Thesis Project Portfolio

Dynamic Application Security Testing - Fuzzing: Brute-Force API Vulnerability Scanning

(Technical Report)

Understanding Phishing as a Social Engineering Problem: Why Societal Educational Efforts Falls Short

(STS Research Paper)

An Undergraduate Thesis

Presented to the Faculty of the School of Engineering and Applied Science
University of Virginia • Charlottesville, Virginia

In Fulfillment of the Requirements for the Degree
Bachelor of Science, School of Engineering

Justin Gou
Spring, 2022
Department of Computer Science

Table of Contents

Sociotechnical Synthesis

With the world becoming more and more reliant on technology, cybersecurity continues to be a growing issue in the world of technology. Attackers are constantly looking for ways to break into systems for monetary reward or to compromise private data. One goal for cybersecurity researchers is to find the best ways to minimize these vulnerabilities. This portfolio focuses on two specific techniques to decrease cybersecurity vulnerabilities. The technical research topic focuses on adding automated web application fuzzing to an existing Application Programming Interface (API). The main focus of this project is to discover vulnerabilities automatically before an attacker is able to take advantage of the weakness. The sociotechnical topic focuses on reducing phishing attacks – a social engineering attack mostly targeted towards individuals with weak understandings of computer systems. With computer system security becoming increasingly difficult to break, attackers often will search for other "vulnerabilities", such as targeting people who already have special access to the systems. Both projects ultimately create ways to reduce various relevant cybersecurity attacks.

One way attackers will target systems is simply by looking at what is publicly accessible and seeing if any vulnerabilities exist within that domain. This research focuses specifically on the architecture of Robinhood Markets, Inc., where the research was performed. Robinhood exposes a large number of API endpoints to the public that are not regularly scanned for potential web vulnerabilities. Large amounts of public API endpoints create a large attack surface for malicious attackers to target. Without regular vulnerability scanning of these publicly accessible endpoints, any vulnerability could pose a large risk on the Robinhood infrastructure. To address this problem, a solution was proposed to build a fuzzing feature, a method of brute-force dynamic analysis, to automatically test all API endpoints using a Dynamic Application Security Testing (DAST) system. Through this research, Robinhood's DAST system was enhanced with

various web vulnerability scanning capabilities, including scanning for HTTP smuggling, server-side request forgery, authentication bypass, etc. With deployment, DAST will be integrated with the company's internal communication system to automatically report findings to the involved parties. At the current state, the DAST system is able to perform automated testing for common web vulnerabilities across over 100 API endpoints, significantly reducing risk and potential for an external breach.

On the other hand, the sociotechnical research paper focuses on social engineering, a completely different approach on cybersecurity, targeting the humans involved rather than the computer systems. Specifically, the research focuses on phishing, where attackers will send malicious emails intended to trick the user into willingly surrendering their information or entire system. Society has been working to prevent these kinds of attacks through proper training of employees, as if all employees can correctly identify a phishing email, no one would fall victim to these scams. Unfortunately, despite these efforts, companies continue to lose millions of dollars each year to simple phishing attacks. To address this, the research question is as follows: how does the average American understand phishing as a social engineering problem? In an effort to understand why phishing continues to be successful, the problem could be framed as a wicked problem. The problem becomes increasingly difficult as technology develops, so no solution has been able to fully resolve the problem. Current solutions attempt to minimize the problem, but have not proven to be incredibly successful. Through this research, the goal is to understand why anti-phishing efforts fail and to search for potential solutions that may make employee training or anti-phishing software more effective. The goal of this research is to reduce the number of successful phishing attacks in society, which may include developments in the field of social engineering.

These studies helped foster a stronger understanding in web application vulnerabilities and social engineering vulnerabilities, both of which are crucial in the modern field of cybersecurity. These research papers presented interesting insights as to how two seemingly completely different topics ultimately work to resolve the same goal. The technical paper focused on finding a technical solution to potential vulnerabilities in web applications. On the other hand, the STS research paper focused on understanding social engineering and finding the best way to address phishing attacks. Both research papers ended up resulting in finding successful ways to reduce vulnerabilities in the cybersecurity field.