Vulnerability Audit and Assessment - Baseline Analysis and Plan

1. Baseline assessment of the website with the potential security challenges

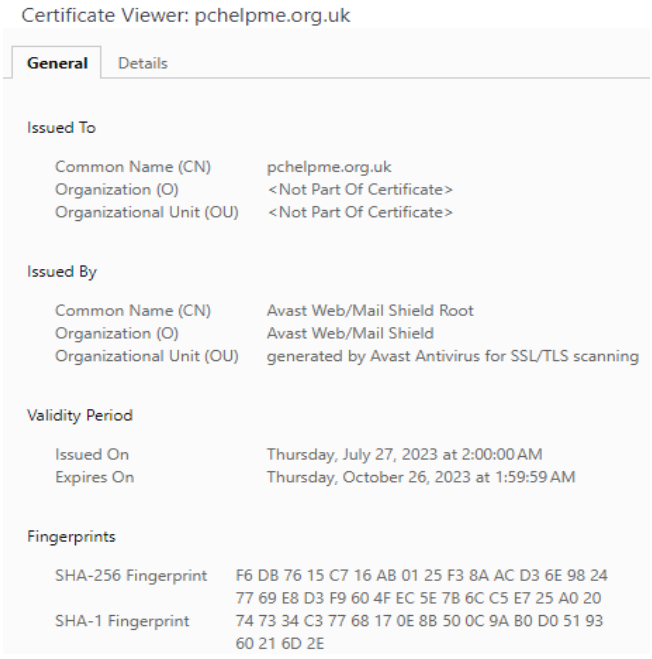
1.1 Website description

My choosen website offers support to computer-related questions (https://pchelpme.org.uk/). The website allows users to submit and view their tickets sent to the support centre. Within the submission form, the website requests for Name, Email, Priority, Subject, Message and two optional attachments. To prevent spamming, website utilizes Captcha mechanism. On the other hand to view a ticket one must enter tracking ID and Email. Finally the website has an Administration Panel with Username and Password fields for login. As a back-end service website uses PHP scripting language together with the Javascript and Softaculous manager.

1.2 Type of the business

The website doesn't have detailed description of what kind of support they offer for a PC, furthermore they don't have any contact information or GDPR compliance listed. From this aspect, the website doesn't seem trusted. Since they offer support to customers it would fall into category of consulting or community forum websites.

From more in-depth research, the website uses cookies, secure connection protocol (https) and Avast certficate (picture below)



1.3 Bulleted list of security challenges (generic plus ones specific to the business)

I have decided to sort OWASP top 10 risks by the vulnerabilities that I think we will be able to identify during the actual scanning, therefore we have two categories, generic one and the one specific to my choosen website (OWASP, N.D.).

Generic:

- Security Misconfiguration
- Vulnerable and Outdated Components
- Software and Data Integrity Failures
- Server-Side Request Forgery
- Cryptographic Failures
- Injection

Business specific:

- Broken Access Control
- Insecure Design
- Identification and Authentication Failures
- Security Logging and Monitoring Failures

1.4 List of standards appropriate to their business and any non-complience against those

1. ISO/IEC 27001GDPR -> The website has no information about control domains implementation, specified by Annex A (DataGuard, 2023).
2. GDPR -> The website does not provide information on how it processes sensitive data.
3. *CIS Benchmark / CIA Triad (Center for Internet Security, N.D.)

2. Tools that will be used and their impact on normal operations, caused by these tools

2.1 Selection of methods/tools (bulleted list with justification matching them against challenges)/approaches

- **Tracert/traceroute:** Getting information of route between two hosts**.** Some systems deliberately “hide” themselves, hence packages may get lost (until their time to live (TTL)).
- **Nslookup:** Retrieves DNS information.
- **Whoise:** To retrive information about website owner and its registration (JavaPoint, N.D.).
- **Nessus:** Scans for security vulnerabilities within network resources (Tenable, 2023). We are limited to perform the scanning remotely.
- **Intruder:** Automated network monitoring and vulnarability scanning software with threat response (Software Advice, N.D.).

2.2 Discussion & Methodology (remote or local, automated or manual, etc.)

The scanning will be performed remotely, hence external network scanning software will be used as we are not able to perform the scans on the host itself.

Most of the contemporary vulnerability scanning tools offer automated solutions. These are the first contact of "exploring" the network, while the manual tests would come into place when human factor is required in order to perform detailed intrusion detection operations, usually performed directly on the host.

I will use automated tools (Nesuss, Intruder) and manual approach to capture basic network data with the use of well known commands (tracert, nslookup, etc.).

2.3 Business impacts on use of tools and methods (scanning in or out of hours, traffic)

The extensive scanning will be performed on the weekend at the late afternoon, as I expect that this will be the time when the website encounters the least traffic.

3. List of assumptions and limitations of the tools and outputs produced

3.1 A summary of recommendations and potential mitigations that could be used to ameliorate any risks. These should be ordered by importance

Limitations from most to least important:

- The main limitation that I see is getting different output of risk reports, therefore false reflection of real risks. Different software may produce distinct results, hence it is important to try and compare different vulnerability scanning tools in order to ameliorate the risks of false outputs.
- Another pitfall resides on the fact that scanning tools are limited to perform the checks for which they have released the plugins (Tang, 2014).
- Limited knowledge of underlying infrastructure and network.
- Limited to perform only network scans. To ameliorate the latter, we should do the full scan on the host and perform Application/system scanning (Lecturecasts, 2023).

3.2 Timeline for the completion of the assessment tests and evaluation

9.10.2023 – 14.10.2023:

Extensive scanning (using command line tools, as well as the software)

14.10.2023 – 25.10.2023:

Performing risk analysis.

25.10.2023 – 29.10.2023:

Final evaluation with the result summary.

30.10.2023:

Assignment submission

References:

- Center for Internet Security. (N.D.). CIS Benchmark. Available from: https://www.cisecurity.org/cis-benchmarks [Accessed 06 October 2023]

- DataGuard. (2023). ISO 27001 Annex A controls - A detailed guide. Available from: https://www.dataguard.co.uk/blog/iso-27001-annex-a-controls [Accessed 06 October 2023]

- JavaPoint. (N.D.). Linux Whois. Available from: https://www.javatpoint.com/linux-whois [Accessed 07 October 2023]

- OWASP Top 10. (N.D.). Top 10 Web Application Security Risks. OWASP. Available from: https://owasp.org/www-project-top-ten/# [Accessed 06 October 2023]

- PcHelpMe. (N.D.). Pc Help Me. Available from: https://www.pchelpme.org.uk/ [Accessed 04 October 2023]

- Software Advice. (N.D.). Intruder. Available from: https://www.softwareadvice.com/vulnerability-management/intruder-profile/ [Accessed 06 October 2023]

- Tang, A. (2014). A guide to penetration testing. Network Security, 2014(8), 8–11. Available from: doi:10.1016/s1353-4858(14)70079-0 [Accessed 07 October 2023]

- Tenable. (2023). The Global Gold Standard in Vulnerability Assessment Built for the Modern Attack Surface. Available from: https://www.tenable.com/products/nessus [Accessed 06 October 2023]

- University Of Essex Online. (2023). Vulnarability Assessments. Lecturecasts. [Accessed 04 October 2023]