

Vulnerability Audit and Assessment - Results and Executive Summary Assignment

1. Introduction

In order to ensure the safety of the EHR-online website, a black box assessment was performed. This report covers the methodology that was used, as well as its limitations, as well as the requirements that the business must meet under GDPR, a brief analysis of the security flaws, and a summary of the recommendations. We provide an in-depth explanation of the security requirements (including compliance with GDPR), as well as recommendations for achieving full compliance. The flow of the web application penetration testing performed on EHR-online is displayed in table 1.0.

Table 1.0

Domain	Health Care
Type of testing	Black box - Penetration testing
Website	https://ehr-online.co.uk
Technique	Web application Penetration testing
Scope	Black box
Method	PTES and OWASP
Model	STRIDE, DREAD
Report	Executive summary

2. Testing Methodology

Our security testing methodology, which is known as PTES, includes the OWASP Web testing framework as one of its components (Penetration Testing Execution Standard). The Penetration Testing Execution Standard (PTES) is a standardized method that outlines a seven-step procedure and offers a structured strategy for conducting penetration tests (Imperva.com 2022). Because there are advantages to be gained from manual testing as well as automated testing, we combined the two methods (owasp.org 2022)

3. Modelling Method

Threats, vulnerabilities in security, and defenses that are insufficient will all be modelled with the assistance of STRIDE. The following diagram provides a visual representation of the STRIDE modelling process, which identifies the site's security objectives as well as the threats to those objectives: 1. (docs.microsoft.com 2022) Utilizes DREAD as a means of identifying and evaluating potential risks. (2016) In light of what David Kohanbash has stated: Figure 2, which can be found over on this page, provides an illustration of the vulnerability scale.

Figure:1

STRIDE model

To better help you formulate these kinds of pointed questions, Microsoft uses the STRIDE model, which categorizes different types of threats and simplifies the overall security conversations.

Category	Description
Spoofing	Involves illegally accessing and then using another user's authentication information, such as username and password
Tampering	Involves the malicious modification of data. Examples include unauthorized changes made to persistent data, such as that held in a database, and the alteration of data as it flows between two computers over an open network, such as the Internet
Repudiation	Associated with users who deny performing an action without other parties having any way to prove otherwise—for example, a user performs an illegal operation in a system that lacks the ability to trace the prohibited operations. Non-Repudiation refers to the ability of a system to counter repudiation threats. For example, a user who purchases an item might have to sign for the item upon receipt. The vendor can then use the signed receipt as evidence that the user did receive the package
Information Disclosure	Involves the exposure of information to individuals who are not supposed to have access to it—for example, the ability of users to read a file that they were not granted access to, or the ability of an intruder to read data in transit between two computers
Denial of Service	Denial of service (DoS) attacks deny service to valid users—for example, by making a Web server temporarily unavailable or unusable. You must protect against certain types of DoS threats simply to improve system availability and reliability
Elevation of Privilege	An unprivileged user gains privileged access and thereby has sufficient access to compromise or destroy the entire system. Elevation of privilege threats include those situations in which an attacker has effectively penetrated all system defenses and become part of the trusted system itself, a dangerous situation indeed

Figure:2

	Rating category	High (3)	Medium (2)	Low (1)
D	Damage potential	Could subvert the security system and gain full trust, ultimately taking over the environment	Could leak sensitive information	Could leak trivial information
R	Reproducibility	Is always reproducible	Can be reproduced only during a specific condition or window of time	Is very difficult to reproduce, even given specific information about the vulnerability
E	Exploitability	Allows a novice attacker to execute the exploit	Allows a skilled attacker to create an attack that could be used repeatedly	Allows only a skilled attacker with in-depth knowledge to perform the attack
A	Affected users	Affects all users, including the default setup user and key customers	Affects some users or specific setups	Affects a very small percentage of users; typically affects an obscure feature
D	Discoverability	Can be easily found in a published explanation of the attack	Affects a seldom-used part, meaning an attacker would need to be very creative to discover a malicious use for it	Is obscure, meaning it's unlikely attackers would find a way to exploit it

Approach:

Step 1: In the case of EHR-online, the most valuable asset is the client personal data

Step 2: Section 4.1.2 of the application's technical requirements provides more information (Server software and technology found)

Step 3: In Section 4.1.3, where we present all the subdomains of the targeted website, we documented the methods for using the digital asset.

Step 4: Section 4.2 ("Security Vulnerabilities") contains the vulnerabilities we explored.

Step 5: We mentioned the threats in Section 4.2 ("Security Vulnerabilities"), along with their description, target, strategies, and risk-management strategy.

Step 6: We identify vulnerabilities and rating their severity using the DREAD risk analysis model (Meier, 2003) Figures 8 and 9 as well as Section 4.2 all display this.

4. Summary of the Findings:

We were unable to carry out additional scans without having our IP address blocked because the targeted platform is protected by Imunify360. Proxychains and TOR, two services that allow us to conceal our IP address and reroute network traffic, were utilized in our scans so that we could get around this restriction. After that, we will present a brief summary of our findings.

4.1 Server software and technology

The targeted website is protected with Imunify 360, which comes from the host A2 Hosting (This can be seen in the Nmap scan print documented in the Imunify360 protects against malware infections, web attacks, vulnerability exploitation, and other threats. (Imunify360, 2022))

4.2 Information gathering:

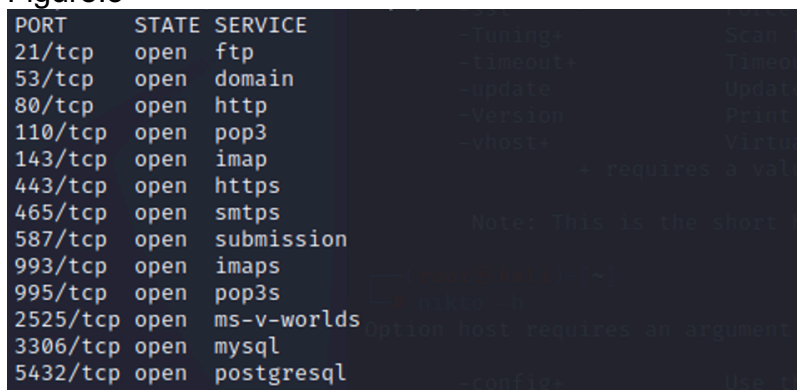
We were able to extract details regarding the open ports, services, application versions, operating system versions, and other features of the system.

4.2.1 Port Scanning

NMAP: Nmap is a utility that can be used for auditing network security or exploring networks. Ping scanning, many different port scanning techniques, version detection (which can determine the service protocols and application versions listening behind ports), and TCP/IP fingerprinting are all supported by it. Ping scanning is used to determine which hosts are online (remote host OS or device identification). Nmap provides a number of additional features, including flexible target and port specification, decoy/stealth scanning, sunRPC scanning, and more. Both graphical user interfaces (GUIs) and command-line interfaces (CLIs) are supported for the majority of Unix and Windows platforms. In addition, support is provided for a variety of well-known handheld devices, such as the Sharp Zaurus and the iPAQ. (kali.org 2022)

We used NMAP for scanning the TCP protocol. Figure 3 presents the TCP results.

Figure:3

A screenshot of a terminal window displaying the output of an Nmap scan. The output is a table with three columns: PORT, STATE, and SERVICE. The ports listed are 21/tcp, 53/tcp, 80/tcp, 110/tcp, 143/tcp, 443/tcp, 465/tcp, 587/tcp, 993/tcp, 995/tcp, 2525/tcp, 3306/tcp, and 5432/tcp. All ports are in the 'open' state. The services listed are ftp, domain, http, pop3, imap, https, smtps, submission, imaps, pop3s, ms-v-worlds, mysql, and postgresql. There are some faint, partially visible text elements in the background of the terminal window, such as 'Tuning', 'Scan', 'update', 'Print', 'Verify', 'requires a val', 'This is the short', 'option host requires an argument', and 'Scan 192.168.1.100'.

PORT	STATE	SERVICE
21/tcp	open	ftp
53/tcp	open	domain
80/tcp	open	http
110/tcp	open	pop3
143/tcp	open	imap
443/tcp	open	https
465/tcp	open	smtps
587/tcp	open	submission
993/tcp	open	imaps
995/tcp	open	pop3s
2525/tcp	open	ms-v-worlds
3306/tcp	open	mysql
5432/tcp	open	postgresql

Observation: The port 80 and 443 are the web browsing ports that needs to open in the web facing applications. The other ports need to be blocked.

4.2.2 Security vulnerabilities overview

We carried out scans on the targeted website with the assistance of OWASP ZAP. As can be seen in Figure 4, there were a total of 10 potential dangers and 19 warnings discovered.

When a threat is given a rating of High, it indicates that it poses a significant risk to your application and needs to be dealt with as quickly as possible. Threats of a medium severity need to be dealt with, but there should be less of a sense of urgency surrounding these situations. Figure 2, which can be found up top, illustrates the classification rating that has been assigned.

Figure 4

Summary of Alerts

Risk Level	Number of Alerts
High	1
Medium	1
Low	7
Informational	1
False Positives:	0

Alerts

Name	Risk Level	Number of Instances
Path Traversal	High	1
Vulnerable JS Library	Medium	1
Absence of Anti-CSRF Tokens	Low	1
Cookie No HttpOnly Flag	Low	1
Cookie Without Secure Flag	Low	1
Cookie without SameSite Attribute	Low	1
Incomplete or No Cache-control Header Set	Low	3
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	Low	3
Timestamp Disclosure - Unix	Low	4
Information Disclosure - Suspicious Comments	Informational	3

Based on the scan result we are focusing on solutioning high and the medium observations

High – Path reversal

Observation: Path Traversal allows an attacker to access files, directories, and commands outside the web document root. An attacker can manipulate a URL to execute or reveal arbitrary server files. Path Traversal can affect any HTTP-based device. Most websites restrict access to the "web document root" or "CGI root" directory. These directories contain user-accessible files and web app executables.

Path Traversal attacks use special-character sequences to access files or execute commands anywhere on the file-system.

Solution: Decode and canonicalize inputs before validating them. Make sure your app doesn't decode duplicate input. By introducing dangerous inputs after they've been checked, such errors can bypass allow list schemes. Use a built-in path canonicalization function (realpath() in C) to remove ".." sequences and symbolic links. Run your code with the fewest privileges needed. If possible, create single-task accounts with limited privileges. A successful attack won't give the attacker immediate access to the software or its environment. In day-to-day operations, database applications rarely run as the database administrator. When the set of acceptable objects, such as filenames or URLs, is limited or known, map a set of fixed input values (such as numeric IDs) to those objects and reject all other inputs.

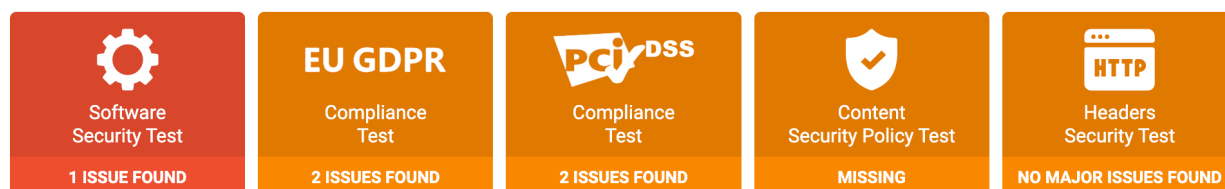
Medium – Vulnerable JS library

Observation: The jQuery library, version 1.4.3, has been found to have a security flaw.

Solution: Upgrade to the latest version.

We also used immuniweb to perform scans on the targeted website. Below in the Figure 5 is the findings. There were 6 categories of issues observed.

Figure 5



4.2.3 JQuery scanning

The following is the result of a scan that we performed using immuniweb on the Java script library.

CVSSv3.1 Score	Vulnerability CVE-ID	Vulnerability Type
5.5 Medium	CVE-2020-7656	CWE-79 – Cross-site scripting
5.5 Medium	CVE-2020-11022	CWE-79 – Cross-site scripting
5.3 Medium	CVE-2015-9251	CWE-79 – Cross-site scripting
5.3 Medium	Not Assigned, see 4 references	CWE-79 – Cross-site scripting
4.8 Medium	CVE-2019-11358	CWE-400 – Prototype pollution
4.1 Medium	CVE-2020-11023	CWE-79 – Cross-site scripting

5.5 Medium – CVE 2020-7657

A flaw was found in jquery in versions prior to 1.9.0. A cross-site scripting attack is possible as the load method fails to recognize and remove "<script>" HTML tags that contain a whitespace character which results in the enclosed script logic to be executed. The highest threat from this vulnerability is to data confidentiality and integrity.

A future update may update JQuery to a fixed version.

5.5 Medium CVE-2020-11022

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 problem is patched in jQuery 3.5.0.

5.3 Medium CVE-2015-9251

jQuery before 3.0.0 is vulnerable to Cross-site Scripting (XSS) attacks when a cross-domain Ajax request is performed without the dataType option, causing text/javascript responses to be executed.

4.8 Medium CVE-2019-11358

A Prototype Pollution vulnerability was found in jquery. Untrusted JSON passed to the `extend` function could lead to modifying objects up the prototype chain, including the global Object. A crafted JSON object passed to a vulnerable method could lead to denial of service or data injection, with various consequences.

These packages are deprecated in Red Hat Virtualization 4.3.

4.1 Medium CVE-2020-11023

In jQuery versions greater than or equal to 1.0.3 and before 3.5.0, passing HTML containing <option> elements 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 problem is patched in jQuery 3.5.0.

Low/informational vulnerabilities

Low:

- Absence of Anti-CSRF Tokens
- Cookie No HttpOnly Flag
- Cookie Without Secure Flag
- Cookie without SameSite Attribute
- Incomplete or No Cache-control Header Set
- Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)
- Timestamp Disclosure - Unix

Informational:

- Information Disclosure - Suspicious Comments

5.0 Security standard analysis & GDPR compliance

The General Data Protection Regulation (GDPR) is a regulation that governs the processing of personal data as well as the sharing of that data. This regulation covers the following categories of personal data: subject identification data, personal data (defined as any data that can be used to identify an individual), spatial data, and cookie identifiers. options.

General Data Protection Regulation EU law that gives customers more control over personal data collection and storage. Potential vulnerabilities include compromised or stolen credentials (from commercially available software, apps, and plugins) and application vulnerabilities (such as potential for injection, privilege escalation and cross-site scripting). (gdpr.eu 2022)

GDPR.EU Article 13, Available at: <https://gdpr.eu/article-13-personal-data-collected/> [Accessed 29 June 2022]

5.1 GDPR Compliance test

PRIVACY POLICY ⓘ

Privacy Policy was not found on the website or is not easily accessible.

Misconfiguration or weakness

WEBSITE SECURITY ⓘ

Website CMS or its components are outdated and contain publicly known security vulnerabilities.

Misconfiguration or weakness

TLS ENCRYPTION ⓘ

HTTPS encryption is present on the web server.

Good configuration

COOKIE PROTECTION ⓘ

No cookies with personal or tracking information seem to be sent.

Information

COOKIE DISCLAIMER ⓘ

No third-party cookies or cookies with tracking information seem to be sent.

Information

5.2 GDPR Compliance test details

The purpose of this section is to provide details about the GDPR compliance test pertaining to the Privacy Policy, Website Security, Transport Layer Security Encryption, Cookie Protection, and Cookie Disclaimer.

5.2.1 Privacy Policy

Article 13 of GDPR requires the data controller to provide a notice to data subjects when collecting personal data. However, privacy policy contains no text as shown below.

PRIVACY POLICY ⓘ		
Article 13 of GDPR requires data controller to provide a conspicuously visible notice to data subjects when collecting their personal data including but not limited to data collected by web applications.	Privacy Policy was not easily accessible.	Misconfiguration or weakness

5.2.2 Web Security

Article 5(1)(f), Article 24(1) and Article 32 of GDPR require implementation, testing and maintenance of adequate security controls to protect personal data. EDPB guidelines provide further technical details and examples including among other things, maintenance of up-to-date web application software and regular website security testing.

5.2.3 TLS Encryption

Article 32 of GDPR requires implementation of adequate protection of processed personal data. This applies to web application when personal data is being sent or retrieved via a browsers or API

5.2.4 Cookie protection

No cookies with personal or tracking information seem to be sent.

5.2.5 Cookie disclaimer

No third-party cookies or cookies with tracking information seem to be sent.

5.3 PCI DSS compliance test

Requirement 6.2 - Website CMS or its components seem to be outdated. Check for available updates.

Ensure that all systems components and software are protected from known vulnerabilities by installing applicable vendor supplied security patches. Install critical security patches within one month of release

Requirement 6.5 - Fingerprinted website CMS or its components contain publicly known vulnerabilities (Ref. PCI DSS 6.5.1-6.5.10).

Address common coding vulnerabilities in software development process. Train developers at least annually in up-to-date secure coding techniques, including how to avoid common vulnerabilities. Develop application based on secure coding guidelines

Requirement 6.6 - The website seems to be protected by a WAF. Review its logs and configuration on a periodic basis.

The requirement of reviewing application or installing web application firewalls is intended to reduce the number of compromises on public facing web application due to poor coding or application management practices

6.0 Penetration testing timeline

Project Timeline							
Activities	Week1	Week 2	Week 3	Week4	Week5	Week6	Week7
Pre-engagement Interactions							
Information Gathering							
Threat Modeling							
Vulnerability Analysis							
Exploitation							
Post Exploitation							
Reporting							

7.0 Conclusion

We carried out a thorough Web Application Pentest in the EHR-online.co.uk site using the PTES, the OWASP Web testing framework, and the Microsoft Threat Modelling Process. We identified informational, high-risk, medium-risk, and low-risk problems. When a threat is deemed high, it poses a serious risk to the application and must be fixed right away. Medium-level threats still require attention, but less urgently. Additionally, we looked at GDPR compliance and offered suggestions. To find any gaps in the cyber security defenses, the management team of the website should make sure that regular security assessments—at least one every year—take place.

8.0 Recommendations

- The server needs to have latest security patches based on vendor releases
 - Best practice is to maintain N-1 version
- The application-level software needs to be patched on regular basis.
 - Best practice is to maintain N-1 version
- Only the web browsing port 80 and 443 need to be opened and other to be blocked based on the traffic

References:

1. Imperva.com (2022) Penetration testing and web application. Available from: <https://www.imperva.com/learn/application-security/penetration-testing/> [Accessed 1st July 2022]
2. owasp.org (2022) Penetration Testing Execution Standard. Available from https://owasp.org/www-project-web-security-testing-guide/latest/3-The_OWASP_Testing_Framework/1-Penetration_Testing_Methodologies [Accessed 2nd July 2022]
3. owasp.org (2022) Vulnerability scanning tools Available at: https://owasp.org/www-community/Vulnerability_Scanning_Tools [Accessed 1st July 2022]
4. docs.microsoft.com STRIDE model. Available at: <https://docs.microsoft.com/en-us/azure/security/develop/threat-modeling-tool-threats> [Accessed 2nd July 2022]
5. GDPR.EU Article 13, Available at: <https://gdpr.eu/article-13-personal-data-collected/> [Accessed 29 June 2022]
6. PCI (2008). Payment Card Industry Security Standards. Available from: https://www.pcisecuritystandards.org/pdfs/pcissc_overview.pdf [Accessed 30th June 2022]
7. Imunify360 (2022). Hosting providers that offer Imunify360. Imunify360. Available from: <https://www.imunify360.com/> [Accessed 20 July 2022].
8. Kali.org nmap, Available at: <https://www.kali.org/tools/nmap/> [Accessed 23 July 2022]