Vulnerability Audit and Assessment – Baseline Analysis and Plan Document

After evaluating and assessing *https://pchelpme.org.uk/*, the following pages will provide insights and descriptions on the:

- Possible Security Vulnerabilities and Challenges,
- Methodologies, Tools and Approaches to be Considered and its Impacts on the Business.
- Standards, Recommendations and Solutions to Reinforce Security.

This ticketing website offers pc support, is UK based (due to '.uk' in its URL) and also allows the user to:

- 'Submit a ticket' by entering the user's name, email, and attach photos.
- 'View existing ticket' by entering a ticket tracking ID and email.
- Log in at the 'Administration Panel' using his/her credentials.

Additionally, it has a SPAM prevention feature that helps with mitigating SPAMs.

As from the above information, below is a description of possible security vulnerabilities and challenges that can hinder the security of the website:

- **Sensitive Data Exposure: -**Lack of adequate protection of sensitive information.
- **Broken Authentication and Session Management: -**Unauthorised access to information by bypassing the authentication (Singh, 2021).

- **Denial of Service (DoS) Attacks: -**Ticket creation requests can cause high resource consumption on the server; therefore, the high traffic of new ticket creation can lead to these attacks (Meyer, 2018).
- **Injection Attacks: -**Unauthorised access to the users' information by injecting malicious codes to SQL databases or URLs.
- **Security Misconfigurations: -**Happens when security controls and settings of the website's layers (application, server, etc) are not implemented properly (Singh, 2021).
- **Cross-Site Request Forgery (CSRF): -**Is where a user is tricked into performing an unintended action (Bassi, 2021).
- **Cross-Site Scripting: -**The attacker manipulates the web application so as to hijack the user's sessions (Atashzar, et al., 2011).

Below are the preferred methodologies, tools and approaches to a more secure website:

- **STRIDE threat modelling: -**For a goal-based approach to identifying threats (Geib, et al., 2022)
- **Cyber Kill Chain model:** -A penetration testing approach that helps in understanding and combating the attacks (Ranum, 2014).
- **DREAD model: -**Calculates the impact of a security threat. (Meier, et al., 2010)

- **Network and Wireless scans: -**Scans for network vulnerabilities and wireless interfaces and traffics using tools like: Traceroute, Nmap, Intruder, etc (Bechenea, 2021).
- **Host-based scans: -**Scans the host with tools like Host-based Intrusion Detection System (HIDS), hardware audits, log analysis (Kotagiri & Leckie, 2002)
- **Application and Database scans: -**Scans web applications and databases (Bocetta, 2020)

The standards, recommendations and solutions that can be implemented so as to reinforce security include:

- Adherence to United Kingdom’s standard Rules and Regulations, as covered by (Team Hallam, 2018), which are:
    - General Data Protection Regulations (GDPR),
    - Companies Act 2006 (for business identification),
    - Company Policies and Procedures e.g., cookie disclosure, privacy policy, disclaimers.
    - Equality Act 2010 (Website Accessibility to everyone).
    - Respecting copyright.
- Use of Multi-Factor Authentication and Authorization.
- Password and Input Validators.
- Cryptography and Data Encryption. (Meier, et al., 2010)
- Use of Firewalls like: Web Application Firewalls, AppTrana (Singh, 2021)
- Endpoint Protection Software

- Blocking spams and bots by using Plug-ins like CAPTCHA, the honeypot technique, etc (Johnston, 2016).
- Intrusion Detection Systems and Intrusion Penetration Systems
- Cybersecurity Awareness Trainings.

Business impacts on use of tools and methods include:

- Reveals vulnerabilities
- Build trust
- The cost of getting the software, hardware, workers, licenses, etc, will have to be factored in.
- Some techniques like internal and external scans, tests, etc., may cause disruptions like Denial of Service. Therefore, techniques with higher server consumption can be done during low traffic time and vice versa.
- Compliance
- Time taken for a vulnerability assessment, analysis and report preparation is 4-5 weeks and 3-5 months is usually the wait-time for vulnerability assessment to start.

Even though Automated testing saves a lot of manual effort, money and time; Manual analysis is still required to confirm vulnerabilities and find errors in business logic thus leading to getting the best results faster (Srinivas, 2018).

Once all the above is implemented, mitigation of cyber risks can be achieved.

References

Ranum, M. J., 2014. *Breaking Cyber Kill Chains.* [Online]
Available at: https://www.tenable.com/blog/breaking-cyber-kill-chains

Atashzar, H., Torkaman, A., Bahrololum, M. & Tadayon , M. H., 2011. *A survey on web application vulnerabilities and countermeasures.* Seogwipo, Korea (South), IEEE, pp. 647-652.

Bassi, B., 2021. *6 Common Website Security Vulnerabilities.* [Online]
Available at: https://www.commonplaces.com/blog/6-common-website-security-vulnerabilities/

Bechenea, D., 2021. *Website Vulnerability Assessment.* [Online]
Available at: https://pentest-tools.com/blog/website-vulnerability-assessment

Bocetta, S., 2020. *4 steps to conducting a proper vulnerability assessment.* [Online]
Available at: https://blog.candid.org/post/4-steps-to-conducting-a-proper-vulnerability-assessment/

Geib, J. et al., 2022. *Getting started with the Threat Modeling Tool.* [Online]
Available at: https://docs.microsoft.com/en-us/azure/security/develop/threat-modeling-tool-getting-started

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/

Kotagiri, R. & Leckie, C., 2002. *A probabilistic approach to detecting network scans.* Florence, Italy, IEEE, pp. 359-372.

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

Meier, J. D. et al., 2010. *Chapter 3 – Threat Modeling.* [Online]

Available at: https://docs.microsoft.com/en-us/previous-versions/msp-n-p/ff648644(v=pandp.10)?redirectedfrom=MSDN

Meyer, J., 2018. *Vulnerabilities Found in Popular Ticketing System.* [Online]

Available at: https://blog.securityevaluators.com/vulnerabilities-found-in-popular-ticketing-system-dd273bda229c

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/

Srinivas, 2018. *Automated Tools vs a Manual Approach.* [Online]

Available at: https://resources.infosecinstitute.com/topic/automated-tools-vs-a-manual-approach/

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/