



Week 9 Technical Guide

Task 1 - Weekly Labs [Mandatory]

SQL Injection Lab

| | | |
|-------------------|---|--------------------------------------|
| 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 SQL Injection for this week. | <u>SQL Injection</u> |



| | | |
|--------|---|---|
| Step 2 | Also make sure to check out the references mentioned at the end of the guide. They are very helpful. | <p>References:</p> <p>PortSwigger :https://portswigger.net/web-security/sql-injection</p> <p>OWASP : https://owasp.org/www-community/attacks/SQL_Injection</p> <p> Lab Documentation</p> |
| 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 |



Learn, Test, and Share!

| | | |
|--------|---|--|
| Step 5 | <p>Once you successfully open the portal link. Click on Login.</p> |  |
| Step 6 | <p>Enter the credentials you received on your registered email on the following page.</p> <p>Enter the Email ID you used to register for the internship.</p> <p>And enter the password: inter@oct#123</p> <p>And you should be logged in</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, there's a logo with the word "HACKTIFY" and "cybersecurity". A "Logout" button is in the top right. Below the header, a large banner says "10 Week Internship Labs" with the Hacktify logo. Underneath, there are four lab cards. The first card, "SQL Injection", has a red border around it. The other three cards are "Insecure Direct Object References", "Server-Side Request Forgery", and "Cross-Site Request Forgery". Each card includes a timer icon, a "FREE" badge, a user profile picture, and a difficulty level (Medium, Hard). The "SQL Injection" card is labeled "14 Hours".</p> |
| Step 8 | <p>From the list of labs, open the SQL Injection Labs.</p> | |



Step 9

Once you open the **SQL Injection Labs**, you will be assigned with sub-labs as shown.

NOTE:

Here there are 12 sub-labs assigned to you.
There might be multiple sub-labs in each of the main labs.

| Duration | Difficulty | Title | Author | Duration | Difficulty | Title | Author |
|------------|------------|--------------------------|--------------|-------------------|------------|----------------------------|--------------|
| 30 Minutes | FREE | Strings & Errors Part 1! | Rohit Gautam | 30 Minutes | FREE | Strings & Errors Part 2! | Rohit Gautam |
| 30 Minutes | FREE | Strings & Errors Part 3! | Rohit Gautam | 1 Hour | FREE | Let's Trick 'Em! | Rohit Gautam |
| 2 Hours | FREE | Booleans And Blind! | Rohit Gautam | 2 Hours | FREE | Error Based : Tricked | Rohit Gautam |
| 1 Hour | FREE | Errors And Post! | Rohit Gautam | 1 Hour | FREE | User Agents Lead Us! | Rohit Gautam |
| 1 Hour | FREE | Referer Lead Us! | Rohit Gautam | 1 Hour 30 Minutes | FREE | Oh Cookies! | Rohit Gautam |
| 2 Hours | FREE | WAF's Are Injected! | Rohit Gautam | 1 Hour | FREE | WAF's Are Injected Part 2! | Rohit Gautam |



Learn, Test, and Share!

Step 10

Now open **Strings & Errors Part 1!**, SQL Injection sub-lab 1 will open up.

The screenshot shows the Hackify website interface. At the top, there's a navigation bar with 'Home' and 'Labs'. Below it, the main title 'SQL Injection Labs' is displayed. The page lists several lab categories arranged in a grid:

| Lab Name | Duration | Difficulty | Author | Cost |
|----------------------------|-------------------|------------|--------------|------|
| Strings & Errors Part 1! | 30 Minutes | Easy | Rohit Gautam | FREE |
| Strings & Errors Part 2! | 30 Minutes | Easy | Rohit Gautam | FREE |
| Strings & Errors Part 3! | 30 Minutes | Easy | Rohit Gautam | FREE |
| Let's Trick 'Em! | 1 Hour | Medium | Rohit Gautam | FREE |
| Booleans And Blind! | 2 Hours | Hard | Rohit Gautam | FREE |
| Error Based : Tricked | 2 Hours | Medium | Rohit Gautam | FREE |
| Errors And Post! | 1 Hour | Easy | Rohit Gautam | FREE |
| User Agents Lead Us! | 1 Hour | Hard | Rohit Gautam | FREE |
| Referer Lead Us! | 1 Hour | Medium | Rohit Gautam | FREE |
| Oh Cookies! | 1 Hour 30 Minutes | Hard | Rohit Gautam | FREE |
| WAF's Are Injected! | 2 Hours | Hard | Rohit Gautam | FREE |
| WAF's Are Injected Part 2! | 1 Hour | Medium | Rohit Gautam | FREE |



| | | |
|---------|--|---|
| Step 11 | After opening the sub-lab, first go through the given details in the lab. | <p>SQL Injection</p> <p>Home Labs Lab 1</p> <p>Attacker</p> <p>Web API Server</p> <p>Victim's SQL Database Server</p> <p>Diagram</p> <p>Watch Videos</p> <p>Join Our Private Community</p> <p>Rohit Gautam Instructor</p> <p>Shifa Cyclewala Instructor</p> |
| Step 12 | The highlighted portion are the goals that you have to accomplish for this lab. | <p>Severity</p> <p>SQL injection can be categorized as P1 or P2 bug with a CVSS score of 7.5 - 9 which is High.</p> <p>Exploiting SQL Injection</p> <ol style="list-style-type: none"><li data-bbox="1062 975 1305 1122">1 Test every entry point on a target website.<li data-bbox="1305 975 1548 1122">2 Refer the SQL Injection Documentation.<li data-bbox="1548 975 2023 1122">3 Check for sql errors on the screen. <p> Start Lab</p> |



Learn, Test, and Share!

| | | |
|----------------|--|--|
| Step 13 | Once you are clear with goals , click on Start Lab . | <p>Severity SQL injection can be categorized as P1 or P2 bug with a CVSS score of 7.5 - 9 which is High.</p> <p>Exploiting SQL Injection</p> <ol style="list-style-type: none"><li data-bbox="1072 404 1136 453">1<li data-bbox="1072 453 1326 600">Test every entry point on a target website. Start Lab<li data-bbox="1431 404 1495 453">2<li data-bbox="1431 453 1727 502">Refer the SQL Injection Documentation.<li data-bbox="1748 404 1812 453">3<li data-bbox="1748 453 2044 502">Check for sql errors on the screen. |
| 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. |  <p>Happy Hacking</p> |



Learn, Test, and Share!

Step 15

After completion of sub-lab 1 **Strings & Errors Part 1!**, 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.

The screenshot shows the Hackify website interface with the title "SQL Injection Labs". Below the title, there are several sub-labs listed in a grid format. The sub-labs are:

| Sub-Lab Name | Author | Duration | Difficulty | Status |
|----------------------------|--------------|-------------------|------------|--------|
| Strings & Errors Part 1! | Rohit Gautam | 30 Minutes | Easy | FREE |
| Strings & Errors Part 2! | Rohit Gautam | 30 Minutes | Easy | FREE |
| Booleans And Blind! | Rohit Gautam | 2 Hours | Hard | FREE |
| Error Based : Tricked | Rohit Gautam | 2 Hours | Medium | FREE |
| Errors And Post! | Rohit Gautam | 1 Hour | Easy | FREE |
| User Agents Lead Us! | Rohit Gautam | 1 Hour | Hard | FREE |
| Oh Cookies! | Rohit Gautam | 1 Hour 30 Minutes | Hard | FREE |
| Referer Lead Us! | Rohit Gautam | 1 Hour | Medium | FREE |
| WAF's Are Injected! | Rohit Gautam | 2 Hours | Hard | FREE |
| WAF's Are Injected Part 2! | Rohit Gautam | 1 Hour | Medium | FREE |



Step 16

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 9 - Assignment Submission Form

VTF Hackify Pentesting Internship

This Form will be accepting response till December 8, 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

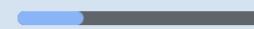
Email *

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](#)



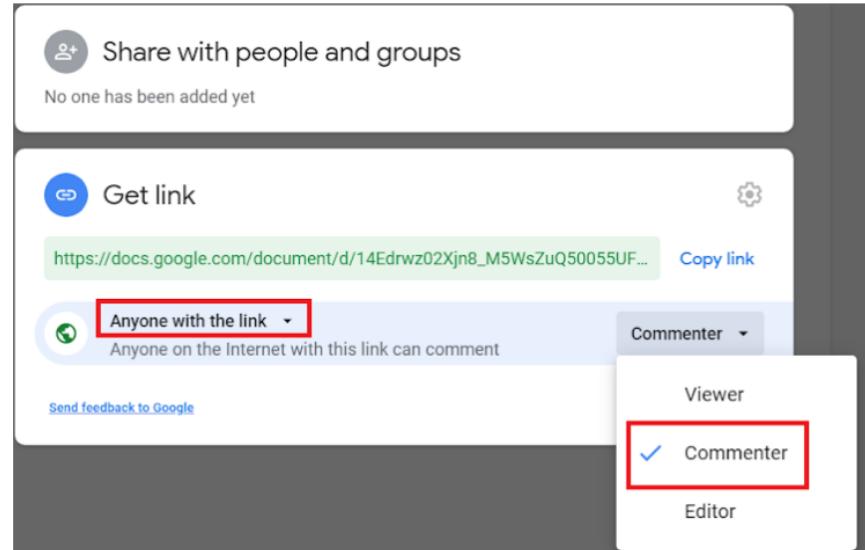
Step 17

- 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 *

A screenshot of a Google Document sharing settings interface. It shows 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 is open, showing 'Anyone with the link' (which is highlighted with a red box) and 'Commenter' (which is checked and also highlighted with a red box). Other options in the dropdown are 'Viewer' and 'Editor'. At the bottom of the interface are 'Back', 'Next', and 'Clear form' buttons.



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> | <p>Penetration Testing Report Template</p> |



Learn, Test, and Share!

Step 2

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 3 | <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 9</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 4 | <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 801 2012 866"><tr><td data-bbox="1062 801 1241 866">Application Name</td><td data-bbox="1241 801 2012 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 5

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 6 | <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 7 | <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> | | | | | | | | | | | | | | | | | | |



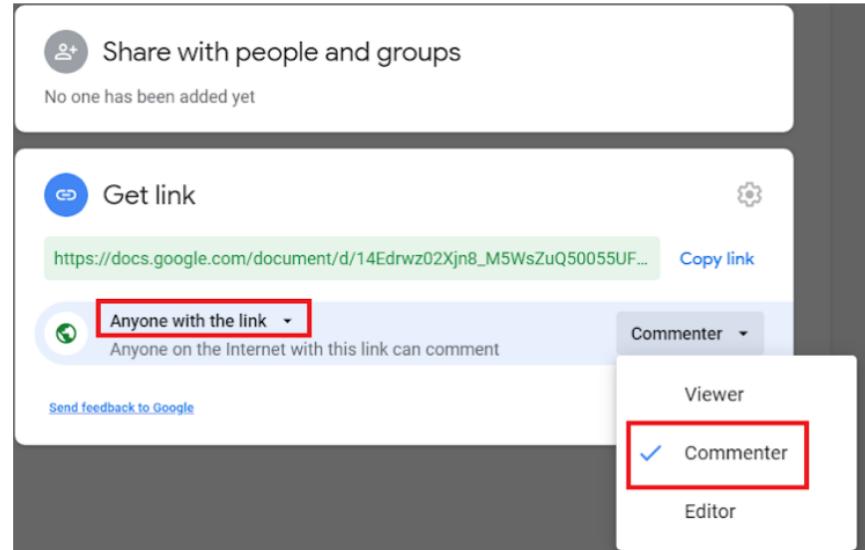
| Step 8 | <p>If you have worked on 2 labs, do the same step 8 and step 9 for the second lab, if not remove those things that are related to the 2nd lab.</p> | <p>2. {Lab 2 Name (if the week has 2 labs)}</p> <p>2.1. {Sub-lab-1 Name}</p> <table border="1" data-bbox="1072 376 2023 858"><thead><tr><th data-bbox="1072 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 9 | 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 10 | 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 showing a generated URL. A dropdown menu for permissions is open, with 'Commenter' checked (indicated by a red box). Other options in the menu are 'Viewer' and 'Editor'.</p> |



Learn, Test, and Share!

| | |
|---|---|
| <p>Important</p> <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></p> <p>Your answer</p> <p>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. | |



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