Vulnerability Audit and Assessment - Results and Executive Summary

This paper will review and assess the vulnerability of *https://pchelpme.org.uk/* website. It will consist of the:

- Work carried out
- Findings
- Recommendations
- Conclusions

Work Carried Out

1). **STRIDE Threat Modelling: -**This modelling technique is a goal-based approach that identifies threats, the threat's security properties, the elements that will be affected from the threat and the countermeasures; as shown in the table below (Hernan, et al., N.D).

STRIDE	Threat Definition	Security Property	Elements Affected	Countermeasures
Spoofing	Faking identity so as to gain unauthorised access to data	Authentication	Processes, Interactors (end points of the system like users)	• Using strong authentication • Better handling and storage of log-in credentials • Protecting authentication cookies with

				Secure Sockets Layer (SSL)
Tampering	Unauthorised modification of data	Integrity	Data flows, Database, Processes	• Using data hashing and signing. • Using strong authorization • Using digital signatures • Securing communication links by using tamper-resistant protocols.
Repudiation	A user performing an action and later on denies performing it	Non-repudiation	Processes, Interactors (end points of the system like users)	• Creating secure audit trails. • Using digital signatures
Information Disclosure	Unauthorised access to information	Confidentiality	Dataflows, Databases, Processes	• Using strong authorisation • Using strong

				encryption • Securing communication links with protocols that enhance message confidentiality • Better handling and storage of log-in credentials
Denial of Service	Exhaustion of resources needed to perform a task or service	Availability	Dataflows, Databases, Processes	• Using resources and bandwidth control techniques • Validating and filtering of input
Elevation of Privilege	Unauthorised control of the system	Authorization	Processes	• Adhering to the principle of least privilege • Using least privileged service accounts to run

				processes and access resources.

Table 1:STRIDE Threat Model

2). **DREAD Model: -**This technique allows calculation of the impact of a security threat so as to prioritize it. Each threat is ranked from 1 to 10, then the additions of the score is divided to 5 (whereby the higher the score, the more priority it is given) (Anon, 2017)

- **D**amage potential- the impact done by the attack
- **R**eproducibility- how easily and often the attack can happen
- **E**xploitability- how easy it is for an attack to occur
- **A**ffected users- the number of users that can be affected by the attack
- **D**iscoverability- how easily the vulnerability can be found

3). **Cyber Kill Chain Model: -** This approach aids in combating an attack at every stage by laying out the stages of a cyberattack and the vulnerabilities. As from (Dholakiya, N.D.), the table below describes the model and security controls that can be placed:

Steps	Definition	Security Controls that can be used to:
Reconnaissance	The attacker studies that target and finds	• **Detect:** Web Analytics; Threat Intelligence; Network Intrusion

	tactics to be used for an attack	Detection System • **Deny:** Information Sharing Policy; Firewall Access Control Lists
Weaponization	Attackers develop malwares	• **Detect:** Threat Intelligence; Network Intrusion Detection System • **Deny:** Network Intrusion Prevention System
Delivery	Attackers deliver the malware by email	• **Detect:** Endpoint Malware Protection • **Deny:** Change Management; Application Whitelisting; Proxy Filter; Host-Based Intrusion Prevention System • **Disrupt:** Inline Anti-Virus • **Degrade:** Queuing • **Contain:** Router Access Control Lists; App-aware Firewall; Trust Zones; Inter-zone Network Intrusion Detection System
Exploitation	The malware is in the victim's system and its perimeter is	• **Detect:** Endpoint Malware Protection; Host-Based Intrusion Detection System

	breached	• **Deny:** Secure Password; Patch Management • **Disrupt:** Data Execution Prevention • **Contain:** App-aware Firewall; Trust Zones; Inter-zone Network Intrusion Detection System
Installation	Attacker gains access through the backdoor that was installed by the malware	• **Detect:** Security Information and Event Management (SIEM); Host-Based Intrusion Detection System • **Deny:** Privilege Separation; Strong Passwords; Two-Factor Authentication • **Disrupt:** Router Access Control Lists • **Contain:** App-aware Firewall; Trust Zones; Inter-zone Network Intrusion Detection System
Command and Control	Attacker gains control over the victim's systems and network	• **Detect:** Network Intrusion Detection System; Host-Based Intrusion Detection System • **Deny:** Firewall Access Control Lists; Network Segmentation • **Disrupt:** Host-Based Intrusion

		Prevention System • **Degrade:** Tarpit • **Deceive:** Domain Name System Redirect • **Contain:** Trust Zones; Domain Name System Sinkholes
Actions on objectives	Attacker gets data from the victim's system	• **Detect:** Endpoint Malware Protection • **Deny:** Data-at-Rest Encryption • **Disrupt:** Endpoint Malware Protection • **Degrade:** Quality of Service • **Deceive:** Honeypot • **Contain:** Incident Response

Table 2: Cyber Kill Chain Model

4). Scans performed:

a). Qualys SSL Labs tool: Is a free scanning tool used to test the website's configurations, vulnerabilities and Secure Socket Layer (SSL) certificates and protocols. (Kumar , 2022). The scan results had a high score, whereby the site:

i. Can be trusted and runs-on Mozilla, Apple, Android, Java and Windows.

ii. Has Transport Layer Security (TLS) 1.2 and 1.3 protocol

iii. Has Certificate Transparency, Downgrade attack prevention

b). Sucuri: Is a tool used to check for vulnerabilities and malwares in a website. The results showed that the site has a medium security risk whereby:

i. No malwares, inject spams, internal server errors were found

ii. Site is not blacklisted

iii. No Website Firewall and Monitoring was detected

iv. It suggested installation of security headers and a cloud-based Website Application Firewall (WAF)

c). HostedScan: Is a tool used to check for network vulnerabilities in a website whereby most TCP ports that were NMAP scanned returned a medium threat level.

d). ImmuniWeb: It scans a website for vulnerabilities and regulatory compliances. It discovered:

i. The website is not compliant to data privacy,

ii. Outdated jQuery and website CMS

iii. The TLS (https) is well encrypted

iv. Misconfigurations of Content Security Policy

Findings

The results of the work carried out indicate that:

Vulnerability Found	Attacks and Issues that can rise	Risk Severity
No firewall	• Denial of Service • Hacks e.g., brute-force • Spams (Danielle, 2016)	High
Outdated jQuery	• Denial of Service • Injection attacks • Bugs	High
No Data Privacy (GDPR) compliancy	• Loss of trust from clients • Lawsuits, Bans and Fines • Damage reputations (Wright, N.D.)	High
Lack of Security Headers e.g., Strict-Transport-Security security header.	• Denial of Service • Hacks • Sniffing	High
Lack of input validation	• Injection attacks • Compromised systems • Bugs • Cross-site scripting (Kaur & Kaur, 2014)	High
Lack of cybersecurity insurance	• Loss of trust from clients	**Medium**

	• Costly in case of a breach	

Table 3:Findings

Recommendations

Below are solutions and recommendations that work towards mitigation of cyber risks.

- Compliance to United Kingdom's standard Rules and Regulations, as mentioned by (Team Hallam, 2018):
    - General Data Protection Regulations (GDPR),
    - Companies Act 2006 (to identify businesses),
    - Company Policies and Procedures e.g., disclaimers, cookie disclosures, privacy policy.
    - Equality Act 2010 (Website Accessibility to everyone).
    - Respecting copyright.
- Multi-Factor Authentication (MFA), Authorization and Access Controls
- Programmers should be trained and prioritise secure coding by patching, upgrading software and utilities like jQuery, etc
- Validating Passwords and Inputs.
- Cryptography and Data Encryption. (Meier, et al., 2010)
- Implementation of Firewalls i.e.: Web Application Firewalls (WAF) (Singh, 2021)
- Endpoint Protection Software installation.
- Intrusion Detection Systems and Intrusion Penetration Systems

- Configuration management and updating of protocols, software, site source codes, etc
- Blocking spams and bots by using Plug-ins like CAPTCHA, the honeypot technique, etc (Johnston, 2016).
- Cybersecurity Awareness Trainings for the end-users.
- Registration to Cybersecurity Insurance covers that will protect the organization in case of a Cyberattack.

Conclusions

Even though some limitations like: lack of complete configuration and architecture of the network and system, were faced, this paper has still managed to provide the website's vulnerabilities and the different ways we approached to these results.

It has further described recommendations and solutions that can be done to patch up these vulnerabilities so as to ensure that the website is more secure from attacks.

It is therefore hoped that in the future we will work towards implementing the recommendations and perform more tests to ensure cybersecurity is achieved.

References

Anon, 2017. *Call to action and resources (threat modeling for drivers).* [Online]
Available at: https://docs.microsoft.com/en-us/previous-versions/windows/hardware/design/dn613894(v=vs.85)
[Accessed 20 July 2022].

Danielle, 2016. *What is a Firewall, and Why Do You Need It?.* [Online]
Available at: https://www.powderkegwebdesign.com/what-is-a-firewall/
[Accessed 24 July 2022].

Dholakiya, P., N.D.. *What Is the Cyber Kill Chain and How It Can Protect Against Attacks.* [Online]
Available at: https://www.computer.org/publications/tech-news/trends/what-is-the-cyber-kill-chain-and-how-it-can-protect-against-attacks
[Accessed 21 July 2022].

Hernan, S., Lambert, S. & Ostwald , T., N.D. *Uncover Security Design Flaws Using The STRIDE Approach.* [Online]
Available at:
https://docs.google.com/viewer?a=v&pid=sites&srcid=ZGVmYXVsdGRvbWFpbnxzZWN1cmVwcm9ncmFtbWluZ3xneDo0MTY1MmM0ZDI0ZjQ4ZDMy
[Accessed 16 July 2022].

Johnston, M., 2016. *6 Best Anti-Spam Plugins for your Website.* [Online]
Available at: https://www.cmscritic.com/6-best-anti-spam-plugins-for-your-website/

Kaur , N. & Kaur, P., 2014. Input Validation Vulnerabilities in Web Applications. *Journal of Software Engineering,* Volume 8, pp. 116-126.

Kumar , C., 2022. *SSL Test Certificate.* [Online]
Available at: https://geekflare.com/ssl-test-certificate/
[Accessed 21 July 2022].

Meier, J. D. et al., 2010. *Chapter 2 – Threats and Countermeasures.* [Online]
Available at: https://docs.microsoft.com/en-us/previous-versions/msp-n-p/ff648641(v=pandp.10)?redirectedfrom=MSDN

Singh, R., 2021. *What is a Website Vulnerability and How Can it be Exploited.* [Online]
Available at: https://www.indusface.com/blog/what-is-a-website-vulnerability-and-how-can-it-be-exploited/

Team Hallam, 2018. *Website legal requirements: laws and regulations in the UK (2018).* [Online]
Available at: https://www.hallaminternet.com/internet-marketing-and-the-law-legal-issues-affecting-you-and-your-website/

Wright, L., N.D.. *The severe ramifications of failing to comply with GDPR.* [Online]
Available at: https://www.core.co.uk/blog/blog/ramifications-failing-comply-with-gdpr#:~:text=Financial%20penalties,of%20a%20company's%20annual%20turnover.
[Accessed 24 July 2022].