



Week 7 Technical Guide

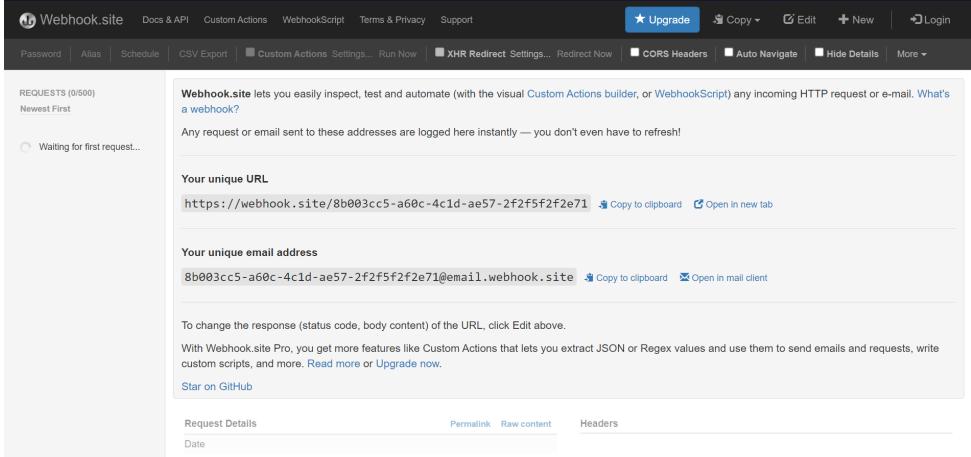
Task 1 - Weekly Labs [Optional]

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	Hope you all have gone through the study material on Clickjacking for this week.	<u>SSRF Server-Side Request Forgery</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>	 <p>The screenshot shows the Webhook.site interface. At the top, there are navigation links: Webhook.site, Docs & API, Custom Actions, WebhookScript, Terms & Privacy, Support, Upgrade, Copy, Edit, New, and Login. Below the header, there are tabs for Password, Alias, Schedule, CSV Export, Custom Actions, XHR Redirect, CORS Headers, Auto Navigate, Hide Details, and More. A message says "REQUESTS (0/600) Newest First" and "Waiting for first request...". To the right, a note says "Webhook.site lets you easily inspect, test and automate (with the visual Custom Actions builder, or WebhookScript) any incoming HTTP request or e-mail. What's a webhook?". It shows a unique URL: https://webhook.site/8b003cc5-a60c-4c1d-ae57-2f2f5f2f2e71 with options to Copy to clipboard and Open in new tab. It also shows a unique email address: 8b003cc5-a60c-4c1d-ae57-2f2f5f2f2e71@email.webhook.site with similar copy and open options. Below this, there's a note about Webhook.site Pro and a link to Star on GitHub. At the bottom, there are tabs for Request Details, Permalink, Raw content, and Headers.</p>
Step 3	<p>Also make sure to check out the references mentioned at the end of the guide. They are very helpful.</p>	
Step 4	<p>Follow the link in the mail to open the Hacktify portal.</p>	<p>Hacktify Labs</p>



Learn, Test, and Share!

Step 5	<p>The portal will look like this. 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	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 .	



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.

The screenshot shows the 'Server-Side Request Forgery Labs' section of the Hackify website. At the top, the Hackify logo and 'VIRTUALLY TESTING FOUNDATION' are visible. Below the title, there are three lab cards, each with a red border:

- Get The 127.0.0.1**: 30 Minutes, FREE, Easy. Instructor: Rohit Gautam.
- Http(s)? Nevermind!!**: 30 Minutes, FREE, Easy. Instructor: Rohit Gautam.
- 1 Hour**: 1 Hour, FREE, FREE.



Step 11

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

HACKIFY

Server-Side Request Forgery

Home | Labs | Lab 1

The diagram illustrates the SSRF attack flow:

- Attacker** (User) sends a request to **Example.com Server** (Host: example.com) with a URL like `GET /uri=http://google.com/ HTTP/1.1`.
- Example.com Server** sends a request to **google.com** (Host: google.com) with the same URL.
- google.com** server responds back to the **Example.com Server**.
- Example.com Server** sends the response from **google.com** back to the **Attacker**.

Annotations in the diagram include:
- "Attacker requests example to fetch google.com"
- "Server send a request to google.com"
- "Sends the response to attacker"
- "Response from google.com is sent to example.com server"
- "GET /uri=http://google.com/ HTTP/1.1 Host: example.com"
- "GET / HTTP/1.1 Host: google.com"

Diagram

Watch Videos
Join Our Private Community
Rohit Gautam Instructor
Shifa Cyclewala Instructor
Enroll Now
Connect With Us
Facebook facebook.com/hackify



Step 12	<p>Go through the details given in the lab. The highlighted portion are the goals you have to reach for this lab.</p>	<p>What Is Server-Side Request Forgery Attack?</p> <p>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).</p> <p>Severity</p> <p>The severity of SSRF varies and depends on case to case basis.</p> <p>Exploiting SSRF</p> <div style="border: 2px solid red; padding: 10px;"><ol style="list-style-type: none">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.<p>Start Lab</p></div>
---------	--	--



Step 13	<p>Then click on Start Lab at the bottom of the page for successfully starting your lab.</p>	<p>What Is Server-Side Request Forgery Attack?</p> <p>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).</p> <p>Severity</p> <p>The severity of SSRF varies and depends on case to case basis.</p> <p>Exploiting SSRF</p> <p>1 Identify the URLs and entry point.</p> <p>2 Copy the payload and replace it with the value of the parameter you have taken.</p> <p>3 Monitor the Logs.</p> <p>Start Lab</p>
----------------	---	--



Learn, Test, and Share!

Step 14

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

Happy Hacking



Online WebPage Loader

Enter URL:

© Copyrights 2021 Hackify Cybersecurity All rights reserved





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.

The screenshot shows the Hackify website interface. At the top, there's a navigation bar with the Hackify logo and links for Home and Labs. The main title "Server-Side Request Forgery Labs" is prominently displayed. Below the title, there are several lab cards arranged in a grid. Each card includes a thumbnail, a title, a duration, a difficulty level, and a "FREE" badge. The highlighted labs are:

- Get The 127.0.0.1**: 30 Minutes, Easy, FREE
- Http(s)? Nevermind!!**: 30 Minutes, Easy, FREE
- ":" The Saviour!**: 1 Hour, Easy, FREE
- Messed Up Domain!**: 1 Hour, Medium, FREE
- Decimal IP**: 1 Hour, Medium, FREE
- Short-Hand IP Address**: 1 Hour, Medium, FREE
- File Upload To SSRF!**: 1 Hour, Easy, FREE
- SSRF With DNS Rebinding**: 2 Hours, Hard, FREE
- Look An SSRF On Cloud!**: 2 Hours, Hard, 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 7 - Assignment Submission Form

VTF Hackify 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](#)



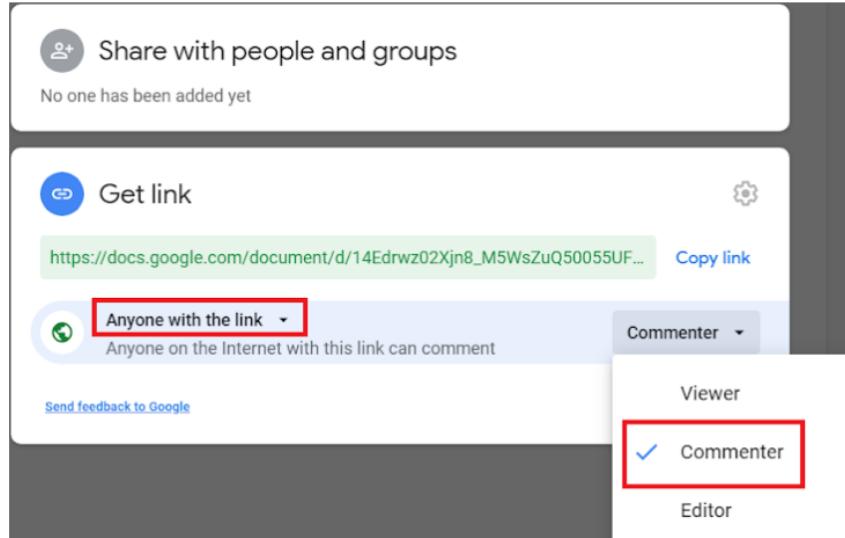
Step 17

- 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 'https://docs.google.com/document/d/14Edrwz02Xjn8_M5WsZuQ50055UF...'. A 'Copy link' button is next to the URL. A dropdown menu shows 'Commenter' checked, while 'Viewer' and 'Editor' are unselected. The entire screenshot is framed by a red border.

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>	<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

Folder

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 7</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="1058 763 2012 833"><tr><td data-bbox="1058 763 1241 833">Application Name</td><td data-bbox="1241 763 2012 833">{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	<p>In section 3, change week {#} and {count} with the number of the sub-labs present.</p> <p>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.</p> <p>Note: {count} is the sum of both labs if 2 labs are present.</p>	<p>3. Summary</p> <p>Outlined is a Black Box Application Security assessment for the Week {#} Labs.</p> <p>Total number of Sub-labs: {count} Sub-labs</p> <table border="1" data-bbox="1072 458 2014 551"><thead><tr><th>High</th><th>Medium</th><th>Low</th></tr></thead><tbody><tr><td>{count}</td><td>{count}</td><td>{count}</td></tr></tbody></table> <p>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</p>	High	Medium	Low	{count}	{count}	{count}
High	Medium	Low						
{count}	{count}	{count}						



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="1072 339 2023 820"><tr><td data-bbox="1072 339 1558 404">Reference {Sub-lab-1 Name}</td><td data-bbox="1558 339 2023 404">Risk Rating Low / Medium / High</td></tr><tr><td colspan="2" data-bbox="1072 404 2023 437">Tools Used Tools that you have used to find the vulnerability.</td></tr><tr><td colspan="2" data-bbox="1072 437 2023 470">Vulnerability Description About the vulnerability and its working</td></tr><tr><td colspan="2" data-bbox="1072 470 2023 502">How It Was Discovered Automated Tools / Manual Analysis</td></tr><tr><td colspan="2" data-bbox="1072 502 2023 535">Vulnerable URLs URLs of the vulnerable pages in the lab</td></tr><tr><td colspan="2" data-bbox="1072 535 2023 567">Consequences of not Fixing the Issue What will be the consequences if the vulnerability is not patched?</td></tr><tr><td colspan="2" data-bbox="1072 567 2023 600">Suggested Countermeasures Give some Suggestions to stand against this vulnerability</td></tr><tr><td colspan="2" data-bbox="1072 600 2023 633">References URLs to the sources used to know more about this vulnerability</td></tr></table>	Reference {Sub-lab-1 Name}	Risk Rating 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 {Sub-lab-1 Name}	Risk Rating 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>																



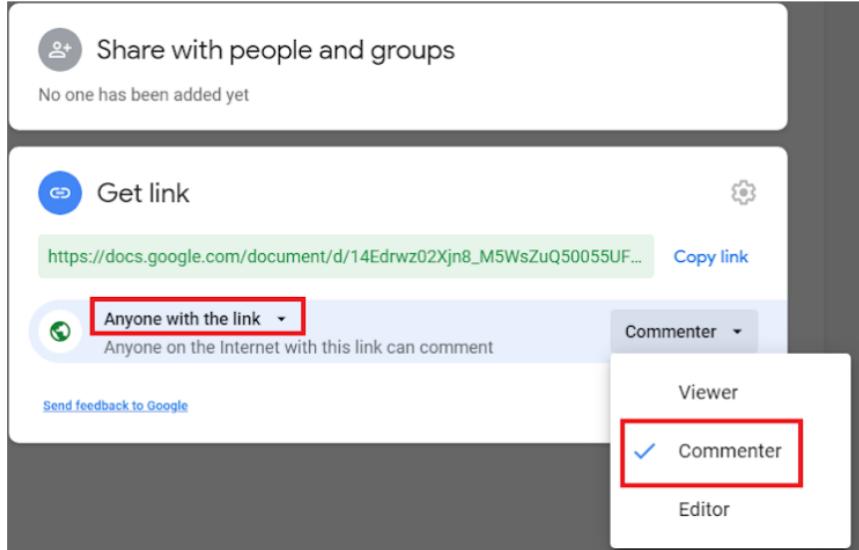
Step 8	<p>If you have worked on 2 labs, do the same step 8 and step 9 for the second lab, if not remove those things that are related to the 2nd lab.</p>	<p>2. {Lab 2 Name (if the week has 2 labs)}</p> <p>2.1. {Sub-lab-1 Name}</p> <table border="1" data-bbox="1062 344 2023 817"><tr><td data-bbox="1062 344 1537 404">Reference {Sub-lab-1 Name}</td><td data-bbox="1537 344 2023 404">Risk Rating Low / Medium / High</td></tr><tr><td colspan="2" data-bbox="1062 404 2023 437">Tools Used Tools that you have used to find the vulnerability.</td></tr><tr><td colspan="2" data-bbox="1062 437 2023 470">Vulnerability Description About the vulnerability and its working</td></tr><tr><td colspan="2" data-bbox="1062 470 2023 502">How It Was Discovered Automated Tools / Manual Analysis</td></tr><tr><td colspan="2" data-bbox="1062 502 2023 535">Vulnerable URLs URLs of the vulnerable pages in the lab</td></tr><tr><td colspan="2" data-bbox="1062 535 2023 567">Consequences of not Fixing the Issue What will be the consequences if the vulnerability is not patched?</td></tr><tr><td colspan="2" data-bbox="1062 567 2023 600">Suggested Countermeasures Give some Suggestions to stand against this vulnerability</td></tr><tr><td colspan="2" data-bbox="1062 600 2023 633">References URLs to the sources used to know more about this vulnerability</td></tr></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 {Sub-lab-1 Name}	Risk Rating 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 {Sub-lab-1 Name}	Risk Rating 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 Document. 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' button and a copied URL. A dropdown menu for permissions is open, showing 'Commenter' is selected (indicated by a checked checkbox). Other options in the dropdown are 'Viewer' and 'Editor'.</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>A screenshot of a Google Document sharing settings interface. It shows a 'Share with people and groups' section with 'No one has been added yet'. Below it is a 'Get link' section with a green button labeled 'Copy link'. A dropdown menu is open, showing 'Commenter' checked (indicated by a red box), 'Viewer', and 'Editor'. At the bottom, there are 'Back' and 'Next' buttons, and a 'Clear form' link.</p>
-----------	---	---



Task 3 - Assessment Test [Optional]

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>Section 4 of 4</p> <p>Technical Assessment</p> <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