1. INTRODUCTION **2**
1.2 LIMITATIONS 2
1.3 METHODOLOGY 2
2. SCAN RESULTS **3**
2.2 SSL SCAN 8
2.3 GDPR COMPLIANCE CHECKLIST 9
2.4 PCI DSS COMPLIANCE 9
3. RECOMMENDATIONS **10**
REFERENCES **11**

1. Introduction

The purpose of the vulnerability scan is to gather data on loadedwithstuff.co.uk security standards.

1.2 Limitations

Difficulty configuring Kali Linux, coupled with the website being nonresponsive led to the decision to scan automatically scan the website for vulnerabilities using lightweight sources online and provide recommendations to the organisation to avoid GDPR fines.

1.3 Methodology

The scans have tested against OWASP security standards and GDPR.

2. Scan results

Type	Tool	Name	Vulnerability	Evidence	Risk	Solution
Insecure cookie setting: missing HttpOnly flag	Pentest-tools.com	Icsid	Unsecure cookie can be accessed via JavaScript code from within the website, which can be malicious injection by attacker using XSS attack	Set-Cookie: lcsid=e72a22443df7dd47f3784fdb0dacaeb2; path=/; domain=loadedwithstuff.co.uk	Medium	Ensure HttpOnly flag is enabled for all cookies
Insecure cookie setting: missing secure flag	Pentest-tools.com	icsid	Data is sent between unencrypted and encrypted channels, making it vulnerable for malicious actor to capture it.	Set-Cookie: lcsid=e72a22443df7dd47f3784fdb0dacaeb2; path=/; domain=loadedwithstuff.co.uk	High	Ensure data is passed through secure tunnels
Insecure cookie setting: domain too loose	Pentest-tools.com	Icsid	Cookies used in subdomains may be accessed under the main domain	Set-Cookie: .loadedwithstuff.co.uk	Medium	Domain attribute should be set to the origin host
Insecure cookie handling: cookie without SameSite attribute	OWASP_Zen via hostedscan.com	SameSite Attribute	Cookie can be sent as result of XSS	Lack of SameSite configuration	Low	Set SameSite to strict for all cookies
Missing Content	Pentest-tools.com	Content Security Header	Content Security Header prevents CSS exploits	Response headers to not include HTTP content security policy security	Low	Configure Content Security

security Policy						Header to be sent with each HTTP response
Missing security header: X-XSS-Protection	Pentest-tools.com	X-XSS Protection HTTP header	X-XSS Protection HTTP header instructs the browser to not load web pages once XSS attacks have been identified.	Response headers do not include HTTP X-XSS Protection security header	Low	Set the X-XSS protection header to X-XSS:1; mode=block
Missing Security header: Referrer-Policy	Pentest-tools.com	Referrer-Policy HTTP security header	When user leaves the site going onto another, the browser send complete URL which may contain sensitive information and can be used for tracking	Response header no not include Referrer-Policy HTTP security header nor <meta> tag is not present	Low	Referrer Policy header should be configured.
Leaked PHP version	Pentest-tools.com	PHP version	PHP version in HTTP header	PHP version found online	Low	Configure to be disabled
Public details should be behind buttons	Manual inspection	Company details	Company details publicly available on website	Public details	High	Hide company details to prevent automatic attacks
Robots.txt file existence	Pentest-tools.com	Robots.txt file existence	URLs can be read from the file, not a threat but often misused to hide URLs	File found	Low	Review vulnerable entities

Malware, viruses, malicious code	sucuri.com	-	-	-	-	-
Application error disclosure	OWASP_ZAP via hostedscan.com	Error message may disclose sensitive information	Error message may disclose location of file that handle exception	https://loadedwithstuff.co.uk/ipn.php	Low	Implement custom error pages
Server leak information via X-Powered.-By HTTP Response header fields	OWASP_Zen via hostedscan.com	Known vulnerabilities in known software can be exploited by attackers	Software and tools identified whose vulnerabilities are known can be exploited by attackers	Software and tools information available	Low	Ensure X-Powered-by headers are configured
Vulnerable JS library	OWASP_ZEN	library angularjs, version 1.6.9	Improper neutralisation of input, XSS vulnerable	CWE-79[1]	Medium	Update library
Absence of Anti-CSRF tokens in HTML submission form	OWASP_ZAP via hostedscan.com	Absence of Anti-CSRF tokens in HTML submission form	CSRF attack vulnerability	URLs/form actions used repeatedly	Medium	Library to generate unique nonce for each (submission) form and verify

[1] nvd.nist.gov. (2020). *NVD - CVE-2020-7676*. [online] Available at: https://nvd.nist.gov/vuln/detail/CVE-2020-7676 [Accessed 21 Jul. 2022].

Type	Tool	Name	Vulnerability	Evidence	Risk	Solution
DMARC policy not found	Upguard.com	DMARC policy	Attackers can impersonate persons and send emails from the website	Lack of DMARC policy	Medium	Configure DMARC policy
SPF Policy authorises ~all	Upguard.com	SPF policy enabled	Sender Policy Framework lenient on permitted source domains	Unauthorised sources able to send messages;	Low	-all should be used[2]

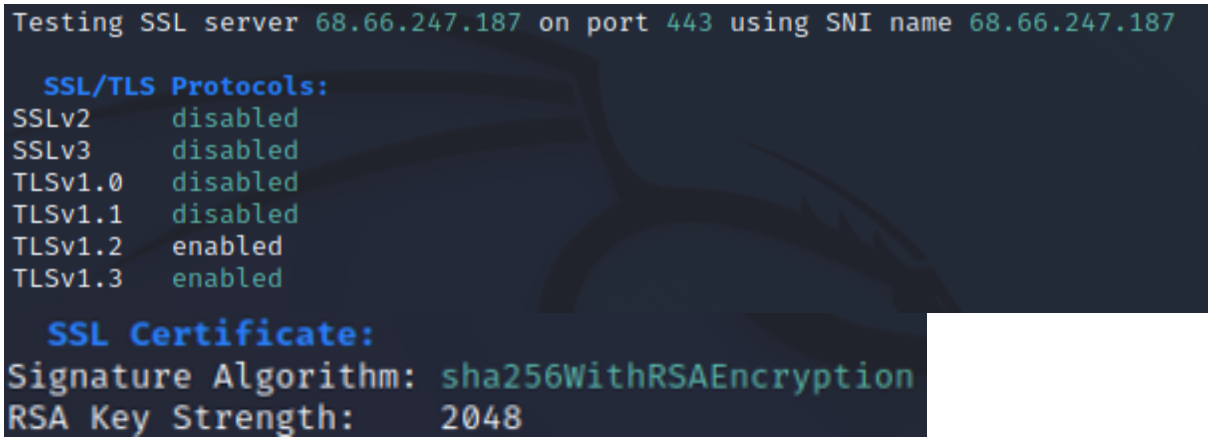
[2] www.upguard.com. (2022). *Instant Security Report | UpGuard Cyber Security Ratings*. [online] Available at: https://www.upguard.com/instant-security-score/report?c=loadedwithstuff.co.uk.

2.1 Open ports

Open TCP Port: 53	NMAP
Open TCP Port: 21	NMAP
Open TCP Port: 80	NMAP
Open TCP Port: 110	NMAP
Open TCP Port: 143	NMAP
Open TCP Port: 443	NMAP
Open TCP Port: 995	NMAP
Open TCP Port: 993	NMAP
Open TCP Port: 2077	NMAP
Open TCP Port: 2078	NMAP
Open TCP Port: 2079	NMAP
Open TCP Port: 2082	NMAP
Open TCP Port: 2083	NMAP
Open TCP Port: 2086	NMAP
Open TCP Port: 2087	NMAP
Open TCP Port: 2095	NMAP
Open TCP Port: 2096	NMAP
Open TCP Port: 2525	NMAP
Open TCP Port: 3306	NMAP
Open TCP Port: 5432	NMAP
Open TCP Port: 6556	NMAP
Open TCP Port: 7822	NMAP
Open TCP Port: 37463	NMAP

3

2.2 SSL scan



Protocol TLSv1.2 protocol is enabled, and port 443 and 80 are open. Key strength 2048 categorises in 112 securities to NIST security standard. Key strength is valid until 2030 (NIST, 2020). The SSL encryption uses SHA-2 hash function. SSL certificate on the website is valid until 5 September 2022.
SSL report SSL Labs score: A+ (SSL Labs Report, 2022). No insecure SSL/TLS versions found (Upguard, 2022).

[3] HostedScan.com (n.d.). *HostedScan.com*. [online] HostedScan.com. Available at: https://hostedscan.com/risks.

2.3 GDPR compliance checklist

Security measure	Tool	Adequate on website	Risk	Improvements	Potential GDPR consequence
Privacy policy	Immuniweb.com	Good configuration	Low	n/a	n/a
Website security	Immuniweb.com	Components outdated and publicly known vulnerabilities	Critical	Update and configure as specified in recommendations	4% of global turnover, or 20 million euro
TLS Encryption	Immuniweb.com	Adequate	High	Ensure unsecure SSL channels are fixed, remove data transfers between secure/unsecure tunnels	Potential breach of GDPR.
Cookie Protection	Immuniweb.com	Inadequate	High	Configure cookie settings	Violation of ePrivacy directive
Cookie Disclaimer	Immuniweb.com	Inadequate	Critical	Implement	Violation of ePrivacy directive

Where is customer data processed? If sent to the US, legal implications apply, and no well-established solution applies since invalidation of Privacy shield[4]

2.4 PCI DSS Compliance

PCI DSS requirements apply to entities that store, process or transmit cardholder data. PCI DSS version 4.0 was realised March 2022 and sets out 12 core requirements merchants must adhere to. Although PCI DSS is not legally binding, it provides detailed guidance on how to protect data that is protected under the GDPR, which carries serious fine for non-compliance.[5]

1. Build and maintain secure network and systems
2. Apply secure configurations to all system components
3. Protect stored account data
4. Protect Cardholder data with strong cryptography during transmission over open public networks
5. Protect all systems and networks from malicious software
6. Develop and maintain secure systems and software
7. Restrict access to system components and cardholder data by business need to know
8. Identify users and authenticate access to system components
9. Restrict physical access to cardholder data
10. Log and monitor all access to system components and cardholder data

[4] Zalnieriute, Monika. "Data Transfers after Schrems II: The EU-US Disagreements over Data Privacy and National Security." Vanderbilt Journal of Transnational Law, vol. 55, no. 1, January 2022, pp. 1-48. HeinOnline.
[5] Itgovernance.co.uk. (2016). *PCI DSS | IT Governance UK*. [online] Available at: https://www.itgovernance.co.uk/pci_dss.

11. Test security of systems and networks regularly
12. Support information security with organisational policies and programs.[6]

No tool available for a scan of the website's capabilities, therefore, access must be given to current standards and practices.

3. Recommendations

1. Configure cookie settings – X-XSS, Content-Security-Header and SameSite to avoid GDPR fine.
2. Evaluate PCI DSS Compliance, take immediate action to avoid GDPR fine.
3. Update software, in particular Apache
4. Cookies missing Secure, HttpOnly and Samesite flag, ensure it does not store sensitive information.
5. Update outdated software
6. Hide company details behind buttons
7. Configure X-XSS, Content security header, and SameSite
8. Configure security flag in cookies, HttpOnly flag and Referer policy header
9. Implement custom error pages
10. Close port 21, 23

[6] Security Standards Council (2022) Payment Card industry – Data Security Standard – Requirements and Testing Procedures version 4.0 *PCI Security Standards Council* Available at: https://www.pcisecuritystandards.org/documents/PCI-DSS-v4_0.pdf?agreement=true&time=1648818981554 [Accessed: 20 July 2022]

References

SSL Lab Report (2022). *SSL Server Test: loadedwithstuff.co.uk (Powered by Qualys SSL Labs)*. [online] Available at: https://www.ssllabs.com/ssltest/analyze.html?d=loadedwithstuff.co.uk [Accessed 15 Jul. 2022].

HostedScan.com (2022). *HostedScan.com*. [online] HostedScan.com. Available at: https://hostedscan.com/risks [Accessed 25 Jul. 2022].

www.upguard.com. (2022). *Instant Security Report | UpGuard Cyber Security Ratings*. [online] Available at: https://www.upguard.com/instant-security-score/report?c=loadedwithstuff.co.uk [Accessed 15 Jul. 2022].

Itgovernance.co.uk. (2016). *PCI DSS | IT Governance UK*. [online] Available at: https://www.itgovernance.co.uk/pci_dss.

www.immuniweb.com. (2022). *Website Security Test | ImmuniWeb*. [online] Available at: https://www.immuniweb.com/websec/loadedwithstuff.co.uk/hu28bJCp/ [Accessed 15 Jul. 2022].

Security Standards Council (2022) Payment Card industry – Data Security Standard – Requirements and Testing Procedures version 4.0 *PCI Security Standards Council* Available at: https://www.pcisecuritystandards.org/documents/PCI-DSS-v4_0.pdf?agreement=true&time=1648818981554 [Accessed: 20 July 2022]

Zalnieriute, Monika. "Data Transfers after Schrems II: The EU-US Disagreements over Data Privacy and National Security." Vanderbilt Journal of Transnational Law, vol. 55, no. 1, January 2022, pp. 1-48. HeinOnline.

Pentest-Tools.com (2013). *Pentest-Tools.com | Powerful Pentesting Tools, Easy to Use*. [online] Pentest-Tools.com. Available at: https://pentest-tools.com/website-vulnerability-scanning/website-scanner