



Learn, Test, and Share!

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



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

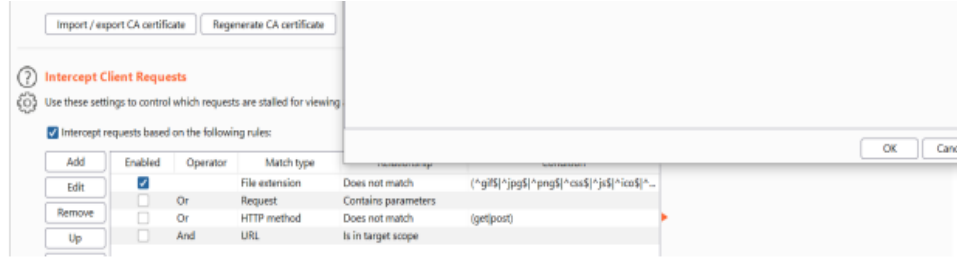
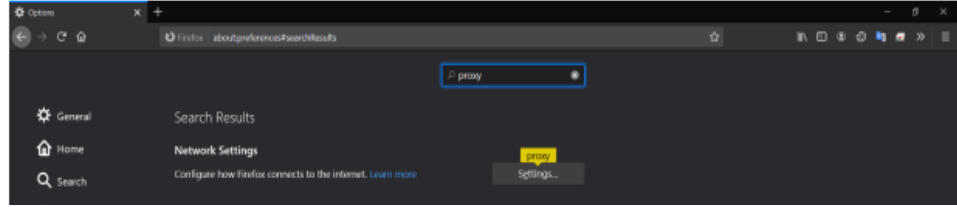
Burp Suite comes with 3 edition out of which community edition is free to download.

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

And Click on "Download the latest version"





Step 3	Follow the steps mentioned to install and configure Burp Suite in your Local Machine.	 <p>5. Click Ok 6. Open Firefox 7. In the options menu search for "proxy"</p> 
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><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>U</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]	U	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]	U	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



Learn, Test, and Share!

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.

Penetration Testing Report Template

File Edit View Insert Format Tools Add-ons Help Last edit was made 9 minutes ago by Anindhira Gupta

Share

New

Open Ctrl+O

Make a copy

1. C

2. S

3. S

1. (

Pro

Version history

2. (

Pro

Rename

N

Move

Add shortcut to Drive

Move to trash

Publish to the web

Document details

Language

Page setup

Print Ctrl+P

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



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!

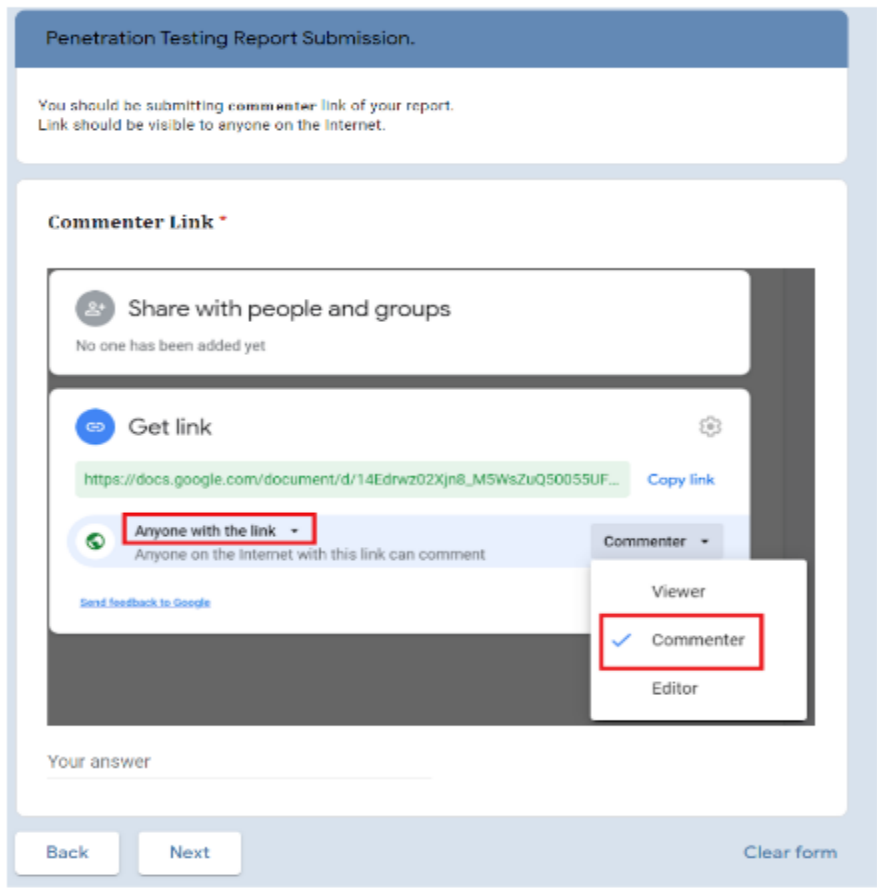
Step 5

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

The screenshot shows the Google Docs sharing interface. At the top, there's a section 'Share with people and groups' with a plus icon and the text 'No one has been added yet'. Below this is the 'Get link' section, which includes a link to the document: https://docs.google.com/document/d/14Edrwz02Xjn8_M5WsZuQ50055UF... and a 'Copy link' button. Under the link, there's a dropdown menu currently set to 'Anyone with the link', with the text 'Anyone on the Internet with this link can comment' below it. A dropdown menu is open to the right, showing three options: 'Viewer', 'Commenter' (which is selected and highlighted with a blue checkmark), and 'Editor'. A 'Send feedback to Google' link is visible at the bottom left of the sharing section.



Learn, Test, and Share!

Step 6	<p>You are required to submit the link to your Report in the weekly submission 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

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 !

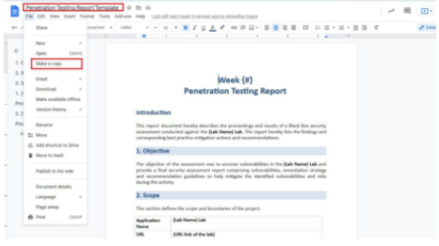
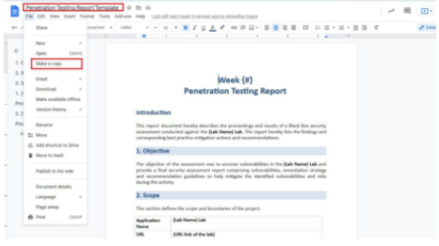
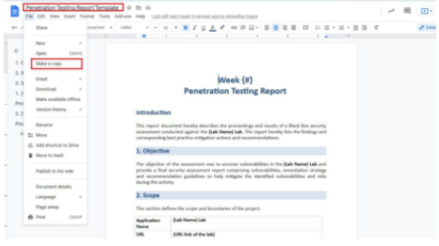
Note:

- 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.



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><tr><td>Step 1</td><td>Go through the model DVWA Penetration Testing Demo Report by using the link provided.</td><td>DVWA Penetration Testing Demo Report</td></tr><tr><td>Step 2</td><td>Copy the model template provided for Penetration Testing Report in your Google Drive.</td><td>Penetration Testing Report Template</td></tr><tr><td>Step 3</td><td>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></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_M5WsZuQ50055UF... [Copy link](#)

Anyone with the link ▼ Commenter ▼

Anyone on the Internet with this link can comment

[Send feedback to Google](#)

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