PHI - Web Application – Vulnerability assessment using penetration testing

Overview:

A penetration test, or "pen test," simulates a cyberattack on your computer to find vulnerabilities. Web application firewalls are often supplemented by penetration testing (WAF). Pen testing involves breaking into application systems, such as APIs or frontend/backend servers, to find vulnerabilities, such as uncleaned inputs that could be used in a code injection attack. You can tweak your WAF security policies based on the penetration test results. (Imperva.com 2022)

Scope:

This design document includes a WPT plan, testing method, and rules. The document lists security holes in LibreHealth medical's web portal https://ehronline.co.uk/interface/login/login.php?site=default and tools to exploit them. Our approach and assumptions are listed, along with a testing and report-writing timeline.

Penetration Testing Execution Standard:

According to the Penetration Testing Execution Standard (PTES), there are seven steps to penetration testing. In particular, the PTES Technical Guidelines give hands-on tips on how to test and suggestions for security testing tools. (owasp.org 2022)

Project Stages:

- Pre-engagement Interactions
- Intelligence Gathering
- Threat Modeling
- Vulnerability Analysis
- Exploitation
- Post Exploitation
- Reporting

After finding application vulnerabilities, we examine each one in detail and make security recommendations. (owasp.org 2022) The project timeline is in Figure 3.

Threat Modelling:

STRIDE will be used to model threats, security vulnerabilities, and inappropriate defenses. Figure 2 of the appendix shows the STRIDE modelling process, which determines the site's security objectives and threats. (docs.microsoft.com 2022) We use

DREAD to identify and evaluate potential risks. (David Kohanbash 2016) Figure 3 of the appendix shows the vulnerability scale.

Regulatory Compliance

In our report, we'll tell customers how to comply with the three regulations below.

- **General Data Protection Regulation** EU law that gives customers more control over personal data collection and storage. Potential vulnerabilities include compromised or stolen credentials (from commercially available software, apps, and plugins) and application vulnerabilities (such as potential for injection, privilege escalation and cross-site scripting). (gdpr.eu 2022)

- **ISO 271001**: a framework for managing information technology security that helps keep customer data safe in both the private and public sectors. This standard was formerly known as ISO/IEC 27001:2005.
` Potential vulnerabilities: The theft of data.

- **PCI DSS**, or the Payment Card Industry Data Security Standard, is a set of technical rules set by the Payment Card Industry Security Standards Council to protect cardholder data.
  Theft of cardholder data is a possible vulnerability. (PCIsecuritystandards.org 2008)

- **HIPAA,** HIPAA is a federal law that requires national standards to protect sensitive patient health information from being disclosed without the patient's consent or knowledge. The HHS Privacy Rule implements HIPAA's requirements. The Security Rule protects some Privacy Rule information. (cdc.gov 2022)

Tool deployment strategy:

- **Pre-engagement**: This document describes the objectives and scope of the Pentest.

- **Information Gathering:** Vulnerability Cross-site scripting, SQL Injection, Command Injection, Path Traversal, and insecure server configuration are scanned for from the outside. This category includes DAST tools. This commercial and open-source tool has pros and cons. OWASP Benchmark evaluates vulnerability detection tools, including DAST. (owasp.org 2022)
- **Threat Modelling:** STRIDE is a prompt for a set of threats – Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service (DoS), and Elevation of Privilege (Microsoft.com 2022)

- **Vulnerability Analysis:** We identify potential vulnerabilities (OWASP Top 10) using Burp Suite, a directory and file-searching tool. (owasp.org 2022)
- **Exploitation phase:** We breach the website using automated and manual penetration tools and techniques. We exploit security weaknesses to gain control of the host server, elevate user privileges, or launch a denial-of-service attack. (Gauravit.org 2022)
- **Post Exploitation:** We record attack methods and screenshots. We'll gather information about the exploited system, identify and document interesting files, try to elevate privileges, and explore other machines or applications on the network. (geeksforgeeks.org 2020)
- **Reporting:** Our Pentest Report will include Summary, Technical Detail, Findings, Risk Level Indication, and Time Estimation.

Assumptions:

- Portal is always available for testing.
- Multiple tests are allowed.
- We can't predict all attack scenarios, so we'll only test the most common ones.

References:

1. Imperva.com (2022) Penetration testing and web application. Available from: https://www.imperva.com/learn/application-security/penetration-testing/ [Accessed 1st July 2022]
2. owasp.org (2022) Penetration Testing Execution Standard. Available from https://owasp.org/www-project-web-security-testing-guide/latest/3-The_OWASP_Testing_Framework/1-Penetration_Testing_Methodologies [Accessed 2nd July 2022]
3. owasp.org (2022) Vulnerability scanning tools Available at: https://owasp.org/www-community/Vulnerability_Scanning_Tools [Accessed 1st July 2022]
4. docs.microsoft.com STRIDE model. Available at: https://docs.microsoft.com/en-us/azure/security/develop/threat-modeling-tool-threats [Accessed 2nd July 2022]
5. David Kohanbash on August 26, 2016 DREAD, Available at https://www.robotsforroboticists.com/book-review-car-hackers-handbook-craig-smith/dread/ [Accessed 1st July 2022]
6. GDPR.EU Article 13, Available at: https://gdpr.eu/article-13-personal-data-collected/ [Accessed 29 June 2022]
7. ISO/IEC (2013) Information technology Security techniques Information security management systems Requirements. Available from: https://www.iso.org/standard/54534.html [Accesssed 30th June 2022]
8. PCI (2008). Payment Card Industry Security Standards. Available from: https://www.pcisecuritystandards.org/pdfs/pcissc_overview.pdf [Accessed 30th June 2022]
9. Cdc.gov HIPAA Privacy Rule Available at: https://www.cdc.gov/phlp/publications/topic/hipaa.html [Accessed 2nd July 2022]
10. Gauravit.org What is exploitation phase in penetration testing. Available at: https://gauravtiwari.org/exploitation-phase-in-penetration-testing/ [Accessed 2nd July 2022]
11. Geeksforgeeks.org Stages of post Exploitation Available at: https://www.geeksforgeeks.org/introduction-to-post-exploitation-phase/ [Accessed 2nd July 2022]

APPENDIX

Figure1: Project Timeline

Project Timeline							
Activities	Week1	Week 2	Week 3	Week4	Week5	Week6	Week7
Pre-engagement Interactions							
Intelligence Gathering							
Threat Modeling							
Vulnerability Analysis							
Exploitation							
Post Exploitation							
Reporting							

Figure 2:

STRIDE model

To better help you formulate these kinds of pointed questions, Microsoft uses the STRIDE model, which categorizes different types of threats and simplifies the overall security conversations.

Category	Description
Spoofing	Involves illegally accessing and then using another user's authentication information, such as username and password
Tampering	Involves the malicious modification of data. Examples include unauthorized changes made to persistent data, such as that held in a database, and the alteration of data as it flows between two computers over an open network, such as the Internet
Repudiation	Associated with users who deny performing an action without other parties having any way to prove otherwise—for example, a user performs an illegal operation in a system that lacks the ability to trace the prohibited operations. Non-Repudiation refers to the ability of a system to counter repudiation threats. For example, a user who purchases an item might have to sign for the item upon receipt. The vendor can then use the signed receipt as evidence that the user did receive the package
Information Disclosure	Involves the exposure of information to individuals who are not supposed to have access to it—for example, the ability of users to read a file that they were not granted access to, or the ability of an intruder to read data in transit between two computers
Denial of Service	Denial of service (DoS) attacks deny service to valid users—for example, by making a Web server temporarily unavailable or unusable. You must protect against certain types of DoS threats simply to improve system availability and reliability
Elevation of Privilege	An unprivileged user gains privileged access and thereby has sufficient access to compromise or destroy the entire system. Elevation of privilege threats include those situations in which an attacker has effectively penetrated all system defenses and become part of the trusted system itself, a dangerous situation indeed

Figure 3: Severity

	Rating category	High (3)	Medium (2)	Low (1)
D	Damage potential	Could subvert the security system and gain full trust, ultimately taking over the environment	Could leak sensitive information	Could leak trivial information
R	Reproducibility	Is always reproducible	Can be reproduced only during a specific condition or window of time	Is very difficult to reproduce, even given specific information about the vulnerability
E	Exploitability	Allows a novice attacker to execute the exploit	Allows a skilled attacker to create an attack that could be used repeatedly	Allows only a skilled attacker with in-depth knowledge to perform the attack
A	Affected users	Affects all users, including the default setup user and key customers	Affects some users or specific setups	Affects a very small percentage of users; typically affects an obscure feature
D	Discoverability	Can be easily found in a published explanation of the attack	Affects a seldom-used part, meaning an attacker would need to be very creative to discover a malicious use for it	Is obscure, meaning it's unlikely attackers would find a way to exploit it