Baseline Analysis and Plan

Your Store [daedalus-systems.co.uk]

# Security Challenges

## Generic Security Challenges in E-Commerce Web Applications

|  |  |
| --- | --- |
| **Issue** | **Description** |
| Broken Access Control | Problems with the application resulting from the absence of validation of relevant rights, privileges, or the bypassing or circumvention of the current authorization procedures. |
| Cryptographic Failures | Application vulnerabilities that enable attackers to sniff clear text data in transit or extract equivalent plaintext from backend services. |
| Injection | Weaknesses in a web application that arise due to the lack of validation, filtration, sanitization of user submitted input. |
| Security Misconfiguration | Risks in the application because it lacks security hardening, has undesired functionality enabled, has security features deactivated, does not adhere to legitimate security directives or is not configured with secure settings. |
| Vulnerable and Outdated Components | Vulnerabilities that occur because the installed packages are out-of-date, legacy, plagued with known vulnerabilities, and not regularly patched under a patch management framework. |
| Identification and Authentication Failures | Lack of restrictions on authentication aspects such as password complexity and reusability, simple password retrieval functionalities, usage of default passwords, inadequate session management and handling, and absence of multi-factor authentication controls give rise to these problems in an application. |
| Server-Side Request Forgery | SSRF vulnerabilities arise when a web application retrieves a remote object without verifying the URL defined by the user. Even when secured by a firewall, VPN, or other sort of network access control lists, it enables the ability to force a programme to submit a specially constructed request to an unexpected address. |

## Unique Security Challenges in E-Commerce Web Applications

|  |  |
| --- | --- |
| **Issue** | **Description** |
| Payment Gateway Compliance | PCI DSS is a set of security guidelines meant to guarantee that ALL businesses who take, handle, store, or transport payment information maintain a secure environment. |
| ISMS Compliance | ISO/IEC 27001:2013 outlines the standards for creating, implementing, maintaining, and constantly improving an organization's information security management system. |
| GDPR Compliance | The GDPR (General Data Protection Regulation) establishes some responsibilities that enterprises must adhere to that restrict how personal data may be used, processed, and stored. |
| Business Logic Flaw | Business logic problems arise when a web application accepts altered and tampered data unintentionally due to the fact that the payloads, although being erroneous, conform to the standards of the underlying code. |

# Assessment Toolset

|  |  |  |
| --- | --- | --- |
| **Name** | **Purpose** | **Type** |
| OpenVAS | Vulnerability Scanning | Open Source |
| Nessus | Vulnerability Scanning | Freemium |
| Nmap | Enumeration | Open Source |
| BurpSuite | Manual Testing | Open Source |
| Dirbuster, Gobuster, FFuF | Directory Fuzzing | Open Source |
| Reengine | Automated Enumeration | Open Source |

# Assessment Methodology

|  |  |
| --- | --- |
| **Assessment** | **Mode** |
| Penetration Testing | Remote, Manual, Automated |
| PCI-DSS, ISO27001, GDPR | On-site, Local Audit |

# Available Methodology

|  |  |
| --- | --- |
| **Methodology** | **Description** |
| Penetration testing | The consultant will perform a simulated cyber attack against the target systems to discover exploitable weaknesses using automated and manual approaches. |
| Vulnerability scanning | A vulnerability scanner will be employed to perform automated scans of the systems and match them with the existing vulnerability databases to uncover exploitable issues. |
| Risk management | Risk management is the identification, evaluation, and prioritization of risks |
| Physical Onsite Audits | Evaluate controls beyond the exposed internet surface in the people, processes, and technologies used for system maintenance. Physical audits led by standards such as PCI-DSS, ISO27001, and GDPR will uncover additional controls and loopholes that cannot be reviewed remotely. |

## Selection and Rationale

The methodologies of penetration testing and vulnerability management will be used to perform a thorough assessment of the systems.

Risk management will be employed to identify, evaluate and prioritize the discovered risks.

# Business Impact

|  |  |
| --- | --- |
| **Impact** | **Description** |
| Network Traffic | High usage of network bandwidth will be observed during the testing hours. |
| Process Utilization | High usage of system resources such as RAM and processing memory could be observed during testing hours. |
| Performance Hindrance | If a production setup, the application could be afflicted with performance hindrance reported by legitimate users during testing hours. |

# Timelines and Scoping

|  |  |
| --- | --- |
| **Page Type** | **Page Count** |
| Dynamic Pages | 55 |

|  |  |
| --- | --- |
| **Effort Required** | **Count (In Man Days)** |
| Assessment | 7 |
| Reporting | 2 |
| **Total** | **9** |

# Limitations and Assumptions

## Limitations

1. The assessment will not include attacks such as DoS and DDoS
2. Proof-of-Concept exploitation and vulnerability discovery will be performed to prevent unwanted application downtime.

## Assumptions

1. Logging and monitoring activities are continuously conducted by dedicated SOC.
2. The target application is not in an already-compromised state.

**References**

* OWASP (2021). OWASP Top Ten. Owasp.org. Available from: https://owasp.org/www-project-top-ten/. [Accessed 1 Jul. 2022].
* PCI Compliance Guide. (n.d.). PCI Compliance Guide Frequently Asked Questions | PCI DSS FAQs. Available from: https://www.pcicomplianceguide.org/faq/#1 [Accessed 1 Jul. 2022].
* ISO - International Organization for Standardization (2019). ISO/IEC 27001:2013. ISO. Available from: https://www.iso.org/standard/54534.html [Accessed 2 Jul. 2022].
* Castagna, R. (n.d.). What is GDPR? An Overview of GDPR Compliance and Conditions. WhatIs.com. Available from: https://www.techtarget.com/whatis/definition/General-Data-Protection-Regulation-GDPR [Accessed 2 Jul. 2022].
* OWASP (2021). A01 Broken Access Control - OWASP Top 10:2021. owasp.org. Available from: https://owasp.org/Top10/A01\_2021-Broken\_Access\_Control/ [Accessed 2 Jul. 2022].
* OWASP (2021). A02 Cryptographic Failures - OWASP Top 10:2021. owasp.org. Available from: https://owasp.org/Top10/A02\_2021-Cryptographic\_Failures/ [Accessed 2 Jul. 2022].
* OWASP (2021). A03 Injection - OWASP Top 10:2021. [online] owasp.org. Available from: https://owasp.org/Top10/A03\_2021-Injection/ [Accessed 2 Jul. 2022].
* OWASP (2021). A05 Security Misconfiguration - OWASP Top 10:2021. owasp.org. Available from: https://owasp.org/Top10/A05\_2021-Security\_Misconfiguration/ [Accessed 2 Jul. 2022].
* OWASP (2021). A06 Vulnerable and Outdated Components - OWASP Top 10:2021. owasp.org. Available from: https://owasp.org/Top10/A06\_2021-Vulnerable\_and\_Outdated\_Components/ [Accessed 2 Jul. 2022].
* OWASP (2021). A07 Identification and Authentication Failures - OWASP Top 10:2021. owasp.org. Available from: https://owasp.org/Top10/A07\_2021-Identification\_and\_Authentication\_Failures/ [Accessed 2 Jul. 2022].
* OWASP (2021). A10 Server Side Request Forgery (SSRF) - OWASP Top 10:2021. Owasp.org. Available from: https://owasp.org/Top10/A10\_2021-Server-Side\_Request\_Forgery\_%28SSRF%29/ [Accessed 2 Jul. 2022].