Table of Contents

1 Vulnerability Audit and Assessment - Baseline Analysis and Plan

1.1 Security challenges

Below is a list of potential security challenges:

1. Passwords threats, including allowing weak passwords, storing them in unencrypted form, and not requiring frequent changes (Bonneau, Herley, & van Oorschot, 2012).

2. Weak database software security measures, including weak access controls, lack of encryption, and lack of backup and recovery measures (Singh, Haridass, & Reddy, 2012).

3. Structured query language (SQL) injection attacks (Schultz, 2002).

4. Cross-site-scripting (XSS) attacks (Barth et al., 2005).

5. Insufficient logging and monitoring (Lippmann et al., 2000).

6. Unvalidated inputs, leaving the potential for code injection and buffer overflows etc. (Schneier, 2000).

7. Third-party component vulnerabilities on all software used (Frei, Christey, & Mohan, 2002).

8. Phishing and pretexting attacks on admin staff (Whittaker & Tygar, 2000).

9. Open port exploits (Schneier, 2003)

1.2 Tools that can be used to mitigate the challenges

Table 1: List of potential tools to address security challenges

Tool	Brief Description	Addresses Security Challenge
SQLMap	Automated SQL injection tool	2, 3
OWASP	Web application security testing framework	2, 3, 4, 6, 7
Burp Suite	Web vulnerability scanner and testing platform	4, 6
Nexus Vulnerability Scanner	Vulnerability scanning tool for web applications	7
Gophish	Open-source phishing toolkit	8
Nmap	Network exploration and security auditing tool	9
Nessus	Vulnerability scanner for various systems and devices	9
OpenVAS	Vulnerability assessment system for networks and devices	9
Metasploit	Framework for security and penetration testing	9
Kali Linux	Open source operating system with a range of cyber security tools	2, 3, 4, 5, 6, 7, 8, 9

1.3 Methodology and Discussion of Tools/Methods and Approaches

The assessment of the website will be done remotely, mainly with the use of automated tools, supplemented with manual tools where necessary. The methodology used will consist of two main stages, namely, “Analysis” in which the website will be analyzed, and “Reporting” in which the results of analyses will be collated and formalized.

The ”Analysis” stage will be based on the Cyber-Kill-Chain model (Tarnowski, 2017), whereby the assessment will aim to investigate the viability of the initial phases of the model, including, reconnaissance to gather information, weaponization and delivery (“scanning and analysis”) to devise and deliver attack vectors identified, and exploitation to determine if the attack vectors are successful, keeping in mind that no damage will be done, and the aim will be purely to investigate exploit viability.

1.4 Selection of methods/tools/approaches and business impact on use of tools and methods

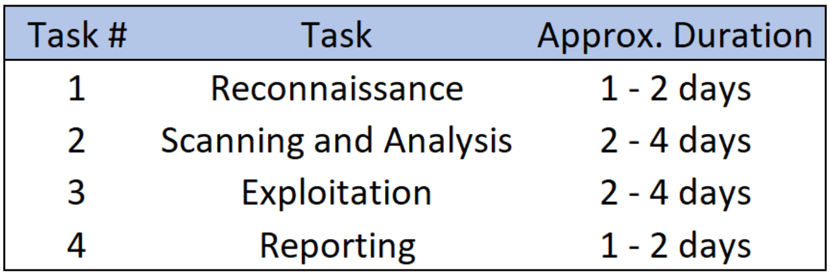
The tools used in this assessment will mainly be Kali Linux, SQLMap, OWASP and Nmap which provide a range of capabilities when assessing the security challenges mentioned previously (Uddin & Lee, 2017).

Several considerations have to be made with regards to the impact of these analyses on the business including:

- Scanning during work hours, which can slow down the website and will be done minimally.
- Automated scans and tools can generate false positive and negative results, requiring manual validation and potentially affecting the accuracy of the results. This will have to be clearly pointed out in the final report.
- Web security software and personnel may be alerted as scans are being carried out; personnel will have to

1.5 Timeline of the completion of the task

Table 2: Timeline of analysis and scanning plan



Task #	Task	Approx. Duration
1	Reconnaissance	1 - 2 days
2	Scanning and Analysis	2 - 4 days
3	Exploitation	2 - 4 days
4	Reporting	1 - 2 days

1.6 Summary of limitations and assumptions.

1.6.1 Limitations:

- Automated scans and tools can generate false positive and negative results,
- The time and resources available for the assessment may limit the scope and depth of the assessment.
- The website and its infrastructure can change during the course of the assessment, affecting the results.
- Technical Limitations: The assessment may be limited by the skills and expertise of the tester.

1.6.2 Assumptions:

- The website is currently under attack or at risk of attack.
- The tester has no access to internal systems or data, and has no prior knowledge of the website or its infrastructure.
- Testing will not interfere with the normal website operations.

2 References

Barth, A., Jackson, C., & Mitchell, J. (2005). Robust defenses for cross-site scripting. Proceedings of the 2005 ACM workshop on Web application security. New York, NY, USA: ACM.

Bonneau, J., Herley, C., & van Oorschot, P.C. (2012). Password policies are hardly ever followed. Proceedings of the 2012 ACM conference on Computer and Communications Security. New York, NY, USA: ACM.

Frei, R., Christey, S., & Mohan, N. (2002). Analysis of third-party component vulnerabilities in commercial software. Proceedings of the 2002 ACM workshop on Computer security. New York, NY, USA: ACM.

Lippmann, R.P., Ortiz, R.R., Osborn, J.A., &Karlof, C. (2000). An evaluation of diagnostic approaches to the intrusion detection problem. Proceedings of the 2000 DARPA information survivability conference and exposition. Los Alamitos, CA, USA: IEEE Computer Society.

Schneier, B. (2000). Cryptographic standards and random numbers. Proceedings of the 2000 workshop on fast software encryption. Berlin, Heidelberg: Springer.

Schneier, B. (2003). Port scanning is not a crime. Communications of the ACM, 46(7), 108-116.

Schultz, E. (2002). SQL injection attacks. Proceedings of the 2002 workshop on practical issues in computer security. New York, NY, USA: ACM.

Singh, C.A., Haridass, S., & Reddy, V.K. (2012). SQL injection attacks and defense. Journal of Network and Computer Applications, 35(3), 801-813.

Tarnowski, I., 2017. How to use cyber kill chain model to build cybersecurity?. European Journal of Higher Education IT.

Uddin, M., & Lee, J. (2017). A systematic review of website security assessment methods. Journal of Information Security and Applications, 36, 68-82.

Whittaker, J. & Tygar, J.D. (2000). Phishing and pretexting. Proceedings of the 2000 workshop on new security paradigms. New York, NY, USA: ACM.