**Vulnerability Audit and Assessment - Baseline Analysis and Plan**

# Introduction

This document provides a baseline plan for a vulnerability assessment of the website <https://ehr-online.co.uk/> to **identify** its security-related **vulnerabilities** via penetration testing and **enhance** its **security and effectiveness** (Nixon, 2021).

# Security challenges

As per the European Union (EU) “General Data Protection Regulation” (GDPR), which protects the data of European citizens (Hussain *et al.*, 2020):

1. **Weak passwords** could be retrieved by unauthorised third parties due to built-in applications or unsafe add-ons.
2. **Injection faults** and **cross-site scripting** may respectively place server- and client-side data at risk.

As per the standard “ISO/IEC 27001:2005” to ensure customers’ data’s security (ISO, 2013):

1. Customers’ data may be accessed due to **compromised application-related accounts**.

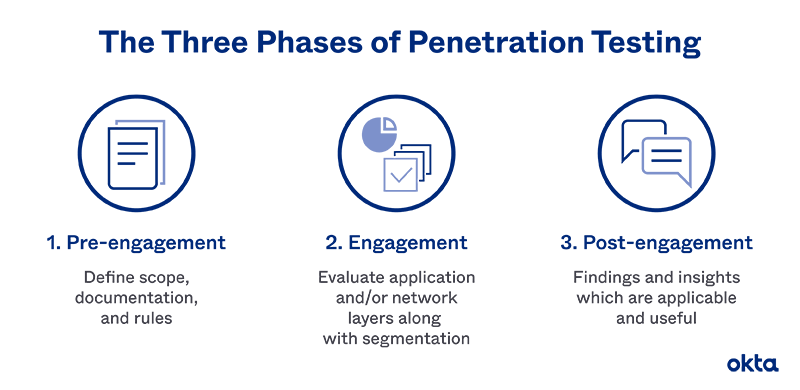
As per the **business-relevant** EU regulation “Medical Device Regulation” (MDR), considering storage and processing of electronic health records (EHR) (Chiara, 2022):

1. Personally identifiable information (**PII**) **and health data** may be **leaked** due to inadequate encryption and blind spots in encrypted traffic.

# Tools

As per the three-phase penetration testing (**Fig. 1**) via the “Penetration Testing Execution Standard” (PTES, 2017) framework:

* During **pre-engagement**: This document will be re-reviewed and used to assess the security challenges in section 2.
* In the **engagement phase** (OWASP, 2021; Sheikh, 2021):
  + **WHOIS**, **Traceroute**, and **NSLookup** will identify the website’s owner, the hosts, the locations and types of servers, etc.
  + **NMAP** will retrieve the ports, MAC addresses, operating system, etc.
  + **BuiltWith** will list the website’s technologies.
  + **Burp Suite** and the “Open Web Application Security ProjectZed Attack Proxy” (**OWASP ZAP**) will detect any of OWASP’s top ten vulnerabilities, as matched to challenges 1-3 in section 2.
  + **Dirstalk** will detect sensitive information on the website, as matched to challenge 4 in section 2.
* In **post-engagement**: A report will summarise the risks identified and recommendations to mitigate them (Mahmood *et al.*, 2022).



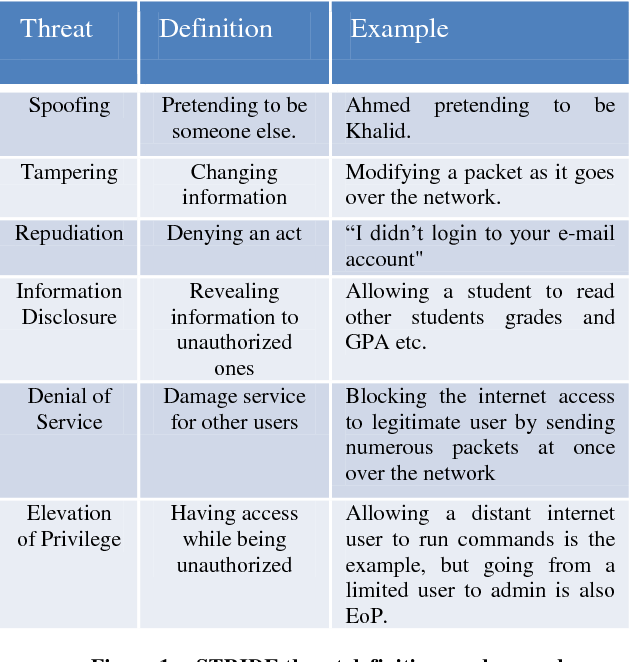
**Figure 1**. Three-phase penetration testing (Okta, 2022).

# Methodology

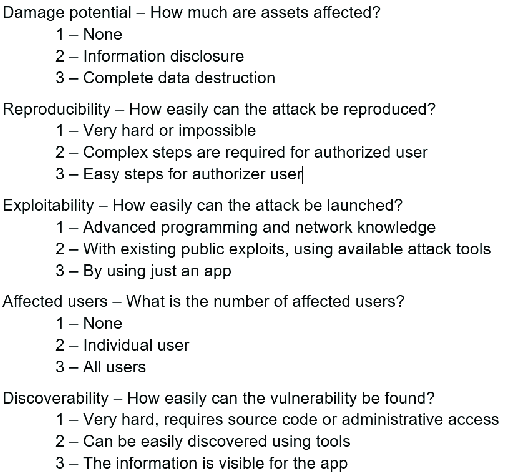
As only the website’s public information can be accessed, **remote** black-box penetration testing (Chapple *et al.*, 2018) will be performed as per the OWASP (2021) and PTES (2017) frameworks. More comprehensive findings and recommendations will be derived via both **manual and automated** tests (Mahmood *et al.*, 2022).

# Approaches

Via the **AWS Well-Architected Framework**’s (Pillar, 2018) and the **STRIDE threat models** (**Fig. 2**), security vulnerabilities will be identified (Khan, 2017). Such threats will be ranked via the **DREAD model** (**Fig. 3**) based on their business impact (Gómez-Hernández *et al.*, 2021).



**Figure 2**. STRIDE model (Khan, 2017).



**Figure 3**. DREAD model (Gómez-Hernández *et al.*, 2021).

# Business impact

Multiple cyber-attacks simulated via penetration testing, transmitting data to web resources, may disrupt system and business operations (Chapple *et al.*, 2018):

* The website’s **performance** may be **lower** than usual.
* The website may become **unavailable at times** due to denial of service (DoS).
* **Sensitive data** may be **leaked**.
* Automated testing may **inject garbage data** in the website’s database**.**
* **Data** may be **inadvertently deleted** from its database.
* **Email flooding** may occur.
* **Several error logs** could be generated, as unexpected or random data may be used in simulated requests.

To partly mitigate such impacts, scanning tools will be **configured not to access sensitive links** and tests will be performed **outside UK business hours** (Leszczyna, 2021).

# Timeline

The project’s timeline is illustrated in **Fig. 4**.

Graphical user interface

Description automatically generated with low confidence

**Figure 4**. Project’s timeline.

# Limitations and assumptions

## 8.1. Assumptions

* The tools and methodology in sections 3-5 are **appropriate**.
* The website is always **available**.
* Multiple approaches will be leveraged for **effective testing**.

## 8.2. Limitations

* The tests may **not** be **exhaustive**.
* This task will be completed in **three weeks**.

**References**

Chapple, M., Stewart, J. M., & Gibson, D. (2018) *(ISC) 2 CISSP Certified Information Systems Security Professional Official Study Guide*. John Wiley & Sons.

Chiara, P. G. (2022) The IoT and the new EU cybersecurity regulatory landscape. *International Review of Law, Computers & Technology*: 1-20.

Gómez-Hernández, J. A., Camacho, J., Holgado-Terriza, J. A., García-Teodoro, P., & Maciá-Fernández, G. (2021) ARANAC: A Bring-Your-Own-Permissions Network Access Control Methodology for Android Devices. *IEEE Access*, 9: 101321-101334.

Hussain, F., Hussain, R., Noye, B., & Sharieh, S. (2020) Enterprise API security and GDPR compliance: Design and implementation perspective. *IT Professional*, 22(5): 81-89.

Khan, S. A. (2017). A stride model based threat modelling using unified and-or fuzzy operator for computer network security. *International Journal of Computing and Network Technology*, 5(01): 13-20.

ISO (2013) ISO/IEC 27001:2013. Information technology - Security techniques - Information security management systems - Requirements. Retrieved from: <https://www.iso.org/standard/54534.html>. Last accessed on June 28th, 2022.

Leszczyna, R. (2021) Review of cybersecurity assessment methods: Applicability perspective. *Computers & Security*, 108: 102376.

Mahmood, S., Nguyen, H. N., & Shaikh, S. A. (2022) Systematic threat assessment and security testing of automotive over-the-air (OTA) updates. *Vehicular Communications*, 35: 100468.

Nixon, I. K. (2021) Standard penetration test State-of-the-art report. In *Penetration testing* (pp. 3-22). Routledge.

Okta (2022) Penetration testing. Retrieved from: <https://www.okta.com/uk/identity-101/penetration-testing/>. Last accessed on June 29th, 2022.

Pillar, R. (2018) AWS well-architected Framework. *Amazon Web Services*, 45.

PTES (2017) PTES Technical Guidelines. Retrieved from: <http://www.pentest-standard.org/index.php/PTES_Technical_Guidelines>. Last accessed on June 30th, 2022.

Sheikh, A. (2021) Penetration Testing. In *Certified Ethical Hacker (CEH) Preparation Guide* (pp. 189-196). Apress, Berkeley, CA.