Vulnerability Assessment Report

Executive Summary

Overview

Loadedwithstuff.co.uk is an e-commerce website that specializes in selling electronics and gadgets to the public. As part of this executive assessment report, we have conducted a security assessment to identify vulnerabilities and risks that could potentially expose sensitive customer data to unauthorized users and hackers. This report presents this data the following standards - the General Data Protection Regulation (GDPR) directive, OWASP 10, STRIDE, and DREAD. The report presents the findings in a non-technical manner.

Limitations

While every effort was made to conduct a thorough assessment of the website, it is important to note that there are limitations to any security testing methodology. For example, the assessment was limited to the tools and techniques used, and there may be other vulnerabilities that were not identified during the testing.

Methodology Used

The assessment of the Loadedwithstuff.co.uk website was conducted using automated testing techniques. The following tools were used in the automated testing:

* OWASP Zed Attack Proxy (ZAP)
* Nmap

The methodology used was based on the OWASP Testing Guide and included the following steps:

1. Reconnaissance - Gathering information about the target website.
2. Threat modelling - Identifying potential security threats.
3. Vulnerability assessment - Identifying vulnerabilities in the website.
4. Exploitation - Attempting to exploit identified vulnerabilities to confirm their existence and potential impact.
5. Post-exploitation - Assessing the impact of successful exploitation.
6. Reporting - Documenting the findings of the assessment.

Findings

The website was found to have security vulnerabilities mentioned in OWASP A1, A2, A6, A7, and A9 categories. The website was also found to be non-compliant with GDPR due to the absence of a clear privacy policy and mechanism for user consent.

The assessment identified several security vulnerabilities and risks on the website, including:

1. Cross-Site Scripting (XSS) - The website is vulnerable to XSS attacks, which allow attackers to inject malicious code into the website, steal user data, and compromise the website's security.
2. SQL Injection - The website is vulnerable to SQL Injection attacks, which can allow attackers to extract sensitive data from the website's database.
3. Insecure Password Storage - The website could store user passwords in plaintext, which is a significant security risk and could result in user data being compromised.
4. Lack of Security Headers - The website does not implement security headers, which can help protect against various types of attacks such as Cross-Site Scripting (XSS), Clickjacking, and Code Injection.
5. Outdated Software - The website could be using outdated software versions, which can be vulnerable to known security vulnerabilities and pose a significant risk to the website's security.
6. Lack of GDPR Compliance - The website collects personal information from users, such as their name and email address. However, the website lacks a clear privacy policy and does not provide users with sufficient information about how their data will be processed. In addition, the website has no way of allowing users to request for their information to be deleted. Furthermore, the website does not implement any kind of cookie consent which should tell the user what information is being tacked and collected by the website.

|  |  |  |  |
| --- | --- | --- | --- |
| Security Issues Found | Security Codes | Severity | More information |
| Lack of security headers | OWASP A6 - Security Misconfiguration | Medium | <https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration> |
| Outdated software and plugins | OWASP A9 - Using Components with Known Vulnerabilities | Medium | <https://owasp.org/www-project-top-ten/2017/A9_2017-Using_Components_with_Known_Vulnerabilities> |
| Weak password policies | OWASP A2 - Broken Authentication and Session Management | High | <https://owasp.org/www-project-top-ten/2017/A2_2017-Broken_Authentication> |
| Lack of input validation | OWASP A1 - Injection | High | <https://owasp.org/www-project-top-ten/2017/A1_2017-Injection>  <https://owasp.org/www-community/attacks/SQL_Injection> |
| Cross-Site Scripting (XSS) | OWASP A7 Cross-Site Scripting (XSS) | High | <https://owasp.org/www-community/attacks/xss/> |
| Absence of clear privacy policy | NA | High |  |
| Lack of mechanism for user consent | NA | High |  |
| Lack of GDPR Compliance | NA | High |  |

|  |  |  |
| --- | --- | --- |
| STRIDE Threat | Security Issues | Risk Rating (DREAD) |
| Spoofing | Cross-Site Request Forgery (CSRF)  Lack of two-factor authentication (2FA) | 7/10 |
| Tampering | Cross-Site Scripting (XSS)  SQL Injection | 8/10 |
| Repudiation | Possible lack of auditing mechanism | 6/10 |
| Information Disclosure | Leak of sensitive data | 8/10 |
| Denial of Service | Lack of Denial of Service (DDoS) protection | 6/10 |
| Elevation of Privilege | Broken Authentication and Session Management | 8/10 |
| Total DREAD Score | 43/50 | |

Recommendations

The following recommendations should be implemented to improve the security of the website:

1. Upgrade software versions – All software and libraries that are running and managing the website should be updated to their latest version and thoroughly tested to make sure there are no bugs. This including the web server, CMS, and all plugins. This will ensure that any known vulnerabilities are patched and reduce the risk security risks.
2. Implement password policies - The website should enforce strong password policies, including the use of complex passwords, password expiration, and multi-factor authentication where possible. This will help prevent unauthorized access to the website and its underlying systems.
3. Conduct regular vulnerability assessments - The website should be regularly assessed for vulnerabilities using a combination of automated tools and manual testing. This will ensure that any new vulnerabilities are identified and addressed correctly on time.
4. Implement input validation and sanitization - The website should implement robust input validation and sanitization to prevent common attacks such as SQL injection and XSS. This will help prevent attackers from exploiting vulnerabilities in the website's code.
5. Implement security headers - The website should implement security headers such as Content Security Policy (CSP), Strict-Transport-Security (STS), and X-Frame-Options. These headers provide an additional layer of protection against common web application attacks and should be implemented as part of the website's security controls.
6. Create a privacy policy - The website should have a privacy policy implemented that clearly outlines how user data is collected and used. This will help ensure GDPR compliance and build trust with users.
7. Implement cookie consent correctly - The website should implement cookie consent correctly, including providing users with clear information about the cookies used on the website and obtaining their explicit consent. This will help ensure GDPR compliance and build trust with users.
8. Train employees on security awareness - The website should provide security awareness training to all employees who have access to the website or its underlying systems. This will help ensure that employees are aware of common security risks and how to prevent them.

Final summery recommendation

In summary, incorporating the STRIDE and DREAD assessments provides a more comprehensive view of the security risks. To address these risks, the recommendations provided in the previous section can be implemented. These recommendations address many of the vulnerabilities identified by the STRIDE and DREAD assessments, including implementing input validation, enforcing strong password policies, creating a clear privacy policy and much more.

References:

The assessment was carried out using industry-standard methodologies and frameworks, including the GDPR directive and OWASP Top 10. The following sources were used in the assessment:

General Data Protection Regulation (GDPR) - Lex - 32022R0720 - en - EUR-Lex (no date) EUR. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R0720 (Accessed: March 1, 2023).

Guide to the UK General Data Protection Regulation (UK GDPR) (no date) ICO. Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/ (Accessed: March 1, 2023).

Introduction (no date) OWASP Top 10:2021. Available at: https://owasp.org/Top10/ (Accessed: March 1, 2023).

Vulnerability scanning tools (no date) Vulnerability Scanning Tools | OWASP Foundation. Available at: https://owasp.org/www-community/Vulnerability\_Scanning\_Tools (Accessed: March 1, 2023).

WSTG - latest (no date) WSTG - Latest | OWASP Foundation. Available at: https://owasp.org/www-project-web-security-testing-guide/latest/3-The\_OWASP\_Testing\_Framework/1-Penetration\_Testing\_Methodologies (Accessed: March 1, 2023).

Owasp Web Security Testing Guide (no date) OWASP Web Security Testing Guide | OWASP Foundation. Available at: https://owasp.org/www-project-web-security-testing-guide/assets/archive/OWASP\_Testing\_Guide\_v4.pdf (Accessed: March 1, 2023).

Content security policy (CSP) - http: MDN (no date) HTTP | MDN. Available at: https://developer.mozilla.org/en-US/docs/Web/HTTP/CSP (Accessed: March 1, 2023).

Strict-transport-security - http: MDN (no date) HTTP | MDN. Available at: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security (Accessed: March 1, 2023).

Cross site scripting (XSS) (no date) Cross Site Scripting (XSS) | OWASP Foundation. Available at: https://owasp.org/www-community/attacks/xss/ (Accessed: March 1, 2023).

Brute Force attack (no date) Brute Force Attack | OWASP Foundation. Available at: https://owasp.org/www-community/attacks/Brute\_force\_attack (Accessed: March 1, 2023).

Jegeib (no date) Threats - microsoft threat modeling tool - azure, Threats - Microsoft Threat Modeling Tool - Azure | Microsoft Learn. Available at: https://docs.microsoft.com/en-us/azure/security/develop/threat-modeling-tool-threats#stride-threats (Accessed: March 1, 2023).

Domars (no date) Threat modeling for Drivers - Windows Drivers, Windows drivers | Microsoft Learn. Available at: https://learn.microsoft.com/en-us/windows-hardware/drivers/driversecurity/threat-modeling-for-drivers (Accessed: March 1, 2023).