Executive Summary Report

Your Store [daedalus-systems.co.uk]

# Executive Summary

A vulnerability assessment and penetration test for Your Store [daedalus-systems.co.uk] was carried out from 18th July 2022 to 24th July 2022. The assessment was carried out remotely.

## The evaluation was completed using a comprehensive manual penetration test utilising a broad range of methodologies, complemented by automated application vulnerability scanning to swiftly identify attack paths and mimic actual exploitation.

## Key Observations

1. Use of deprecated TLS/SSL versions [TLS 1.0 and 1.1] was detected.
2. The application was using obsolete client-side JavaScript [multiple outdated versions of jQuery]
3. The application was running outdated server-side processing PHP version 7.4.3.
4. The application was missing security enhancing HTTP headers; for instance, HSTS.
5. Multiple GDPR non-compliance were detected.

## Assessment Scope

|  |
| --- |
| **Assessment Scope** |
| Your Store [daedalus-systems.co.uk] |

|  |  |
| --- | --- |
| **User Account** | **Privilege** |
| ynss@dispostable.com | Customer |

# Security Issues Discovered

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Issue Name** | **Baseline Comparison** | **Impact** | **Likelihood** | **Risk Rating [CVSS]** |
| Deprecated TLS/SSL Versions in used | Cryptographic Failures | **Critical** | **Critical** | **9.8** |
| Weak Password Reset and Password Policy | Identification and Authentication Failures | **High** | **High** | **7.7** |
| Missing Multi-Factor Authentication | Identification and Authentication Failures | **High** | **High** | **7.7** |
| SMTP uses Cleartext Protocol | Cryptographic Failures | **High** | **High** | **7.7** |
| Outdated PHP version 7.4.3 | Vulnerable and Outdated Components | **Moderate** | **Moderate** | **5.6** |
| Outdated jQuery vulnerable to XSS | Vulnerable and Outdated Components | **Moderate** | **Moderate** | **5.6** |
| Outdated JavaScript Dependencies | Vulnerable and Outdated Components | **Moderate** | **Moderate** | **5.6** |
| User Enumeration via Web Response | Security Misconfiguration | **Low** | **Moderate** | **5.6** |
| Missing Security HTTP Headers | Security Misconfiguration | **Low** | **Low** | **3.7** |
| Missing Cookie Flags | Security Misconfiguration | **Low** | **Low** | **3.7** |

# Security Non-Compliance Discovered

|  |  |  |
| --- | --- | --- |
| **Issue** | **Baseline** | **Compliance Status** |
| Missing Deactivate /Delete Account Function | GDPR Compliance | **Non-Compliant** |
| Explicit Consent for Cookies not set | GDPR Compliance | **Non-Compliant** |
| Missing Multi-Factor Authentication | GDPR Compliance | **Non-Compliant** |

# Limitations Encountered

* **Vulnerability Scanning:** The use of an automatic scanner activated the site's IP blocking mechanism, making it unavailable under certain circumstances.
* **Penetration Testing:** Performing security checks related to horizontal and vertical privilege movements was skipped due to a lack of availability of privileged accounts in the application.
* **PCI-DSS Testing:** PCI-DSS Tests were commenced however, they were discontinued due to a lack of functioning payment gateway within the cart checkout function.
* **GDPR Checks:** Security checks related to data protection by design and default, and data storage could not be performed due to lack of access to onsite access and access to application server.

# Summary of Findings

## Security Risks by Rating

## Security Risks by Category

# Evaluation and Results

## Evaluation in comparison to OWASP Top 10

The Web Application was evaluated against OWASP Top 10 and the results are as follows:

|  |  |
| --- | --- |
| **OWASP Top 10** | **Security Issues Found** |
| A01:2021-Broken Access Control | 0 |
| A02:2021-Cryptographic Failures | 2 |
| A03:2021-Injection | 0 |
| A04:2021-Insecure Design | Untested |
| A05:2021-Security Misconfiguration | 3 |
| A06:2021-Vulnerable and Outdated Components | 3 |
| A08:2021-Software and Data Integrity Failure | Untested |
| A07:2021-Identification and Authentication Failures | 2 |
| A09:2021-Security Logging and Monitoring Failures | Untested |
| A10:2021-Server-Side Request Forgery | 0 |

It is obvious from the preceding table that the application is presently making some steps to secure the environment. However, there is a need to strengthen the overall security in accordance with global security best practises and regulations.

In addition, it is observed that owing to a lack of access and permissions, several evaluation categories are left unchecked, which prevents a comprehensive view of the assessment standings and ratings.

## Evaluation in comparison to GDPR Rights

The Web Application was audited against the GDPR privacy rights of a ‘data subject’ and the results are as follows:

|  |  |  |
| --- | --- | --- |
| **Privacy Rights** | **Compliance Status** | **Evidence** |
| Right to be Informed | Non-Compliant | Information about data processing and handling information missing from website. |
| Right of Access | Non-Compliant | Information about data processing and handling by processor or third party missing from website. |
| Right to rectification | Compliant | Personal data can be updated and modified readily. |
| Right to erasure | Non-Compliant | Account deletion or deactivation feature not implemented. |
| Right to restrict processing | Non-Compliant | Missing controls to restrict processing post deletion of records. |
| Right to data portability | Non-Compliant | Lack of option to export date for portability |
| Right to object | Non-Compliant | Data processing clauses and information not set. |
| Rights in relation to automated decision making and profiling. | Non-Compliant | Information about data processing and handling information missing from website. |

On the basis of the preceding facts, it is obvious that the application lacks the required controls for GDPR compliance. This might result in hefty penalties and a loss of confidence among users and consumers who use the website to make essential transactions.

# Conclusion

The post-assessment led to the following conclusions:

* A further thorough assessment and audit for the application is required.
* Retesting of the application must be conducted to verify if existing risks were mitigated.
* A GDPR compliance team must be setup to fix current issues with the help of an assigned data protection officer.

# Fixes & Recommendations

* Disable the use of TLS 1.0 and 1.1 from server configuration.
* Reconfigure error messages to generic messages as to prevent enumeration.
* Enable password complexity for user passwords.
* Setup Multi-Factor authentication service to strengthen account security.
* Enable SMTP over Secure channel by using SMTPS
* Upgrade old components to their latest stable version. Additionally, consider implementing continuous patch management process to address outdated components at an early.
* Add security enhancing headers and cookie flags via server configuration changes.

# Vulnerability Rating Methodology

**Risk Rating**

|  |  |
| --- | --- |
| **Rating** | **Definition** |
| **Critical** | * Identified vulnerabilities have an immediate impact. * Vulnerability details and/or Proof of Concept (PoC) code are/is publicly available * Successful exploitation may result in significant loss. * Data confidentially, integrity and availability are significantly at risk * The compromise of an application/system/network and/or user is highly probable. * Remediation actions should be performed immediately**.** |
| **High** | * Identified vulnerabilities are likely to have a significant impact. * Vulnerability details and/or Proof of Concept (PoC) code are/is publicly available. * Data confidentially, integrity and availability are significantly at risk. * The compromise of an application/system/network and/or user is likely. * Remediation actions should be performed quickly. |
| **Moderate** | * Identified vulnerabilities may pose a risk of loss/disclosure of data/information and hence harm the reputation. * An additional vulnerability may be required to fully leverage this finding. |
| **Low** | * Exploitation is not trivial and/or exposure is minimal. * Public exploit code doesn't exist or requires specialised conditions. * Information/data may be disclosed that harms the reputation. * An additional vulnerability may be required to fully leverage this finding. |
| **Informational** | * Not conforming to best practise guidelines, but provided information may help improve the overall security posture of the company. * These findings are for informational purposes only. |

**Impact Rating**

|  |  |
| --- | --- |
| **Rating** | **Definition** |
| **Critical** | * Identified vulnerabilities could have a severe impact. |
| **High** | * Identified vulnerabilities could have a significant impact. |
| **Moderate** | * Identified vulnerabilities could have a serious adverse impact. |
| **Low** | * Identified vulnerabilities could have a limited effect. |
| **Informational** | * Identified vulnerabilities could have no effect. |

**Likelihood Rating**

|  |  |
| --- | --- |
| **Rating** | **Definition** |
| **High** | * Identified vulnerabilities are highly likely to be exploited by a malicious actor. |
| **Moderate** | * Identified vulnerabilities are somewhat likely to be exploited by a malicious actor. |
| **Low** | * Identified vulnerabilities are unlikely to be exploited by a malicious actor. |

# **References**

* GDPR.eu. (n.d.). Chapter 3 (Art. 12-23) Archives. Available from: <https://gdpr.eu/tag/chapter-3/>. [Accessed 15 Jul. 2022].
* FIRST — Forum of Incident Response and Security Teams. (2019). Common Vulnerability Scoring System SIG. Available from: <https://www.first.org/cvss/>. [Accessed 15 Jul. 2022].
* OWASP (2021). OWASP Top Ten. Owasp.org. Available from: https://owasp.org/www-project-top-ten/. [Accessed 15 Jul. 2022].
* NIST (2019). Cybersecurity Framework. NIST. Available from: https://www.nist.gov/cyberframework [Accessed 22 Jul. 2022].