



## Week 9 Technical Guide


### Task 1 - Weekly Labs [Mandatory]

#### SQL Injection Lab

<b>Important:</b>	<p>Make sure to take <b>Notes</b> as you proceed with your labs. It can include</p> <ul style="list-style-type: none"><li>• The steps you have taken</li><li>• Tools you have used</li><li>• The payloads you have used, and so on</li></ul> <p>And also do your research on that specific vulnerability as all of this will help you in the <b>Weekly Assessment Test</b> which will be provided to you.</p>	
<b>Step 1</b>	<p>Hope you all have gone through the study material on SQL Injection for this week.</p>	<a href="#">SQL Injection</a>



Learn, Test, and Share!

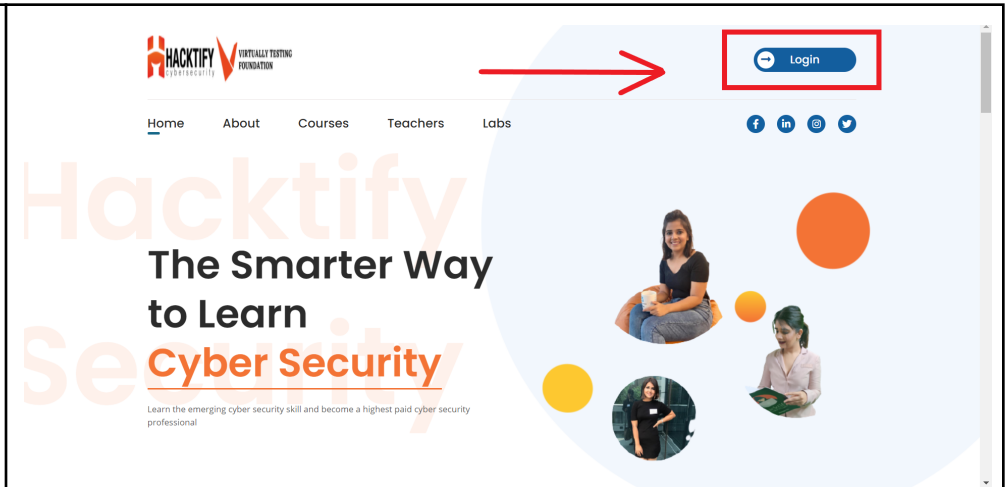
Step 2	Also make sure to check out the <b>references</b> mentioned at the end of the guide. They are very helpful.	<b>References:</b>  <b>PortSwigger</b> : <a href="https://portswigger.net/web-security/sql-injection">https://portswigger.net/web-security/sql-injection</a> <b>OWASP</b> : <a href="https://owasp.org/www-community/attacks/SQL_Injection">https://owasp.org/www-community/attacks/SQL_Injection</a>   <a href="#">Lab Documentation</a>
Step 3	Open your registered <b>email</b> containing the Hacktify portal <b>credentials</b> .	
Step 4	Follow the <b>link</b> in the mail to open the Hacktify portal.	<a href="#">Hacktify Labs</a>



Learn, Test, and Share!

**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





Learn, Test, and Share!

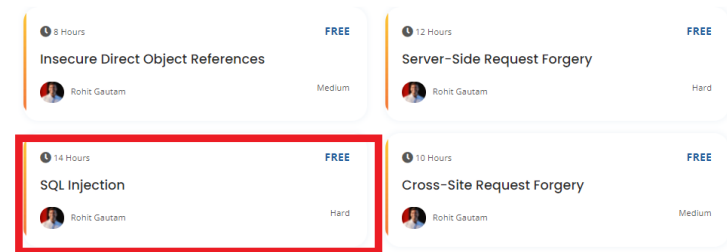
**Step 7**

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



**Step 8**

From the list of labs, open the **SQL Injection Labs**.





Learn, Test, and Share!

## 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.

The screenshot displays the 'SQL Injection Labs' interface. At the top, there's a header with the title 'SQL Injection Labs' and a 'Hacktify' watermark. Below the header, a grid of 12 sub-labs is shown, each with a timer icon, duration, title, author profile, difficulty level, and a 'FREE' tag. The sub-labs are:

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


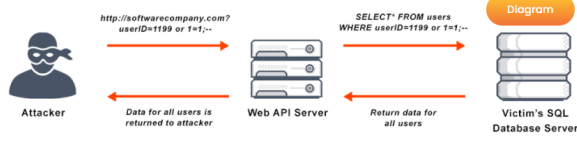
# SQL Injection Labs

Home | Labs

<div><div>30 Minutes</div><div>FREE</div><div>Strings &amp; Errors Part 1!</div><div><div>Rohit Gautam</div><div>Easy</div></div></div>	<div><div>30 Minutes</div><div>FREE</div><div>Strings &amp; Errors Part 2!</div><div><div>Rohit Gautam</div><div>Easy</div></div></div>
<div><div>30 Minutes</div><div>FREE</div><div>Strings &amp; Errors Part 3!</div><div><div>Rohit Gautam</div><div>Easy</div></div></div>	<div><div>1 Hour</div><div>FREE</div><div>Let's Trick 'Em!</div><div><div>Rohit Gautam</div><div>Medium</div></div></div>
<div><div>2 Hours</div><div>FREE</div><div>Booleans And Blind!</div><div><div>Rohit Gautam</div><div>Hard</div></div></div>	<div><div>2 Hours</div><div>FREE</div><div>Error Based : Tricked</div><div><div>Rohit Gautam</div><div>Medium</div></div></div>
<div><div>1 Hour</div><div>FREE</div><div>Errors And Post!</div><div><div>Rohit Gautam</div><div>Easy</div></div></div>	<div><div>1 Hour</div><div>FREE</div><div>User Agents Lead Us!</div><div><div>Rohit Gautam</div><div>Hard</div></div></div>
<div><div>1 Hour</div><div>FREE</div><div>Referer Lead Us!</div><div><div>Rohit Gautam</div><div>Medium</div></div></div>	<div><div>1 Hour 30 Minutes</div><div>FREE</div><div>Oh Cookies!</div><div><div>Rohit Gautam</div><div>Hard</div></div></div>
<div><div>2 Hours</div><div>FREE</div><div>WAF's Are Injected!</div><div><div>Rohit Gautam</div><div>Hard</div></div></div>	<div><div>1 Hour</div><div>FREE</div><div>WAF's Are Injected Part 2!</div><div><div>Rohit Gautam</div><div>Medium</div></div></div>


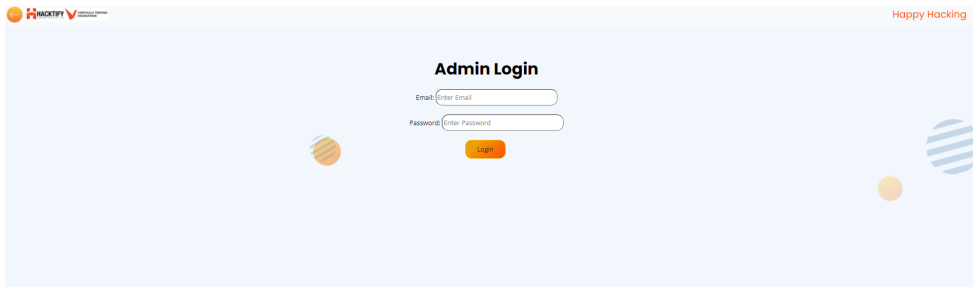


Learn, Test, and Share!

<b>Step 11</b>	After opening the sub-lab, first go through the given details in the lab.	<div data-bbox="1050 240 2016 402"><h1>SQL Injection</h1><p>Home   Labs   Lab 1</p></div> <div data-bbox="1129 500 1732 695"><p>Attacker</p><p>Web API Server</p><p>Victim's SQL Database Server</p></div> <div data-bbox="1129 722 1717 787"><p><b>What Is SQL Injection?</b></p><p>CSQL Injection ⇒ Allows attacker ⇒ to view "data" ⇒ that attacker normally not able to retrieve ⇒ But using SQLI we now able to retrieve data "Data" ⇒ Information about Users and their passwords etc Attacker can ⇒ modify or delete this data ⇒ causing</p></div> <div data-bbox="1759 500 1942 787"><p>Watch Videos</p><p>Join Our Private Community</p><p>Rohit Gautam Instructor</p><p>Shifa Cyclewala Instructor</p></div>
----------------	---	--



Learn, Test, and Share!

<b>Step 13</b>	Once you are clear with <b>goals</b> , click on <b>Start Lab</b> .	<p><b>Severity</b></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><b>Exploiting SQL Injection</b></p> <div><div><b>1</b> Test every entry point on a target website.</div><div><b>2</b> Refer the SQL Injection Documentation.</div><div><b>3</b> Check for sql errors on the screen.</div></div> <div></div>
<b>Step 14</b>	<p>Once the lab starts, hack through the goals that you need to accomplish. Happy Hacking.</p> <p><b>NOTE:</b> Make sure to take <b>Notes</b> as you proceed with your labs.</p>	





## 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.

# SQL Injection Labs

Home | Labs

30 Minutes

FREE

Strings & Errors Part 1!

Rohit Gautam

Easy

30 Minutes

FREE

Strings & Errors Part 3!

Rohit Gautam

Easy

2 Hours

FREE

Booleans And Blind!

Rohit Gautam

Hard

1 Hour

FREE

Errors And Post!

Rohit Gautam

Easy

1 Hour

FREE

Referer Lead Us!

Rohit Gautam

Medium

2 Hours

FREE

WAF's Are Injected!

Rohit Gautam

Hard

30 Minutes

FREE

Strings & Errors Part 2!

Rohit Gautam

Easy

1 Hour

FREE

Let's Trick 'Em!

Rohit Gautam

Medium

2 Hours

FREE

Error Based : Tricked

Rohit Gautam

Medium

1 Hour

FREE

User Agents Lead Us!

Rohit Gautam

Hard

1 Hour 30 Minutes

FREE

Oh Cookies!

Rohit Gautam

Hard

1 Hour

FREE

WAF's Are Injected Part 2!

Rohit Gautam

Medium



## 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 Hacktify 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**

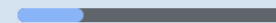
Email \*

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 \*

 Share with people and groups  
No one has been added yet


 Get link 

[https://docs.google.com/document/d/14Edrwz02Xjn8\\_M5WsZuQ50055UF...](https://docs.google.com/document/d/14Edrwz02Xjn8_M5WsZuQ50055UF...) [Copy link](#)


 **Anyone with the link** 

Anyone on the Internet with this link can comment

[Send feedback to Google](#)

Commenter 

Viewer

 **Commenter**

Editor

BackNext

Clear form

©2021 VIRTUALLY TESTING. All rights reserved.

Revised:11/18/2021



## Task 2 - Penetration Testing Report

### [Mandatory]

<b>Important</b>	<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"><li>• The steps you have taken</li><li>• Tools you have used</li><li>• The payloads you have used, and so on</li></ul> <p>And also do your research on that specific vulnerability as all of this will help you in the <b>Weekly Assessment Test</b> which will be provided to you.</p>	
<b>Step 1</b>	<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>	<a href="#">Penetration Testing Report Template</a>



Learn, Test, and Share!

**Step 2**

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



<b>Step 3</b>	<p>Open the renamed copy of the template and start editing. Firstly edit the <b>Week {#}</b> of the template with the week number.</p> <p>e.g) From Week {#} to Week 9</p> <p><b>Note:</b> <b>Everything mentioned with the {} has to be changed.</b></p>	<div><h2>Week {#}</h2><h1>Penetration Testing Report</h1></div> <p><b>Introduction</b></p> <p>This report document hereby describes the proceedings and results of a Black Box security assessment conducted against the <b>Week {#} Labs</b>. The report hereby lists the findings and corresponding best practice mitigation actions and recommendations.</p>		
<b>Step 4</b>	<p>In section 2, edit the <b>Application Name</b> with the lab names.</p> <p><b>Note:</b> <b>Some weeks have 2 labs so you are required to provide both names in such cases, if not 1 is enough.</b></p>	<div><h2>2. Scope</h2><p>This section defines the scope and boundaries of the project.</p><table><tr><td>Application Name</td><td>{Lab 1 Name}, {Lab 2 Name (if the week has 2 labs)}</td></tr></table></div>	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



<b>Step 6</b>	<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><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></p>	<div>1. {Lab 1 Name}</div> <div>1.1. {Sub-lab-1 Name}</div> <table><tr><th>Reference</th><th>Risk Rating</th></tr><tr><td>{Sub-lab-1 Name}</td><td>Low / Medium / High</td></tr><tr><th colspan="2">Tools Used</th></tr><tr><td colspan="2">Tools that you have used to find the vulnerability.</td></tr><tr><th colspan="2">Vulnerability Description</th></tr><tr><td colspan="2">About the vulnerability and its working</td></tr><tr><th colspan="2">How It Was Discovered</th></tr><tr><td colspan="2">Automated Tools / Manual Analysis</td></tr><tr><th colspan="2">Vulnerable URLs</th></tr><tr><td colspan="2">URLs of the vulnerable pages in the lab</td></tr><tr><th colspan="2">Consequences of not Fixing the Issue</th></tr><tr><td colspan="2">What will be the consequences if the vulnerability is not patched?</td></tr><tr><th colspan="2">Suggested Countermeasures</th></tr><tr><td colspan="2">Give some Suggestions to stand against this vulnerability</td></tr><tr><th colspan="2">References</th></tr><tr><td colspan="2">URLs to the sources used to know more about this vulnerability</td></tr></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																																		
<b>Step 7</b>	<p>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.</p> <p><b>Note:</b> <b>1 Screenshot is needed for each sub-labs and not more than that.</b></p>	<div>Proof of Concept</div> <p>This section contains the proof of the above vulnerabilities as the screenshot of the vulnerability of the lab</p>																																





## Step 8

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)}

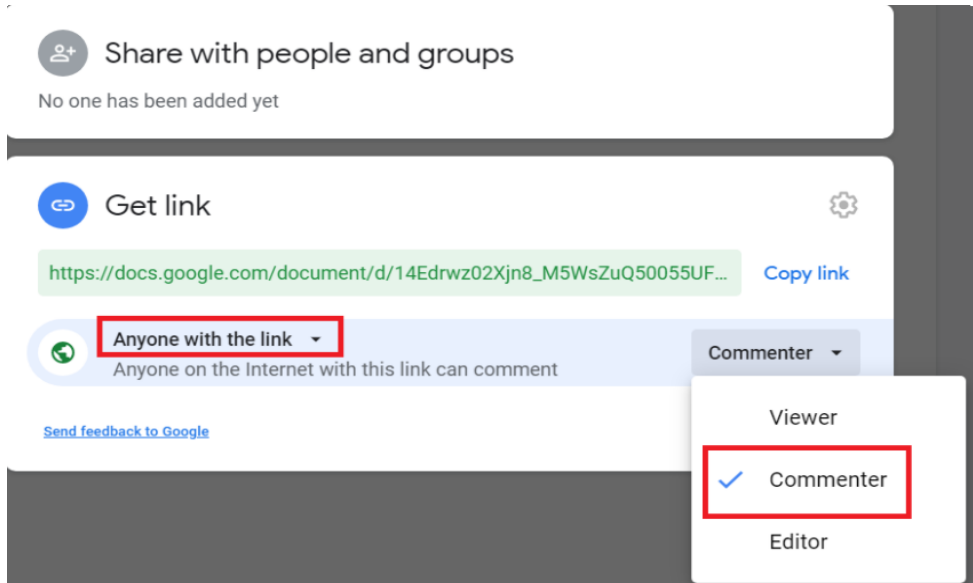
### 2.1. {Sub-lab-1 Name}

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



<b>Step 9</b>	Don't forget to remove the <b>NOTES</b> given in the template. It is just for your reference.	<p><b>NOTES:</b></p> <ul style="list-style-type: none"><li>• Everything mentioned inside () has to be changed based on your lab and sub-labs.</li><li>• Here it is given with 2 Sub-labs vulnerability, you need to add all the sub-labs based on your lab.</li><li>• Don't forget to take the screenshot of the vulnerability in the sub-labs</li><li>• Add the screenshots to google drive and share the link of the folder containing those screenshots in the Proof of Concept session.</li><li>• This NOTE session is only for your reference, don't forget to delete this in the report you submit.</li></ul>
<b>Step 10</b>	After completing the work, now click on the <b>share</b> button and create a share link with the <b>Commenter</b> permission.	



Learn, Test, and Share!

**Important**

You are required to submit the link to your Report in the **weekly assessment form**.

Penetration Testing Report Submission.

You should be submitting **commenter** link of your report.  
Link should be visible to anyone on the Internet.

**Commenter Link \***

Back

Next

Clear form



## Task 3 - Assessment Test [Mandatory]

### 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.

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

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.



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**