POLYTECHNIC UNIVERSITY
SAN JUAN • ORLANDO • MIAMI

Vulnerability Assessment of Puerto Rico's Health Department Webserver

Author: Alondra Marrero Cabrera
Advisor: Jeffrey Duffany
Computer Science Department

Abstract

As technology progresses in the cyber environment, so do new threats; now, with the (COVID-19), pandemic biosafety and biosecurity concerns are even more rigorously scrutinized. The cyber- and biological sciences are uniting quickly, making benefits, new and favorable applications, and expanding dangers to all countries. Cyber biosecurity is a generally new field that aims to identify and mitigate these security risks fostered by digitizing biology and biotechnology automation. There has been an expanding number of high-profile online protection breaks lately that have raised public attention to possible social, political, and monetary outcomes that assaults to biological databases can bring about. This project will be focusing on the exploration of vulnerabilities regarding to the covid-19 data website for Puerto Rico's Health Department utilizing the tool burp suite as well as suggest proactive measures to avoid the stealing of information or any cyber-attacks.

Introduction

The covid-19 pandemic has also been the protagonist to many cyberattacks specially targeted towards covid-19 databases. This introduces the field of biology to the world of cyber threat space. Much more work needs to be done to better comprehend the emerging risk landscape and to establish adequate protective measures. Cyber overlaps and cyberphysical systems turn the bioscience field into a platform for high-impact adverse consequences Prior to the pandemic, about 20% of cyberattacks used previously unseen malware or methods. During the pandemic, the proportion has risen to 35%.

Background

As cyber threat space continues to evolve, we must take action to prevent serious consequences to valuable data. This involved the merging of distinct disciplines to create a new field called cyber bio security which is the main theme of covid 19 related cyber-attacks. Puerto Rico reported over 187 cyber-attack attempts. In the state of Maryland an ongoing cyber attack compromised its health departments data as well as network systems, affecting all employees and patients. This resulted in the state paralyzing the covid 19 data uploads in fear of any other data compromises.

Problem

Puerto Rico's government sites have been victims of ongoing cyberattacks since the beginning of the covid 19 pandemic. Mots of these have been classified as ransomware attacks such as the attack on *Departamento de Hacienda* which compromised the web server infrastructure and resulted in the loss of over 25 million dollars according to El nuevo dia. This is likely to become a threat unless immediate action is taken

Methodology

To conduct the project, a penetration testing analysis of vulnerabilities using the Burp suite community tool was utilized through a virtual machine using OWASP standards. One of Burp Suite's main features is its ability to intercept HTTP requests. It does this by using a proxy either a built-in browser or a maxilla Firefox add on. Usually, HTTP requests go from a browser straight to a web server and then the web server response is sent back to the browser. However, With Burp Suite, however, HTTP requests go from your browser straight to Burp Suite, which intercepts the traffic. In Burp Suite you can then tweak the raw HTTP in various ways before forwarding the request on to the web server. Essentially this tool is acting as a proxy, a "man in the middle," between you and the web application, allowing you to have finer control over the exact traffic you are sending and receiving. Our goal with the Burp intercepting proxy feature is to tweak requests so they still follow the rules of HTTP but can make the application act unexpectedly. For this project we will using the community version of burp suite through OWASP BWA VM. This allows us to intercept network traffic through a proxy manually instead of using the built-in browser for burp suite. This program can be used to identify many flaws in a webserver infrastructure as well as simulate cyber-attacks. As the testing is over list of vulnerabilities along with its classification in OWASP Top 10 will be discussed.

Results and Discussion

After conducting testing through burp suite, the tool indicates flags along with levels of risk. The overall risk level for the website is medium, however, Puerto Rico's government has been attacked before on different departments such as Hacienda which was a victim of a ransomware attack back in 2017. In Table 1 identified vulnerabilities with their corresponding classifications can be observed.

Risk	OWASP Classification Top 10	CWE Classification
Strict transfer security	A5, A6 security Misconfiguration	693
X-XSS Protection	A5, A6 Security misconfiguration	693
Insecure Cookie Setting	A5, A6 Security Misconfiguration	693
SSL-TLS certificate is NOT trusted	A5, A6 Security Misconfiguration	693
Missing security header Strict Transfer Security	A5, A6 Security Misconfiguration	693

Table 1. Identified Risks in website & OWASP's Classification

Results and Discussion

As it is observable through table 1 many "small" security measures are missing indicating an unstable cybersecurity infrastructure. Let's begin by discussing the issues with cookies found. Our first flag is Insecure cookie setting as it is missing *HttpOnly* flag. This indicates that which means that it can be accessed by the JavaScript code running inside the web page. If an attacker manages to inject malicious JavaScript code on the page such as an XSS attack, then the cookie will be accessible, and it can be transmitted to another site. In case of a session cookie, this could lead to session hijacking. Since the Secure flag is not set on the cookie, the browser will send it over an unencrypted channel (plain HTTP) if such a request is made. Thus, the risk exists that an attacker will intercept the clear-text communication between the browser and the server, and he will steal the cookie of the user. If this is a session cookie, the attacker could gain unauthorized access to the victim's web session. There were 3 medium risk level vulnerabilities found on the software side for the server. These vulnerabilities expose the affected applications to the risk of unauthorized access to confidential data and possibly to denial-of-service attacks. An attacker could search for an appropriate exploit or create one themselves for any of these vulnerabilities and use it to attack the system. They are displayed on Table 2.

CVSS	CVE	Affected Software
4.3	CVE-2019-11358	jquery
4.3	CVE-2020-11022	jquery
4.3	CVE-2020-11023	jquery

Table 2. Identified Risks in Software

For CVE-2019-11358 jQuery before 3.4.0, as used in CMS, mishandles commands such as the *jQuery.extend* because of *Object.prototype* pollution. If an "unsanitized" source object contained an enumerable __proto__ property, it could extend the native *Object.prototype*. This extends in CVE-2020-11022 as In jQuery versions greater than or equal to 1.2 and before 3.5.0, passing HTML from untrusted sources - even after sanitizing it – to one of jQuery's DOM manipulation methods (i.e. .html (),.append(), and others) may execute untrusted code. This issue is patched in jQuery 3.5.0. However, the website itself is using out of date software generating these risks. This makes the website vulnerable to many types of attacks such as clickjacking, data leak, unauthorized access, expired certificate breakthrough etc.

Conclusions and Future Work

Though the overall risk isn't high enough to cause major concern the analysis showed that there is no active website monitoring network traffic. This is not good cybersecurity practice as in case of an attack no one would be able to prevent major damage or be informed of what is happening. The site is propense to various types of attacks such as SQL Injection and brute force entry. As for each problem detailed above it is in good practice to update software and pay attention to cybersecurity standards such as NIST framework and OWASP recommendations. Preemptively detecting security flaws and establishing processes to detect attacks before they occur are all part of a proactive cybersecurity strategy.

This project is just the beginning of pen testing tools to be utilized on a health departments website. This may be further studied using other tools in combination with burp suite to obtain a more detailed vulnerability report including in depth scans. It may also be expanded to other government websites and establish a cybersecurity infrastructure in all areas of Puerto Rico's government that complies with the cybersecurity CIA triad. We may also develop a study of key aspects and vulnerabilities found the integrity of the data as well recollected not just for covid-19 cases and/or vaccines but hospital records as well.

Acknowledgements

I would like to acknowledge Dr Duffany for being my mentor and guide through this project and giving me advice on both this project and my career I would also like to thank Dr.Alfredo Cruz and Elena Guerra for their continuous support through the Cybercorps Program.

References

[1] Henry Dalziel, in How to Hack and Defend your Website in Three Hours, 2015
[2] Thomas Wilhelm, in Professional Penetration Testing (Second Edition), 2013
[3] J. Ayala, "Anatomia de un Ciberataque," El Nuevo Dia, 21-Jun-2021.
[4] K. C. S. F. B. J. T. M. DK; "Cybersecurity in Healthcare: A systematic review of modern threats and Trends," Technology and health care : official journal of the European Society for Engineering and Medicine, 2017. [Online]. Available:https://pubmed.ncbi.nlm.nih.gov/27689562/. [Accessed: 2021].
[5]S. Thompson, O. Wiggins, and E. Cox, "Maryland health workers, lawmakers want answers as problems persist a month after cyberattack," The Washington Post, 08-Jan-2022. [Online]. Available: https://www.washingtonpost.com/dc-md-va/2022/01/08/cyberattack-still-disrupting-maryland-department-of-health/. [Accessed: 20-Jan-2022].