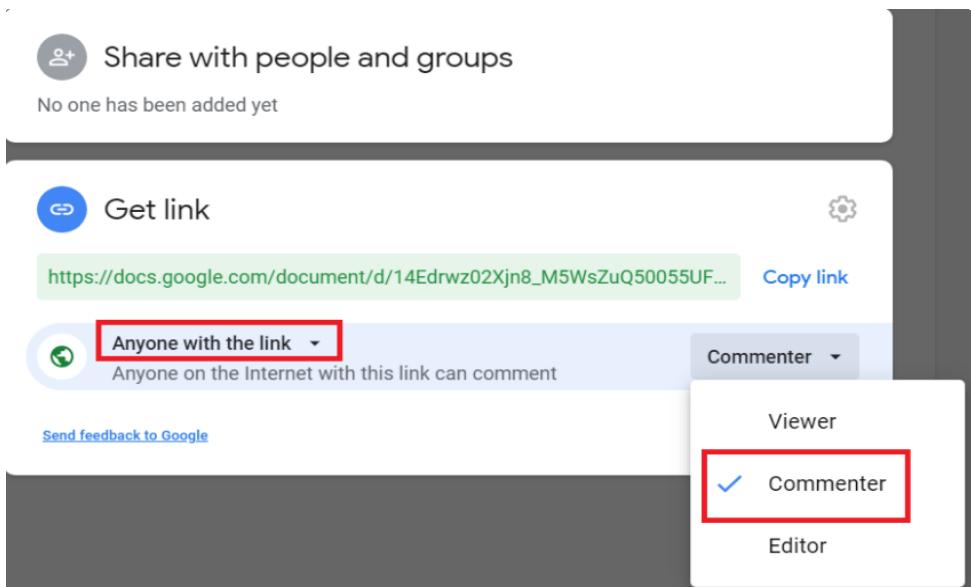


Step 7	<p>Now it's time to update the vulnerability for lab 1. Change {Lab 1 Name} to the lab assigned for the week and Change {Sub-lab-1 Name} to the name of the first sub-lab you worked. Update the table given with the information on the vulnerability.</p> <p>Note: Do the same for all the sub-labs. 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="1072 372 2023 855"><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 sharing settings for a Google Doc. 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 and a 'Copy link' button. A dropdown menu for permissions is open, showing three options: 'Viewer' (unchecked), 'Commenter' (checked with a blue checkmark), and 'Editor' (unchecked). The 'Commenter' option is highlighted with a red box.</p>



Learn, Test, and Share!

Important	<p>You are required to submit the link to your Report in the weekly assessment form.</p>	<p>Penetration Testing Report Submission.</p> <p>You should be submitting commenter link of your report. Link should be visible to anyone on the Internet.</p> <p>Commenter Link *</p> <p> Share with people and groups No one has been added yet</p> <p> Get link Copy link https://docs.google.com/document/d/14Edrwz02Xjn8_M5WsZuQ50055UF...</p> <p> Anyone with the link ▼ Anyone on the Internet with this link can comment</p> <p> Commenter ▼ Viewer <input checked="" type="checkbox"/> Commenter Editor</p> <p>Your answer</p> <p style="text-align: center;">Back Next Clear form</p>
------------------	---	--



Task 3 - Assessment Test [Mandatory]

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>You need to score 70% in this specific Week's Technical Assessment in order to proceed with the internship.</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.	



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