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 HACKSPLEINING 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 ________________, ______________, ________________, _________________. 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.

Copyright © 2021 Iowa State University
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? ________________________________

Copyright © 2021 Iowa State University
P. Describe what happens when you 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 HACKSPLEINING 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.

Copyright © 2021 Iowa State University
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 HACKSPLEINING 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? __________________
________________________

Copyright © 2021 Iowa State University
II. What are other uses of monitoring?

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

YOU ARE DONE!!!