Learning Guide Unit 6

Site: University of the People
Course: CS 3340-01 Systems and Application Security - AY2025-T1
Book: Learning Guide Unit 6

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

Description

Learning Guide Unit 6

Table of contents

Overview

UNIT 6: Web Applications Vulnerabilities and Countermeasures-Part 2

Topics

- User Enumeration
- Cookies and Session Hijacking
- Prefetching and Spiders
- PHP-special issues
- Truncation and trimming attacks, and SQL injection

Learning Objectives

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

1. Discuss web application security risks.
2. Discuss user enumeration.
3. Explain the mechanism of truncation and trimming attacks in the context of SQL injection.

Tasks

- Peer assess Unit 5 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
- Take the Graded Quiz

Introduction

Users have always been considered at high risk with computer systems and networks. A cybersecurity expert (Ryerse, 2020) from ConnectWise software company that provides organizations with secure solutions for remote access operations, points out that - “Clients think that once they’ve hired a technology solution provider (TSP) to manage their security, they’re completely protected and no longer at risk. However, the biggest risk to an organization’s information security is the inaction of employees”.

Furthermore, according to an article presenting cybersecurity statistical analysis conducted in the UK and presented by (Kelly, 2017), “90% of all cyber claims stemmed from some type of human error or behavior”.

Another category of cybersecurity exploits is related to bad programming practices; for which we can blame a human again! Human programmers neglect best practices, miss security details, and being under the pressure to deliver applications as soon as possible, they do the “shortcuts”.

In this unit, we will discuss various issues related to user interaction with web applications and websites. We will keep our primary focus on user enumeration, truncation and trimming attacks, prefetching, spiders attacks, PHP-special issues, and SQL injection.

References:

Ryerse, J. (2020, September 7). *The basics of cybersecurity training for end users*. ConnectWise. https://www.connectwise.com/blog/cybersecurity/the-basics-of-cybersecurity-training-for-end-users

Kelly, R. (2017, March 3). *Almost 90% of cyber-attacks are caused by human error or behavior.* ChiefExecutive. https://chiefexecutive.net/almost-90-cyber-attacks-caused-human-error-behavior/

User Enumeration

Enumeration is used to gather the following: Usernames, group names; Hostnames; Network shares and services; IP tables and routing tables; Service settings and audit configurations; Application and banners; and SNMP and DNS details.

Thus, user enumeration is related to gathering information about users, user access credentials, user groups, and network shares and services associated with users. When users interact with web applications (i.e. using username and password to access website) cybercriminals might be able to collect user-specific sensitive data and use it to gain access to protected websites and applications. The most frequent information targets are users' internet cookies and session IDs. In simple words, enumeration is a listing of all things. Thus, cybercriminals are interested in extracting and verifying the existence of usernames, passwords, and other web applications' access confidential data.

Reading Assignments:

Read What Is User Enumeration?

Watch User enumeration Vulnerability

Resources:

Chakravartula, R. (2021, January 22). *What is enumeration? [updated 2021]*. Infosec. https://resources.infosecinstitute.com/topic/what-is-enumeration/

Lara, H. (2018, March 10). *User enumeration vulnerability* [Video]. YouTube. https://www.youtube.com/watch?v=IahnJVOhak4

Hacksplaining. (2018, September 30). *What is user* enumeration? [Video]. YouTube. https://www.youtube.com/watch?v=fP0VVzPI4jQ

Laverty, P. (2017, June 15). *What Is user enumeration?* RAPID1. https://www.rapid7.com/blog/post/2017/06/15/about-user-enumeration/

Cookies and Session Hijacking

This topic will discuss the vulnerabilities of web cookies and sessions. Practically all websites use cookies. Cookies have many good purposes such as tracking browsers, holding user customization for a web application, storing information on every web session. On the other hand, Web session refers to time spent on a website. Cookies are essential for some websites to function properly. In general, cookies are specific to every website you visit, not executable, not a security risk by itself. It is a way the browser stores information on a user's computer and allows the user to access a website faster without providing full login credentials.

The term "hijacking" is just another example of a "man-in-the-middle" attack attempting to gain full access to a user's online account. Session hijacking is executed when an attacker obtains a session ID. Criminals use network analyzers and other tools to collect network information to catch user IDs and session IDs.

Reading Assignments:

Read The Ultimate Guide to Session Hijacking aka Cookie Hijacking

Watch Cookie Stealing - Computerphile

Resources:

Computerphile. (2016, June 1). *Cookie stealing – computerphile* [Video]. YouTube. https://www.youtube.com/watch?v=T1QEs3mdJoc

Mr Code. (2021, January 10). *What is session hijacking a short introduction* [Video]. YouTube. https://www.youtube.com/watch?v=rqDuDSPhiCs&list=PL6jT6oPokSnIhwaEwRATkmLkVl_TX9xgF

Vojtko, M. (2020, November 16). *The ultimate guide to session hijacking aka cookie hijacking*. hashedout. https://www.thesslstore.com/blog/the-ultimate-guide-to-session-hijacking-aka-cookie-hijacking/

Prefetching and Spiders

The online dictionary Technopedia (2021) defines “Prefetching is the loading of a resource before it is required to decrease the time waiting for that resource.” Prefetching is used to speed up web resource loading, i.e. web-form filling. Whenever a user interacts with a web browser, the information is stored in temporal files which can be preloaded. Fetch directives tell the browser the locations to trust and where to load the resources from. This information could be harvested by “spiders”, also referred to as “web crawlers”, “spider bots”, just as “crawlers”. Cybercriminals use spiders to harvest information that allows them to access restricted resources and valuable information, steal scientific, commercial, military, and other secrets. The combination of prefetching and spiders represent serious cybersecurity risks.

Reading Assignments:

Read Spiderbot, Spiderbot, Does Whatever A Hacker Thought

Watch

- Intro To Web Crawlers & Scraping With Scrapy

References:

Oxylabs. (2019, October 10*). Web crawling vs. web scraping | oxylabs* [Video]. YouTube. https://www.youtube.com/watch?v=cwZF87qlF7c

Grobman, S. (2015, August 8). *Spiderbot, spiderbot, does whatever a hacker thought*. DARKReading, Informa PLC. https://www.darkreading.com/partner-perspectives/intel/spiderbot-spiderbot-does-whatever-a-hacker-thought/a/d-id/1321850

Traversy Media. (2020, January 14). *Intro to web crawlers & scraping with scrapy* [Video]. YouTube. https://www.youtube.com/watch?v=ALizgnSFTwQ

Prefetching. (2020, June 30). Techopedia. https://www.techopedia.com/definition/32421/prefetching

PHP-special issues

According to OWASP PHP (2021) data, “There are 1.8 billion websites on the internet today. Nearly 80% are powered by the PHP programming language.” Considering the scale of application, it is crucial to consider the implementation of IT and Data security measures to secure data and operations delivered and exchanged via the Internet. PHP is an open-source server-side programming language that requires a web server to process its instructions. PHP is used a lot for legitimate business. Unfortunately, it can also be used by cybercriminals to access web databases (primarily MySQL) and steal sensitive data.

Let us watch a video demonstrating how PHP injection works.

Reading Assignments:

Read

- The 2018 Guide to Building Secure PHP Software
- Web Application Security Guide/Print version (PHP- specific issues)

Watch PHP Code Injection | Step By Step Guide | Bug Bounty

Resources:

BUG XS. (2020, April 12). *PHP code injection | step by step guide | bug bounty* [Video]. YouTube. https://www.youtube.com/watch?v=UIROTF-OspY

HackerSploit. (2019, May 13). *Bug bounty hunting - PHP code injection* [Video]. YouTube. https://www.youtube.com/watch?v=GE2HyC7Gwrs

The 2018 guide to building secure PHP software. (2017, December 12). *Paragon initiative enterprises blog*. https://paragonie.com/blog/2017/12/2018-guide-building-secure-php-software

OWASP. (n.d.). *Anatomy of a webshell - d0n quix0te* [Video]. YouTube. https://www.youtube.com/watch?v=tVKucIWH0w0

OWASP Php. (n.d.). *What does PHP security mean?* https://owasp.org/www-project-php/migrated_content

Web application security guide/PHP-specific issues. (n.d.). Wikibooks. Retrieved June 15, 2021 from https://en.wikibooks.org/wiki/Web_Application_Security_Guide/PHP-specific_issues

Truncation and trimming attacks, and SQL injection

Another widely spread attack is SQL injection. First SQL injection attacks were recorded in the late 90s. The most common targets of SQL injections are websites using PHP and MySQL, though the attacks can be executed on SQL database servers as well. The attack is executed by injecting an SQL query to note, SQL, MySQL, Oracle have the same SQL standard core, also known as ANSI SQL first adopted in 1986. The database server runs a database engine to process any queries containing Insert/Update/Delete.

In SQL injection attacks "SQL commands are injected into data-plane input to affect the execution of predefined SQL commands" (Kingstoring, 2021). The main reasons these attacks are possible are lack of user input validation/sanitizing, scanning of web applications and web servers, database server misconfiguration, and overall lack of up-to-date protective mechanisms.

Let us watch a short video explaining and demonstrating the basics of SQL injection.

Reading Assignments:

Read What is SQL Injection (SQLi) and How to Prevent It

Watch What is SQL Injection? | SQL Injection Tutorial | Cybersecurity Training | Edureka

Resources:

edureka! (2019, October 3). *What is sql injection? | sql injection tutorial | cybersecurity training | edureka* [Video]. YouTube. https://www.youtube.com/watch?v=3Axp3VDnf0I

Henry, D. (2020, June 16). *SQL injection attack explained [2020] with SQL injection examples* [Video]. YouTube. https://www.youtube.com/watch?v=VZfTmu7tn34

Kingthorin. (n.d.) SQL Injection. *OWASP*. Retrieved January 10 2022 from https://owasp.org/www-community/attacks/SQL_Injection

What is SQL injection (SQLi) and how to prevent it. (n.d.). Acunetix by invicti. https://www.acunetix.com/websitesecurity/sql-injection/

Reading Assignment

1. Chakravartula, R. (2021, January 22). *What is enumeration? [updated 2021]*. Infosec. **https://resources.infosecinstitute.com/topic/what-is-enumeration/**
2. Grobman, S. (2015, August 8). *Spiderbot, spiderbot, does whatever a hacker thought*. DARKReading, Informa PLC. **https://www.darkreading.com/partner-perspectives/intel/spiderbot-spiderbot-does-whatever-a-hacker-thought/a/d-id/1321850**
3. Kelly, R. (2017, March 3). *Almost 90% of cyber-attacks are caused by human error or behavior*. ChiefExecutive. https://chiefexecutive.net/almost-90-cyber-attacks-caused-human-error-behavior/
4. Kingthorin. (n.d.) SQL Injection. *OWASP*. Retrieved January 10 2022 from **https://owasp.org/www-community/attacks/SQL_Injection**
5. Laverty, P. (2017, June 15). *What Is user enumeration?* RAPID1. **https://www.rapid7.com/blog/post/2017/06/15/about-user-enumeration/**
6. OWASP Php. (n.d.). *What does PHP security mean?* **https://owasp.org/www-project-php/migrated_content**
7. *Prefetching*. (2020, June 30). Techopedia. **https://www.techopedia.com/definition/32421/prefetching**
8. Ryerse, J. (2020, September 7). *The basics of cybersecurity training for end users*. ConnectWise. **https://www.connectwise.com/blog/cybersecurity/the-basics-of-cybersecurity-training-for-end-users**
9. The 2018 guide to building secure PHP software. (2017, December 12). *Paragon initiative enterprises blog*. **https://paragonie.com/blog/2017/12/2018-guide-building-secure-php-software**
10. Vojtko, M. (2020, November 16). *The ultimate guide to session hijacking aka cookie hijacking*. hashedout. **https://www.thesslstore.com/blog/the-ultimate-guide-to-session-hijacking-aka-cookie-hijacking/**
11. *Web application security guide/PHP-specific issues*. (n.d.). Wikibooks. Retrieved June 15, 2021 from **https://en.wikibooks.org/wiki/Web_Application_Security_Guide/PHP-specific_issues**
12. *What is SQL injection (SQLi) and how to prevent it*. (n.d.). Acunetix by invicti. **https://www.acunetix.com/websitesecurity/sql-injection/**

Video Resources

1. BUG XS. (2020, April 12). *PHP code injection | step by step guide | bug bounty* [Video]. YouTube. **https://www.youtube.com/watch?v=UIROTF-OspY**
2. Computerphile. (2016, June 1). *Cookie stealing – computerphile* [Video]. YouTube. **https://www.youtube.com/watch?v=T1QEs3mdJoc**
3. edureka! (2019, October 3). *What is sql injection? | sql injection tutorial | cybersecurity training | edureka* [Video]. YouTube. **https://www.youtube.com/watch?v=3Axp3VDnf0I**
4. HackerSploit. (2019, May 13). *Bug bounty hunting - PHP code injection* [Video]. YouTube. **https://www.youtube.com/watch?v=GE2HyC7Gwrs**
5. Hacksplaining. (2018, September 30). *What is user* enumeration? [Video]. YouTube. **https://www.youtube.com/watch?v=fP0VVzPI4jQ**
6. Henry, D. (2020, June 16). *SQL injection attack explained [2020] with SQL injection examples* [Video]. YouTube. **https://www.youtube.com/watch?v=VZfTmu7tn34**
7. Lara, H. (2018, March 10). *User enumeration vulnerability* [Video]. YouTube. **https://www.youtube.com/watch?v=IahnJVOhak4**
8. Mr Code. (2021, January 10). *What is session hijacking a short introduction* [Video]. YouTube. **https://www.youtube.com/watch?v=rqDuDSPhiCs&list=PL6jT6oPokSnIhwaEwRATkmLkVl_TX9xgF**
9. OWASP. (n.d.). *Anatomy of a webshell - d0n quix0te* [Video]. YouTube. **https://www.youtube.com/watch?v=tVKucIWH0w0**
10. Oxylabs. (2019, October 10*). Web crawling vs. web scraping | oxylabs* [Video]. YouTube. **https://www.youtube.com/watch?v=cwZF87qIF7c**
11. Traversy Media. (2020, January 14). *Intro to web crawlers & scraping with scrapy* [Video]. YouTube. **https://www.youtube.com/watch?v=ALizgnSFTwQ**

Discussion Assignment

For this discussion assignment, review Top 10 Web Application Security Risks

Select One of the following topics listed on the page:

- Injections (focus on SQL injection)
- Identification and Authentication Failures
- Broken Access Control
- Software and Data Integrity Failures

For your post, answer the following:

- Explain vulnerabilities that allow the attack (as per your selection)
- Discuss the purpose of the attack (as per your selection).
- Explain countermeasures to mitigate and/or prevent the attack (as per your selection).
- Give an example of the attack recorded within the last 12 months to the current date. Who was the victim? What damage was inflicted? What lessons were learned?

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.

Reference:

Top 10 web application security risks. (n.d.). OWASP Foundation, Inc. https://owasp.org/www-project-top-ten/. Creative Commons Attribution-ShareAlike v4.0

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.

There is an established opinion that users are the weakest part of cybersecurity defense. For this assignment conduct research and discuss what organizations can and should do to enforce cybersecurity compliance by users of organizational computer systems.

In a separate paragraph discuss user enumeration. Is this a common exploit? Why or why not. Support your argument with appropriate research.

1. Write a paragraph with not less than 100 words discussing what organizations can and should do to enforce cybersecurity compliance by their users. Support your arguments with appropriate research.
2. In a separate paragraph (minimum of 100 words) discuss the impact and scale of user enumeration exploits. Is this a common exploit? Why or why not. Support your argument with appropriate research.

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%).

Refer 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.

Based on what you have learned in the topic “Truncation and trimming attacks, and SQL injection” of this unit, answer the following questions:

1. Describe what was the most interesting fact you learned about in this unit. Think about the reasons why you noticed this topic, your impression, your plans for further exploration of this topic.

2. When you were working on this task of the unit, you were doing your internet research on the topics discussed. Did you find something related to issues discussed that surprised you?

- List your findings.
- Give rationale to support your answer.

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.

Graded Quiz

The Graded Quiz will test your knowledge of all the materials learned thus far. The results of the quiz will count towards your final grade.

Please access the Graded Quiz on the main course homepage; it will be listed inside the Unit. After you click on it, the quiz's introduction will inform you of any time or attempt limits in place.

Good luck!

Checklist

- Peer assess Unit 5 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
- Take the Graded Quiz