Learn, Test, and Share!

Week 8 Technical Guide

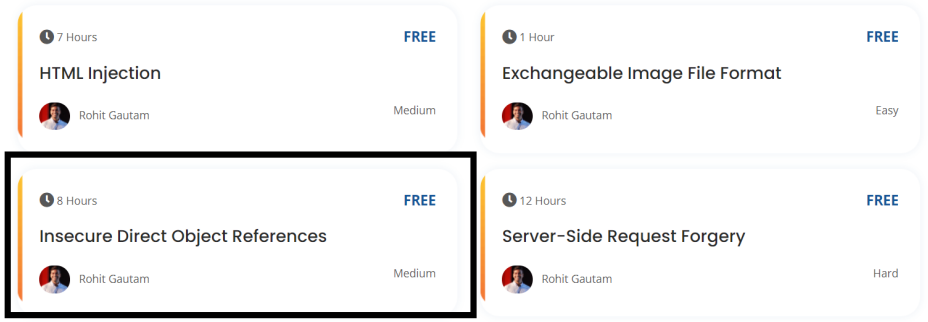
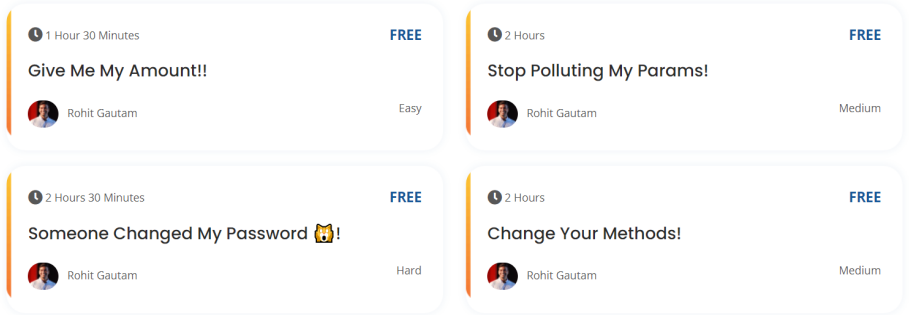
Task 1 - Weekly Labs

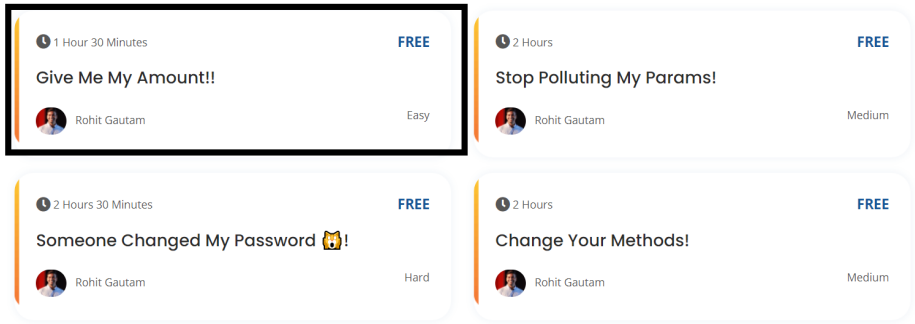
Insecure Direct Object Reference (IDOR) Lab

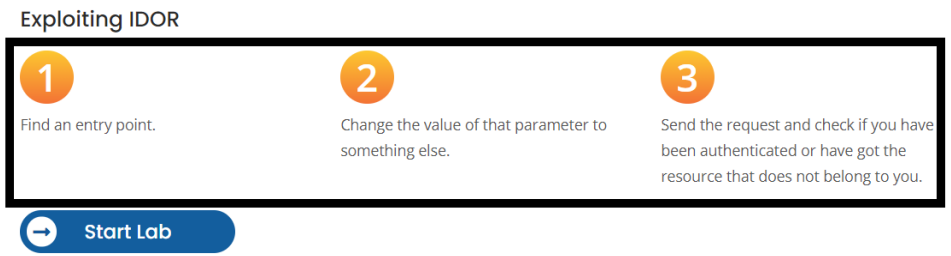
Important:	Make sure to take **Notes** as you proceed with your labs. It can include • The steps you have taken • Tools you have used • The payloads you have used, and so on And also do your research on that specific vulnerability as all of this will help you in the **Weekly Assessment Test** which will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

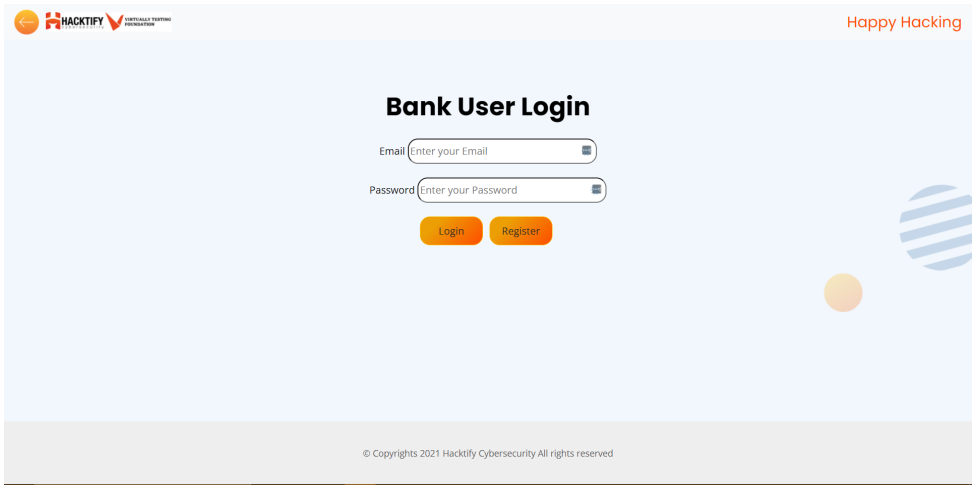
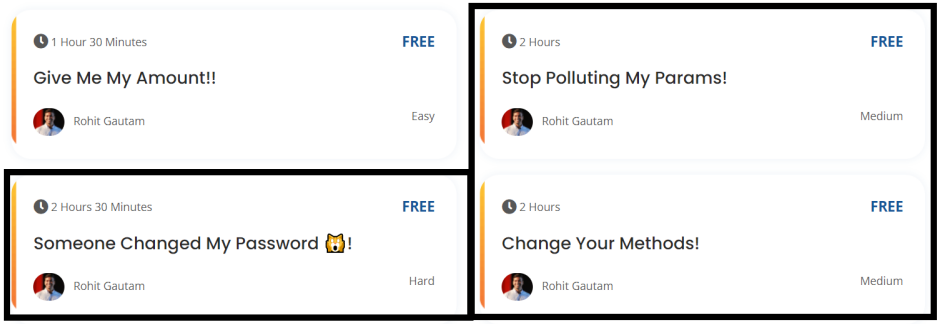
Step 2	Also make sure to check out the **references** mentioned at the end of the guide. They are very helpful.	**References** • IDOR by Port Swigger: https://portswigger.net/web-security/access-control/idor • IDOR by OWASP: https://cheatsheetseries.owasp.org/cheatsheets/Insecure_Direct_Object_Reference_Prevention_Cheat_Sheet.html • How to find IDOR's by Bugcrowd: https://www.bugcrowd.com/blog/how-to-find-idor-insecure-direct-object-reference-vulnerabilities-for-large-bounty-rewards/ Lab Documentation
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	Once you successfully open the portal link. Click on **Login**.	

Step 6	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	
Step 7	Once you successfully logged in, you will see the **homepage** listed with labs.	

Step 8	From the list of labs, open the **Insecure Direct Object References Lab**.	
Step 9	Once you open the **Insecure Direct Object References Lab,** you will be assigned with sub-labs as shown. **NOTE:** Here there are 4 sub-labs assigned to you. There might be multiple sub-labs in each of the main labs.	

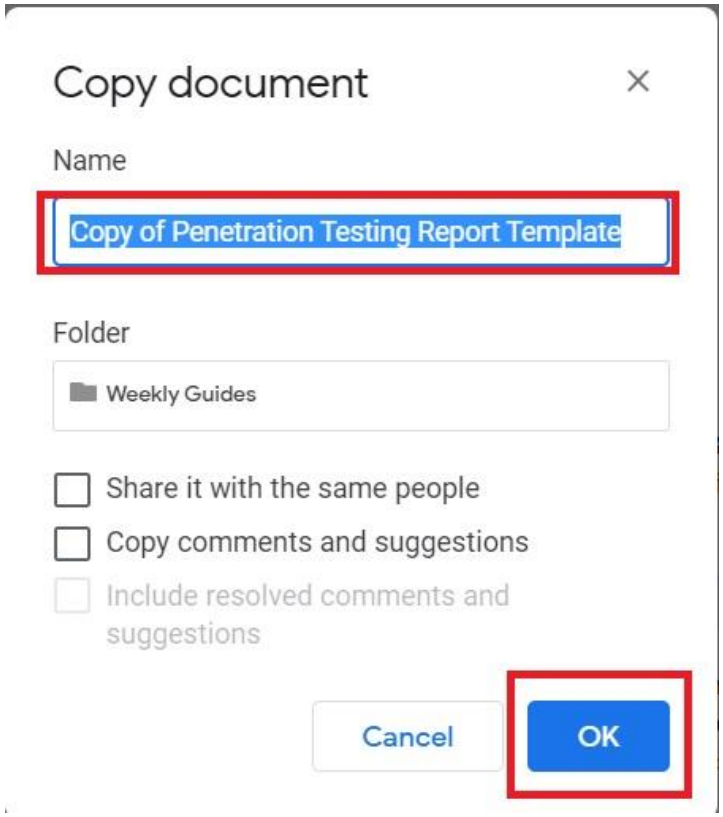
Step 10	Now open **Give me My Amount!!,** Insecure Direct Object References sub-lab 1 will open up.	
Step 11	After opening the sub-lab, first go through the given details in the lab.	**What Is Insecure Direct Object References Attack?** An insecure direct object reference (IDOR) is an access control vulnerability where invalidated user input can be used for unauthorized access to resources or operations. It occurs when an attacker gains direct access by using user-supplied input to an object that has no authorization to access. Attackers can bypass the authorization mechanism to access resources in the system directly by exploiting this vulnerability.Every resource instance can be called as an object and often, represented with and ID. And if these IDs are easy enough to guess or an object can be used by an attacker to bypass access check somehow, we can talk about an IDOR at this point. Referring to the above image, an attacker by ethical means can only get the document numbered 101 which is legally his. But what if the web application does not validate the number and an attacker puts the number of its victim. This can cause the attacker get hold of the sensitive document which he should not have access to. **Severity** The severity of IDOR varies from P3 to P2 depending on what data is being exposed.

Step 12	The highlighted portion are the **goals** that you have to accomplish for this lab.	
Step 13	Once you are clear with **goals,** click on **Start Lab.**	

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.	
Step 15	After completion of sub-lab 1 **Give Me My Amount!!**, move on to the next sub-lab and repeat the process from step 11. You have to follow the same procedure for every sub-lab available in the list.	

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

Step 2	Rename the copy to **Week_#_Penetration_Testing_Report** where # is the week number.	

<table>
<tr>
<td>Step 3</td>
<td>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 8

Note:
Everything mentioned with the {} has to be changed.</td>
<td>
<h1>Week {#}
Penetration Testing Report</h1>
<h2>Introduction</h2>
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.
</td>
</tr>
<tr>
<td>Step 4</td>
<td>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.</td>
<td>
<h2>2. Scope</h2>
This section defines the scope and boundaries of the project.
<table>
<tr><td>Application Name</td><td>{Lab 1 Name}, {Lab 2 Name (if the week has 2 labs)}</td></tr>
</table>
</td>
</tr>
</table>

<table>
<tr>
<td>Step 5</td>
<td>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.</td>
<td>
3. Summary

Outlined is a Black Box Application Security assessment for the Week {#} Labs.

Total number of Sub-labs: {count} Sub-labs

<table>
<tr><th>High</th><th>Medium</th><th>Low</th></tr>
<tr><td>{count}</td><td>{count}</td><td>{count}</td></tr>
</table>

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
</td>
</tr>
</table>

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

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

Note:
1 Screenshot is needed for each sub-labs and not more than that.</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>Step 8</td>
<td>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.</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>Low / Medium / High</td></tr>
<tr><td colspan="2">Tools Used</td></tr>
<tr><td colspan="2">Tools that you have used to find the vulnerability.</td></tr>
<tr><td colspan="2">Vulnerability Description</td></tr>
<tr><td colspan="2">About the vulnerability and its working</td></tr>
<tr><td colspan="2">How It Was Discovered</td></tr>
<tr><td colspan="2">Automated Tools / Manual Analysis</td></tr>
<tr><td colspan="2">Vulnerable URLs</td></tr>
<tr><td colspan="2">URLs of the vulnerable pages in the lab</td></tr>
<tr><td colspan="2">Consequences of not Fixing the Issue</td></tr>
<tr><td colspan="2">What will be the consequences if the vulnerability is not patched?</td></tr>
<tr><td colspan="2">Suggested Countermeasures</td></tr>
<tr><td colspan="2">Give some Suggestions to stand against this vulnerability</td></tr>
<tr><td colspan="2">References</td></tr>
<tr><td colspan="2">URLs to the sources used to know more about this vulnerability</td></tr>
</table>
<h2>Proof of Concept</h2>
This section contains the proof of the above vulnerabilities as the screenshot of the vulnerability of the lab
</td>
</tr>
</table>

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.**

Reminder

All Interns are required to participate in our Technical Skills Assignment. We will be using https://www.bugbountyhunter.org.

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.

Make sure to take Notes as you proceed with your labs