University of Essex Online

Network and Information Security Management March 2022 B

Development Team Project:
Design Document

Target: https://loadedwithstuff.co.uk
Domain: Ecommerce Website

Team 1: Chan Kei Yiu Yvone, HungWei Lin, Thien Liu, Yusuf Fahry

15 Apr 2022

Table of Contents

Word count: 1100

Overview

Security checks are essential for maintaining web applications' usability and integrity.

This document will outline the theoretical risks of **loadedwithstuff.co.uk** and suggest the methodologies and possible risk mitigation strategies.

Assumptions

Loadedwithstuff.co.uk is an e-commerce website that cybercriminals may target to steal personal and payment information from potential vulnerabilities (Fireside Agency, 2020). By referencing the OWASP top ten list, possible vulnerabilities are suggested. Each vulnerability's details will be explained in the next section.

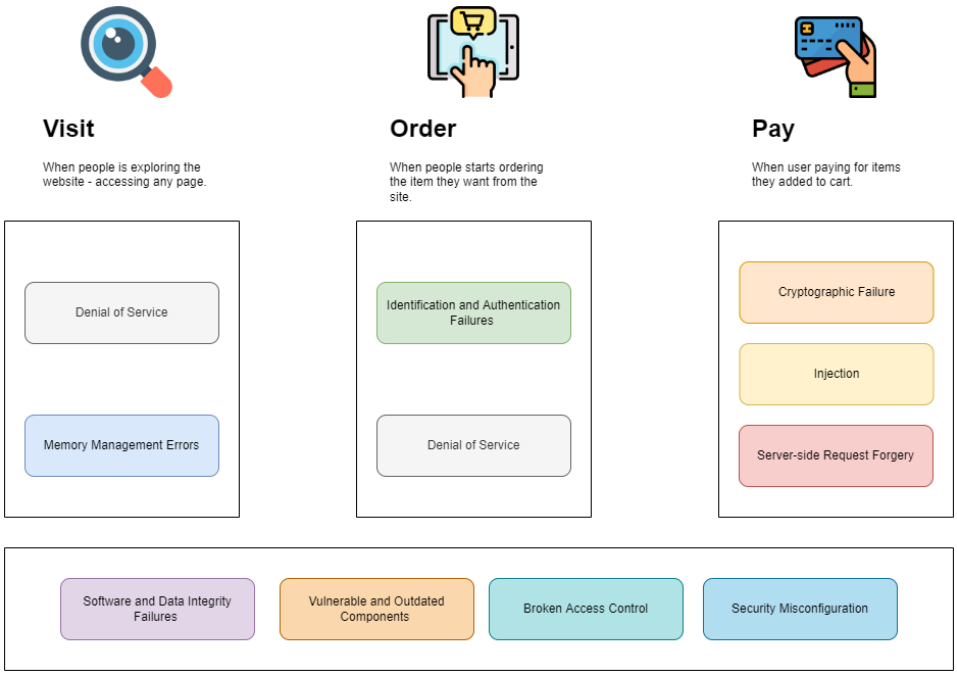


Figure 1- Assumptions

Regulation Compliance

General Data Protection Regulation (GDPR)

The website is a United Kingdom e-commerce site; it must comply with the GDPR. GDPR is Europe's data privacy and security law that imposes obligations on collecting EU people's data. Organizations must handle data securely by implementing appropriate measures, for example, end-to-end encryption on data transition (GDPR.EU, N.D.).

Payment Card Industry Data Security Standard (PCI DSS)

PCI DSS is a security standard on credit card information and applies to all organizations that accept, transmit, or store cardholder data. The standard requires building, maintaining, and securing networks and systems. Other requirements include protecting account data, maintaining a vulnerability management program, implementing strong access control measures, and maintaining an information security policy (PCI Compliance Guide, N.D.).

ISO/IEC 27001

ISO/IEC 27001 provides an information security management system (ISMS) requirements. It enables organizations to manage information security (ISO, N.D.).

Methodology

Engebretson (2013) suggested the following methodology:

1. **Pre-Engagement Interactions**: This phase defines the purpose of the test, the targets to be verified, the parameters of when the testing is valid and permissible, and the overall budget.

2. **Intelligence Gathering**: This phase collects as much information as possible and produces a document for planning the test strategy. Network utilities will be used to fetch website-related information, e.g., DNS/MX records, domain registration, network hosts, public and private IP blocks, TCP and UDP running services, SSL certificates, and open ports.

3. **Threat Modelling**: The Microsoft Threat Modeling Process will be applied to identify, quantify, and address the website's security risks. Identified threats will also be categorized by the STRIDE model and ranked by the DREAD risk assessment model.

4. **Vulnerability Analysis:** The OWASP's top ten vulnerabilities and other common attacks will be analyzed.

5. **Exploitation**: This phase focuses on using various testing techniques, including automated and manual approaches, to bypass the security flaw and compromise of the application.

6. **Post-Exploitation:** This step elevates the access gained from the exploitation phase through the use and implementation of backdoors, rootkits, and shells. It provides proof of concept of the realistic scenario of the attacker returning to the target.

7. **Reporting:** A security testing report will be released to communicate our findings and recommendations, including the detailed output from each tool and a walkthrough of security test steps.

Potential risks

Threat type	Potential risks
Broken Access Control	▪ External initialization of trusted variables or data stores in Softaculous before 5.5.7 ▪ Privilege escalation on the localhost • Unauthorized access to sensitive data
Cryptographic Failures	▪ exposure of sensitive data
Injection	▪ malicious code may pass through if the user-supplied data is not validated, filtered, or sanitized ▪ Softaculous Webuzo's File Manager module before 2.1.4 allows injection of arbitrary web script or HTML ▪ XSS vulnerability ▪ data breach
Security Misconfiguration	▪ Softaculous Webuzo's login function before 2.1.4 provides different error messages ▪ Attackers can enumerate usernames through a series of requests
Vulnerable and Outdated Components	▪ Dependent components may be outdated ▪ Introducing security risks
Identification and Authentication Failures	▪ Unauthorized access of data
Software and Data Integrity Failures	▪ Potential for unauthorized access, malicious code, or system compromise
Server-Side Request Forgery	▪ Attackers can send requests to unexpected destinations ▪ data breach
Denial of Service	▪ Prevent legitimate users from using the site

Adapted from OWASP and CVE Details.

Tools and Justifications

Reconnaissance and Scanning

Tool	Purposes	Risks
The Harvester	• Accurately catalog the target's email addresses and subdomains (Martorella, 2019)	Identification and Authentication Failures
WHOIS, nslookup, dig	• Explore the target's specific information, e.g., IP addresses, hostnames of the company's DNS servers, domain registration contact information	Registrar hijacking, Typosquatting, Cache Poisoning (Hollis, 2017)
NMAP	• Perform port scanning and network mapping to identify open ports • Determine the target's available services (nmap.org, 2022)	Broken Access Control
Nessus and Nikto	• Automate the web scanning process for vulnerabilities, out-of-date and unpatched software • Search for dangerous files on web servers (Engebretson, 2013)	Security Misconfiguration, Vulnerable and Outdated Components

Threat Modelling

After identifying the vulnerabilities, the **STRIDE** methodology is used for classification. (Mahmood, 2017)

	Threat	Property Violated	Threat Definition
S	Spoofing	Authentication	Pretending to be something or someone other than yourself
T	Tampering	Integrity	Modifying something on disk, network, memory, or elsewhere.
R	Repudiation	Non-Repudiation	Claiming that you didn't do something or we're not responsible. Can be honest or false
I	Information Disclosure	Confidentiality	Providing information to someone not authorized to access it.
D	Denial of service	Availability	Exhausting resources needed to provide service.
E	Elevation of Privilege	Authorization	Allowing someone to do something they are not authorized to do.

Figure 2 - STRIDE methodology (Sketchbubble, N.D.)

The **DREAD** methodology is used to rate, compare and prioritize the severity of risk presented by each threat classified by STRIDE (Mahmood, 2017).

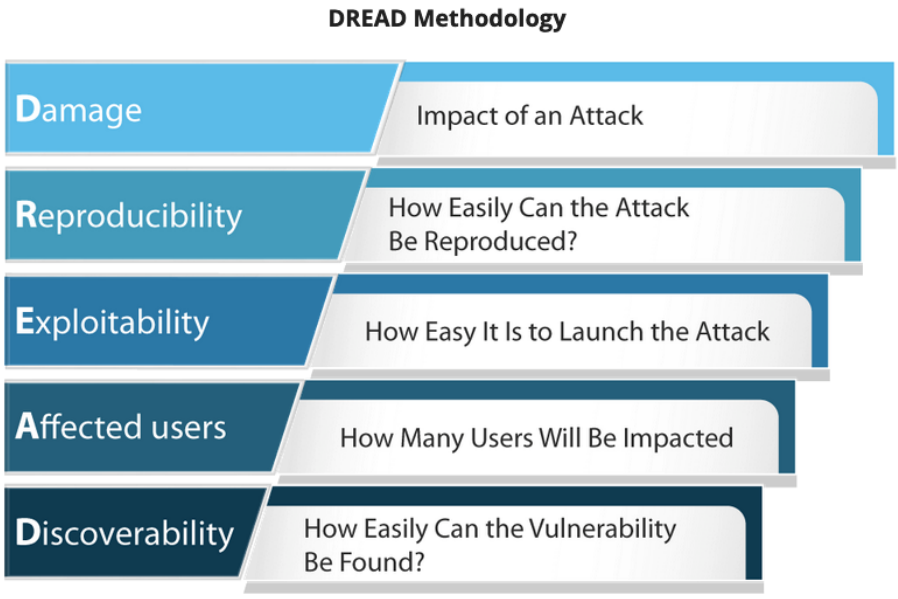
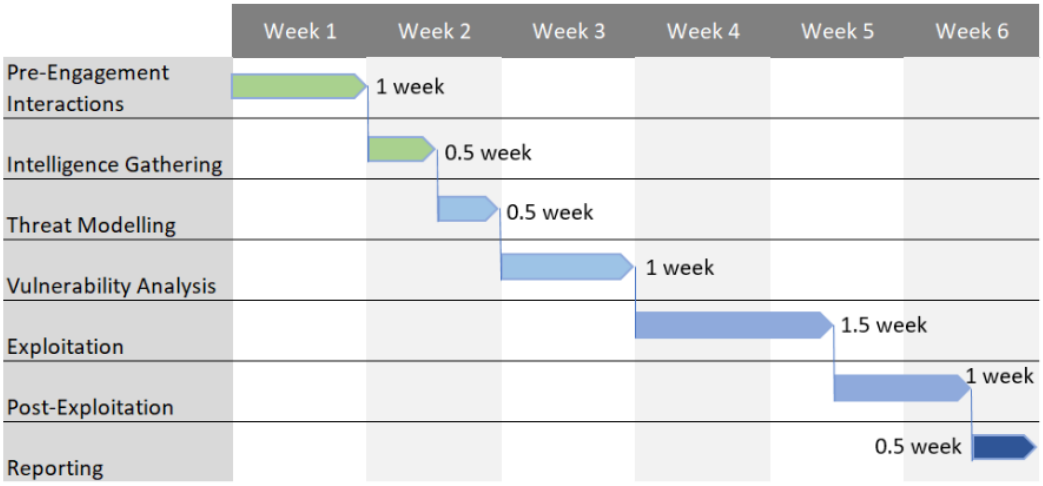


Figure 3 – DREAD Methodology (EC-Council, 2022)

Exploitation Tools

Tool	Purpose	Risk
Metasploit framework	• Provides exploit management (lookup, update, documentation) and a plethora of payloads (tasks performed after successful target system exploitation) (Holik, 2014)	Buffer overflow, code injection, and web application exploits (docs.rapid7.com, N.D.)
Burp Suite	• Actively or passively scan web applications' vulnerabilities • Intruder and sequencer options to perform brute force attacks or fuzz testing (PortSwigger, 2020)	OWASP Top Ten (refer to ***Potential Risks***)

Schedule and Impacts



- While various testing techniques are applied, the website might confront the performance issue such as slowness
- To ensure the website's user experience would not be affected, the testing actions should be schedule carefully.

Figure 4 – Suggested timeline

Potential mitigations and recommendations

Threat	Tool	Mitigation
Broken Access Control	NMAP	▪ Set deny-by-default except for public resources ▪ Log access control failures ▪ Rate limit API and controller access
Cryptographic Failures	Burp Suite	▪ Classify data according to sensitivity ▪ Encrypt sensitive data at rest and all data in transit ▪ Ensure up-to-date and robust standard algorithms and protocols ▪ Disable caching for responses containing sensitive data ▪ Store passwords using vital adaptive and salted hashing functions with a work factor
Injection	Metasploit framework	▪ Use a safe API with parameterized interface ▪ Validate input positively on server-side ▪ Escape interpreter specific special characters ▪ Use SQL controls within queries to prevent massive data disclosure
Security Misconfiguration	Nessus and Nikto	▪ Review and update configurations ▪ Automate the process to verify the effectiveness of configurations and settings
Vulnerable and Outdated Components	Nessus and Nikto	▪ Removing unused dependencies ▪ Inventory continuously the components and dependencies ▪ Monitor CVE and NVD for vulnerabilities ▪ Monitor for unmaintained libraries and components
Identification and Authentication Failures	The Harvester	▪ Implement multi-factor authentication where possible ▪ Implement weak password checks ▪ Harden registration, credential recovery, and API pathways against enumeration attacks by returning the same message ▪ Limit or increasingly delay failed login attempts
Software and Data Integrity Failures	Metasploit framework	▪ Use digital signatures or similar mechanisms to verify the software or data ▪ Ensure libraries and dependencies are consuming trusted repositories

		▪ Review code and configuration changes to minimize malicious code attacks
Server-Side Request Forgery	NMAP	▪ Enforce “deny by default” security system policies or network access control rules ▪ Sanitize and validate client-supplied input
Denial of Service	Burp Suite	▪ Perform performance tests ▪ Cache expensive operations ▪ Access controls for larger objects

Adapted from OWASP.

References

1. CVE Details (2021). Softaculous: Security Vulnerabilities. Available from: https://www.cvedetails.com/vulnerability-list/vendor_id-12960/Softaculous.html [Accessed 17 Apr 2022].
2. docs.rapid7.com. (N.D.) Using Exploits | Metasploit Documentation. Available from: https://docs.rapid7.com/metasploit/using-exploits [Accessed 17 Apr 2022].
3. EC-Council. (2022) DREAD Threat Modeling: An Introduction to Qualitative Risk Analysis. Available from: https://eccouncil.org/cybersecurity-exchange/threat-intelligence/dread-threat-modeling-intro/ [Accessed 15 Apr 2022].
4. Engebretson, P. (2013). *Ethical Hacking and Penetration Testing Made Easy*. 2nd ed. Massachusetts: Syngress Publishing. Inc.
5. Engebretson, P. (2013) T*he basics of hacking and penetration testing*. Amsterdam: Syngress, an imprint of Elsevier.
6. Fireside Agency. (2020) Why You Can’t Ignore Security for Your E-Commerce Website. Available from: https://www.firesideagency.ca/website-design-development/why-you-cant-ignore-security-for-your-e-commerce-website/ [Accessed 10 Apr 2022].
7. GDPR.EU. (N.D.) What is GDPR, the EU’s new data protection law? Available from: https://gdpr.eu/what-is-gdpr/ [Accessed 15 Apr 2022].
8. Holik, F., Horalek, J., Marik, O., Neradova, S., & Zitta, S. (2014) Effective penetration testing with Metasploit framework and methodologies. *2014 IEEE 15th International Symposium on Computational Intelligence and Informatics (CINTI)* 2014: 237-242. DOI: 10.1109/CINTI.2014.7028682.
9. Hollis, R. (2017) Security Think Tank: Top three DNS-related security risks. Available from: https://www.computerweekly.com/opinion/Security-Think-Tank-Top-three-DNS-related-security-risks [Accessed 17 Apr 2022].
10. ISO. (N.D.) ISO/IEC 27001 Information Security Management. Available from: https://www.iso.org/isoiec-27001-information-security.html [Accessed 15 Apr 2022].
11. Mahmood, H. (2017) Application Threat Modeling using DREAD and STRIDE. Available from: https://haiderm.com/application-threat-modeling-using-dread-and-stride/ [Accessed 15 Apr 2022].

12. Martorella, C. (2019) GitHub - laramies/theHarvester. Available from: https://github.com/laramies/theHarvester. [Accessed 15 Apr 2022].
13. nmap.org. (2022.) Nmap: the Network Mapper - Free Security Scanner. Available from: https://nmap.org/ [Accessed 15 Apr 2022].
14. OWASP. (2021) OWASP Top 10:2021. Available from: https://owasp.org/Top10/ [Accessed 9 Apr 2022].
15. OWASP. (2022) OWASP Threat Dragon. Available from: https://owasp.org/www-project-threat-dragon/ [Accessed 15 Apr 2022].
16. PCI Compliance Guide. (N.D.) PCI FAQs. Available from: https://www.pcicomplianceguide.org/faq/ [Accessed 6 Apr 2022].
17. PortSwigger. (N.D.) Burp Suite's web vulnerability scanner. Available from: https://portswigger.net/burp/vulnerability-scanner [Accessed 15 Apr 2022].
18. Rogers, R. (2008). *Nessus network auditing*. 2nd ed. Massachusetts: Syngress Publishing. Inc.
19. SketchBubble. (N.D.) Stride Threat Model. Available from: https://www.sketchbubble.com/en/presentation-stride-threat-model.html [Accessed 15 Apr 2022].