Vulnerability Assesment of Puerto Rico's Health Department Web Application

Alondra Marrero Cabrera
Jeffrey Duffany, Ph.D.
Master in Computer Science
Polytechnic University of Puerto Rico

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.*

Key Terms — *Biosecurity, Burp suite, Covid-19, Risk, Vulnerability, Web security.*

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%. Some of the new attacks use a form of machine learning that adapts to its environment and remains undetected. As an example, phishing attacks are becoming more sophisticated and using different channels such as SMS and voice (vishing). Moreover, news about vaccine developments is used for phishing campaigns. Ransomware attacks are also becoming more sophisticated. For example, hackers are combining data leakage attacks with ransomware to persuade victims to pay the ransom.

Cyberbiosecurity threats are becoming increasingly important as technological progress continues to accelerate in fields such as artificial intelligence, automation, and synthetic biology. Moreover, not only is the pace of progress in these fields accelerating, but they are also becoming increasingly integrated, leading to a growing overlap that is generating new security vulnerabilities. Many of the potential risks from future progress in bioengineering that were identified by researchers fall within the bounds of cyberbiosecurity, for instance, the use of cyberattacks to exploit bio-automation for malicious purposes.

Cyberthreat Landscape

As the pandemic evolves the cyberthreat landscape emerges at an alarming rate. continuity in terms of the types of attacks, threats actors, and the volume of attacks. Adversarial behavior has, however, changed and evolved in terms of scale, sophistication, targets, and motivation. Among disruptive malware, the most prevalent form found in the wild was ransomware, with ransomware as-a-service increasingly becoming an established criminal enterprise. Indeed, a report by the cybersecurity company *Coveware n*otes that ransom demands in the first quarter of this year increased by 33 per cent compared to the last months of 2019 (2020). "Operationally, these come later in the attack chain and usually infect the victim's system via email attachments, links, or through compromised credentials obtained with coronavirus lures or other techniques, such as RDP brute force attacks" [1].

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 [2]. This resulted in the state paralyzing the Covid-19 data uploads in fear of any other data compromises. The Coronavirus Disease 2019 (Covid-19) pandemic has resulted in widespread disruption to the healthcare industry. Alongside complex issues relating to ensuring sufficient healthcare capacity and resourcing, healthcare organizations and universities are now also facing heightened cyber-security threats during the pandemic. Since the outbreak began, various healthcare providers and academic institutions across the world have been targeted in a variety of complex and coordinatized cyber-attacks. International and national regulatory bodies have stressed the urgent need for healthcare providers and universities to protect themselves against cyber-attacks during Covid-19, recognizing that a growing number of cyber-criminals are seeking to capitalize on the vulnerabilities of the healthcare sector during this period. This includes a desire to steal intellectual property such as data relating to Covid-19 vaccine development, modelling and experimental therapeutics. It is therefore essential that healthcare providers and universities ensure they are informed, protected and prepared to respond to any cyber-threat. Cybersecurity has been a separate field which has been primarily focused on the security of information technology-based systems, from personal computers and communications devices to large infrastructures and networks. Up until just the past few years, the "cyber" overlaps with biosecurity have not been realized or fleshed out. The important interrelationship between biosecurity and cybersecurity is gaining increasing attention. In 2014, the American Association for the Advancement of Science (AAAS), FBI and the United Nations Interregional Crime and Justice Research Institute (UNICRI) published a report entitled "National and Transnational Security Implications of Big Data in the Life Sciences [3].

In 2017 a study by Technol Health care concluded that the healthcare industry is a prime target for medical information theft as it lags other leading industries in securing vital data. It is imperative that time and funding is invested in maintaining and ensuring the protection of healthcare technology and the confidentially of patient information from unauthorized access. In addition to being the target of media, governmental and individual attention pertaining to the pandemic, the WHO has also been the target of a very high number of cyberattacks. According to its own CISO, Flavio Aggio, since the pandemic began, the cyberattacks against the WHO have increased at least fivefold [4].

Problem

As previously stated, Puerto Rico's government sites have been victims of ongoing cyberattacks since the beginning of the Covid-19 pandemic. Most 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 [5].

Methodology

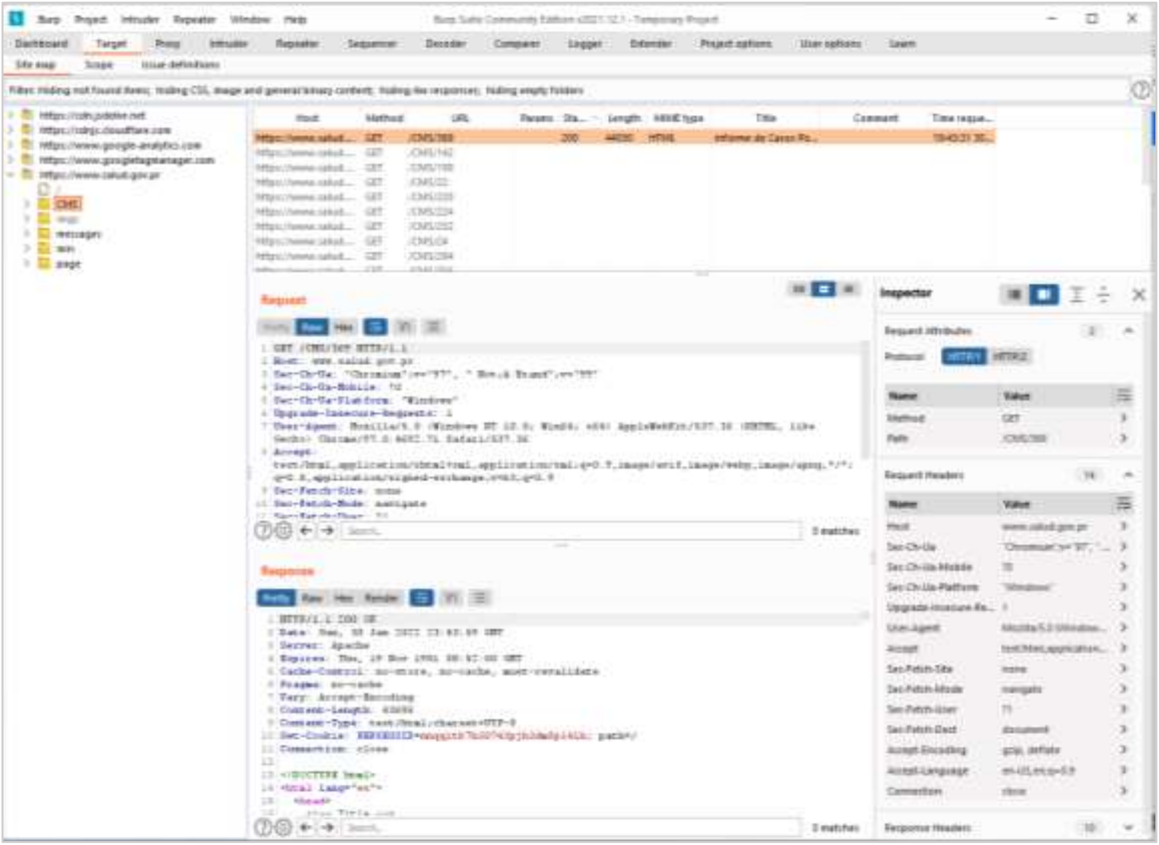
To conduct the project, a penetration testing analysis of vulnerabilities using the Burp suite community tool was utilized through a virtual machine using OWASP standards. One of Burp Suite's main features is its ability to intercept HTTP requests. It does this by using an epoxy either a built in browser 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 (refer to Figure 1) 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.

The OWASP Top 10 is a standard awareness document for developers and web application security. It represents a broad consensus about the most critical security risks to web applications. Results will also be discussed through CWE standards as well CWE™ is a community-developed list of software and hardware weakness types. This helps better understand the issues and identify key concepts.

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.

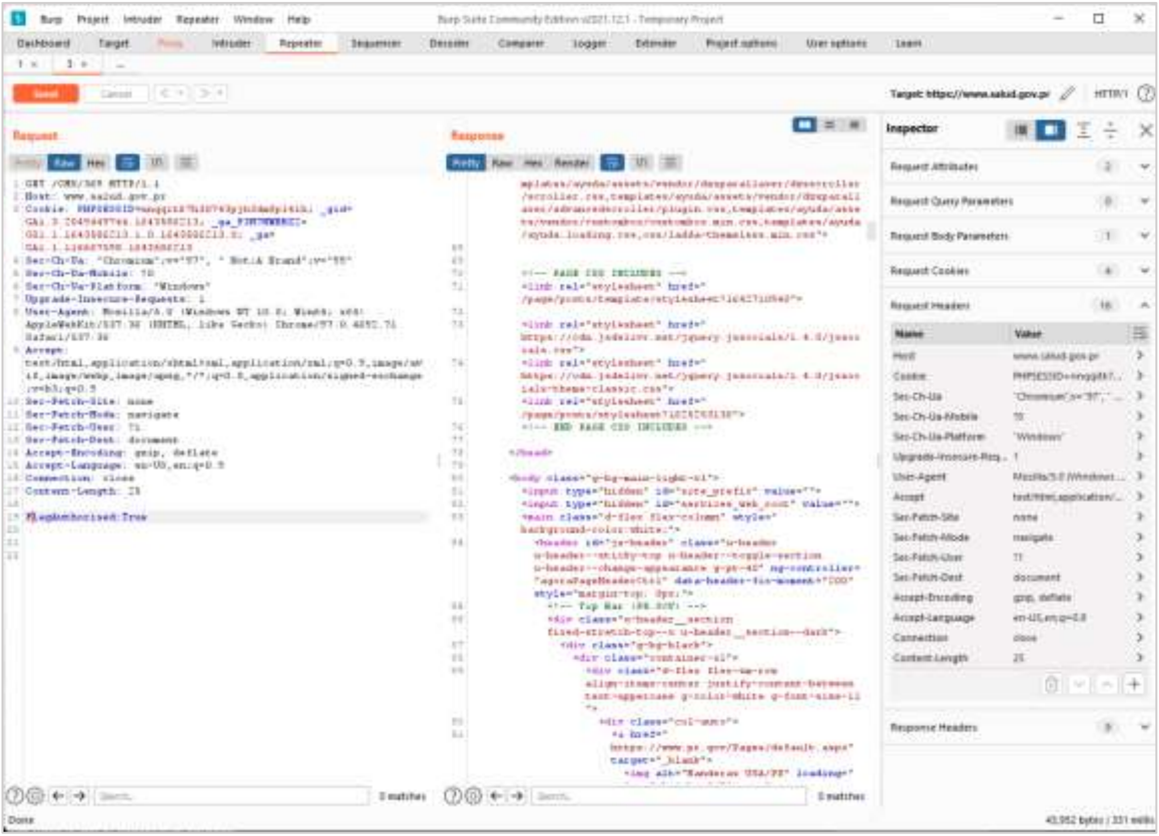


```
GET /CMS/[illegible] HTTP/1.1
Host: www.salud.gov.pr
Sec-Ch-Ua: [illegible]
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/[illegible] Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
```

```
HTTP/1.1 200 OK
Date: [illegible] GMT
Server: Apache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Vary: Accept-Encoding
Content-Length: [illegible]
Content-Type: text/html; charset=UTF-8
Set-Cookie: [illegible]; path=/
Connection: close

<!DOCTYPE html>
<html lang="en">
  <head>
```

Figure 1
Burp Suite Interface



Burp Project Intruder Repeater Window Help
Burp Suite Community Edition v2021.12.1 - Temporary Project
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
Send
Cancel
Target: https://www.salud.gov.pr
HTTP/1
Request
Pretty Raw Hex
Response
Pretty Raw Hex Render
Inspector
Request Attributes
Request Query Parameters
Request Body Parameters
Request Cookies
Request Headers
Response Headers
Search...
0 matches
Done

```
GET /CMS/369 HTTP/1.1
Host: www.salud.gov.pr
Cookie: PHPSESSID=[illegible]; _gid=
GA1.3.[illegible]; _ga_[illegible]=
GS1.1.[illegible]; _ga=
GA1.1.[illegible]
Sec-Ch-Ua: "Chromium";v="97", " Not;A Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/av
if,image/webp,image/apng,*/*;q=0.8,application/signed-exchange
;v=b3;q=0.9
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
Content-Length: 25

flagAuthorized:True
```

```
      mplates/ayuda/assets/vendor/dzsparallaxer/dzsscroller
      /scroller.css,templates/ayuda/assets/vendor/dzsparall
      axer/advancedscroller/plugin.css,templates/ayuda/asse
      ts/vendor/custombox/custombox.min.css,templates/ayuda
      /ayuda.loading.css,css/ladda-themeless.min.css">


      <!-- PAGE CSS INCLUDES -->
      <link rel="stylesheet" href="
      /page/posts/template/stylesheet?[illegible]">

      <link rel="stylesheet" href="
      https://cdn.jsdelivr.net/jquery.jssocials/1.4.0/jssoc
      ials.css">
      <link rel="stylesheet" href="
      https://cdn.jsdelivr.net/jquery.jssocials/1.4.0/jssoc
      ials-theme-classic.css">
      <link rel="stylesheet" href="
      /page/posts/stylesheet?[illegible]">
      <!-- END PAGE CSS INCLUDES -->

    </head>

    <body class="g-bg-main-light-v1">
      <input type="hidden" id="site_prefix" value="">
      <input type="hidden" id="services_web_root" value="">
      <main class="d-flex flex-column" style="
      background-color:white;">
        <header id="js-header" class="u-header
        u-header--sticky-top u-header--toggle-section
        u-header--change-appearance g-pt-40" ng-controller=
        "agencyPageHeaderCtrl" data-header-fix-moment="200"
        style="margin-top: 0px;">
          <!-- Top Bar (HB.DIV) -->
          <div class="u-header__section
          fixed-stretch-top--x u-header__section--dark">
            <div class="g-bg-black">
              <div class="container-xl">
                <div class="d-flex flex-md-row
                align-items-center justify-content-between
                text-uppercase g-color-white g-font-size-11
                ">
                  <div class="col-auto">
                    <a href="
                    https://www.pr.gov/Pages/default.aspx"
                    target="_blank">
                      <img alt="Banderas USA/PR" loading="
```

Name	Value
Host	www.salud.gov.pr
Cookie	PHPSESSID=[illegible]...
Sec-Ch-Ua	"Chromium";v="97", "...
Sec-Ch-Ua-Mobile	?0
Sec-Ch-Ua-Platform	"Windows"
Upgrade-Insecure-Req...	1
User-Agent	Mozilla/5.0 (Windows ...
Accept	text/html,application/...
Sec-Fetch-Site	none
Sec-Fetch-Mode	navigate
Sec-Fetch-User	?1
Sec-Fetch-Dest	document
Accept-Encoding	gzip, deflate
Accept-Language	en-US,en;q=0.9
Connection	close
Content-Length	25

43,962 bytes | 331 millis

Figure 2
Sending requests to the server

When we first capture some of the network traffic through the proxy we get several alerts such as the SSL certificate is expired. This is an issue in network security as it leaved the site vulnerable as the Certificate Administrator (CA) is unable to verify the site encryption. Also, an expired certificate could lead to having the site date stolen as the website becomes insecure.

An attacker could easily mount a man-in-the-middle attack to sniff the SSL communication by presenting the user a fake SSL certificate. On Table 1 several risk along with its OWASP classification can we observed. In Figure 2 we can observe how Burp Suite sends http requests and obtains responses.

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. The identified risks and their corresponding OWASP & CWE classifications are listed in Table 1.

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.

Table 1
Identified Risks

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 2
Identified Risks in Software

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

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. Some security headers are missing such as: Xframe options and XSS protection making the website vulnerable to various types of attacks. The X-XSS-Protection HTTP header instructs the browser to stop loading web pages when they detect reflected Cross-Site Scripting (XSS) attacks. The lack of this header exposes application users to XSS attacks in case the web application contains such vulnerability. Because the X-Frame-Options header is not sent by the server, an attacker could embed this website into an iframe of a third-party website. By manipulating the display attributes of the iframe, the attacker could trick the user into performing mouse clicks in the application, thus performing activities without user's consent (ex: delete user, subscribe to newsletter, etc.). This is known as Clickjacking. The content security header is missing as well and needs to be configured it is sent with each HTTP response to apply the specific policies needed by the application.

Proactive Measures

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. Employees should also be educated on cyber-attack trends and taught cybersecurity safety measures. Preemptively detecting security flaws and establishing processes to detect attacks before they occur are all part of a proactive cybersecurity strategy. A reactive strategy, on the other hand, entails responding to problems like cyberattacks and data breaches after they happen.

FUTURE WORK

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. This is an ongoing issue as Covid-19 data for Puerto Rico is not updated in real time therefore it fails to comply with CIA triad in accessibility and integrity hence important databases as WHO and Mayo clinic opted out of including PR's current data. Therefore, a future work would aim to fix this issue and establish a system that's effective for these types of situations.

References

[1] K. M. Berger and P. A. Schneck, "National and transnational security implications of asymmetric access to and use of biological data," *Frontiers in Bioengineering and Biotechnology*, February 25, 2019. [Online]. Available: https://doi.org/10.3389/fbioe.2019.00021

[2] S. Thompson, O. Wiggins, and E. Cox, "Maryland health workers, lawmakers want answers as problems persist a month after cyberattack," *The Washington Post*, January 8, 2022. [Online]. Available: https://www.washingtonpost.com/dc-md-va/2022/01/08/cyberattack-still-disrupting-maryland-department-of-health/.

[3] T. Wilhelm, *Professional Penetration Testing*. San Francisco: CA: Syngress, 2013.

[4] C. S. Kruse, B. Frederick, T. Jacobson, and D. K. Monticone, "Cybersecurity in healthcare: A systematic review of modern threats and trends," *Technology and Health Care*, vol. 25, no. 1, pp. 1–10, 2017.

[5] J. Ayala, "Anatomía de un ciberataque," *El Nuevo Dia*, June 21, 2021. [Online]. Available: https://www.elnuevodia.com/tecnologia/otros/notas/anatomia-de-un-ciberataque-el-incidente-de-ransomware-que-provoco-una-emergencia-en-el-departamento-de-hacienda/