Project Proposal

Hack the Box Challenge: Signing Factory

Instructor
Dr. Ali Zarafshani

CSCE 5552
Cybersecurity Essentials

Group 1

Group Members: Arkaan Sheikh
Clint Martinez
Monica Thomas
Victor Morales

University of North Texas

Department of Computer Science and Engineering

Date: September 2024

Table of Contents

Proposal Hack the Box Challenge: Signing Factory

First Option

Hack the Box selection name: Signing Factory

Category: Crypto

Difficulty rating: Medium

Description: A group of researchers has developed a new modern method for signing tokens used for authentication, and they are getting ready for an ultimate security audit before their product is released. We were assigned to perform the security evaluation of their signing mechanism and server. The challenge focuses on the assessment of the new method of signing messages against past known attacks on similar systems (Hack the Box, 2024).

Second Option

Hack the Box selection name: RedTrails

Category: Forensics

Difficulty rating: Medium

Project Scope for First Option

The goal of this project is to identify, analyze and exploit any vulnerabilities in the signing mechanisms used for tokens on the assigned server. We will start gathering information to identify vulnerabilities, accessible services, endpoints and exposed APIs. The information obtained may show us the internal architecture or specific implementations related to the signing process. After the analysis we will have a clearer understanding of the signing process, which includes the analysis of the algorithms, cryptographic methods, and protocols and identify potential weaknesses.

Plan for Resolving the Challenge

We will start gathering information about the assigned server and the signing mechanism by using tools such as Nmap, Gobuster, etc. to identify open ports, services, endpoints and vulnerable APIs. Also, we will focus identifying debugging information that may show details about the operation of the signing mechanism.

We will then perform a cryptographic analysis on the signing endpoints, obtaining tokens to understand their structure and the signing algorithm used. We will utilize advanced tools such as Wireshark to intercept and analyze the traffic, performing an extensive inspection of the tokens to verify secure hashing tokens and critical lengths to identify unusual patterns in the token format that could be exploitable. In addition, we will perform a vulnerability assessment, testing the server for vulnerabilities related to padding oracle attacks, which is a cryptographic attack targeting block cipher algorithms that decrypts encrypted data provided by a client. This attack allows data encryption without knowledge of the key usage for cryptographic operations. Moreover, we will perform a timing analysis to identify vulnerabilities that could arise from differences in response times between valid and invalid tokens and identify common vulnerabilities that could lead to security breaches.

References

KirstenS. (2023, Cross site request forgery (CSRF). https://owasp.org/www-community/attacks/csrf. https://owasp.org

https://owasp.org/www-project-web-security-testing-guide/latest/4-Web_Application_Security_Testing/09-Testing_for_Weak_Cryptography/02-Testing_for_Padding_Oracle

I