A black background with grey leaves

AI-generated content may be incorrect.

ExterNal passive penetration test detailed report

Stamford Health/Stamford Hospital

A grey logo on a black background

AI-generated content may be incorrect.

**By**

**Charlize Aponte – Technical Writer and OSINT Analyst**

**Henry Cort – Certificate OSINT Analyst**

**Caden Effrece – Technical Writer and OSINT Analyst**

**Barath Reddy Kondam – Risk and OSINT Analyst**

**Tapiwanashe Mutume – Social Media Analyst**

**Evan Quinn – Network and Website OSINT Analyst**

**Peter Zegarek – Reconnaissance Specialist and lead OSINT Analyst**

**Version 1.0**

# **Document Control**

|  |  |
| --- | --- |
| Document Name | External Passive Penetration Testing – Detailed Report |
| Technical Writer | Caden Effrece |
| Version | 1.0 |
| Date of submission | 5th of May, 2025 |

Table of Contents

[**Document Control** 1](#_Toc197369092)

[**1.** **Introduction** 3](#_Toc197369093)

[**2. Project Summary** 3](#_Toc197369094)

[**3. Assessment Approach** 3](#_Toc197369095)

[**4. Executive Summary** 4](#_Toc197369096)

[**5. Summary of Findings** 4](#_Toc197369097)

[**6. Findings and Recommended Actions** 5](#_Toc197369098)

[**5. Conclusion** 24](#_Toc197369099)

[5. Remediation Summary 36](#_Toc197369100)

# **1.** **Introduction**

This report details the findings of a passive security assessment performed on Stamford Healthcare and Stamford Hospital, henceforth referred to as the single entity “Stamford Healthcare” or “the company”. The assessment was conducted by a team of students from Quinnipiac University’s Spring 2025 CYB615 Introduction to Ethical Hacking class. The assessment aimed to simulate what a potential adversary can do with only publicly accessible information and non-intrusive methods. The goal was to identify possible exposures, vulnerabilities, and weaknesses in the company’s system that could be leveraged in cyberattacks, both in physical and virtual environments. The anticipated result is to help Stamford Healthcare strengthen their security and consider publicly available information.

# **2. Project Summary**

The project involved a comprehensive examination of Stamford Healthcare’s publicly facing information. This included URLs under the domain of Stamford Healthcare and Stamford Hospital, social media accounts of employees and the company itself, publicly available posts regarding the company on LinkedIn, Reddit, Instagram, and Facebook, publicly available and easy to find certificate information, publicly found email addresses, cache statuses, content encoding, and headers. DNS configurations, SSL/TLS implementations, and general OSINT tactics were searched and used to find information that may be potentially harmful to the company.

All findings were documented with screenshots or web links if applicable and categorized by severity and potential effect on the company’s infrastructure. Actionable recommendations are listed for each finding to help mitigate or remove the effects of the found vulnerabilities and weaknesses.

# **3. Assessment Approach**

Each penetration tester, referred to as “OSINT Analyst” on the cover page, had their designated area to cover. Each analyst went about searching the internet and finding possible weaknesses in their own way, however, all had similar approaches, which can be broken down into phases as follows:

1. Enumeration of Stamford Heathcare’s resources and locations of possible weaknesses in the analyst’s designated area.
2. OSINT performance, gathering of data, finding of vulnerabilities and risks.
3. Data collection, finalization and risk analysis

All activities were performed passively and were non-intrusive. There was no interruption or disruption to Stamford Healthcare’s operations, patient or consumer operations, or network operations.

# **4. Executive Summary**

During our penetration testing for Stamford Health, several security vulnerabilities and risks were identified across their web infrastructure and publicly available data sources. This test was conducted from a purely open-source standpoint, and no vulnerabilities were exploited, following the scoping document.

Critical Findings:

* API key located on publicly facing page of Stamford Healthcare website
* Cleartext Username and Password combinations found in network packets sent from Stamford Hospital login page

Other Findings:

* Sensitive personal information
  + Employee ID badges
  + Video footage of employee ID numbers and clocking out system
* Third-party service breaches
* Unsecured certificate expiration dates
* Discovery of C-Suite and high-level employee email addresses

No active scanning or exploitation of the findings was conducted. However, the nature of the findings makes the company prone to a number of possible attacks:

* Active account grabbing and exploitation and exfiltration of private patient and employee data
* Unauthorized access to Stamford Healthcare’s API using the publicly available API key
* Physical attacks using information found to create a persona
* Phishing, Whaling, and other virtual Social Engineering attacks
* Man-In-The-Middle attacks using certificate expiration dates

These attacks have the potential to disrupt and/or deny Stamford Healthcare’s operations. It also has the potential to result in a loss of customer trust even if breaches are minimal to operations.

# **5. Summary of Findings**

Quinnipiac University’s student group assessment resulted in three categories of findings listed in terms of severity: High Severity, Medium Severity, Low Severity.

# **6. Findings and Recommended Actions**

|  |  |
| --- | --- |
| **OSINT Analyst Responsible** | **Peter Zegarek** |
| **Description** | Publicly available API key located in Stamford Health’s website. This API key could be used to potentially abuse access on other endpoints, since it can be taken and re-used with malicious intent. It is not hard to find, as it was found on publicly facing website infrastructure. Also, this exact same API key was checked and found a week apart, meaning that API keys are not being rotated, and a compromised key such as this could have lasting permissions / power. This vulnerability was found just by browsing the Stamford Health website and watching the network tab in Google Chrome, on a Windows 11 system. |
| **Risk Rating** | **HIGH** |
| **Proof of Concept** | A screen shot of a computer  AI-generated content may be incorrect. |
| **Recommendations** | * Use environment variables server side for the API key and verify the client in a different way. * Rotate API keys frequently to minimize risk. |

|  |  |
| --- | --- |
| **OSINT Analyst Responsible** | **Caden Effrece** |
| **Description** | Cleartext usernames and passwords are visible when network packets are scanned. They are clearly spelled out with “username=” and “password=”. This is the same with the Forgot Password Website as well. This can allow attackers sniffing the network to gather account usernames, passwords, and emails. |
| **Risk Rating** | **HIGH** |
| **Proof of Concept** |  |
| **Recommendations** | * Hash passwords and usernames so they are not cleartext * Use an encryption algorithm to secure network packets |

|  |  |
| --- | --- |
| **OSINT Analyst Responsible** | **Caden Effrece and Charlize Aponte** |
| **Description** | Publicly available photos of ID cards can aid physical adversaries in gaining access to the company’s facilities by pretending to be an employee or worker. |
| **Risk Rating** | **LOW** |
| **Proof of Concept** |  |
| **Recommendations** | * Inform employees about the dangers of revealing company information publicly. * Encourage employees to blur or hide sensitive information when posting pictures online. |

|  |  |
| --- | --- |
| **OSINT Analyst Responsible** | **Bharath Reddy Kondam** |
| **Description** | Email signatures publicly available are a security risk. They allow attackers to more easily impersonate one of the executives or higher-ranking employees. |
| **Risk Rating** | **MEDIUM** |
| **Proof of Concept** |  |
| **Recommendations** | * Inform employees of possible social engineering attacks and how to avoid them * Try to keep personal information like signatures off of the internet as best as possible. |

|  |  |
| --- | --- |
| **OSINT Analyst Responsible** | **Evan Quinn** |
| **Description** | Certificate expiration dates are publicly available on crt.sh. It lists all publicly issued SSL/TLS certificates for a domain. Shows certificate expiration dates, issuers, subdomains, and sometimes internal domains.  **Potential vulnerabilities or implications:**  **Expired certificates:** May suggest poor maintenance or allow MITM (man-in-the-middle) attacks on systems where expired certs are still in use.  **Subdomain discovery:** May reveal forgotten, deprecated, or unprotected subdomains, which are often low-hanging fruit.  **Internal dev/staging environments:** If internal subdomains or wildcard certs show up, these might not be as tightly secured as production. |
| **Risk Rating** | **MEDIUM** |
| **Proof of Concept** |  |
| **Recommendations** | * Set a timer to ensure that certificates are renewed after they are expired to avoid security risks |

|  |  |
| --- | --- |
| **OSINT Analyst Responsible** | **Bharath Reddy Kondam** |
| **Description** | Identifying hidden or undocumented API endpoints embedded within the website's JavaScript files. By manually inspecting JavaScript code loaded on stamford.org |
| **Risk Rating** | **Low** |
| **Proof of Concept** |  |
| **Recommendations** | Avoid revealing sensitive paths in public files, apply input validation and rate limiting, enforce role-based access control, sanitize file uploads, monitor endpoint activity, and use an API gateway for centralized security management. |

|  |  |
| --- | --- |
| **OSINT Analyst Responsible** | **Henry Cort** |
| **Description** | SSL/TLS certificate for mychart.stamfordhealth.org is valid and issued by Sectigo RSA OV CA. While it meets standard validation and supports TLS 1.2/1.3, several best practices are **not enforced**, including DNS CAA records, OCSP Must-Staple, and OCSP Stapling. It also includes a weak CBC cipher suite and over-includes the root anchor in the certificate chain. |
| **Risk Rating** | **Medium** |
| **Proof of Concept** | Certificate details were retrieved using:  openssl s\_client -connect mychart.stamfordhealth.org:443   * Shows expiration: Jan 10, 2026 * No DNS CAA configured * OCSP Must-Staple: Not enabled * Weak CBC-mode cipher suites still present |
| **Recommendations** | * Configure **DNS CAA** to restrict certificate authorities. * **Enable OCSP Must-Staple** and **OCSP Stapling** for improved revocation checking. * **Remove weak ciphers** (e.g., CBC-AES). * Trim certificate chain to remove unnecessary anchors. * Audit HSTS preload status. |

|  |  |
| --- | --- |
| **OSINT Analyst Responsible** | **Tapiwanashe Mutumhe** |
| **Description** | During a passive reconnaissance exercise, publicly available footage was discovered on Instagram (posted by @thessa\_canlas) showing a hospital employee punching in with their ID badge. The reel was accessible via QR code and potentially exposes employee identification information and physical access behaviour |
| **Risk Rating** | **Medium** |
| **Proof of Concept** | * OSINT & Social Media Recon: Identified public video content showing internal operations. * Physical Observation: Captured behavior could be exploited to replicate badge or enable social engineering. |
| **Recommendations** | * Launch staff training on social media and OPSEC. * Mask badge details during use or adopt biometric/MFA solutions. * Perform a physical security audit of access points. |

|  |  |
| --- | --- |
| **OSINT Analyst Responsible** | **Henry Cort** |
| **Description** | The JavaScript file answers.min.js used on Stamford Health’s website includes **unauthenticated client-side API calls** to multiple Yext endpoints. These APIs accept input and return results without authentication or origin control (CORS), presenting risks of **data enumeration**, **PHI exposure**, and **unauthorized scraping**. |
| **Risk Rating** | **HIGH** |
| **Proof of Concept** | python3 linkfinder.py -i <https://assets.sitescdn.net/answers-search-bar/v1.2/answers.min.js> -o cli  Discovered endpoints:   * /v2/accounts/me/answers/query * /v2/accounts/me/answers/autocomplete * /v2/accounts/me/createQuestion, etc.  All callable without authentication from browser. |
| **Recommendations** | * Move all sensitive queries to **authenticated backend endpoints**. * Enforce **CORS policies** to limit origin access. * Use **API gateway or proxying** to obscure client API interactions. * Rotate and secure API keys used in embedded scripts. |

|  |  |
| --- | --- |
| **OSINT Analyst Responsible** | **Evan Quinn** |
| **Description** | The associated email address, KSilard@stamhealth.org , has appeared in 11 known public data breaches. This indicates credential reuse risk, potential for targeted phishing, and possibly password spray attacks if the email is associated with users or staff at the target organization.  Potential vulnerabilities or implications:  Credential stuffing: If that email was reused with the same or similar passwords, attackers may try it across other services (especially if MFA isn't in place).  Phishing/social engineering: Emails that have been compromised could be used to craft convincing phishing emails to users in the org.  Username enumeration: If an attacker can confirm which breached emails are active accounts, they may now know valid usernames for login portals. |
| **Risk Rating** | **Medium** |
| **Proof of Concept** |  |
| **Recommendations** | It is recommended that the organization immediately assess whether the exposed email address is currently active within their systems and, if so, ensure the associated password has been changed and MFA is enforced. Additionally, monitor for unusual login attempts and educate users on phishing risks, as compromised emails increase the likelihood of targeted social engineering attacks. Consider implementing credential monitoring to detect future exposures and limit username enumeration through login portals. |

|  |  |
| --- | --- |
| **OSINT Analyst Responsible** | **Henry Cort** |
| **Description** | The certificate issued for mychart.stamfordhealth.org includes a SHA256 fingerprint and metadata indicating strong key usage but lacks extended validation, OCSP Must-Staple, and DNS CAA. It also supports older CBC-mode ciphers and lacks public key pinning. |
| **Risk Rating** | **Medium** |
| **Proof of Concept** | Details from certificate inspection:   * SHA256 Fingerprint: 48f5...e084e1 * Public Key: RSA 2048-bit, exponent 65537 * Weak ciphers: CBC-AES * No PKP, OCSP Must-Staple, or DNS CAA |
| **Recommendations** | * Enforce modern **cipher suite policies** (remove CBC). * Configure **DNS CAA** and **Must-Staple** to strengthen trust. * Enable **Forward Secrecy** and **OCSP Stapling**. * Consider **Public Key Pinning** for advanced hardening (with caution). |

|  |  |
| --- | --- |
| **OSINT Analyst Responsible** | **Evan Quinn** |
| **Description** | 93 Publicly scraped or disclosed email addresses tied to the domain. Usually includes job titles, email formats, and organizational structure clues.  Potential vulnerabilities or implications:  User enumeration: Helps attackers find valid users for brute force or phishing.  Spear phishing: Role-specific emails (like “itadmin@” or “hr@”) can be high-value  Social engineering: Insight into org structure helps craft targeted attacks or fake communications (e.g., CEO fraud).  Email pattern discovery: Confirms the org’s email format (e.g., first.last@company.com), which makes guessing other addresses easier. |
| **Risk Rating** | **Medium** |
| **Proof of Concept** |  |
| **Recommendations** | Conduct a review of public sources to identify and, where possible, remove or obfuscate exposed email addresses. Implement email security controls such as SPF, DKIM, and DMARC to protect against spoofing. Educate staff, especially those in high-value roles, on phishing awareness, and monitor for unusual activity targeting these accounts. |

|  |  |
| --- | --- |
| **OSINT Analyst Responsible** | **Charlize Aponte** |
| **Description** | We conducted an open-source intelligence (OSINT) investigation using platforms like LinkedIn, Instagram, and Twitter, uncovering publicly shared photos displaying employee and guest ID badges, uniforms, and names. By cross-referencing these with publicly available staff details on the Stamford Health website, including emails and biographies, we identified a vulnerability. The abundance of personal and professional information online—such as names, departments, and roles—could enable malicious actors to launch social engineering attacks or impersonate staff. Additionally, the visibility of uniform styles and guest badges increases the risk of physical intrusion into restricted areas. |
| **Risk Rating** | **Low** |
| **Proof of Concept** |  |
| **Recommendations** | 1) Implement policies and awareness campaigns discouraging the posting of identifiable ID badges, uniforms, or guest passes on public platforms.  2) Train employees to obscure badges in photos and avoid posting sensitive work-related images.  3) Consider limiting publicly accessible employee information  4) Provide regular training on phishing and impersonation tactics to help staff recognize and report suspicious activity.  5) Use tools to monitor social media for unauthorized sharing of internal visuals and identifiers. |

|  |  |
| --- | --- |
| **OSINT Analyst Responsible** | **Evan Quinn** |
| **Description** | Using VirusTotal, it was found that he HTTP response headers indicate that the target site is fronted by Cloudflare and hosted on Azure, with dynamic, gzip-compressed content and standard configurations for modern web delivery. While no direct vulnerabilities are evident, several security best practices are missing, including important headers like Content-Security-Policy, Strict-Transport-Security, X-Frame-Options, and X-Content-Type-Options, which help mitigate common web threats such as XSS, clickjacking, and MIME-type confusion. The use of gzip compression alongside dynamic content may pose a low-risk BREACH vulnerability if user-controlled input is reflected. Additionally, the presence of the x-azure-ref header reveals underlying infrastructure details, contributing to potential information leakage useful during reconnaissance. |
| **Risk Rating** | **Low** |
| **Proof of Concept** | A screenshot of a computer  AI-generated content may be incorrect. |
| **Recommendations** | Test for reflection-based input in compressed responses (BREACH test)  Confirm presence/absence of key headers like:  X-Content-Type-Options: nosniff  Content-Security-Policy  Strict-Transport-Security  X-Frame-Options  Use x-azure-ref and other fingerprinting clues to map infrastructure and check for public Azure blobs, misconfigured subdomains, or known Azure CVEs. |

# **5. Conclusion**

This passive security assessment identified several critical, medium, and low-severity vulnerabilities in Stamford Healthcare’s publicly accessible information. Exposed API keys, cleartext credentials, and sensitive employee data present significant risks that could enable cyberattacks, physical intrusions, or social engineering efforts. Many of these vulnerabilities were found without the use of advanced software, further showcasing the accessibility of these exploits to a non-advanced adversary.

While no exploitation was conducted, the findings demonstrate that an attacker could leverage this information to harm Stamford Healthcare’s operations, reputation, and even patients. Immediate action should be taken to secure exposed assets, rotate credentials, encrypt sensitive communications, and improve employee awareness of information security best practices.

Addressing these vulnerabilities will strengthen Stamford Healthcare’s defenses and reduce its risk of future compromise.