University of Essex Online

Network and Information Security Management March 2022 B

Development Team Project:
Executive Summary

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

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

21 May 2022

Introduction

Online commerce giant eBay announced in March of 2014 that hackers have stolen encrypted passwords and other credential information of their 145 million users. Although the breach did not involve the credit card number or financial information, the incident has caused a negative impact on eBay's reputation, and its share dropped 12.94% after the attack. (Andrea, 2014)

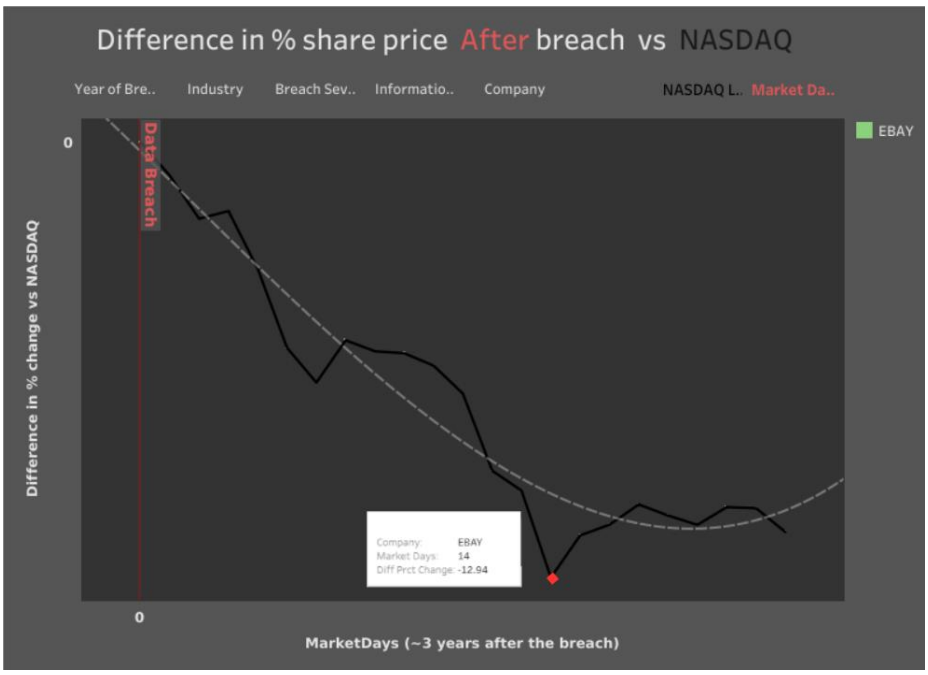


Figure 1: Difference in % share price after breach (Tableau ,2021)

As e-commercial websites have increasingly become the common target of hacking activities, it is necessary for companies to follow and adopt the best practice to minimize the vulnerabilities and risks of their web applications. 'Through risk assessment, we can understand the security situation and take targeted security measures which control the risk within an acceptable range.' (Lai Z. et al., 2016).

Executive Summary

This report gives the detailed results from a risk assessment performed on the ecommerce website https://loadedwithstuff.co.uk. The assessment focused on identifying threats and vulnerabilities applicable to the web application and the services running on the webserver. This evaluation also offers recommendations of risk mitigation to each of the identified system vulnerabilities. Furthermore, security standards compliance was simultaneously evaluated and suggestions for full compliance were also included.

Assessment Execution Schedule

Figure 2 shows the complete timeline from receiving the requirement until this report is ready to deliver. The illustration also highlights different stages when the security assessment was being carried out.

Figure 2. Timeline of the whole project

System Characteristics

With the use of several network utilities, the following information can be retrieved from the website at the time the assessment was performed.

Domain Name	loadedwithstuff.co.uk
Top Level Domain	UK (United Kingdom)
IP Address	68.66.247.187
DNS Server	ns1.a2hosting.com ns2.a2hosting.com ns3.a2hosting.com ns4.a2hosting.com
ASNN	AS55293
Geolocation	US (United States), MI, Michigan, 48106 Ann Arbor
Reverse DNS	68.66.247.187.static.a2webhosting.com
HTTP Server	Apache
PHP	7.4.29
Software	Loaded Commerce Community Edition v6.6 jQuery 1.12.4 Bootstrap 3.3.6, 3.3.7
Email	sales@loadedwithstuff.co.uk
Hosts	autodiscover.loadedwithstuff.co.uk:68.66.247.187 cpanel.loadedwithstuff.co.uk:68.66.247.187 cpcalendars.loadedwithstuff.co.uk:68.66.247.187 cpcontacts.loadedwithstuff.co.uk:68.66.247.187 mail.loadedwithstuff.co.uk:68.66.247.187 webdisk.loadedwithstuff.co.uk:68.66.247.187 webmail.loadedwithstuff.co.uk:68.66.247.187 www.loadedwithstuff.co.uk:68.66.247.187

Ports and Services Scanning

The following network ports and the associated services were discovered during the assessment. It is recommended to review and understand what processes or protocols are using the ports. Any ports that the system admins do not recognize might indicate a security vulnerability (SecurityScorecard, 2020).

PORT	STATE	SERVICE	VERSION
21/tcp	open	ftp	Pure-FTPd
25/tcp	open	smtp?	
53/tcp	open	domain	ISC BIND 9.11.4-P2 (RedHat Enterprise Linux 7)
53/udp	open	domain	
80/tcp	open	http	Apache httpd (W3 Total Cache/0.9.4.6.4)
110/tcp	open	pop3	Dovecot pop3d
143/tcp	open	imap	Dovecot imapd
443/tcp	open	ssl/http	Apache httpd (W3 Total Cache/0.9.4.6.4)
465/tcp	open	ssl/smtp	Exim smtpd 4.94.2
587/tcp	open	smtp	Exim smtpd 4.94.2
993/tcp	open	ssl/imap	Dovecot imapd
995/tcp	open	ssl/pop3	Dovecot pop3d
2525/tcp	open	smtp	Exim smtpd 4.94.2
3306/tcp	open	mysql	MySQL 5.5.5-10.3.23-MariaDB-cll-lve
5432/tcp	open	postgresql	PostgreSQL DB 9.6.0 or later
6556/tcp	filtered	Checkmk-agent	
7822/tcp	filtered	unknown	

Summary of Findings

- SQL Injection testing was performed using SQLMap, the result shows that none of the tested parameters appear to be injectable. (Refer to Appendix C for the detailed log).
- During the testing period, it was observed that the website will block an IP address if it detects unusual traffic coming from that IP address. This states that an effective DDOS prevention mechanism has been implemented to protect the website.
- Besides the good indicators, the assessment has resulted in several security threats as can be summarized below. No issues of high impact were found. Six medium impact and nine low impact issues were identified (Chart 2).

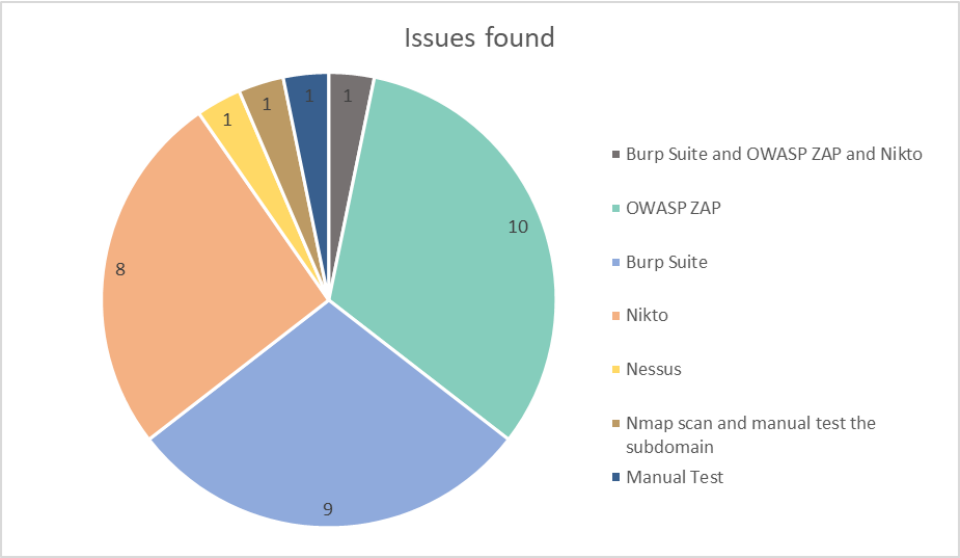


Chart 1: Issues found by tools

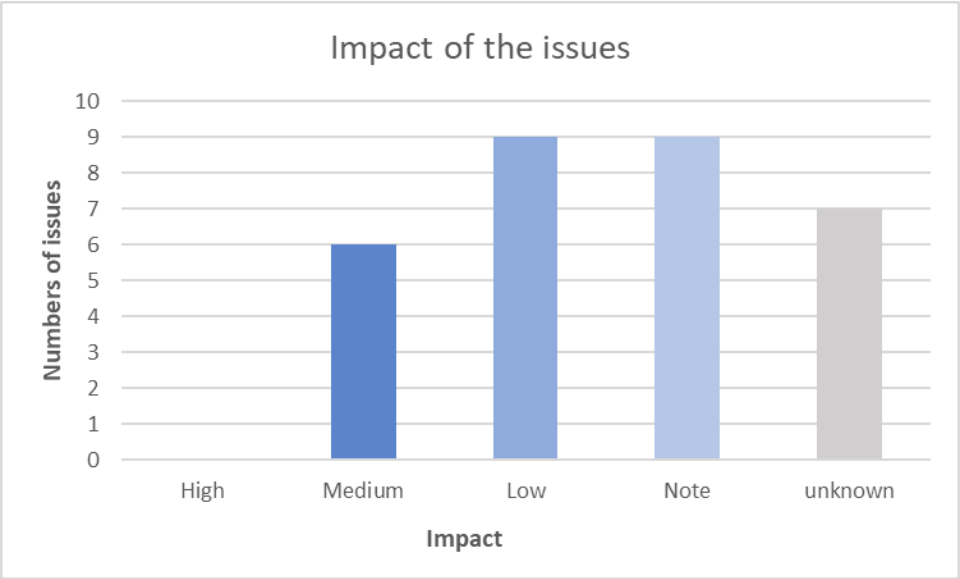


Chart 2: Impact of the issues

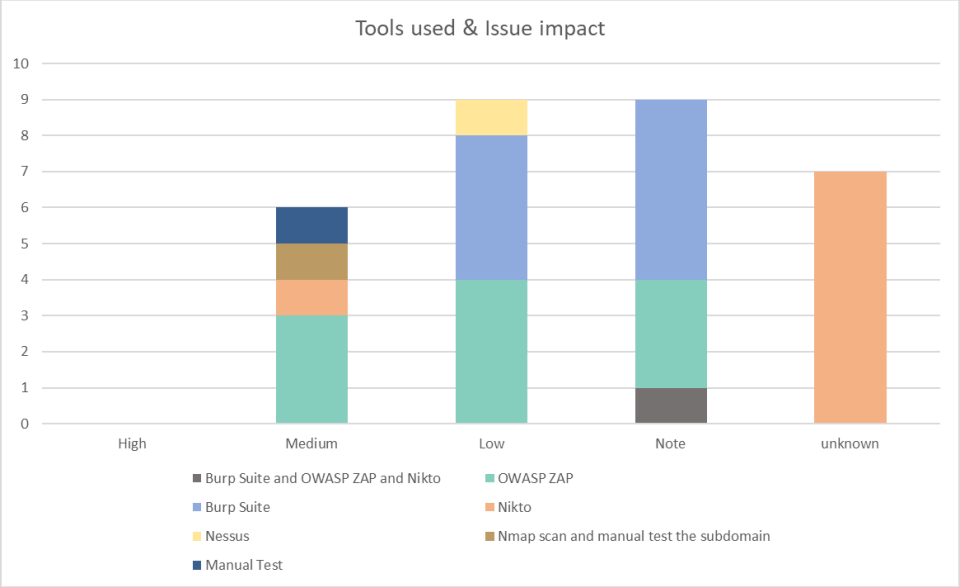


Chart 3: Tools used and Issue impact

Assessment Methodology

Assessment Tools

Following PTES guidelines, various tools were used to carry out the testing. The rationale for choosing these tools is listed below.

Testing Phase	Tool	Ranking/Popularity
Pre-Engagement **Interaction** **Information Gathering**	nslookup, whatweb, dig, whois	These popular tools are widely used and recommended by professionals and organizations in the cybersecurity industry.
Vulnerability Analysis **Exploitation** **Post-Exploitation**	OWASP Zap	Ranked #6 by PeerSpot, OWASP Zap is also one of the most popular tools used since it is free, provides automated attack operation and the results are interpreted comprehensively.
	Burp Suite	PeerSpot's top 10 tools in Fuzz Testing, AST, and app security tools. Having customer from big companies such as Google, Amazon, and NASA.
	Qualys SSL Labs	With a rating of 4.4 on Garter Peer Insights, it provides automated scanning, up-to-date threat & vulnerabilities database, and automated asset monitoring.
	Nmap	Having a score of 9.4 in TrustRadius, it provides a complete automated network scan. Popular among sysadmins.
	Nikto	An open-source tool that's being used and scaled up in Metasploit and Burp Suite.

Threat Modelling

Finding vulnerabilities is vital but estimating the associated risk to the business is just as important (OWASP, N.D.). The determination and categorization of threats during the

assessment process have employed OWASP's threat modelling process and risk rating since OWASP inherits STRIDE and DREAD for this purpose. The methodology details are available at:

- https://owasp.org/www-community/Threat_Modeling_Process#determine-and-rank-threats
- https://owasp.org/www-community/OWASP_Risk_Rating_Methodology

The risk severity of each finding can be summarized in the table below, where **Risk Severity** = **Likelihood** * **Impact**.

Overall Risk Severity				
Impact	HIGH	Medium	High	Critical
	MEDIUM	Low	Medium	High
	LOW	Note	Low	Medium
		LOW	MEDIUM	HIGH
	Likelihood			

Figure 3. Risk Severity (OWASP, n.d)

Detailed Findings

Six issues with the most impacts are listed in this section. They can be roughly categorized into exposure of internal resources, inappropriate settings, and vulnerable design or libraries (Chart 3). The full list of issues with low or informational impact can be found in the Appendix. It is recommended to update the related settings and components to minimize possible threats.

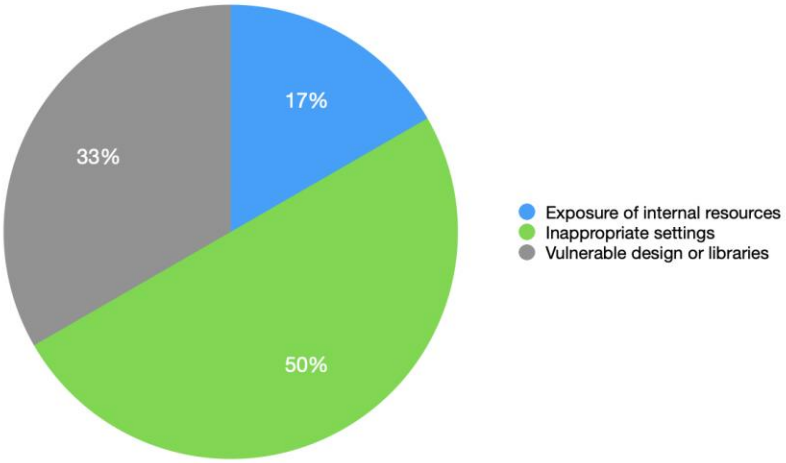


Chart 4: Threat by categories

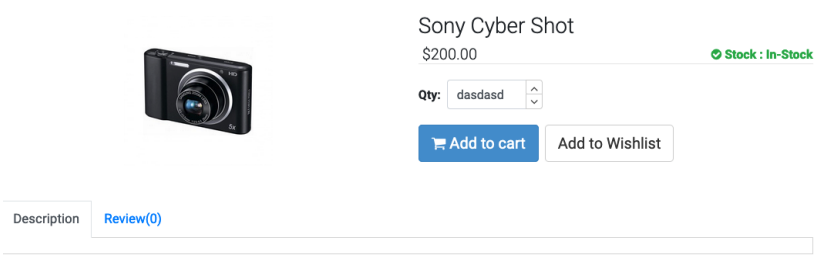
Threat	**Server vulnerable to BREACH attacks**
Description	The Content-Encoding header is set to ‘deflate’ which may be vulnerable to BREACH attacks
Risk Severity	Medium
Recommendation	Disabling the compression-only if the referrer is not the own application
Original Scan Result	Appendix D
Tool	Nikto
Reference	https://nvd.nist.gov/vuln/detail/CVE-2013-3587

Threat	**cPanel and Webmail are visible to the public**
Description	cPanel is supposed to be only accessible by administrators to manage the website content and users. Webmail is supposed to be only accessible by internal users. They should not be visible to the public as it may be vulnerable to Bruce Force Attack or Broken Access Control. URLs: https://cpanel.loadedwithstuff.co.uk/, https://webmail.loadedwithstuff.co.uk/
Risk Severity	Medium
Recommendation	Restrict the public users to access these URLs or automatically navigate them back to the homepage
Original Scan Result	Appendix E, Appendix F
Tool	Nmap scan and manually test the subdomain
Reference	https://owasp.org/Top10/A01_2021-Broken_Access_Control/ https://owasp.org/www-community/attacks/Brute_force_attack

Threat	**Absence of Anti-CSRF Tokens**
Description	CSRF attacks cause the victim users to carry out an action unintentionally. If the compomised user has a privileged role within the application, then the attacker might be able to take full control of all the application's data and functionality. (PortSwigger, n.d)
Risk Severity	Medium
Recommendation	• Generate and use a long and hard-to-guess CSFR token. • Strictly validate user's session in every case before the relevant action is executed (PortSwigger, n.d). • Utilise the built-in CSRF protection of the web frameworks if available. • Follow the potential mitigations suggested by MITRE (n.d) to handle improper encoding or escaping of output. More details at: https://cwe.mitre.org/data/definitions/116.html.
Original Scan Result	Appendix H
Tool	OWASP ZAP
Reference	http://projects.webappsec.org/Cross-Site-Request-Forgery http://cwe.mitre.org/data/definitions/352.html

Threat	**Content Security Policy (CSP) Header Not Set**
Description	Content Secure Policy is used to enhance the security of the resources such as Javascript, CSS. The CSP was designed to reduce the Cross Site Scripting (XSS) attacks. (Foundeo Inc, 2015)
Risk Severity	Medium
Recommendation	Ensure that the servers are configured to set the Content-Security-Policy header. CSP directive reference is accessible at: http://content-security-policy.com
Original Scan Result	Appendix I
Tool	OWASP ZAP
Reference	https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html http://www.w3.org/TR/CSP/ http://w3c.github.io/webappsec/specs/content-security-policy/csp-specification.dev.html http://www.html5rocks.com/en/tutorials/security/content-security-policy/ http://caniuse.com/#feat=contentsecuritypolicy

Threat	**Vulnerable JS Library**
Description	The identified library angularjs, version 1.6.9 is vulnerable.
Risk Severity	Medium
Recommendation	Upgrade to the latest version of angularjs
Original Scan Result	Appendix J
Tool	OWASP ZAP
Reference	https://github.com/angular/angular.js/commit/726f49dcf6c23106ddaf5cfd5e2e592841db743a https://github.com/advisories/GHSA-5cp4-xmrw-59wf https://nvd.nist.gov/vuln/detail/CVE-2020-7676 https://github.com/angular/angular.js/blob/master/CHANGELOG.md#179-pollution-eradication-2019-11-19

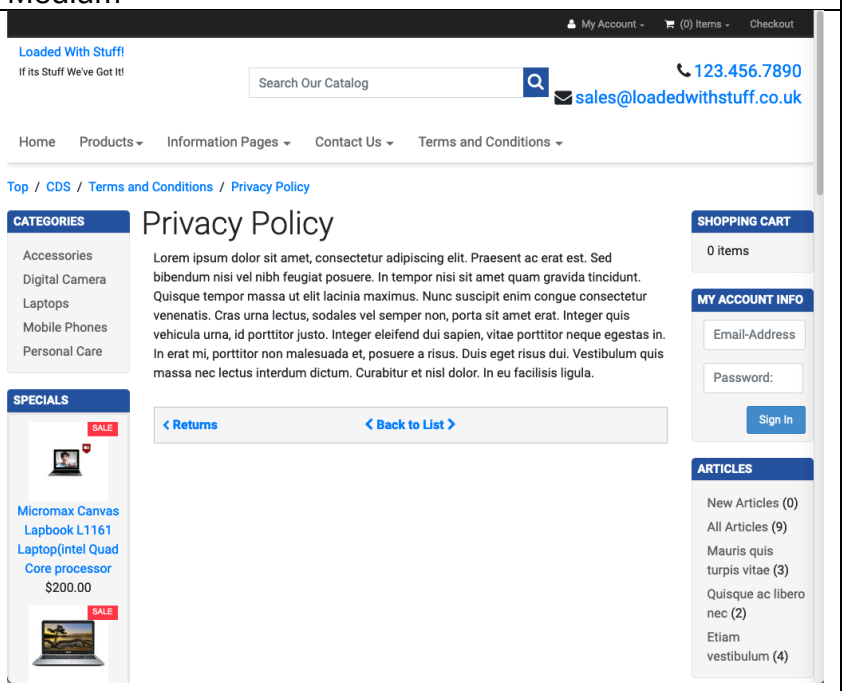
Threat	**Absence of data validation**
Description	Every field in a form should be validated in the corresponding validation form. (OWASP, n.d). Unchecked input is the root cause of security problems such as cross-site scripting, SQL injection.
Risk Severity	Medium
Recommendation	Perform validation for all the form inputs before sending any requests to the server.
Original Test Result	
Tool	Manual Test
Reference	https://owasp.org/www-community/vulnerabilities/Improper_Data_Validation

Security Standards Compliance Analysis

The website is evaluated against the GDPR and PCI DSS. Several non-compliances were identified, and immediate remedy actions are recommended to be implemented to avoid legal consequences.

GDPR Compliance Analysis

1. Privacy Policy

Description	Article 13 of GDPR requires a conspicuously visible notice of the personal data subjects collected by web applications.
Result	The Privacy Policy link is always available at the bottom section. However, the content only contains dummy texts.
Risk Severity	Medium
Screenshot	
Recommendation	Add meaningful content inform site's visitors about how the website collects, uses, stores, and discloses their personal data

2. Website Security

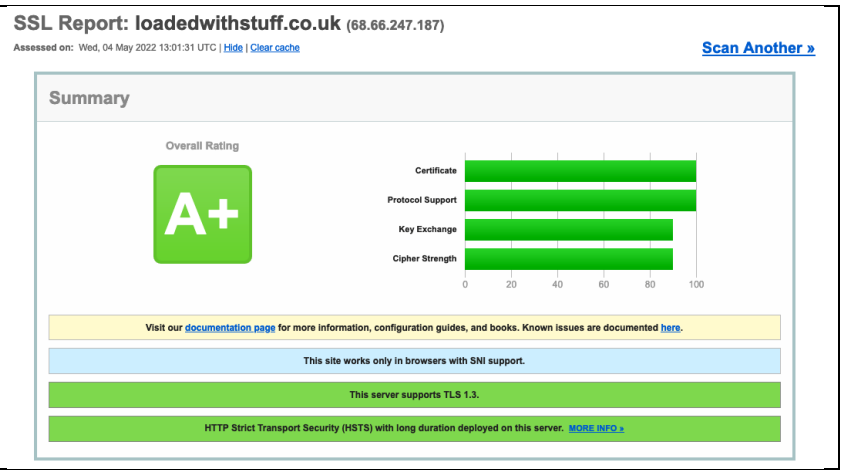
Description	Article 5(1)(f), Article 24(1) and Article 32 of GDPR require implementation, regular website security testing, and maintenance of adequate security controls to protect personal data.

Screenshot	
	`> ./whatweb -v https://loadedwithstuff.co.uk`
	`WhatWeb report for https://loadedwithstuff.co.uk`
	`Status  : 200 OK`
	`Title  : Captcha`
	`IP  : 68.66.247.187`
	`Country  : UNITED STATES, US`
	
	`Summary  : Bootstrap[3.3.6,3.3.7], Cookies[cl-bypass-cache], HTML5, HTTPServer[imunify360-webshield/1.18], HttpOnly[cl-bypass-cache], JQuery[1.12.4], PoweredBy[Imunify360], Script, UncommonHeaders[cf-edge-cache]`

Result	**Bootstrap version 3.3.7** is being used. This version is vulnerable to Cross-site Scripting (XSS) as reported in: • https://security.snyk.io/vuln/SNYK-JS-BOOTSTRAP-173700 • https://security.snyk.io/vuln/SNYK-JS-BOOTSTRAP-72889 • https://security.snyk.io/vuln/SNYK-JS-BOOTSTRAP-72890 • https://security.snyk.io/vuln/npm:bootstrap:20160627 • https://security.snyk.io/vuln/npm:bootstrap:20180529 **JQuery version 1.12.4** is being used. This version is vulnerable to Cross-site Scripting (XSS) and Prototype Pollution as reported in: • https://security.snyk.io/vuln/SNYK-JS-JQUERY-567880 • https://security.snyk.io/vuln/SNYK-JS-JQUERY-565129 • https://security.snyk.io/vuln/SNYK-JS-JQUERY-174006 • https://security.snyk.io/vuln/npm:jquery:20150627
Risk Severity	Medium
Reference	https://snyk.io/test/npm/bootstrap/3.3.7 https://snyk.io/test/npm/jquery/1.12.4
Recommendation	Upgrade to bootstrap@3.4.1 or higher version. Upgrade to jquery@3.5.0 or higher version.

3. TLS Encryption

Description	Article 5(1)(f), Article 24(1) and Article 32 of GDPR require implementation, regular website security testing, and maintenance of adequate security controls to protect personal data.
Result	No issue found. TLS is implemented properly.
Tool	https://www.ssllabs.com

Screenshot	
Recommendation	• Regularly check and make sure the SSL certificates are not expired. • Setup notification to alert the system admin when the SSL certificates are going to expire.

4. Cookie Protection

Description	Article 32 of GDPR requires implementation of data encryption while the data is being processed. This requirement applies to cookies as they contain personal data or identifiers attributable to data subjects (see GDPR Recital 30).
Result	Cookies with personal or tracking information are sent without a Secure flag.
Recommendation	All cookies used to transmit sensitive data should have a secure flag set. The session tokens should never be sent over unencrypted communications.

5. Cookie Disclaimer

Description	In addition to Article 13 of GDPR, the EU ePrivacy Directive requires website operators to obtain an informed data subject's consent prior to setting any cookies except strictly necessary cookies.
Result	Cookies with tracking information were sent, but no cookie disclaimer was found on the website.
Recommendation	Add a cookie banner to inform visitors about how the website uses cookies, what information will be stored, and user right to refuse the storage of cookies.

PCI DSS Compliance Analysis

The website falls into a CDE (Cardholder Data Environment) scope, the following requirements of PCI DSS have been tested to verify its compliance with the standards.

Requirement	Description
Requirement 6.2	Install applicable vendor-supplied security patches to protect all system components and software from known vulnerabilities. Install critical security patches no later than one month after they are released.
Requirement 6.5	Address the following common coding flaws in software development processes: 1. Regularly conduct training for developers to catch up with the most recent secure coding techniques. 2. Design and develop applications based on secure coding guidelines and best practices
Requirement 6.6	The requirement for application review or installation of web-application firewalls to intentionally reduce the number of compromises on public web applications caused by poor implementation or maintenance practices.

The table below shows the results of PCI DSS analysis.

Requirement	Result	Recommendation
Requirement 6.2	The target website is not being complied with the requirement 6.2, 6.5 as it contains the vulnerabilities in the web application software. Refer to the Website Security result in GDPR compliance section for the details of outdated components.	Refer to the Website Security result in GDPR compliance section for the suggested mitigations.
Requirement 6.5		
Requirement 6.6	No WAF (Web Application Firewall) was detected on the website using the following nmap script. ***nmap --script=http-waf-fingerprint loadedwithstuff.co.uk***	Implement a WAF to protect the website against common web attacks.

Conclusion

Regarding the technical side, no major immediate threats have been identified, however, quite several non-compliances with related standards. It is our

recommendation to make compliances with GDPR and PCI DSS top priority as it may result in penalties from the authorities. Other vulnerabilities should be addressed next and incorporating regular reviews and testing are recommended in the development or business cycle.

References

Andrea, P. (2014) eBay asks 145 million users to change passwords after data breach - The Washington Post. Available from https://www.washingtonpost.com/news/the-switch/wp/2014/05/21/ebay-asks-145-million-users-to-change-passwords-after-data-breach/ [Accessed 14 May 2022].

Foundeo Inc. (2015) Content Security Policy CSP Reference & Examples. Content-security-policy.com. Available from: https://content-security-policy.com/. [Accessed 21 May 2022]

Lai, Z., Shen, Y., & Zhang, G. (2016) A security risk assessment method of website based on threat analysis combined with AHP and entropy weight. *Proceedings of the IEEE International Conference on Software Engineering and Service Sciences, ICSESS* 0: 481–484. https://doi.org/10.1109/ICSESS.2016.7883113

OWASP. (N.D.) Cross-Site Request Forgery Prevention · OWASP Cheat Sheet Series. Available from: https://cheatsheetseries.owasp.org/cheatsheets/Cross-Site_Request_Forgery_Prevention_Cheat_Sheet.html. [Accessed 4 May 2022]

OWASP. (N.D.) Improper Data Validation | OWASP. Available from: https://owasp.org/www-community/vulnerabilities/Improper_Data_Validation [Accessed 21 May 2022].

OWASP. (N.D.) OWASP Risk Rating Methodology. Available from: https://owasp.org/www-community/OWASP_Risk_Rating_Methodology. [Accessed 21 May 2022]

Portswigger.net. (2019) What is CSRF (Cross-site request forgery)? Tutorial & Examples. Available from: https://portswigger.net/web-security/csrf. [Accessed 21 May 2022]

PTES. (2014) The Penetration Testing Execution Standard. Pentest-standard.org. Available from: http://www.pentest-standard.org/index.php/Main_Page. [Access 21 May 2022]

securityscorecard.com. (2020). How Can You Secure Risky Open Ports? | SecurityScorecard. Available at: https://securityscorecard.com/blog/how-can-you-secure-risky-open-ports [Accessed 22 May 2022].

Tableau. (2021) Data Breach vs Share Price Analysis 2020 | Tableau Public. Available from: https://public.tableau.com/app/profile/paul.bischoff/viz/DataBreachvsSharePriceAnalysis2020/DifferenceinchangeAfterDataBreach [Accessed 16 May 2022].

Appendix

Low and Informational threats

Threat	**POP3 Cleartext Logins Permitted**
Description	The remote host is running a POP3 daemon that allows cleartext logins over unencrypted connections. An attacker can uncover user names and passwords by sniffing traffic to the POP3 daemon if a less secure authentication mechanism (eg, USER command, AUTH PLAIN, AUTH LOGIN) is used.
Risk Severity	Low
Recommendation	Encrypt traffic with SSL / TLS using stunnel
Original Scan Result	Appendix B
Tool	Nessus
Reference	https://tools.ietf.org/html/rfc2222 https://tools.ietf.org/html/rfc2595

Threat	**Password submitted using GET method**
Description	The page contains a form with the following action URL, which is submitted using the GET method: • https://loadedwithstuff.co.uk/ The form contains the following password field: • password
Risk Severity	Low
Recommendation	All forms submitting passwords should use the POST method. To achieve this, applications should specify the method attribute of the FORM tag as method="POST". It may also be necessary to modify the corresponding server-side form handler to ensure that submitted passwords are properly retrieved from the message body, rather than the URL.
Original Scan Result	Appendix G
Tool	Burp Suite
Reference	https://cwe.mitre.org/data/definitions/598.html https://capec.mitre.org/data/definitions/37.html

Threat	**Password field with autocomplete enabled**
Description	The page contains a form with the following action URL: • https://loadedwithstuff.co.uk/index.php?rt=core/login The form contains the following password field with autocomplete enabled: • password This issue was found in multiple locations under the reported path.

Risk Severity	Low
Recommendation	To prevent browsers from storing credentials entered into HTML forms, include the attribute autocomplete="off" within the FORM tag (to protect all form fields) or within the relevant INPUT tags (to protect specific individual fields). Please note that modern web browsers may ignore this directive. In spite of this there is a chance that not disabling autocomplete may cause problems obtaining PCI compliance.
Original Scan Result	Appendix G
Tool	Burp Suite
Reference	https://cwe.mitre.org/data/definitions/200.html

Threat	**Vulnerable JavaScript dependency**
Description	We observed a vulnerable JavaScript library. We detected jquery version 3.4.1.min, which has the following vulnerabilities: • CVE-2020-11022: Regex in its jQuery.htmlPrefilter sometimes may introduce XSS • CVE-2020-11023: Regex in its jQuery.htmlPrefilter sometimes may introduce XSS
Risk Severity	Low
Recommendation	Develop a patch-management strategy to ensure that security updates are promptly applied to all third-party libraries in your application. Also, consider reducing your attack surface by removing any libraries that are no longer in use.
Original Scan Result	Appendix G
Tool	Burp Suite
Reference	https://cwe.mitre.org/data/definitions/1104.html https://owasp.org/www-project-top-ten/2017/A9_2017-Using_Components_with_Known_Vulnerabilities

Threat	**TLS certificate**
Description	The server presented a valid, trusted TLS certificate. This issue is purely informational. The server presented the following certificates: **Server certificate** Issued to: , loadedwithstuff.co.uk, autodiscover.loadedwithstuff.co.uk, cpanel.loadedwithstuff.co.uk, cpcalendars.loadedwithstuff.co.uk, cpcontacts.loadedwithstuff.co.uk, loadedwithstuff.tech-sourcery.co.uk, mail.loadedwithstuff.co.uk, webdisk.loadedwithstuff.co.uk,

	webmail.loadedwithstuff.co.uk, www.loadedwithstuff.co.uk, www.loadedwithstuff.tech-sourcery.co.uk Issued by: , cPanel\ Valid from: , Wed Mar 23 02:00:00 EET 2022 Valid to: , Wed Jun 22 02:59:59 EEST 2022 **Certificate chain #1** Issued to: , cPanel\ Issued by: , COMODO RSA Certification Authority Valid from: , Mon May 18 03:00:00 EEST 2015 Valid to: , Sun May 18 02:59:59 EEST 2025 **Certificate chain #2** Issued to: , COMODO RSA Certification Authority Issued by: , AAA Certificate Services Valid from: , Thu Jan 01 02:00:00 EET 2004 Valid to: , Mon Jan 01 01:59:59 EET 2029 **Certificate chain #3** Issued to: , AAA Certificate Services Issued by: , AAA Certificate Services Valid from: , Thu Jan 01 02:00:00 EET 2004 Valid to: , Mon Jan 01 01:59:59 EET 2029
Risk Severity	Note
Recommendation	TLS (or SSL) helps to protect the confidentiality and integrity of information in transit between the browser and server, and to provide authentication of the server's identity. To serve this purpose, the server must present an TLS certificate that is valid for the server's hostname, is issued by a trusted authority and is valid for the current date. If any one of these requirements is not met, TLS connections to the server will not provide the full protection for which TLS is designed.
Original Scan Result	Appendix G
Tool	Burp Suite
Reference	https://cwe.mitre.org/data/definitions/295.html https://cwe.mitre.org/data/definitions/326.html https://cwe.mitre.org/data/definitions/327.html

Threat	**TLS cookie without secure flag set**
Description	The following cookie was issued by the application and does not have the secure flag set: • lcsid The cookie does not appear to contain a session token, which may reduce the risk associated with this issue. You should review the contents of the cookie to determine its function.This issue was found in multiple locations under the reported path.

Risk Severity	Note
Recommendation	The secure flag should be set on all cookies that are used for transmitting sensitive data when accessing content over HTTPS. If cookies are used to transmit session tokens, then areas of the application that are accessed over HTTPS should employ their own session handling mechanism, and the session tokens used should never be transmitted over unencrypted communications.
Original Scan Result	Appendix G
Tool	Burp Suite
Reference	https://cwe.mitre.org/data/definitions/614.html

Threat	**Cross-domain Referer leakage**
Description	The application contains the following link to another domain from URLs containing a query string: • https://www.facebook.com/loadedcommerce/?CDpath=6_9 This issue was found in multiple locations under the reported path.
Risk Severity	Note
Recommendation	Applications should never transmit any sensitive information within the URL query string. In addition to being leaked in the Referer header, such information may be logged in various locations and may be visible on-screen to untrusted parties. If placing sensitive information in the URL is unavoidable, consider using the Referer-Policy HTTP header to reduce the chance of it being disclosed to third parties.
Original Scan Result	Appendix G
Tool	Burp Suite
Reference	https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy https://portswigger.net/web-security/information-disclosure

Threat	**Cookie without HttpOnly flag set**
Description	The following cookie was issued by the application and does not have the HttpOnly flag set: • lcsid The cookie does not appear to contain a session token, which may reduce the risk associated with this issue. You should review the contents of the cookie to determine its function.This issue was found in multiple locations under the reported path.
Risk Severity	Note
Recommendation	There is usually no good reason not to set the HttpOnly flag on all cookies. Unless you specifically require legitimate client-side scripts within your application to

	read or set a cookie's value, you should set the HttpOnly flag by including this attribute within the relevant Set-cookie directive. You should be aware that the restrictions imposed by the HttpOnly flag can potentially be circumvented in some circumstances, and that numerous other serious attacks can be delivered by client-side script injection, aside from simple cookie stealing.
Original Scan Result	Appendix G
Tool	Burp Suite
Reference	https://portswigger.net/web-security/cross-site-scripting/exploiting https://portswigger.net/research/web-storage-the-lesser-evil-for-session-tokens#httponly

Threat	**Email addresses disclosed**
Description	The following email address was disclosed in the response: • sales@example.com This issue was found in multiple locations under the reported path.
Risk Severity	Note
Recommendation	Consider removing any email addresses that are unnecessary, or replacing personal addresses with anonymous mailbox addresses (such as helpdesk@example.com). To reduce the quantity of spam sent to anonymous mailbox addresses, consider hiding the email address and instead providing a form that generates the email server-side, protected by a CAPTCHA if necessary.
Original Scan Result	Appendix G
Tool	Burp Suite
Reference	https://portswigger.net/web-security/information-disclosure

Threat	**Robots.txt file**
Description	The web server contains a robots.txt file. The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
Risk Severity	Note

Recommendation	The robots.txt file is not itself a security threat, and its correct use can represent good practice for non-security reasons. You should not assume that all web robots will honor the file's instructions. Rather, assume that attackers will pay close attention to any locations identified in the file. Do not rely on robots.txt to provide any kind of protection over unauthorized access. For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must-revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Original Scan Result	Appendix G
Tool	Burp Suite and OWASP ZAP
Reference	https://cwe.mitre.org/data/definitions/200.html https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html#web-content-caching https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Cache-Control

Threat	**Entries in robots.txt returned a non-forbidden or redirect HTTP code (200)**
Description	line: /temp/ + Entry '/temp/' in robots.txt returned a non-forbidden or redirect HTTP code (200) line: /templates/ line: /admin/ + Entry '/admin/' in robots.txt returned a non-forbidden or redirect HTTP code (200) line: /cert/ + Entry '/cert/' in robots.txt returned a non-forbidden or redirect HTTP code (200) line: /ext/ line: /debug/ + Entry '/debug/' in robots.txt returned a non-forbidden or redirect HTTP code (200) line: /wpcallback.php + Entry '/wpcallback.php' in robots.txt returned a non-forbidden or redirect HTTP code (200) line: /paypal_notify.php + Entry '/paypal_notify.php' in robots.txt returned a non-forbidden or redirect HTTP code (200) line: /ipn.php + Entry '/ipn.php' in robots.txt returned a non-forbidden or redirect HTTP code (500) line: /pear/ + Entry '/pear/' in robots.txt returned a non-forbidden or redirect HTTP code (200)

	line: /tmp/ + Entry '/tmp/' in robots.txt returned a non-forbidden or redirect HTTP code (200) line: /pub/ + Entry '/pub/' in robots.txt returned a non-forbidden or redirect HTTP code (200) line: /includes/ line: /download/ + Entry '/download/' in robots.txt returned a non-forbidden or redirect HTTP code (200) line: /cache/ + Entry '/cache/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
Risk Severity	Note
Recommendation	
Original Scan Result	Appendix D
Tool	Nikto
Reference	N/A

Threat	**Cacheable HTTPS response**
Description	Unless directed otherwise, browsers may store a local cached copy of content received from web servers. Some browsers, including Internet Explorer, cache content accessed via HTTPS. If sensitive information in application responses is stored in the local cache, then this may be retrieved by other users who have access to the same computer at a future time.
Risk Severity	Note
Recommendation	Applications should return caching directives instructing browsers not to store local copies of any sensitive data. Often, this can be achieved by configuring the web server to prevent caching for relevant paths within the web root. Alternatively, most web development platforms allow you to control the server's caching directives from within individual scripts. Ideally, the web server should return the following HTTP headers in all responses containing sensitive content: • Cache-control: no-store • Pragma: no-cache
Original Scan Result	Appendix G
Tool	Burp Suite
Reference	https://portswigger.net/web-security/information-disclosure

Threat	**Application Error Disclosure**

Description	A page contains an error/warning message that may disclose sensitive information like the location of the file that produced the unhandled exception. This information can be used to launch further attacks against the web application. The alert could be a false positive if the error message is found inside a documentation page. URL: https://loadedwithstuff.co.uk/ipn.php
Risk Severity	Low
Recommendation	Review the source code of this page. Implement custom error pages. Consider implementing a mechanism to provide a unique error reference/identifier to the client (browser) while logging the details on the server side and not exposing them to the user.
Original Scan Result	Appendix K
Tool	OWASP ZAP
Reference	https://owasp.org/Top10/A05_2021-Security_Misconfiguration/

Threat	**Cookie without SameSite Attribute**
Description	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Risk Severity	Low
Recommendation	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Original Scan Result	Appendix L
Tool	OWASP ZAP
Reference	https://tools.ietf.org/html/draft-ietf-httpbis-cookie-same-site

Threat	**Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)**
Description	The web/application server is leaking information via one or more "X-Powered-By" HTTP response headers. Access to such information may facilitate attackers identifying other frameworks/components your web application is reliant upon and the vulnerabilities such components may be subject to.
Risk Severity	Low
Recommendation	Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.
Original Scan Result	Appendix M
Tool	OWASP ZAP

Reference	http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.aspx http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html

Threat	**Timestamp Disclosure**
Description	A timestamp was disclosed by the application/web server
Risk Severity	Low
Recommendation	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Original Scan Result	Appendix N
Tool	OWASP ZAP
Reference	http://projects.webappsec.org/w/page/13246936/Information%20Leakage

Threat	**Information Disclosure - Sensitive Information in URL**
Description	The request appeared to contain sensitive information leaked in the URL. This can violate PCI and most organizational compliance policies. You can configure the list of strings for this check to add or remove values specific to your environment. Example: https://loadedwithstuff.co.uk/?email=foo-bar%40example.com&enquiry&name=ZAP&self=on&subject=ZAP&topic=Tracking&urgent=on
Risk Severity	Note
Recommendation	Do not pass sensitive information in URIs, or those information must be encrypted.
Original Scan Result	Appendix O
Tool	OWASP ZAP
Reference	https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html

Threat	**Information Disclosure - Suspicious Comments**
Description	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments. Example: https://loadedwithstuff.co.uk/index.php?rt=core/shopping_cart The following pattern was used: \bSELECT\b and was detected 2 times, the first in the element starting with: "<script type="text/javascript"><!-- var form = ""; var submitted = false;

	var error = false; var error_message = "";
Risk Severity	Note
Recommendation	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Original Scan Result	Appendix P
Tool	OWASP ZAP
Reference	https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html

Threat	**Information Disclosure - Suspicious Comments**

Description	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
	Example:
	https://loadedwithstuff.co.uk/index.php?rt=core/shopping_cart
	
	The following pattern was used: \bSELECT\b and was detected 2 times, the first in the element starting with:
	"<script type="text/javascript"><!--
	var form = "";
	var submitted = false;
	var error = false;
	var error_message = "";

Risk Severity	Note
Recommendation	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Original Scan Result	Appendix P
Tool	OWASP ZAP
Reference	https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html

Threat	**Retrieved x-powered-by header: PHP/7.4.29**
Description	The X-Powered-By header describes the technologies used by the webserver. This information exposes the server to attackers. Using the information in this header, attackers can find vulnerabilities easier.
Risk Severity	Note
Recommendation	Remove all X-Powered-By headers.
Original Scan Result	Appendix D
Tool	Nikto

Reference	https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Headers_Cheat_Sheet.html

Threat	**Cookie lcsid created without the secure flag**
Description	If the secure flag is set on a cookie, then browsers will not submit the cookie in any requests that use an unencrypted HTTP connection, thereby preventing the cookie from being trivially intercepted by an attacker monitoring network traffic. If the secure flag is not set, then the cookie will be transmitted in clear-text if the user visits any HTTP URLs within the cookie's scope. An attacker may be able to induce this event by feeding a user suitable links, either directly or via another web site.
Risk Severity	Note
Recommendation	The secure flag should be set on all cookies that are used for transmitting sensitive data.
Original Scan Result	Appendix D
Tool	Nikto
Reference	https://portswigger.net/kb/issues/00500200_tls-cookie-without-secure-flag-set

Threat	**Cookie lcsid created without the httponly flag**
Description	If the HttpOnly attribute is set on a cookie, then the cookie's value cannot be read or set by client-side JavaScript. This measure makes certain client-side attacks, such as cross-site scripting, slightly harder to exploit by preventing them from trivially capturing the cookie's value via an injected script.
Risk Severity	Note
Recommendation	Set the HttpOnly flag on all cookies.
Original Scan Result	Appendix D
Tool	Nikto
Reference	https://portswigger.net/kb/issues/00500600_cookie-without-httponly-flag-set

Threat	Uncommon header 'x-redirect-by' found, with contents: WordPress
Description	WordPress is indicated in the ‘x-redirect-by' header. It may expose to public the technolocy stack of the website and make the site more vulnerable to attacks.
Risk Severity	Note
Recommendation	Disable the ‘x-redirect-by' header
Original Scan Result	Appendix D

Tool	Nikto
Reference	https://webtechsurvey.com/response-header/x-redirect-by

Appendix A – Nmap Scan Result

```
❯ sudo nmap -sU loadedwithstuff.co.uk
Password:
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-01 12:10 +07
Nmap scan report for loadedwithstuff.co.uk (68.66.247.187)
Host is up (0.36s latency).
rDNS record for 68.66.247.187: 68.66.247.187.static.a2webhosting.com
Not shown: 998 closed udp ports (port-unreach)
PORT       STATE         SERVICE
53/udp     open          domain
21780/udp  open|filtered unknown
```

UDP Scan Result

```
❯ sudo nmap -sV loadedwithstuff.co.uk
Password:
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-01 12:13 +07
Nmap scan report for loadedwithstuff.co.uk (68.66.247.187)
Host is up (0.33s latency).
rDNS record for 68.66.247.187: 68.66.247.187.static.a2webhosting.com
Not shown: 889 filtered tcp ports (no-response), 26 filtered tcp ports (port-unreach), 1 filtered tcp ports
(admin-prohibited), 70 closed tcp ports (reset)
PORT     STATE SERVICE    VERSION
21/tcp   open  ftp        Pure-FTPd
25/tcp   open  smtp?
53/tcp   open  domain     ISC BIND 9.11.4-P2 (RedHat Enterprise Linux 7)
80/tcp   open  http       Apache httpd (W3 Total Cache/0.9.4.6.4)
110/tcp  open  pop3       Dovecot pop3d
143/tcp  open  imap       Dovecot imapd
443/tcp  open  ssl/http   Apache httpd (W3 Total Cache/0.9.4.6.4)
465/tcp  open  ssl/smtp   Exim smtpd 4.94.2
587/tcp  open  smtp       Exim smtpd 4.94.2
993/tcp  open  ssl/imap   Dovecot imapd
995/tcp  open  ssl/pop3   Dovecot pop3d
2525/tcp open  smtp       Exim smtpd 4.94.2
3306/tcp open  mysql      MySQL 5.5.5-10.3.23-MariaDB-cll-lve
5432/tcp open  postgresql PostgreSQL DB 9.6.0 or later
1 service unrecognized despite returning data. If you know the service/version, please submit the following
fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port5432-TCP:V=7.92%I=7%D=5/1%Time=626E1729%P=x86_64-apple-darwin17.7.0
SF:%r(SMBProgNeg,8C,"E\0\0\0\x8bSFATAL\0VFATAL\0C0A000\0Munsupported\x20fr
SF:ontend\x20protocol\x2065363\.19778:\x20server\x20supports\x201\.0\x20to
SF:\x203\.0\0Fpostmaster\.c\0L2050\0RProcessStartupPacket\0\0");
Service Info: Host: nl1-ss5.a2hosting.com; OS: Linux; CPE: cpe:/o:redhat:enterprise_linux:7

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 214.46 seconds
```

TCP Scan Result

Appendix B – POP3 Cleartext Logins Permitted

Vulnerabilities 22

LOW POP3 Cleartext Logins Permitted

Description

The remote host is running a POP3 daemon that allows cleartext logins over unencrypted connections. An attacker can uncover user names and passwords by sniffing traffic to the POP3 daemon if a less secure authentication mechanism (eg, USER command, AUTH PLAIN, AUTH LOGIN) is used.

Solution

Contact your vendor for a fix or encrypt traffic with SSL / TLS using stunnel.

See Also

https://tools.ietf.org/html/rfc2222
https://tools.ietf.org/html/rfc2595

Output

```
The following cleartext methods are supported :
USER
SASL PLAIN LOGIN
```

Port	Hosts
110 / tcp / pop3	68.66.247.187

Plugin Details

Severity:	Low
ID:	15855
Version:	$Revision: 1.22 $
Type:	remote
Family:	Misc.
Published:	November 30, 2004
Modified:	June 12, 2017

Risk Information

Risk Factor: Low
CVSS v2.0 Base Score: 2.6
CVSS v2.0 Vector: CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N

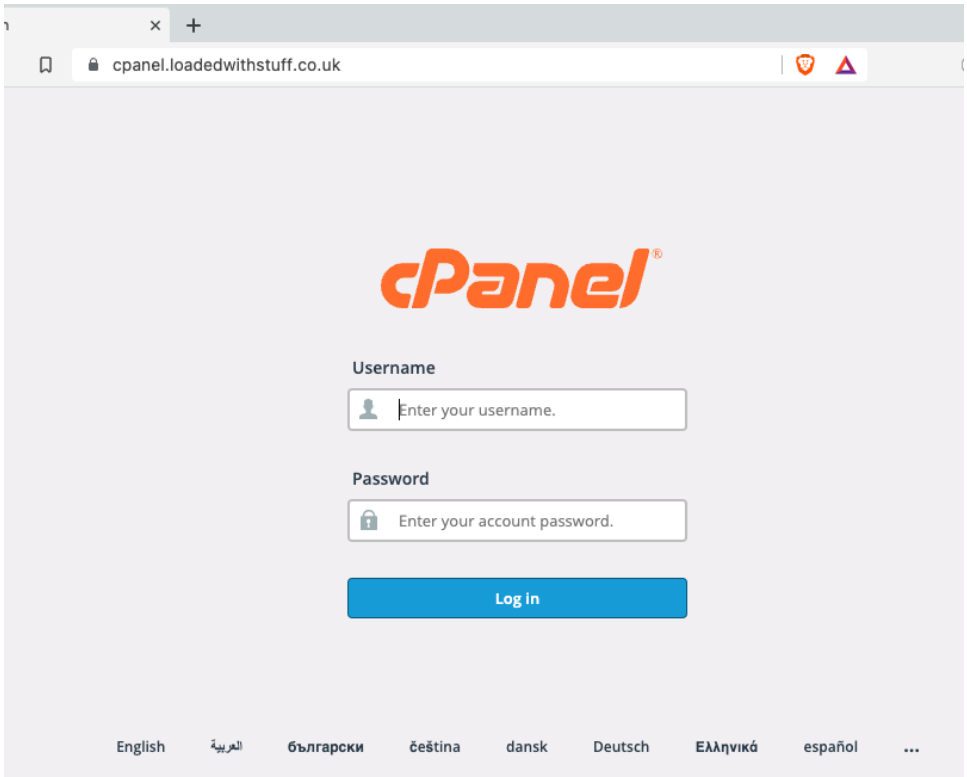
Appendix C – SQLMap scan result

```
❯ sqlmap -u https://loadedwithstuff.co.uk/index.php\?rt\=core/product_info\&products_id\=1 --dbs

        ___
       __H__
 ___ ___[(]_____ ___ ___  {1.6.4#stable}
|_ -| . [)]     | .'| . |
|___|_  [(]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsi
bility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse
 or damage caused by this program

[*] starting @ 23:23:08 /2022-05-01/

[23:23:08] [INFO] testing connection to the target URL
[23:23:10] [WARNING] the web server responded with an HTTP error code (403) which could interfere with the results of the tests
you have not declared cookie(s), while server wants to set its own ('lcsid=bdfdedbc76f...32eaa73636'). Do you want to use those [Y
/n] y
[23:23:29] [INFO] testing if the target URL content is stable
[23:23:31] [WARNING] target URL content is not stable (i.e. content differs). sqlmap will base the page comparison on a sequence m
atcher. If no dynamic nor injectable parameters are detected, or in case of junk results, refer to user's manual paragraph 'Page c
omparison'
how do you want to proceed? [(C)ontinue/(s)tring/(r)egex/(q)uit] c
[23:23:41] [INFO] testing if GET parameter 'rt' is dynamic
[23:23:42] [WARNING] GET parameter 'rt' does not appear to be dynamic
[23:23:44] [WARNING] heuristic (basic) test shows that GET parameter 'rt' might not be injectable
[23:23:45] [INFO] testing for SQL injection on GET parameter 'rt'
[23:23:45] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[23:24:07] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[23:24:11] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[23:24:18] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[23:24:24] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'
[23:24:31] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
[23:24:37] [INFO] testing 'Generic inline queries'
[23:24:38] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[23:24:43] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[23:24:48] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'
[23:24:53] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'
[23:25:00] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'
[23:25:06] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'
[23:25:13] [INFO] testing 'Oracle AND time-based blind'
it is recommended to perform only basic UNION tests if there is not at least one other (potential) technique found. Do you want to
 reduce the number of requests? [Y/n] y
[23:25:23] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[23:25:35] [WARNING] GET parameter 'rt' does not seem to be injectable
[23:25:35] [INFO] testing if GET parameter 'products_id' is dynamic
[23:25:37] [WARNING] GET parameter 'products_id' does not appear to be dynamic
[23:25:38] [WARNING] heuristic (basic) test shows that GET parameter 'products_id' might not be injectable
[23:25:39] [INFO] testing for SQL injection on GET parameter 'products_id'
[23:25:39] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[23:25:59] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[23:26:03] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[23:26:09] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[23:26:16] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'
[23:26:22] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
[23:26:28] [INFO] testing 'Generic inline queries'
[23:26:29] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[23:26:34] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[23:26:40] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'
[23:26:44] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'
[23:26:50] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'
[23:26:56] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'
[23:27:03] [INFO] testing 'Oracle AND time-based blind'
[23:27:09] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[23:27:22] [WARNING] GET parameter 'products_id' does not seem to be injectable
[23:27:22] [CRITICAL] all tested parameters do not appear to be injectable. Try to increase values for '--level'/'--risk' options
if you wish to perform more tests. Please retry with the switch '--text-only' (along with --technique=BU) as this case looks like
a perfect candidate (low textual content along with inability of comparison engine to detect at least one dynamic parameter). If y
ou suspect that there is some kind of protection mechanism involved (e.g. WAF) maybe you could try to use option '--tamper' (e.g.
'--tamper=space2comment') and/or switch '--random-agent'
```

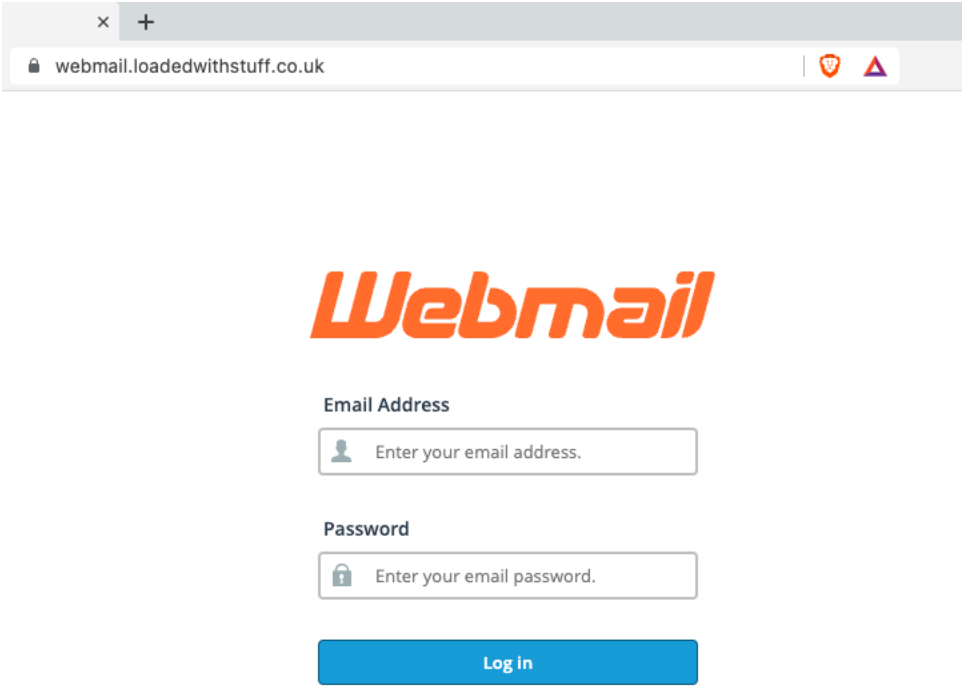
Appendix D – Nikto scan result

```
yvonechan@Yvones-MacBook-Air program % ./nikto.pl -h https://loadedwithstuff.co.uk/
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          68.66.247.187
+ Target Hostname:    loadedwithstuff.co.uk
+ Target Port:        443
---------------------------------------------------------------------------
+ SSL Info:        Subject:  /CN=loadedwithstuff.co.uk
                   Altnames: loadedwithstuff.co.uk, autodiscover.loadedwithstuff.co.uk, cpanel.loadedwithstuff.co.uk, cpcalendars.loadedwithstuff.co.uk, cpcontacts.loadedwithstuff.co.uk, loadedwithst
uff.tech-sourcery.co.uk, mail.loadedwithstuff.co.uk, webdisk.loadedwithstuff.co.uk, webmail.loadedwithstuff.co.uk, www.loadedwithstuff.co.uk, www.loadedwithstuff.tech-sourcery.co.uk
                   Ciphers:  AEAD-AES256-GCM-SHA384
                   Issuer:   /C=US/ST=TX/L=Houston/O=cPanel, Inc./CN=cPanel, Inc. Certification Authority
+ Start Time:         2022-05-02 11:56:56 (GMT8)
---------------------------------------------------------------------------
+ Server: Apache
+ Retrieved x-powered-by header: PHP/7.4.29
+ Cookie lcsid created without the secure flag
+ Cookie lcsid created without the httponly flag
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Server may leak inodes via ETags, header found with file /robots.txt, inode: 76735791, size: 1239, mtime: Mon Oct 19 04:09:34 2020
line: /ipn.php
+ Entry '/ipn.php' in robots.txt returned a non-forbidden or redirect HTTP code (500)
line: /debug/
+ Entry '/debug/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
line: /download/
+ Entry '/download/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
line: /includes/
line: /cache/
+ Entry '/cache/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
line: /templates/
line: /temp/
+ Entry '/temp/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
line: /pear/
+ Entry '/pear/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
line: /wpcallback.php
+ Entry '/wpcallback.php' in robots.txt returned a non-forbidden or redirect HTTP code (200)
line: /paypal_notify.php
+ Entry '/paypal_notify.php' in robots.txt returned a non-forbidden or redirect HTTP code (200)
line: /cert/
+ Entry '/cert/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
line: /pub/
+ Entry '/pub/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
line: /tmp/
+ Entry '/tmp/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
line: /ext/
line: /admin/
+ Entry '/admin/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
line: /admin/
+ Entry '/admin/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ "robots.txt" contains 15 entries which should be manually viewed.
+ Uncommon header 'x-redirect-by' found, with contents: WordPress
+ The Content-Encoding header is set to "deflate" this may mean that the server is vulnerable to the BREACH attack.
+ Server banner changed from 'Apache' to 'imunify360-webshield/1.18'
+ ERROR: Error limit (20) reached for host, giving up. Last error: opening stream: can't connect (timeout): Interrupted system call
+ SCAN TERMINATED:  19 error(s) and 20 item(s) reported on remote host
+ End Time:           2022-05-02 12:21:10 (GMT8) (1454 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
yvonechan@Yvones-MacBook-Air program %
```

Appendix E – CPanel is visible to the public



Appendix F – Webmail is visible to the public



Appendix G – Burp Suite scan result

Issues found on https://loadedwithstuff.co.uk

URLs By issue type	Severity	Confidence
Password submitted using GET method [1] /index.php	Low	Certain
Password field with autocomplete enabled [1] /index.php	Low	Certain
Vulnerable JavaScript dependency [1] /	Low	Tentative
TLS certificate [1] /	Info	Certain
TLS cookie without secure flag set [1] /	Info	Certain
Cross-domain Referer leakage [5] /	Info	Certain
/	Info	Certain
/index.php	Info	Certain
/index.php	Info	Certain
/index.php	Info	Certain
Cookie without HttpOnly flag set [1] /	Info	Certain
Email addresses disclosed [5] /	Info	Certain
/	Info	Certain
/index.php	Info	Certain
/index.php	Info	Certain
/index.php	Info	Certain
Robots.txt file [1] /robots.txt	Info	Certain
Cacheable HTTPS response [1] /robots.txt	Info	Certain

Appendix H - Absence of Anti-CSRF Tokens

Absence of Anti-CSRF Tokens

URL: https://loadedwithstuff.co.uk
Risk: Medium
Confidence: Low
Parameter:
Attack:
Evidence: <form name="search" action="https://loadedwithstuff.co.uk/index.php?rt=core/advanced_search_result" method="get" role="form" class="form-inline" id="search">
CWE ID: 352
WASC ID: 9
Source: Passive (10202 - Absence of Anti-CSRF Tokens)

Description:

No Anti-CSRF tokens were found in a HTML submission form.
A cross-site request forgery is an attack that involves forcing a victim to send an HTTP request to a target destination without their knowledge or intent in order to perform an action as the victim. The underlying cause is application functionality using

Other Info:

No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token] was found in the following HTML form: [Form 1: "keywords" "rt"].

Solution:

Phase: Architecture and Design
Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness easier to avoid.

Reference:

http://projects.webappsec.org/Cross-Site-Request-Forgery
http://cwe.mitre.org/data/definitions/352.html

Alert Tags:

Key	Value
WSTG-v42-SESS-05	https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_S...
OWASP_2017_A05	https://owasp.org/www-project-top-ten/2017/A5_2017-Broken_Access_Control.html
OWASP_2021_A01	https://owasp.org/Top10/A01_2021-Broken_Access_Control/

Appendix I - Content Security Policy (CSP) Header Not Set

Content Security Policy (CSP) Header Not Set

URL: https://loadedwithstuff.co.uk
Risk: Medium
Confidence: High
Parameter:
Attack:
Evidence:
CWE ID: 693
WASC ID: 15
Source: Passive (10038 - Content Security Policy (CSP) Header Not Set)

Description:

Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of

Other Info:

Solution:

Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header, to achieve optimal browser support: "Content-Security-Policy" for Chrome 25+, Firefox 23+ and Safari 7+, "X-Content-Security-Policy" for Firefox 4.0+ and Internet Explorer 10+, and "X-WebKit-CSP" for Chrome 14+ and Safari 6+.

Reference:

https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy
https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html
http://www.w3.org/TR/CSP/

Alert Tags:

Key	Value
OWASP_2017_A06	https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html
OWASP_2021_A05	https://owasp.org/Top10/A05_2021-Security_Misconfiguration/

Appendix J - Vulnerable JS Library

Vulnerable JS Library

URL: https://loadedwithstuff.co.uk/templates/default/library/angular/angular.min.js
Risk: Medium
Confidence: Medium
Parameter:
Attack:
Evidence: /*
AngularJS v1.6.9
CWE ID: 829
WASC ID:
Source: Passive (10003 - Vulnerable JS Library)

Description:

The identified library angularjs, version 1.6.9 is vulnerable.

Other Info:

CVE-2020-7676

Solution:

Please upgrade to the latest version of angularjs.

Reference:

https://github.com/angular/angular.js/commit/726f49dcf6c23106ddaf5cfd5e2e592841db743a
https://github.com/advisories/GHSA-5cp4-xmrw-59wf
https://nvd.nist.gov/vuln/detail/CVE-2020-7676

Alert Tags:

Key	Value
OWASP_2017_A09	https://owasp.org/www-project-top-ten/2017/A9_2017-Using_Components_with_Kno...
OWASP_2021_A06	https://owasp.org/Top10/A06_2021-Vulnerable_and_Outdated_Components/

Appendix K - Application Error Disclosure

Application Error Disclosure

URL: https://loadedwithstuff.co.uk/ipn.php
Risk: Low
Confidence: Medium
Parameter:
Attack:
Evidence: HTTP/1.1 500 Internal Server Error
CWE ID: 200
WASC ID: 13
Source: Passive (90022 - Application Error Disclosure)

Description:

This page contains an error/warning message that may disclose sensitive information like the location of the file that produced the unhandled exception. This information can be used to launch further attacks against the web application. The alert could be a false positive if the error message is found inside a documentation page.

Other Info:

Solution:

Review the source code of this page. Implement custom error pages. Consider implementing a mechanism to provide a unique error reference/identifier to the client (browser) while logging the details on the server side and not exposing them to the user.

Reference:

Alert Tags:

Key	Value
WSTG-v42-ERRH-02	https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_S...
WSTG-v42-ERRH-01	https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_S...
OWASP_2017_A06	https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html
OWASP_2021_A05	https://owasp.org/Top10/A05_2021-Security_Misconfiguration/

Appendix L - Cookie without SameSite Attribute

Cookie without SameSite Attribute

URL: https://loadedwithstuff.co.uk
Risk: Low
Confidence: Medium
Parameter: lcsid
Attack:
Evidence: Set-Cookie: lcsid
CWE ID: 1275
WASC ID: 13
Source: Passive (10054 - Cookie without SameSite Attribute)

Description:

A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.

Other Info:

Solution:

Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.

Reference:

https://tools.ietf.org/html/draft-ietf-httpbis-cookie-same-site

Alert Tags:

Key	Value
WSTG-v42-SESS-02	https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Te...
OWASP_2017_A05	https://owasp.org/www-project-top-ten/2017/A5_2017-Broken_Access_Control.html
OWASP_2021_A01	https://owasp.org/Top10/A01_2021-Broken_Access_Control/

Appendix M - Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)

Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)

URL: https://loadedwithstuff.co.uk
Risk: Low
Confidence: Medium
Parameter:
Attack:
Evidence: X-Powered-By: PHP/7.4.29
CWE ID: 200
WASC ID: 13
Source: Passive (10037 - Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s))

Description:

The web/application server is leaking information via one or more "X-Powered-By" HTTP response headers. Access to such information may facilitate attackers identifying other frameworks/components your web application is reliant upon and the vulnerabilities such components may be subject to.

Other Info:

Solution:

Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.

Reference:

http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.aspx
http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html

Alert Tags:

Key	Value
WSTG-v42-INFO-08	https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Te...
OWASP_2017_A03	https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html
OWASP_2021_A01	https://owasp.org/Top10/A01_2021-Broken_Access_Control/

Appendix N - Timestamp Disclosure

Timestamp Disclosure - Unix

URL: https://loadedwithstuff.co.uk/templates/sevenofsix/css/template.css
Risk: Low
Confidence: Low
Parameter:
Attack:
Evidence: 42857143
CWE ID: 200
WASC ID: 13
Source: Passive (10096 - Timestamp Disclosure)

Description:

A timestamp was disclosed by the application/web server - Unix

Other Info:

42857143, which evaluates to: 1971-05-12 08:45:43

Solution:

Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.

Reference:

http://projects.webappsec.org/w/page/13246936/Information%20Leakage

Alert Tags:

Key	Value
OWASP_2017_A03	https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html
OWASP_2021_A01	https://owasp.org/Top10/A01_2021-Broken_Access_Control/

Appendix O - Port scanning result from Metasploit

```
Module options (auxiliary/scanner/portscan/tcp):

   Name         Current Setting            Required  Description
   ----         ---------------            --------  -----------
   CONCURRENCY  10                         yes       The number of concurrent ports to check per host
   DELAY        0                          yes       The delay between connections, per thread, in milliseconds
   JITTER       0                          yes       The delay jitter factor (maximum value by which to +/- DELAY) in milliseconds.
   PORTS        1-10000                    yes       Ports to scan (e.g. 22-25,80,110-900)
   RHOSTS       www.loadedwithstuff.co.uk  yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   THREADS      1                          yes       The number of concurrent threads (max one per host)
   TIMEOUT      1000                       yes       The socket connect timeout in milliseconds

msf6 auxiliary(scanner/portscan/tcp) > run

[+] 68.66.247.187:        - 68.66.247.187:25 - TCP OPEN
[+] 68.66.247.187:        - 68.66.247.187:21 - TCP OPEN
[+] 68.66.247.187:        - 68.66.247.187:80 - TCP OPEN
[+] 68.66.247.187:        - 68.66.247.187:110 - TCP OPEN
[+] 68.66.247.187:        - 68.66.247.187:143 - TCP OPEN
[+] 68.66.247.187:        - 68.66.247.187:443 - TCP OPEN
[+] 68.66.247.187:        - 68.66.247.187:465 - TCP OPEN
[+] 68.66.247.187:        - 68.66.247.187:587 - TCP OPEN
[+] 68.66.247.187:        - 68.66.247.187:993 - TCP OPEN
[+] 68.66.247.187:        - 68.66.247.187:995 - TCP OPEN
[+] 68.66.247.187:        - 68.66.247.187:2077 - TCP OPEN
[+] 68.66.247.187:        - 68.66.247.187:2079 - TCP OPEN
[+] 68.66.247.187:        - 68.66.247.187:2080 - TCP OPEN
[+] 68.66.247.187:        - 68.66.247.187:2078 - TCP OPEN
[+] 68.66.247.187:        - 68.66.247.187:2087 - TCP OPEN
[+] 68.66.247.187:        - 68.66.247.187:2083 - TCP OPEN
[+] 68.66.247.187:        - 68.66.247.187:2082 - TCP OPEN
[+] 68.66.247.187:        - 68.66.247.187:2086 - TCP OPEN
[+] 68.66.247.187:        - 68.66.247.187:2096 - TCP OPEN
[+] 68.66.247.187:        - 68.66.247.187:2095 - TCP OPEN
[+] 68.66.247.187:        - 68.66.247.187:2525 - TCP OPEN
[+] 68.66.247.187:        - 68.66.247.187:3306 - TCP OPEN
[+] 68.66.247.187:        - 68.66.247.187:5432 - TCP OPEN
[+] 68.66.247.187:        - 68.66.247.187:6556 - TCP OPEN
[+] 68.66.247.187:        - 68.66.247.187:7822 - TCP OPEN
[*] www.loadedwithstuff.co.uk: - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```