



Week 1 Technical Skills Guide

Task 1 - Burp Suite

Important:	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.	
Step 1	Click on the link provided on the right to access the Burp Suite Guide.	Burp Suite



Learn, Test, and Share!

Step 2

Go through the Burp Suite Guide.

What is Burp Suite?

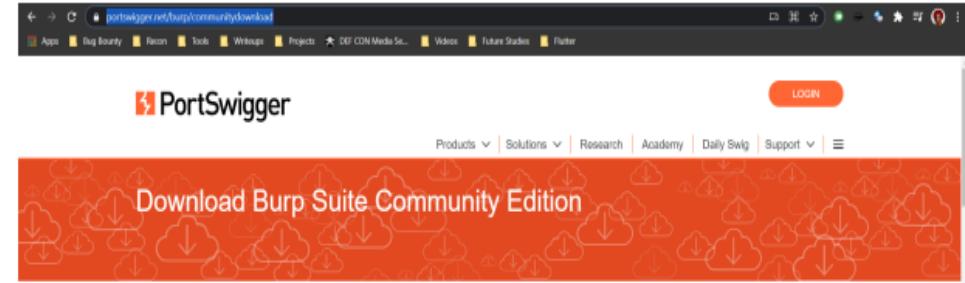
Burp Suite, the Swiss Army Knife, is a proxy tool which can intercept requests and is often used for evaluating security of web-based applications and doing hands-on testing.

Burp Suite Community Edition

Burp Suite comes with 3 edition out of which community edition is free to download.

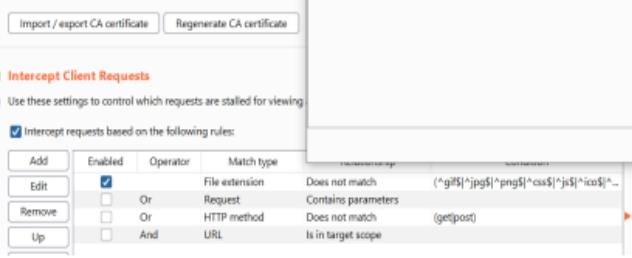
To Download visit: <https://portswigger.net/burp/communitydownload>

And Click on "Download the latest version"





Learn, Test, and Share!

Step 3	Follow the steps mentioned to install and configure Burp Suite in your Local Machine.	 <p>Import / export CA certificate Regenerate CA certificate</p> <p>Intercept Client Requests</p> <p>Use these settings to control which requests are stalled for viewing.</p> <p><input checked="" type="checkbox"/> Intercept requests based on the following rules:</p> <table border="1"> <thead> <tr> <th>Add</th> <th>Enabled</th> <th>Operator</th> <th>Match type</th> </tr> </thead> <tbody> <tr> <td><input type="checkbox"/></td> <td><input checked="" type="checkbox"/></td> <td>File extension</td> <td>Does not match (^gif\$ ^jpg\$ ^png\$ ^css\$ ^js\$ ^ico\$ ^...</td> </tr> <tr> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> <td>Request</td> <td>Contains parameters</td> </tr> <tr> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> <td>Or</td> <td>Does not match (get post)</td> </tr> <tr> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> <td>And</td> <td>Is in target scope</td> </tr> <tr> <td>Up</td> <td></td> <td></td> <td></td> </tr> </tbody> </table>	Add	Enabled	Operator	Match type	<input type="checkbox"/>	<input checked="" type="checkbox"/>	File extension	Does not match (^gif\$ ^jpg\$ ^png\$ ^css\$ ^js\$ ^ico\$ ^...	<input type="checkbox"/>	<input type="checkbox"/>	Request	Contains parameters	<input type="checkbox"/>	<input type="checkbox"/>	Or	Does not match (get post)	<input type="checkbox"/>	<input type="checkbox"/>	And	Is in target scope	Up			
Add	Enabled	Operator	Match type																							
<input type="checkbox"/>	<input checked="" type="checkbox"/>	File extension	Does not match (^gif\$ ^jpg\$ ^png\$ ^css\$ ^js\$ ^ico\$ ^...																							
<input type="checkbox"/>	<input type="checkbox"/>	Request	Contains parameters																							
<input type="checkbox"/>	<input type="checkbox"/>	Or	Does not match (get post)																							
<input type="checkbox"/>	<input type="checkbox"/>	And	Is in target scope																							
Up																										
Step 4	Start exploring Burp Suite & have fun.																									
Important	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.																									



Task 2 - OWASP

Important	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.																						
Step 1	Click on the link provided on the right to access the OWASP Study Guide.	OWASP																					
Step 2	Go through the Study Guide more than once for better understanding.	<p>What is OWASP?</p> <p>OWASP stands for Open Web Application Security Project which is a standard awareness document for developers and web application security. It represents a broad consensus about the most critical security risks to web applications. It categorizes vulnerability of each type</p> <p>OWASP 2013 v/s OWASP 2017</p> <table border="1"><thead><tr><th>OWASP Top 10 - 2013</th><th>→</th><th>OWASP Top 10 - 2017</th></tr></thead><tbody><tr><td>A1 – Injection</td><td>→</td><td>A1:2017-Injection</td></tr><tr><td>A2 – Broken Authentication and Session Management</td><td>→</td><td>A2:2017-Broken Authentication</td></tr><tr><td>A3 – Cross-Site Scripting (XSS)</td><td>→</td><td>A3:2017-Sensitive Data Exposure</td></tr><tr><td>A4 – Insecure Direct Object References [Merged+A7]</td><td>→</td><td>A4:2017-XML External Entities (XXE) [NEW]</td></tr><tr><td>A5 – Security Misconfiguration</td><td>→</td><td>A5:2017-Broken Access Control [Merged]</td></tr><tr><td>A6 – Sensitive Data Exposure</td><td>→</td><td>A6:2017-Security Misconfiguration</td></tr></tbody></table>	OWASP Top 10 - 2013	→	OWASP Top 10 - 2017	A1 – Injection	→	A1:2017-Injection	A2 – Broken Authentication and Session Management	→	A2:2017-Broken Authentication	A3 – Cross-Site Scripting (XSS)	→	A3:2017-Sensitive Data Exposure	A4 – Insecure Direct Object References [Merged+A7]	→	A4:2017-XML External Entities (XXE) [NEW]	A5 – Security Misconfiguration	→	A5:2017-Broken Access Control [Merged]	A6 – Sensitive Data Exposure	→	A6:2017-Security Misconfiguration
OWASP Top 10 - 2013	→	OWASP Top 10 - 2017																					
A1 – Injection	→	A1:2017-Injection																					
A2 – Broken Authentication and Session Management	→	A2:2017-Broken Authentication																					
A3 – Cross-Site Scripting (XSS)	→	A3:2017-Sensitive Data Exposure																					
A4 – Insecure Direct Object References [Merged+A7]	→	A4:2017-XML External Entities (XXE) [NEW]																					
A5 – Security Misconfiguration	→	A5:2017-Broken Access Control [Merged]																					
A6 – Sensitive Data Exposure	→	A6:2017-Security Misconfiguration																					



Step 3	Go through all the vulnerabilities given.	<p>What are XML External Entities? Many older or poorly configured XML processors evaluate external entity references within XML documents. External entities can be used to disclose internal files using the file URI handler, internal file shares, internal port scanning, remote code execution, and denial of service attacks.</p> <p>What is Broken Access Control? Restrictions on what authenticated users are allowed to do are often not properly enforced. Attackers can exploit these flaws to access unauthorized functionality and/or data, such as access other users' accounts, view sensitive files, modify other users' data, change access rights, etc.</p> <p>What is Security Misconfiguration? Security misconfiguration is the most commonly seen issue. This is commonly a result of insecure default configurations, incomplete or ad hoc configurations, open cloud storage, misconfigured HTTP headers, and verbose error messages containing sensitive information. Not only must all operating systems, frameworks, libraries, and applications be securely configured, but they must be patched/upgraded in a timely fashion.</p>
Step 4	Start exploring more about each vulnerability and case study for each.	
Important	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.	



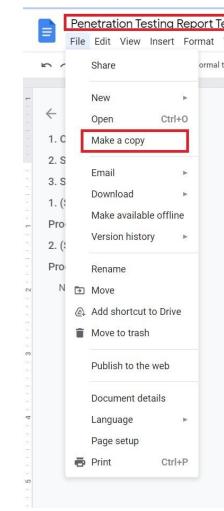
Task 3 - Penetration Testing Report

Important	Go through the steps more than once because you are requested to submit a Penetration Testing Report every week.	
Step 1	Go through the model DVWA Penetration Testing Demo Report by using the link provided. This is only for study purposes.	DVWA Penetration Testing Demo Report
Step 2	Copy the Report template provided for Penetration Testing Report in your Google Drive.	Penetration Testing Report Template



Step 3

It is recommended to make a copy of both **Creating Penetration Testing Report** and **Penetration Testing Report Template** in your **Google Drive** because you need to submit Penetration Testing Report every week.



The screenshot shows a Google Docs document titled "Penetration Testing Report Template". The "File" menu is open, and the "Share" option is selected. A sub-menu is displayed with "Make a copy" highlighted by a red box. The main document area contains the following text:

Week {#}
Penetration Testing Report

Introduction
This report document hereby describes the proceedings and results of a Black Box security assessment conducted against the **(Lab Name) Lab**. The report hereby lists the findings and corresponding best practice mitigation actions and recommendations.

1. Objective
The objective of the assessment was to uncover vulnerabilities in the **(Lab Name) Lab** and provide a final security assessment report comprising vulnerabilities, remediation strategy and recommendation guidelines to help mitigate the identified vulnerabilities and risks during the activity.

2. Scope
This section defines the scope and boundaries of the project.

Application Name	(Lab Name) Lab
URL	(URL link of the lab)



Learn, Test, and Share!

Step 4

Save the Recreated Penetration Testing Report as **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



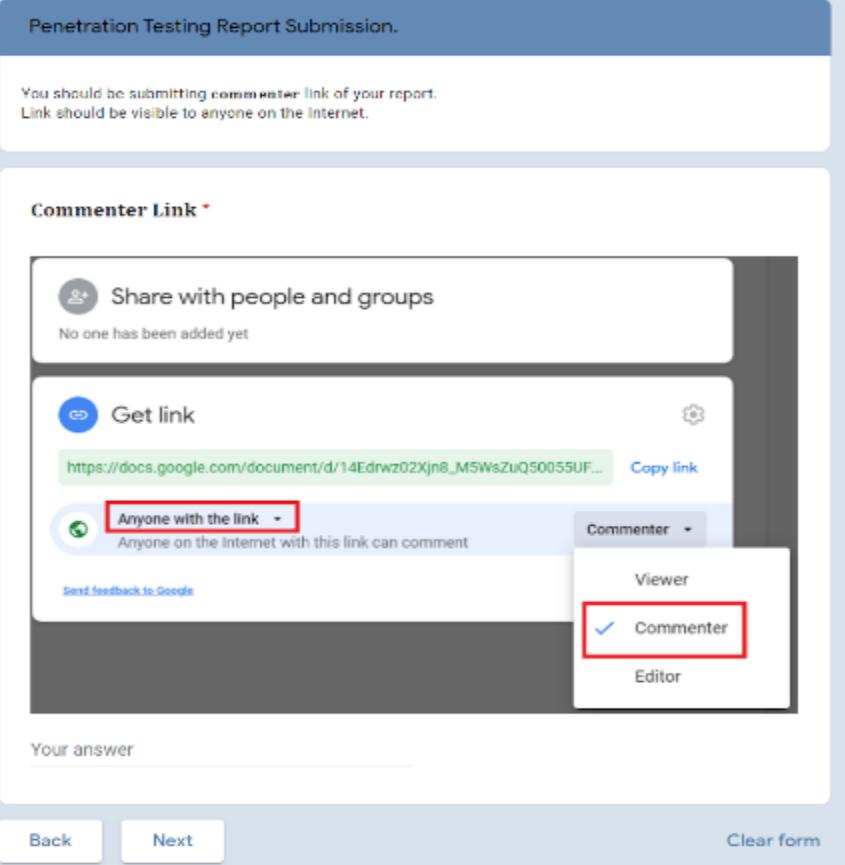
Learn, Test, and Share!

Step 5

After completing the work, now click on the **share** button and create a share link with the **commenter permission**.

The screenshot shows the sharing settings for a Google Doc. At the top, it says "Share with people and groups" and "No one has been added yet". Below that is a "Get link" button and a link URL. A dropdown menu is open, showing "Anyone with the link" (which is highlighted with a red box) and "Commenter" (which is also highlighted with a red box). A tooltip for "Commenter" says "Anyone on the Internet with this link can comment". Other options in the dropdown include "Viewer" and "Editor".



Step 6	<p>You are required to submit the link to your Report in the weekly submission 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>Share with people and groups No one has been added yet</p> <p>Get link https://docs.google.com/document/d/14Edrwz02Xjn8_M5WsZuQ50055UF... Copy link</p> <p>Anyone with the link ▾ Anyone on the Internet with this link can comment</p> <p>Commenter ▾ Viewer <input checked="" type="checkbox"/> Commenter Editor</p> <p>Your answer</p> <p>Back Next Clear form</p> 
Important	<p>It is recommended to make a copy of both Creating Penetration Testing Report and Penetration Testing Report Template in your Google Drive because you need to submit Penetration Testing Report every week.</p>	



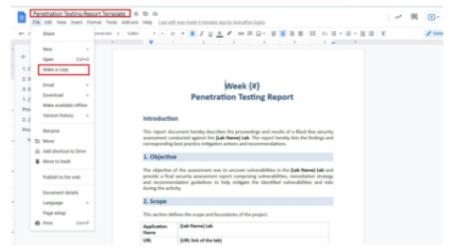
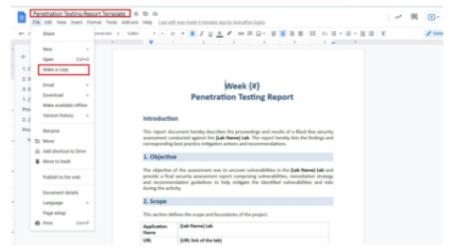
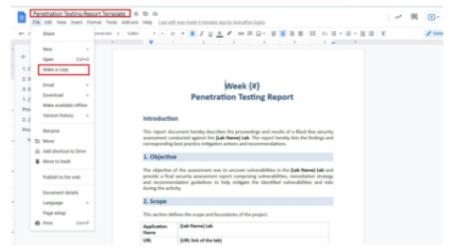
Task 4 - Assessment Test

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> <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.	



Challenge Yourself

[Optional Task]

Step 1	<p>This is an optional task. You would not be graded for it's submission.</p> <p>We recommend you to try recreating the DVWA Report Provided to you. This will be helpful in future weeks in which you will be making Pentesting Reports based on hacktify labs as a mandatory task.</p>										
Step 2	<p>Get the instructions from here. Please go through steps 1 to 3 again.</p>	<table border="1"><tr><td data-bbox="1062 817 1184 866">Step 1</td><td data-bbox="1184 817 1539 866">Go through the model DVWA Penetration Testing Demo Report by using the link provided.</td><td data-bbox="1539 817 2021 866">DVWA Penetration Testing Demo Report</td></tr><tr><td data-bbox="1062 866 1184 915">Step 2</td><td data-bbox="1184 866 1539 915">Copy the model template provided for Penetration Testing Report in your Google Drive.</td><td data-bbox="1539 866 2021 915">Penetration Testing Report Template</td></tr><tr><td data-bbox="1062 915 1184 1183">Step 3</td><td data-bbox="1184 915 1539 1183">It is recommended to make a copy of both Creating Penetration Testing Report and Penetration Testing Report Template in your Google Drive because you need to submit Penetration Testing Report every week.</td><td data-bbox="1539 915 2021 1183"></td></tr></table>	Step 1	Go through the model DVWA Penetration Testing Demo Report by using the link provided.	DVWA Penetration Testing Demo Report	Step 2	Copy the model template provided for Penetration Testing Report in your Google Drive.	Penetration Testing Report Template	Step 3	It is recommended to make a copy of both Creating Penetration Testing Report and Penetration Testing Report Template in your Google Drive because you need to submit Penetration Testing Report every week.	
Step 1	Go through the model DVWA Penetration Testing Demo Report by using the link provided.	DVWA Penetration Testing Demo Report									
Step 2	Copy the model template provided for Penetration Testing Report in your Google Drive.	Penetration Testing Report Template									
Step 3	It is recommended to make a copy of both Creating Penetration Testing Report and Penetration Testing Report Template in your Google Drive because you need to submit Penetration Testing Report every week.										



Learn, Test, and Share!

Step 3

After you have created your own report and are satisfied with it, submit the **Commenter Link** in the submission 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 *

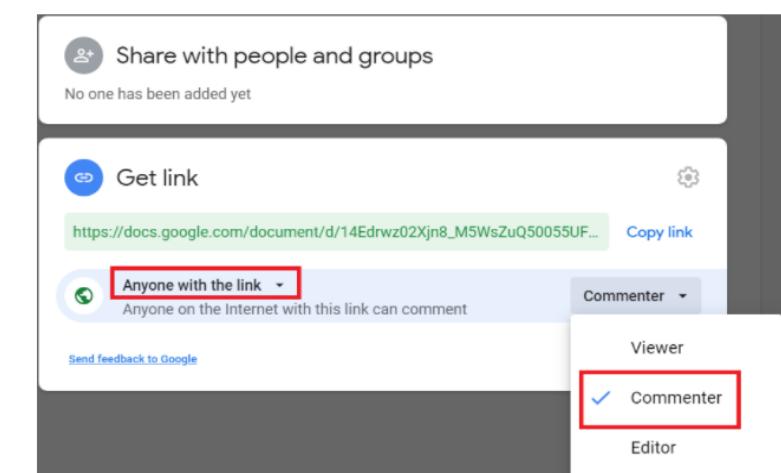
Share with people and groups
No one has been added yet

Get link
https://docs.google.com/document/d/14Edrwz02Xjn8_M5WsZuQ5005UF... [Copy link](#)

Anyone with the link ▾
Anyone on the Internet with this link can comment

Commenter ▾
Viewer
 Commenter
Editor

Short answer text





Learn, Test, and Share!

Reminder

All Interns are required to participate in our Technical Skills Assignment. If you do not participate you will be removed from the internship and your access to our content will be revoked.

**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**