Vulnerability Audit and Assessment - Baseline Analysis and Plan

Overview

The aim of the audit is to identify security weaknesses and evaluate their implications regarding the Security Tweets website found at https://testhtml5.vulnweb.com/#/popular, which is a social media web application.

Introduction

Cyber security is a critical concern for both users and developer of web-applications: Users will need to protect their identity with strong passwords and be aware of being vulnerable to social engineering attacks; developers will need to ensure they protect personal information in line with the GDPR requirements (ICO, 2024) and stay up to date with the latest risks, such as those published by OSWAP and their solutions (OSWAP, 2021). Companies can inspire confidence with stakeholders by obtaining industry standard certification such as Cyber Essentials Plus from the British Assessment Bureau (NCSC, 2023). By contrast, there has been on-going controversy regarding the harvesting and use of personal data by TiKTok where users are not protected by the GDPR or other legislation. 'The Chinese government has easy access to their [users] personal information based on its domestic law and resolve on intelligence gathering for the protection of its national security.' (Uya, 2024).

Security Vulnerabilities

Vulnerability	Threat	Description	Solution
1. Unauthorised Access	Users access admin functionality	Users gain access to modules and functions which are not needed for their role	Role Based Permissions
2. Insecure Passwords	Identify fraud; Spoofing; Reputational damages	Intruders access other users' accounts with access to personal information	Establish Password policy
3. Ineffective Firewall	Sensitive data can be stolen	Malware can penetrate the system an insert	Implement Firewall Policy and

Vulnerability	Threat	Description	Solution
		malicious code to eavesdrop or steal data	checking protocols. Architecture Threat Modelling.
4. Backdoor Access	Intruder can access and modify source code	Intruders access the system through an	Code Analysis
5. Social Engineering	Legitimate users share their data with unauthorised intruders	Phishing emails are sent to users, persuading them to share personal data	User Education Program
6. Denial of Service	Users can not access the application	Servers are overloaded by repeated requests, such as Ping of Death	Scanning and blocking potential intruders via an Intrusion Detection Service (IDS)
7. Third Party Developers	Persona Data is disclosed to third party developers	Third Party Applications access unnecessary personal data in development.	Use of API Sandbox for third party developers.
8. Insider Threat	Sensitive data or code is disclosed to unauthorised actor.	Employees share log-in details, code or sensitive information	Hardware asset management. Network scanning. Acceptable use of IT policy. Activity logging and monitoring.

Methodology and Tools

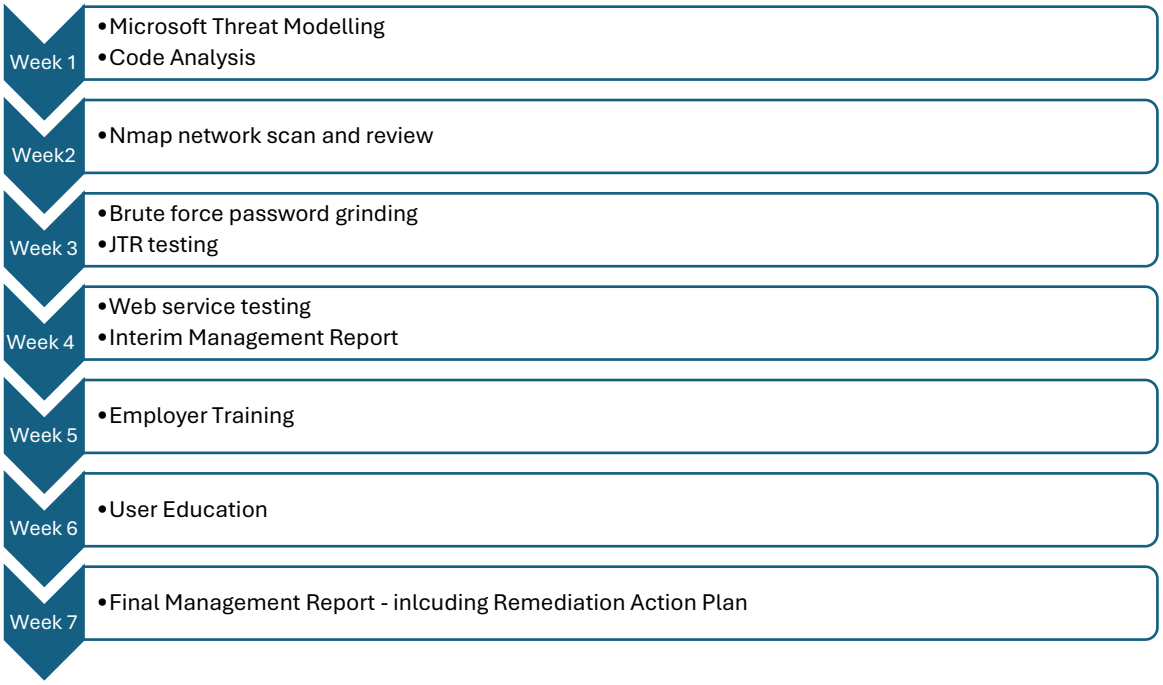
Tool/Method	Justification	Challenge	Dynamic/ Static
1. Microsoft Threat Modelling Tool	Identify STRIDE risks for secure web applications	Insecure design architecture	S
2. Nmap	Network scanning tool	Identify network vulnerabilities	D

Tool/Method	Justification	Challenge	Dynamic/ Static
3. Hydra	Brute force password grinding	Evaluate password strength	D
4. John the Ripper (JTR)	Obtaining sensitive data	Evaluate security of passwords and sensitive data	D
5. Web service testing	Check against elevated privileges	Users access information/functionality beyond their role privilege	D
	Check security of API	Insecure API for third party development	D
6. Code Threat	Code Analysis	Evaluate code against known threats	S
7. Employee Education	Ensure staff understand importance of working securely	Insider threat	S
8. User Training	Raise awareness of social engineering attacks such as phishing.	Social Engineering	S

Business Impact

Nmap scanning and other dynamic actions will take place outside of peak usage hours, to minimise disruption to the service (McNab, 2017). Users access social media 24hours per day, but the actions will be aligned to blocks of 4-hour access time where time blocks are RAG rated based on an audit of server traffic.

Timeline



Summary and Limitations

The cyber-security audit will allow the management team to evaluate the effectiveness of the hardware architecture, the security of the application and the impact of existing policies and processes to achieve security in the workplace. The cyber threat surface is constantly evolving and while all actions will be in-line with OSWAP guidance and ISO/IEC 27002 standards regular reviews are recommended. While the user education and training will raise awareness, it cannot guarantee compliance against malicious use.

References

Alshamrani, A. et al. (2019) 'A survey on advanced persistent threats: Techniques, solutions, challenges, and research opportunities', *IEEE Communications Surveys & Tutorials*, 21(2), pp.1851-1877.

Bennouk, K. et al. (2024) 'A Comprehensive Review and Assessment of Cybersecurity Vulnerability Detection Methodologies', *Journal of Cybersecurity and Privacy*, 4(4), pp.853-908.

Dewhurst, R. (2013). *Static Code Analysis* | *OWASP*. Available at: https://owasp.org/www-community/controls/Static_Code_Analysis [Accessed 08 February 2025]

ICO (2024). UK GDPR guidance and resources. Available at: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/ [Accessed 08 February 2025]

Kaufman, C. et al. (2022) *Network Security: Private Communications in a Public World.* Addison-Wesley Professional

Lachkov, P., Tawalbeh, L.A. and Bhatt, S. (2022) 'Vulnerability assessment for applications security through penetration simulation and testing', *Journal of Web Engineering*, 21(7), pp. 2187-2208.

McNab, C. (2017). *Network Security Assessment: Know your Network*. 3rd ed. Beijing: O'Reilly Media

National Cyber Security Centre (2023). *Cyber Essentials: Requirements for IT infrastructure v3.1.* Available at: Cyber-Essentials-Requirements-for-Infrastructure-v3-1-April-2023.pdf [Accessed 08 February 2025]

OSWAP (2021). *Top 10 Web Application Security Risks*. Available from: OWASP Top Ten | OWASP Foundation [Accessed 08 February 2025].

Sinha, S. (2017). *Beginning ethical hacking with Python*. West Bengal: Apress

Spraul, V.A. (2015). *How Software Works: The Magic Behind Encryption, CGI, Search Engines, and Other Everyday Technologies*. San Francisco: No Starch Press.

Uya, F. (2024). *Cybersecurity and Social Media: Does TikTok Pose Cybersecurity Risk to the United States?* Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4784942 [Accessed 08 February 2025]