# OWASP Top 10 Part 2

Module 9 | Activity 2

## Introduction

In Module 9, we learned all about web vulnerabilities and the Open Web Application Security Project (OWASP). We discovered the top ten list of web vulnerabilities created by OWASP. In Activity 1, we covered the top 1-5 vulnerabilities. Activity 2 will go over the last 6-10 of the vulnerabilities: Security Misconfiguration, Cross-Site Scripting XSS, Insecure Deserialization, Using Components with Known Vulnerabilities, Insufficient Logging & Monitoring. This activity will help you grasp a better understanding of each vulnerability and put them in practice.

## Getting Started

Similar to Activity 1 of this module, we will be using HACKSPLAINING to complete this online activity. The instructions will guide you through the exercises on the website, and help emphasize the most important material. We will be completing the corresponding exercises for the web vulnerabilities below.

First, go on over to the Link and click the sign up button on the top right corner. Sign up either through email or GitHub (common hacker website).

## 6. Security Misconfiguration

The HACKSPLAINING link will lead you on over to the OWASP Top Ten list.

Scroll down to "6. Security Misconfiguration". Read the paragraph explaining it, and fill in the blanks below.

Security misconfiguration is the most commonly seen issue. This
is commonly a result of insecure ____________________,
___________ or ________________, _________________,
_______________________, and _______________________________
_______________________. Not only must all operating systems,
frameworks, libraries, and applications be securely configured,
but they must be ________/__________ in a timely fashion.

Now hop on over to this [Link] to learn a little more about the misconfiguration of the LAX Security Settings. Click on the icon to start the exercise. Answer the following questions as you read through the components.

A. What is an extreme cause of security holes that can be taken advantage of? ____________________________
B. What must be disabled by developers once they are in production? _______________________________________
C. What can expose sensitive files to attackers? _____________
D. List what must be turned off to configure a more secure system. ________________________________________________
E. What is recommended to be done if you allow team members to manage production data?_____________________________________
F. Explain what Content Delivery Networks (CDNs) are.______________________________________________________
G. Find the default username and password for JBoss on google to get access to the site.

Feel free to click on the orange icon to learn how to help prevent human error in configuration.

Next, go on over to [Link] to learn about Information Leakage. Answer the following questions as you read through the components.

H. What is the first thing an attacker will try to find out about a website? ____________________________________
I. What feature must you turn off to protect your website from attackers? __________________________________________________
J. What can also expose information to hackers, and what path should you avoid to prevent this? __________________________
K. What type of page is important for storing error messages and AJAX responses.________________________________________
L. Uncover the user's Social Security Number within the exercising.

## 7. Cross-site Scripting (XSS)

Head back to the HACKSPLAINING link to jump on over to the OWASP Top Ten list.

Scroll down to "7. Cross-site Scripting (XXS)". Read the paragraph explaining it, and fill in the blanks below.

XSS flaws occur whenever an application includes _____________ in a new web page without proper validation or escaping, or __________ an existing web page with user-supplied data using a browser API that can create _______ or ____________. XSS allows attackers to execute scripts in the victim's browser which can ____________________, ____________________, or ________________________________.

Now, go on over to [Link] to learn about Cross-site Scripting. Answer the following questions as you read through the components.

M. What do you have to be careful about constructing when building a website with a comment section? ________________
N. What can hackers inject into a comment section? ____________
O. Using cross-site scripting, what can hackers steal? ____________________________________________________________

P. Describe what happens when your inject a script tag into the chat.________________________________________________

Once you have completed the exercise, click on the orange icon to learn about how to protect against Cross-site Scripting (XXS).

Q. List the five things a hacker can implement by exploiting XSS? ________________

R. Read the “PROTECTION” section and write a quick summary of how to best protect a web application for XXS attacks?
____________________________________________________________
____________________________________________________________
____________________________________________________________
____________________________________________________________
____________________________________________________________
____________________________________________________________

Let's continue with Cross-site Scraping (XXS) by going to the [Link] about Rejected XXS.

S. What is another way attackers can inject malicious JavaScript using XXS? _______________________________________

T. What can a hacker do once he gets its victim to click on its URL link? ___________________________________________

Last thing we are going to talk about concerning Cross-site Scripting (XXS) is DOM-Based XXS. Click on the [Link]

U. What is the vulnerability that is common when using URI fragments? ______________________________________________

## 8. Insecure Deserialization

Go back on over to the HACKSPLAINING OWASP Top Ten list.

Scroll down to “8. Insecure Deserialization”. Read the paragraph explaining it, and fill in the blanks below.

Insecure deserialization often leads to ____________________. Even if deserialization flaws do not result in remote code execution, they can be used to perform attacks, including ___________, ________________, and ________________________.

Once again we are going to click on the [Link] to learn about Privilege Escalation.

V. What is privilege escalation? _____________________________
_____________________________________________________________

W. What is horizontal escalation? ____________________________
_____________________________________________________________

X. What is vertical escalation? ______________________________
_____________________________________________________________

Y. Click on the orange click to read about how to protect against privilege escalation. Write a quick summary on what you read to protect web applications. _____________________
_____________________________________________________________
_____________________________________________________________
_____________________________________________________________
_____________________________________________________________
_____________________________________________________________

## 9. Using Components with Known Vulnerabilities

Just like before, we will be using the HACKSPLAINING OWASP Top Ten list to fill in the blank below.

Scroll down to "9. Privilege Escalation". Read the paragraph explaining it to fill in the blanks.

Components, such as ___________, __________, and other ________ _________, run with the same privileges as the application. If a vulnerable component is exploited, such an attack can facilitate serious ___________ or _____________. Applications and APIs using components with known vulnerabilities may undermine application ____________ and enable various ________ and ________.

You know the deal, use the [Link] to do the Toxic Dependencies exercise.

Z. What is Apache Struts? ________________________________________

________________________________________________________________

AA. What are the vulnerabilities of Apache Struts 2? _________

________________________________________________________________

BB. What is Ruby on Rails? _______________________________________

________________________________________________________________

What are the vulnerabilities of Rails? ______________________

________________________________________________________________

CC. XCodeGhost is designed to do what? _________________________

________________________________________________________________

DD. What vulnerabilities were found in 2014 and 2020? ________

________________________________________________________________

## 10. Insufficient Logging & Monitoring

One last time, go to the HACKSPLAINING OWASP Top Ten list and fill in the blanks below.

Scroll down to "10. Insufficient Logging & Monitoring". Read the paragraph explaining it, to fill in the blanks below.

Insufficient logging and monitoring, coupled with missing or ineffective integration with incident response, allows attackers to _______________________, ____________________, ____________ ________________, and ___________, ____________, or __________ data. Most breach studies show time to detect a breach is over ______ days, typically detected by _________ parties rather than ______________ processes or monitoring.

Use this final [Link] of the activity to complete the Logging and Monitoring exercise.

EE. What is logging? ____________________________________________

________________________________________________________________

________________________________________________________________

FF. Each logging statement should have what data? ____________

________________________________________________________________

GG. What should you not write in a log file?

________________________________________________________________

HH. What does monitoring measure? ______________________________

________________________________________________________________

II. What are other uses of monitoring?________________________

______________________________________________________________

JJ. Why do you need a response plan? What does it include?___

______________________________________________________________

______________________________________________________________

YOU ARE DONE!!!