



Week 7 Technical Guide

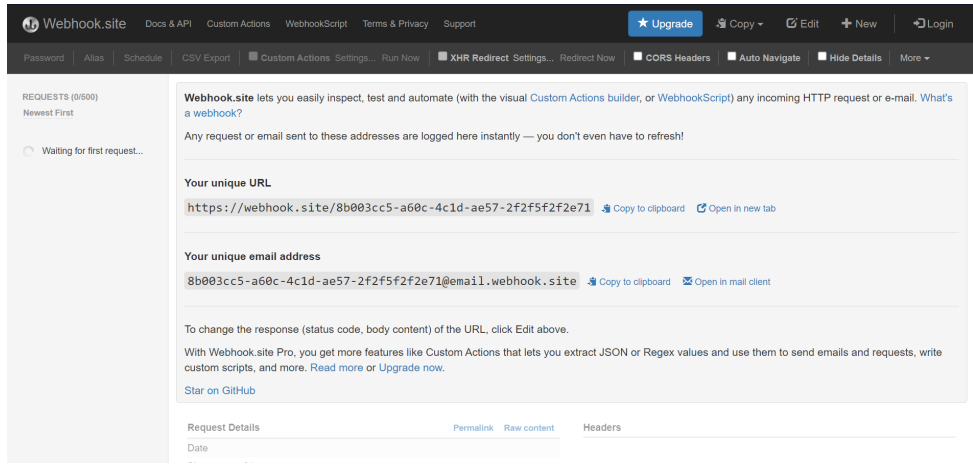
Task 1 - Weekly Labs [Optional]

Lab - Server-Side Request Forgery

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	<p>Hope you all have gone through the study material on Clickjacking for this week.</p>	SSRF Server-Side Request Forgery



Learn, Test, and Share!

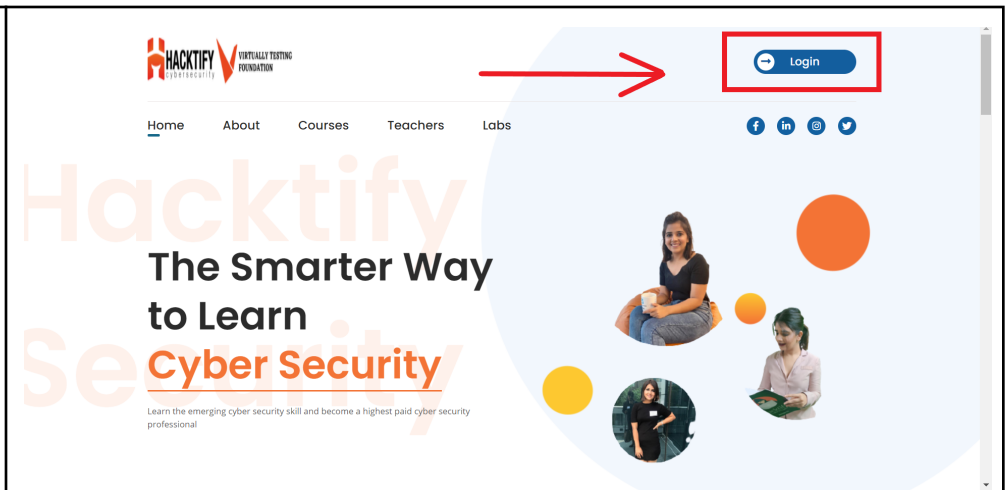
Step 2	Go through the links mentioned in the guide as they have examples of vulnerable websites as shown to the right, and you can practice that on your own to get a better understanding of vulnerabilities before accessing the labs.	
Step 3	Also make sure to check out the references mentioned at the end of the guide. They are very helpful.	
Step 4	Follow the link in the mail to open the Hacktify portal.	Hacktify Labs



Learn, Test, and Share!

Step 5

The portal will look like this.
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	The following home page of your portal will open up.	
Step 8	Open your Weekly assigned course and start accessing your labs.	
Step 9	Open the Server-Side Request Forgery Lab .	



Learn, Test, and Share!

Step 10

Once you open that, the **Server-Side Request Forgery Labs Page** will open as shown.

NOTE:

Here there are 9 sub-labs assigned to you.
There might be multiple sub-labs in each of the main labs.



Server-Side Request Forgery Labs

Home | Labs

30 Minutes

FREE

Get The 127.0.0.1



Rohit Gautam

Easy

1 Hour

FREE

30 Minutes

FREE

Http(s)? Nevermind!!



Rohit Gautam

Easy

1 Hour

FREE



Learn, Test, and Share!

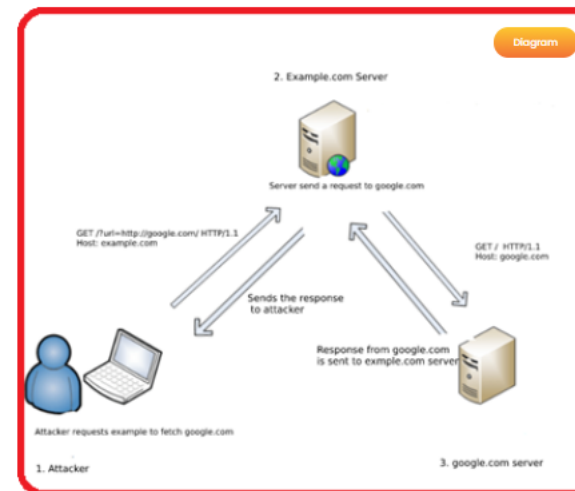
Step 11

Now, if you open **Get The 127.0.0.1**, Server-Side Request Forgery sub-lab 1 will open up.



Server-Side Request Forgery

[Home](#) | [Labs](#) | [Lab 1](#)



Watch Videos

Join Our Private Community

Rohit Gautam
Instructor

Shifa Cyclewala
Instructor

Connect With Us

Facebook
facebook.com/hacktifycs



Learn, Test, and Share!

Step 12

Go through the details given in the lab.
The highlighted portion are the **goals** you have to reach for this lab.

What Is Server-Side Request Forgery Attack?

Server-side request forgery (also known as SSRF) is a web security vulnerability that allows an attacker to induce the server-side application to make HTTP requests to an arbitrary domain of the attacker's choosing. In a typical SSRF attack, the attacker might cause the server to make a connection to internal-only services within the organization's infrastructure. In other cases, they may be able to force the server to connect to arbitrary external systems, potentially leaking sensitive data such as authorization credentials. In simple words, Server-Side Request Forgery (SSRF) refers to an attack, wherein an attacker can send a crafted request from a vulnerable web application. SSRF is mainly used to target internal systems behind WAF (web application firewall), that are unreachable to an attacker from the external network. Additionally, it's also possible for an attacker to mark SSRF, for accessing services from the same server that is listening on the loopback interface address called (127.0.0.1).

Severity

The severity of SSRF varies and depends on case to case basis.

Exploiting SSRF

1

Identify the URLs and entry point.

2

Copy the payload and replace it with the value of the parameter you have taken.

3

Monitor the Logs.



Start Lab



Step 13

Then click on **Start Lab** at the bottom of the page for successfully starting your lab.

What Is Server-Side Request Forgery Attack?

Server-side request forgery (also known as SSRF) is a web security vulnerability that allows an attacker to induce the server-side application to make HTTP requests to an arbitrary domain of the attacker's choosing. In a typical SSRF attack, the attacker might cause the server to make a connection to internal-only services within the organization's infrastructure. In other cases, they may be able to force the server to connect to arbitrary external systems, potentially leaking sensitive data such as authorization credentials. In simple words, Server-Side Request Forgery (SSRF) refers to an attack, wherein an attacker can send a crafted request from a vulnerable web application. SSRF is mainly used to target internal systems behind WAF (web application firewall), that are unreachable to an attacker from the external network. Additionally, it's also possible for an attacker to mark SSRF, for accessing services from the same server that is listening on the loopback interface address called (127.0.0.1).

Severity

The severity of SSRF varies and depends on case to case basis.

Exploiting SSRF

1

Identify the URLs and entry point.

2

Copy the payload and replace it with the value of the parameter you have taken.

3

Monitor the Logs.



Start Lab



Learn, Test, and Share!

Step 14

The lab will be started and you can continue doing the tasks assigned to you.



Learn, Test, and Share!

Step 15

After completion of Sub-Lab 1 **Get The 127.0.0.1**, move on to do the other sub-labs that are available. You must follow the same procedure from step 11 as mentioned above for this lab too.



Server-Side Request Forgery Labs

[Home](#) | [Labs](#)

30 Minutes

FREE

Get The 127.0.0.1

Rohit Gautam

Easy

30 Minutes

FREE

Http(s)? Nevermind!!

Rohit Gautam

Easy

1 Hour

FREE

🔪 The Saviour!

Rohit Gautam

Easy

1 Hour

FREE

Messed Up Domain!

Rohit Gautam

Medium

1 Hour

FREE

Decimal IP

Rohit Gautam

Medium

1 Hour

FREE

Short-Hand IP Address

Rohit Gautam

Medium

1 Hour

FREE

File Upload To SSRF!

Rohit Gautam

Easy

2 Hours

FREE

SSRF With DNS Rebinding

Rohit Gautam

Hard

2 Hours

FREE

Look An SSRF On Cloud!

Rohit Gautam

Hard



Learn, Test, and Share!

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 7 - Assignment Submission Form

VTF Hacktify Pentesting Internship

This Form will be accepting response till November 24, 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

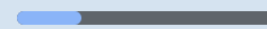
Email *

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](#)



Learn, Test, and Share!

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... [Copy link](#)

Anyone with the link

Anyone on the Internet with this link can comment

[Send feedback to Google](#)

Viewer
☒ **Commenter**
Editor

Your answer

[Back](#)

[Next](#)

[Clear form](#)



Task 2 - Penetration Testing Report

[Optional]

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 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



Learn, Test, and Share!

<div>Step 3</div>	<div>Open the renamed copy of the template and start editing. Firstly edit the Week {#} of the template with the week number.</div> <div>e.g) From Week {#} to Week 7</div> <div>Note: Everything mentioned with the {} has to be changed.</div>	<div><div>Week {#}</div><div>Penetration Testing Report</div></div> <div>Introduction</div> <div>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.</div>		
<div>Step 4</div>	<div>In section 2, edit the Application Name with the lab names.</div> <div>Note: Some weeks have 2 labs so you are required to provide both names in such cases, if not 1 is enough.</div>	<div>2. Scope</div> <div>This section defines the scope and boundaries of the project.</div> <div><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



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>	<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																																		
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>	<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}

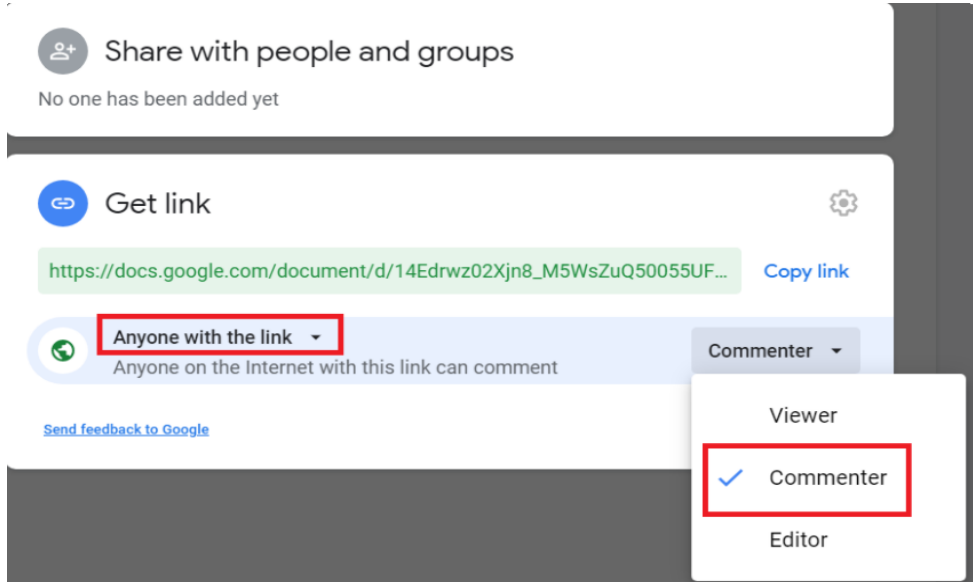
Reference	Risk Rating
{Sub-lab-1 Name}	Low / Medium / High
Tools Used	
Tools that you have used to find the vulnerability.	
Vulnerability Description	
About the vulnerability and its working	
How It Was Discovered	
Automated Tools / Manual Analysis	
Vulnerable URLs	
URLs of the vulnerable pages in the 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



Learn, Test, and Share!

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.	



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 *

The screenshot shows the Google Docs sharing interface. At the top, it says 'Share with people and groups' with a note 'No one has been added yet'. Below this is the 'Get link' section. A green box highlights the URL: https://docs.google.com/document/d/14Edrwz02Xjn8_M5WsZuQ50055UF.... Below the URL, a dropdown menu is set to 'Anyone with the link', with a note 'Anyone on the Internet with this link can comment'. To the right of this dropdown is another dropdown set to 'Commenter'. A red box highlights the 'Anyone with the link' dropdown, and another red box highlights the 'Commenter' option in the second dropdown menu. Other options in the second menu include 'Viewer' and 'Editor'. A 'Copy link' button is visible next to the URL. At the bottom of the sharing settings, there is a 'Send feedback to Google' link.

Your answer

Back

Next

Clear form



Task 3 - Assessment Test [Optional]

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.

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