Learning Guide Unit 5

Site: University of the People
Course: CS 3340-01 Systems and Application Security - AY2025-T1
Book: Learning Guide Unit 5

Printed by: Mejbaul Mubin
Date: Thursday, 5 September 2024, 2:37 PM

Description

Learning Guide Unit 5

Table of contents

Overview

UNIT 5: Web Application Vulnerabilities and Countermeasures -Part I

Topics

- Web Security Basics
- Cross-site scripting (XSS)
- Cross-site request forgery (CRFR)
- XML injection
- Buffer overflow

Learning Objectives

By the end of this Unit, you will be able to:

1. Discuss XSS (XXE) and Man-in-the-Middle attacks
2. Explain buffer overflow attack and vulnerability
3. Identify cyber threats and their mitigation

Tasks

- Peer assess Unit 4 Written Assignment
- Read the Learning Guide and Reading Assignments
- Participate in the Discussion Assignment (post, comment, and rate in the Discussion Forum)
- Complete and submit the Written Assignment
- Make entries to the Learning Journal
- Take the Self-Quiz

Introduction

Web applications are playing a significant role in the world economy. We manage our finances via banking websites, communicate with friends and professionals via email and other messaging applications, pursue education and professional careers via web-accessible content management systems, find interesting readings, exchange reports, and research papers, do online shopping, and much more. It is hard to list everything that web content and web applications enable us to do.

In this unit, we will discuss and explore topics such as web security basics, cross-site scripting, cross-site forgeries, XML injection, and buffer overflow. Topics, related to other web applications vulnerabilities, including user enumeration, cookies and session hijacking, truncation and trimming attacks, PHP-special issues, prefetching and spiders, and SQL injection will be discussed in the next unit.

Web Security Basics

Web cybersecurity (same as security) is a subdivision of cybersecurity that is explicitly dedicated to the detection and countermeasure of cyber threats targeting websites and web applications. Moreover, web security investigates cybersecurity vulnerabilities associated with websites and web applications.

To start our exploration into the secure web, let us familiarize ourselves with some features of web security.

Reading Assignments:

Read Web Security Basics: Is Your Web Application Safe?

Watch Top Web Applications Vulnerabilities | Web Application Vulnerabilities For Beginners (2020) Edureka

Resources:

Crashtest security. (2022, November17). *Web security basics and best practices* [Video]. YouTube.

Cyber citadel. (2021, November 24). *OWASP top 10 2021 - The list and how you should use it* [Video]. YouTube.

edureka! (2020, July 13). *Top web applications vulnerabilities | web application vulnerabilities for beginners | edureka* [Video]. YouTube. https://www.youtube.com/watch?v=loyVGklGpjU&t=2s

Nidecki, T. A. (2021, September9). *Web security basics: Is your web application safe?* Acunetix . https://www.acunetix.com/blog/web-security-zone/web-security-basics/

Telusko. (2021, August 3). *OWASP top 10 web application security risks* [Video]. YouTube.

Cross-site scripting (XSS)

Cross-site scripting attacks were first discovered in the late 1990s. Cross-Site Scripting (XSS) attack injects a malicious script into trusted websites. The Open Web Application Security Project (OWASP) promotes and supports the security of web applications for almost two decades. Cybersecurity professional Kirsten & Others (2021) in their contribution to OWASP notes stated "XSS attacks occur when an attacker uses a web application to send malicious code, generally in the form of a browser side script, to a different end-user. Flaws that allow these attacks to succeed are quite widespread and occur anywhere a web application uses input from a user within the output it generates without validating or encoding it".

Reading Assignments:

Read: Cross Site Scripting (XSS) Attack Tutorial with Examples, Types & Prevention

Watch: What is Cross Site Scripting?| Cross Site Scripting Attack | Cross Site Scripting Tutorial | Edureka

Resources:

Cross site scripting (XSS) attack tutorial with examples, types & prevention. (2021, November 29). Software testing help. https://www.softwaretestinghelp.com/cross-site-scripting-xss-attack-test/

edureka! (2019, December 10). *What is cross site scripting?| cross site scripting attack | cross site scripting tutorial | edureka* [Video]. YouTube. https://www.youtube.com/watch?v=cWu_FJUrH5Y

KristanS., Manico, J., Williams, J., Wichers, D., Weidman, A., Roman., Jex, A., Smith, A., Knutson, J., Imifos., Yalon, E., Kingthorin., & Khanna, V. (n.d.). *Cross site scripting (XSS*). Open Web Application Security Project. https://owasp.org/www-community/attacks/xss/ licensed under Creative Commons Attribution – ShareAlike 4.0.

Secure Code Warrior. (2017, August 25). *Cross-site scripting (xss) | owasp top 10 explainer video | secure code warrior* [Video]. YouTube. https://www.youtube.com/watch?v=H22cJTqCgUA

Cross-site request forgery (CRFR)

Cross-Site Request Forgery which is also known as CRFR is a malicious attack. It pressurizes an end-user to perform undesired actions on a web application in which they are currently authenticated. A hacker might trick the end-user of the web application as per his or her will with a little help from social engineering. For example- sending a link via email or chat. If the victim is a naive user, a successful CSRF attack can make the user perform state-changing requests like transferring money, changing their email credentials, and so on. If the victim is an administrative account, CSRF can destroy the entire web application.

Reading Assignments:

Read Cross Site Request Forgery (CSRF)

Watch CSRF Tutorial - A Guide to Better Understand and Defend Against Cross-Site Request Forgery (CSRF)

Resources:

Fullstack Academy. (2017, September 29). *CSRF tutorial - a guide to better understand and defend against cross-site request forgery (CSRF)* [Video]. YouTube. https://www.youtube.com/watch?v=13QPmRuhbhU

KristanS., Wichers, D., Davisnw., Petefish, P., Weidman, A., Brooks, M., Mir, A., Dc., D0ubl3 h3lix, Manico, J., Gilbert, R., Tgondrom., Krawczyk, P., Brandt, Minhaz, A. V., Lorenzo, K., Smith, A., Schelin, C., Elias-Bachrach, A., Sarciszewski., kingthorin & Spatafora, B. (2021). *Cross site request forgery (CSRF)).* OWASP. https://owasp.org/www-community/attacks/csrf. licensed under Creative Commons Attribution – ShareAlike 4.0.

Udacity. (2016, June 6). *XSRF cross site request forgery* [Video]. YouTube. https://www.youtube.com/watch?v=9JrzPX1pVjs

XML injection

XML injection attack, also known as the XML External Entity (XXE) attack can make a user vulnerable to; confidential data theft, inaccessible to any application services, Server Side Request Forgery (SSRF), port scanning potential vulnerabilities, and also a possible target for any future attacks.

Reading Assignments:

Read:

- XML external entity (XXE) injection
- XML Vulnerabilities and Attacks cheatsheet

Watch OWASP Top 10: XML External Entities

Resources:

AppSecAcademy. (2019, February 21). *#1 XML external entity (XXE) in 2 minutes | AppSec academy* [Video]. YouTube. https://www.youtube.com/watch?v=_gfhgWvI6XI

F5DevCentral. (2018, January 18). *OWASP top 10: XML external entities* [Video]. YouTube. https://www.youtube.com/watch?v=g2ey7ry8_CQ

mgeeky. (n.d.). *XML vulnerabilities and attacks cheatsheet*. GitHub Gist. https://gist.github.com/mgeeky/4f726d3b374f0a34267d4f19c9004870

XML external entity (XXE) injection. (n.d.). PortSwigger. https://portswigger.net/web-security/xxe

Buffer Overflow

Buffer overrun, also called buffer overflow, occurs when the amount of information exceeds the storage power of the memory buffer. Typically, when a user provides an input to an application, the input first goes into a buffer, and the frame buffer is sent to a memory address that defines a variable to store that input. Some programming languages have built-in security for memory allocation feature that prevents attempts to write a large piece of data into a variable reserved for a smaller size of data. Applications developed with C and C++ programming languages are most susceptible to buffer overflow attacks.

Reading Assignments:

Read Buffer Overflow

Watch Buffer Overflow attack tutorial - 0x00

Resources:

Buffer overflow. (2021). Open Web Application Security Project. https://owasp.org/www-community/vulnerabilities/Buffer_Overflow licensed under Creative Commons Attribution- SharAlike 4.0.

Eye on Tech. (2021, September 23). *What is a buffer overflow attack?* [Video]. YouTube. https://www.youtube.com/watch?v=YNkjX2Wqgh0

w3w3w3. (2020, January 29). *Buffer overflow attack tutorial - 0x00* [Video]. YouTube. https://www.youtube.com/watch?v=j7AEzGKuKUU

Reading Assignment

1. *Buffer overflow.* (2021). Open Web Application Security Project. **https://owasp.org/www-community/vulnerabilities/Buffer_Overflow** licensed under Creative Commons Attribution- SharAlike 4.0.
2. *Cross site scripting (XSS) attack tutorial with examples, types & prevention*. (2021, November 29). Software testing help. **https://www.softwaretestinghelp.com/cross-site-scripting-xss-attack-test/**
3. KristanS., Manico, J., Williams, J., Wichers, D., Weidman, A., Roman., Jex, A., Smith, A., Knutson, J., Imifos., Yalon, E., Kingthorin., & Khanna, V. (n.d.). *Cross site scripting (XSS*). Open Web Application Security Project. **https://owasp.org/www-community/attacks/xss/** licensed under Creative Commons Attribution – ShareAlike 4.0.
4. KristanS., Wichers, D., Davisnw., Petefish, P., Weidman, A., Brooks, M., Mir, A., Dc., D0ubl3 h3lix, Manico, J., Gilbert, R., Tgondrom., Krawczyk, P., Brandt, Minhaz, A. V., Lorenzo, K., Smith, A., Schelin, C., Elias-Bachrach, A., Sarciszewski., kingthorin & Spatafora, B. (2021). *Cross site request forgery (CSRF)).* OWASP. **https://owasp.org/www-community/attacks/csrf**. licensed under Creative Commons Attribution – ShareAlike 4.0.
5. mgeeky. (n.d.). *XML vulnerabilities and attacks cheatsheet*. GitHub Gist. **https://gist.github.com/mgeeky/4f726d3b374f0a34267d4f19c9004870**
6. Nidecki, T. A. (2021, September9). *Web security basics: Is your web application safe?* Acunetix. **https://www.acunetix.com/blog/web-security-zone/web-security-basics/**
7. *XML external entity (XXE) injection*. (n.d.). PortSwigger. **https://portswigger.net/web-security/xxe**

Video Resources

1. AppSecAcademy. (2019, February 21). *#1 XML external entity (XXE) in 2 minutes | AppSec academy* [Video]. YouTube. **https://www.youtube.com/watch?v=_gfhgWvI6XI**
2. edureka! (2019, December 10). *What is cross site scripting?| cross site scripting attack | cross site scripting tutorial | edureka* [Video]. YouTube. **https://www.youtube.com/watch?v=cWu_FJUrH5Y**
3. edureka! (2020, July 13). *Top web applications vulnerabilities | web application vulnerabilities for beginners | edureka* [Video]. YouTube. **https://www.youtube.com/watch?v=loyVGklGpjU&t=2s**
4. Eye on Tech. (2021, September 23). *What is a buffer overflow attack?* [Video]. YouTube. **https://www.youtube.com/watch?v=YNkjX2Wqgh0**
5. F5DevCentral. (2018, January 18). *OWASP top 10: XML external entities* [Video]. YouTube. **https://www.youtube.com/watch?v=g2ey7ry8_CQ**
6. Fullstack Academy. (2017, September 29). *CSRF tutorial - a guide to better understand and defend against cross-site request forgery (CSRF)* [Video]. YouTube. **https://www.youtube.com/watch?v=13QPmRuhbhU**
7. Secure Code Warrior. (2017, August 25). *Cross-site scripting (xss) | owasp top 10 explainer video | secure code warrior* [Video]. YouTube. **https://www.youtube.com/watch?v=H22cJTqCgUA**
8. Udacity. (2016, June 6). *XSRF cross site request forgery* [Video]. YouTube. **https://www.youtube.com/watch?v=9JrzPX1pVjs**
9. w3w3w3. (2020, January 29). *Buffer overflow attack tutorial - 0x00* [Video]. YouTube. **https://www.youtube.com/watch?v=j7AEzGKuKUU**

Discussion Assignment

Year over year, several cyberattacks on web applications are on the rise. Conduct an online search to find the latest data (within 12 years of the current date) on XSS (XXE) and Man-in-the-Middle attacks, and:

- Review the data.
- Prepare your interpretation.
- Derive the conclusion of your interpretation. Support the case with external research references.

Your Discussion should be a minimum of 200 words in length and not more than 500 words. Please include a word count. Following the APA standard, use references and in-text citations for the textbook and any other sources.

Written Assignment

Submit a paper that is 2-3 pages in length exclusive of the reference page, double-spaced using 12-point Times New Roman font. The paper must cite at least two (2) outside sources in APA format and be well-written. Check all content for grammar, spelling and be sure that you have correctly cited all resources (in APA format) used. Refer to the UoPeople APA Tutorials in the LRC for help with APA citations.

Conduct online research to explore Buffer Overflow attacks and Vulnerabilities. Write an essay discussing and analyzing Buffer Overflow issues in the present day scenario. Consider the below points/questions while working on the essay.

- Are buffer overflow attacks a serious threat to applications these days? Why and why not?
- Support your discussion and analysis using a minimum of two examples and research data. Statistical data should not be older than 12 months.
- Use your own words in developing your point of view and making a conclusion.
- Reinforce your arguments with appropriate quotes in the text and research references.
- Must use the APA style for a reference list and quotations in the text.

Written Assignment Peer Assessment

In the unit following the submission of your written assignment, you will peer assess three (3) of your classmates' assignments according to the instructions found in the Assessment Form. During this peer assessment period, you are expected to provide details in the feedback section of the Assessment Form, indicating why you awarded the grade that you did to your peer. The written assignment grade is comprised of a combination of your submission (90%) and your peer assessments (10%).

Written Assignment Peer Assessment Rubric

Learning Journal

The Learning Journal is a tool for self-reflection on the learning process. In addition to completing directed tasks, you should use the Learning Journal to document your activities, record problems you may have encountered, and draft answers for Discussion Forums and Assignments. The Learning Journal should be updated regularly (weekly), as your instructor will assess the learning journals as part of your Final Grade.

In this unit, we have learned about different types of cyber threats and how they can be mitigated or prevented from damaging your computer networks and data. To reflect your learning, please respond to each of the following questions:

- Describe the most interesting facts you learned about cyber threats and their mitigation in this unit. Think about reasons why you noticed these facts, your impression, your plans for further exploration of “cyber threats and their mitigation”.
- Describe how you exercise safe web browsing and the use of web applications for your personal needs. What is it that inspires you?
- List the additional facts about cyber threats and their mitigation you would like to explore based on this unit’s concepts.

The Learning Journal entry should be a minimum of 500 words and not more than 750 words. Use APA citations and references if you use ideas from the readings or other sources

Refer Learning Journal Rubrics

Self-Quiz

The Self-Quiz gives you an opportunity to self-assess your knowledge of what you have learned so far.

The results of the Self-Quiz do not count towards your final grade. However,the quiz is an important part of the University's learning process and it is expected that you will take it to ensure understanding of the materials presented. Reviewing and analyzing your results will help you perform better on future Graded Quizzes and the Final Exam.

Please access the Self-Quiz on the main course homepage; it is listed inside the Unit.

Checklist

- Peer assess Unit 4 Written Assignment
- Read the Learning Guide and Reading Assignments
- Participate in the Discussion Assignment (post, comment, and rate in the Discussion Forum)
- Complete and submit the Written Assignment
- Make entries to the Learning Journal
- Take the Self-Quiz