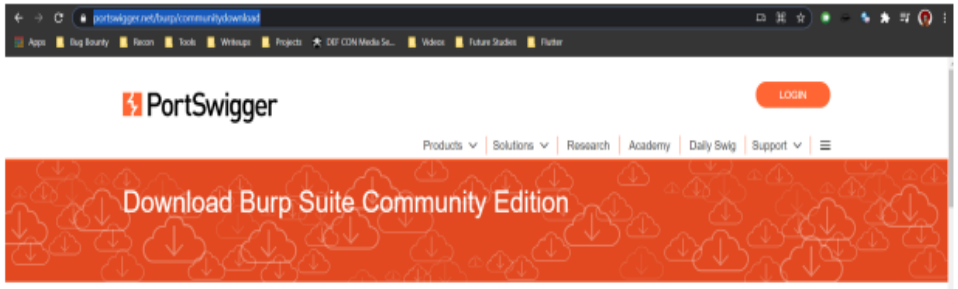
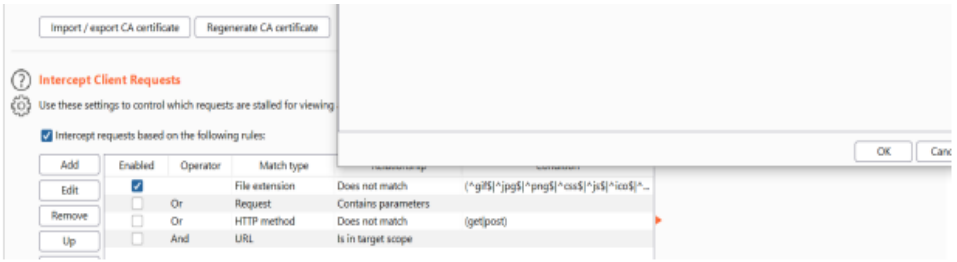
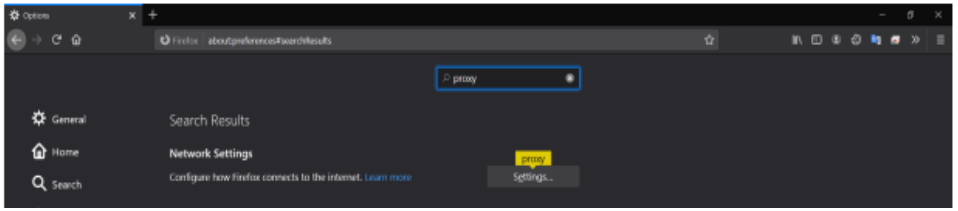
Learn, Test, and Share!

Week 1 Technical Skills Guide

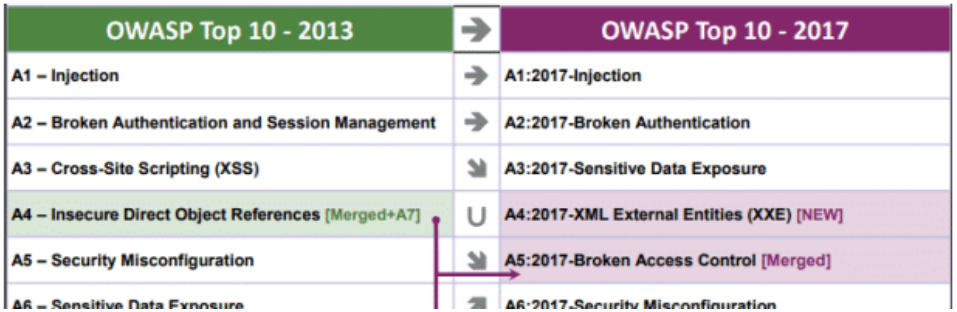
Task 1 - Burp Suite

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.	 5. Click Ok 6. Open Firefox 7. In the options menu search for “proxy” 
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

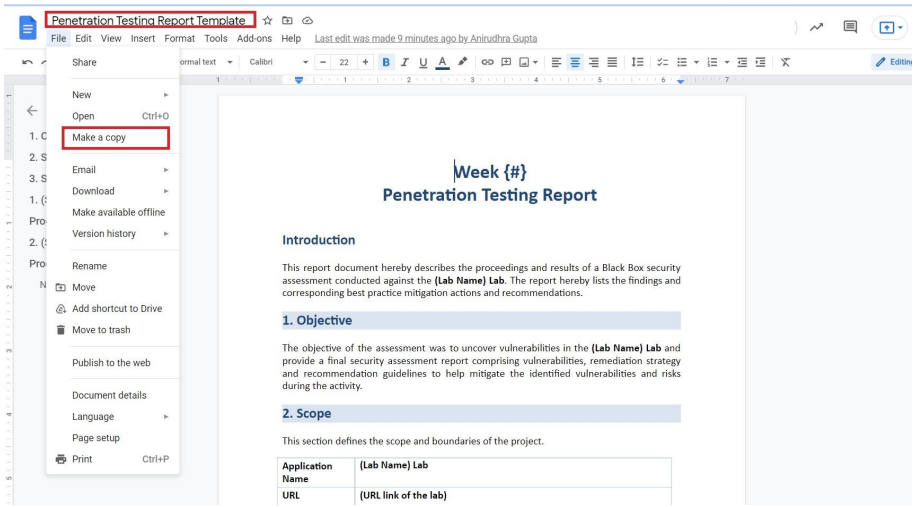
Important	Make sure to take **Notes** on what you do. It is recommended to do research as all of this will help you in the **Weekly Assessment Test** which will be provided to you.	
Step 1	Click on the link provided on the right to access the OWASP Study Guide.	OWASP
Step 2	Go through the Study Guide more than once for better understanding.	**What is OWASP?** 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 **OWASP 2013 v/s OWASP 2017** 

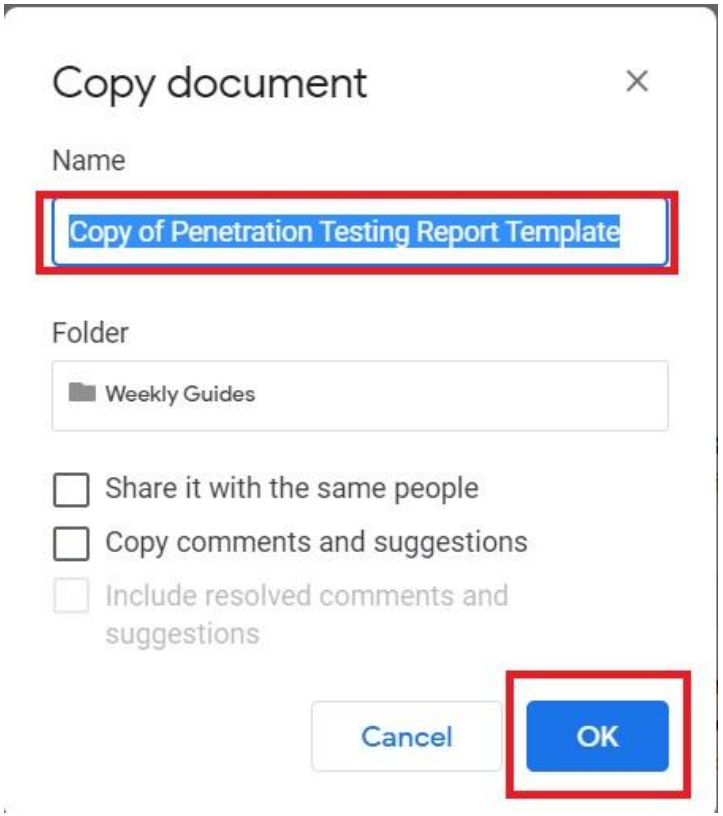
OWASP Top 10 - 2013		OWASP Top 10 - 2017
A1 – Injection	→	A1:2017-Injection
A2 – Broken Authentication and Session Management	→	A2:2017-Broken Authentication
A3 – Cross-Site Scripting (XSS)	↘	A3:2017-Sensitive Data Exposure
A4 – Insecure Direct Object References [Merged+A7]	U	A4:2017-XML External Entities (XXE) [NEW]
A5 – Security Misconfiguration	↘	A5:2017-Broken Access Control [Merged]
A6 – Sensitive Data Exposure		A6:2017-Security Misconfiguration

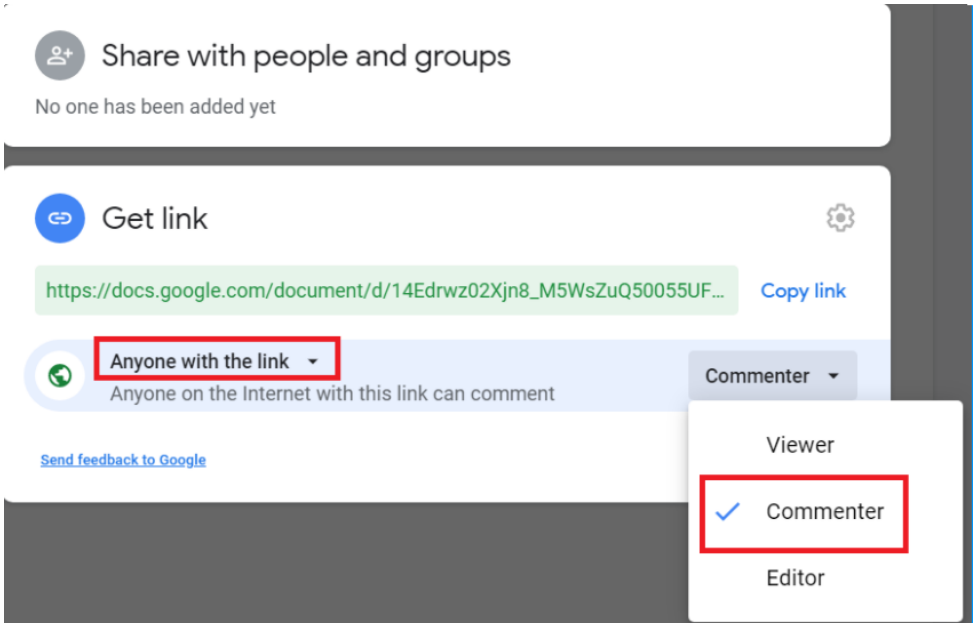
Step 3	Go through all the vulnerabilities given.	**What are XML External Entities?** Many older or poorly configured XML processors evaluate external entity references within XML documents. External entities can be used to disclose internal files using the file URI handler, internal file shares, internal port scanning, remote code execution, and denial of service attacks. **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. **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.
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.	

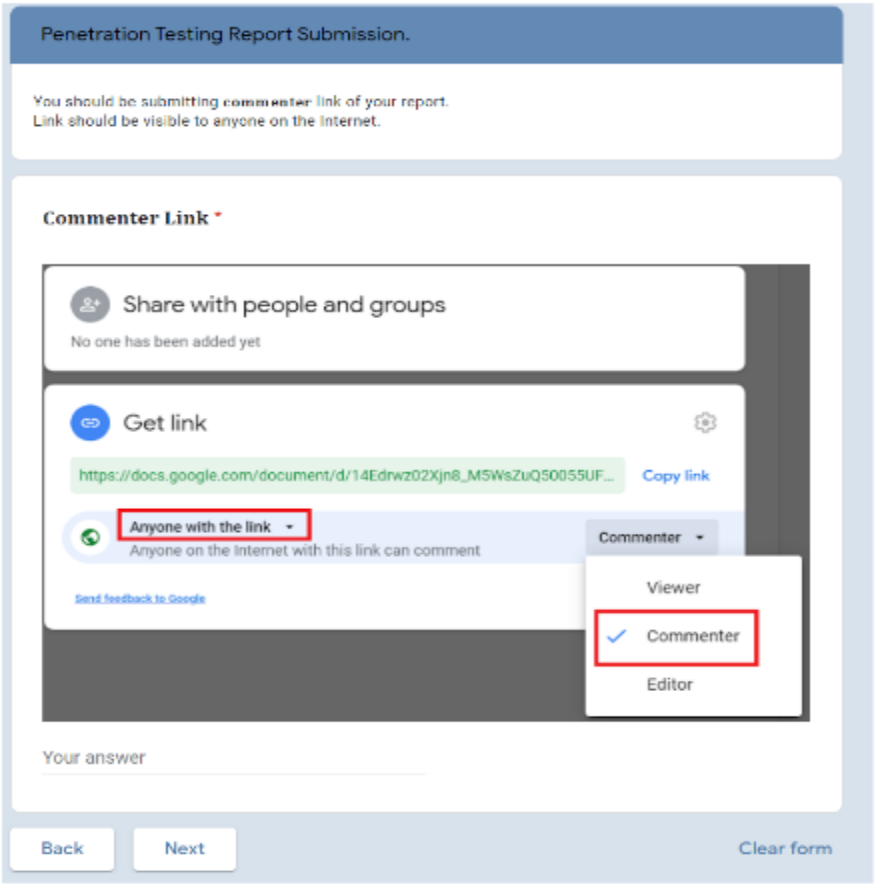
Task 3 - Penetration Testing Report

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

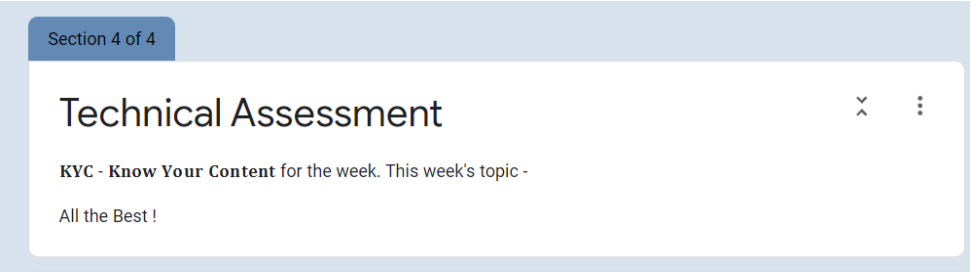
Step 3	It is recommended to make a copy of both **Creating Penetration Testing Report** and **Penetration Testing Report Template** in your **Google Drive** because you need to submit Penetration Testing Report every week.	

Step 4	Save the Recreated Penetration Testing Report as **Week_#_Penetration_Testing_Report** where # is the week number.	

Step 5	After completing the work, now click on the **share** button and create a share link with the **commenter permission**.	

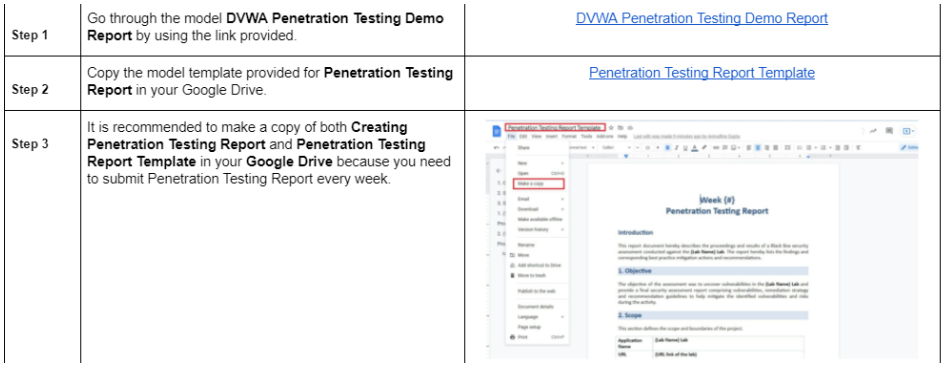
Step 6	You are required to submit the link to your Report in the **weekly submission form**.	
Important	It is recommended to make a copy of both **Creating Penetration Testing Report** and **Penetration Testing Report Template** in your **Google Drive** because you need to submit Penetration Testing Report every week.	

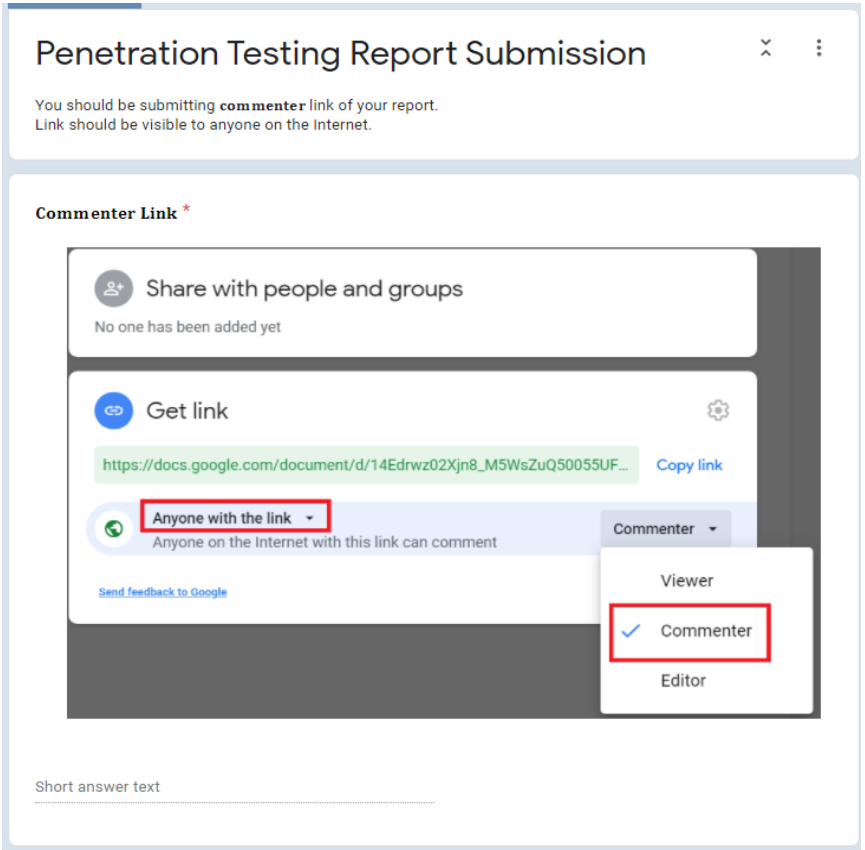
Task 4 - Assessment Test

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.	
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	This is an optional task. You would not be graded for it's submission. 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.	
Step 2	Get the instructions from here. Please go through steps 1 to 3 again.	

Step 3	After you have created your own report and are satisfied with it, submit the **Commenter Link** in the submission form.	

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