Baseline Analysis and Plan for http://demo.testfire.net/

General Considerations

When evaluating a website for vulnerabilities, security concepts should be considered to help define areas of concern. The CIA (Confidentiality, integrity and availability) triad forms the basis of how data and systems should be approached (Shelley & Gibson, 2023). Does the website promote this? AAA (Access control, authentication, and accounting) supports CIA through controlling and monitoring resource interaction (Sadiqui, 2020). Does the website follow this? Finally, website design should be considered; does the site mitigate common web security risks (OWASP, 2021).

General Security Risks and their Area of Concern

SECURITY RISK	AREA OF CONCERN
Broken Access Control	Access Control
Cryptographic Failures	Confidentiality
Injection Attack	Integrity / Availability
Misconfiguration	All
Outdated Components	All
ID & Authentication Failures	Integrity, Access Control & Authentication
Logging & Monitoring Failures	Accounting

Online Banking Risks

For online banks serious risks are those that attack CIA components:

- Sensitive data stored without encryption.
- Malicious actors altering data.
- Questionable data reliability.
- Inability to access funds.
- Insecure transfer of funds.

Banks must adhere to regulatory standards. GDPR (General Data Protection Regulation) regulates how data of European citizens is processed (European Union, 2016). PSR (The Payment Services Regulation) adherence is required for UK government authorisation (UK Government, 2017).

Website Expectations

To evaluate website security, expectations should be set for existing security elements. The following table shows elements recommended in government frameworks and expected counters to the most common vulnerabilities (NCSC, 2018; NCSC, 2021;

OWASP, 2021). These frameworks have existed for over 3 years, enough time to have met the expectations.

SECURITY ASPECT	EXPECTED ELEMENT
Authentication Management	Multi-factor Authentication
Passwords	Minimum length
Brute Force Password Attack	Account lockout
Password Storage	Stored as hash
Data in Transit	Use of HTTPS
Outdated Systems	Update policy
Injection Attack	Input validation
Outdated Cryptographic Protocol	Minimum TLS 1.2.

Testing Approach and Tools

A remote external approach has been selected and will be based in part upon recommendations given by NIST, starting with reconnaissance, then enumeration, before vulnerability testing (Scarfone et al., 2008). Kali Linux will be the operating system due to its inherent library of tools.

Automated and manual testing will be used. Testing is planned to be minimally invasive and disruptive, however some scans are performance / resource intensive; these scans will take place outside peak business hours.

Testing time is approximately one week. This is given response time to a phishing email that will be sent out, after sourcing employee details. Scanning will be conducted during this time. A report will be produced after one further week.

Testing Tools

TOOL	STAGE / CHALLENGE	ALTERNATIVE	REASONING
theHarvester	Reconnaissance	Recon-ng	Recon-ng has more features, many are duplicated in other tools selected. theHarvester sources email addresses for use in a phishing attack.
Dig	Reconnaissance	Nslookup	Dig selected for DNS searching. More detailed output and more customizable than Nslookup.
WHOIS	Reconnaissance	N/A	Searches database of domain names and owners.
Nmap	Enumeration	Angry IP Scanner	Nmap chosen for extra functionality. For port scanning and OS detection.
Zap	Vulnerability Scanning	Burp suite	Chosen due to being open-source, free to use, and links to

	the OWASP Top Ten web application security risks (OWASP, 2021).

Tool Limitations and Challenges

The tools shown are some of the tools that will be used. Others may be used to supplement the data returned, or to counter limitations and challenges experienced.

theHarvester does not sort returned data. This may result in a large amount of obsolete data that will need time to sort. All its data is from public sources. If email addresses of employees are private, they cannot be accessed.

Nmap has multiple limitations. Firewalls / IDS' can block network scanning. Scanning can impact website performance.

The WHOIS protocol's use in reconnaissance has been noticed, leading to security notes in its documentation (Daigle, 2004). Subsequently fewer users add their details.

ZAP can be resource intensive, affecting usage scheduling (Checkmarx, 2025).

Word Count: 645

References

Checkmarx (2025) *Zap Documentation*. Available at: https://www.zaproxy.org/docs/ (Accessed 16 February 2025).

Daigle, L. (2004) *WHOIS Protocol Specification*. RFC 3912. Available at https://datatracker.ietf.org/doc/html/rfc3912 (Accessed 14 February 2025).

European Union. (2016) *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*. Official Journal of the European Union, L119, 1 – 88. Available at: https://eur-lex.europa.eu/eli/reg/2016/679/oj (Accessed 17 February 2025).

Gibson, D. & Shelley, J. (2023) *CompTIA Security+: Get Certified Get Ahead SYO-701 Study Guide*. United States: Certification Experts LLC.

IBM. (2024) *dig Command*. Available at https://www.ibm.com/docs/en/aix/7.3?topic=d-dig-command (Accessed 16 February 2025).

IBM. (2024) *nslookup Command*. Available at https://www.ibm.com/docs/en/aix/7.3?topic=n-nslookup-command (Accessed 16 February 2025).

Lyon, Gordon. (2009) *Nmap Network Scanning: Official Nmap Project Guide to Network Discovery and Security Scanning*. Sunnyvale, CA, USA: Insecure.

Martorella, C. (2025) *theHarvester*, GitHub. Available at https://github.com/laramies/theHarvester (Accessed 16 February 2025).

National Cyber Security Centre (2018) *Password administration for system owners*. Available at https://www.ncsc.gov.uk/collection/passwords/updating-your-approach#tip2-password-collection (Accessed 16 February 2025).

National Cyber Security Centre (2021) *10 Steps to Cyber Security*. Available at https://www.ncsc.gov.uk/collection/10-steps/data-security (Accessed 16 February 2025).

Scarfone, K. et al. (2008) Technical Guide to Information Security Testing and Assessment (National Institute of Standards and Technology, Gaitherburg, MD), NIST Special Publication (SP) 800-115. Available at: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf (Accessed 16 February 2025).

OWASP Foundation. (2021) *OWASP Top Ten*. Available at https://owasp.org/www-project-top-ten/ (Accessed 15 February 2025).

Portswigger. (2023) *Burp Suite Documentation*. Available at https://portswigger.net/burp/documentation (Accessed 15 February 2025).

Sadiqui, A. (2020) *Computer network security*. London, England: Wiley-ISTE.

Shehab et al. (2024) Assessment of Cybersecurity Risks and threats on Banking and Financial Services. *Journal of Internet Services and Information Security (JISIS)*, 14(3), pp. 167-190. Available at: DOI: 10.58346/JISIS.2024.I3.010

Temoshok, D., et al. (2024) Digital Identity Guidelines (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-63-4 2pd. Available at: https://doi.org/10.6028/NIST.SP.800-63-4.2pd

Tomes, T. (2024) *recon-ng,* GitHub. Available at https://github.com/lanmaster53/recon-ng (Accessed 16 February 2025).

UK Government. (2017) *The Payment Services Regulations 2017 (SI 2017/752).* Available at https://www.legislation.gov.uk/uksi/2017/752/introduction (Accessed 15 February 2025).