Vulnerability Audit and Assessment - Executive Summary
Word Count: 1193

Table of Contents Page

1 - Executive Summary introduction

The purpose of this vulnerability audit and assessment is to discover, collate and present findings that may be present within 'allthegear.org.uk' that could lead to vulnerability exploitation and which may also impact compliance and regulations such as GDPR and PCI-DSS. It is possible that some findings may be a false positive but have been included if the risk level warrants highlighting.

Findings will then be supported with recommendations/Mitigations to reduce risk and improve compliance.

2 - Methodology

The method for assessment had been done remotely with a passive scan approach to reduce business and system impact. There had been a four step process and each of the four steps had a different approach which is explained below.
(Step 4 is integrated into section '3 -Findings').

Below is a visual illustration (fig.1) of the four steps used throughout the methodology.

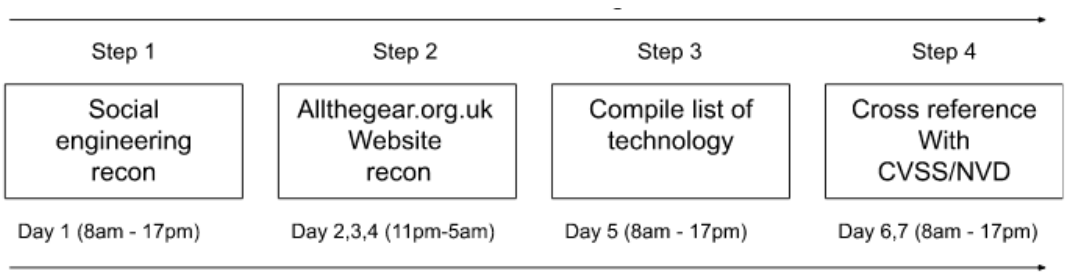

fig.1. Four steps of the vulnerability assessment process.

The following details explains which tools were used in each step and the reason why.

Step 1 - Social Engineering Recon

Firstly, a full recon would be out of scope for this assessment, therefore, a mitigation package has been created and shared in section 4 of this report to benefit the company.

Step 2 - Allthegear.org.uk Website Recon

Secondly, recon on the website and network had been carried out by using an array of commands and tools to gather information about potential vulnerabilities within the website.

Scans had been initiated on the following 'Host Information' (*Table.1*).

DNS Name	allthegear.org.uk
IP	68.66.247.187

Table.1 - Host Information

The two tools which had been used for the website vulnerability Recon are listed below (*Table.2.*)

Tool	Why Did this assessment use that tool
OWASP ZAP	Used to automate a passive scan for Vulnerabilities
Nessus	Used For a security scan of Vulnerabilities in allthegear.org.uk

Table.2 - Tools used for allthegear.org website recon.

Step 3 - List of Technology

Thirdly, a list was compiled of the software and hardware associated with the website (In section 3) using an array of commands (Table.3) and tools (Table.4).

Command	Why Did this assessment use that Command
DIG	Used for retrieving information about DNS name servers
Traceroute	Used to determine the path between two connections
MTR	To analyze the network traffic loss during hop-to-hop using ICMP packets
Whois	Used to find out who owns or registered the IP Address and when
WhatWeb	Used to identify different web technologies used by this website

Table.3 commands

Tool	Why Did this assessment use that Tool
DNSDumpster	Tool that can discover hosts related to a domain
Builtwith	Tool that provides technology profiles of the chosen website

Table.4 Tools

Step 4 - Cross Reference with CVSS/NVD

Lastly, the findings of potential vulnerabilities which had been discovered via the vulnerability scanners and also via a manual cross reference search of the vulnerability databases have been presented in section 3.

3 - Findings

Summary of Findings

The vulnerability scans in step two discovered 4 ‘High Risk’, 18 ‘Medium Risk’, 5 ‘Low Risk ’ Potential Vulnerabilities and 155 ‘Informational’ elements. A number of these vulnerabilities have the potential to breach both GDPR and PCI-DSS compliance and should therefore be addressed.

A further analysis of the technology stack within step three provided additional vulnerabilities associated with the PHP (7.3.44) framework, Magento 2 and Apache Name server could lead to a GDPR breach.

Findings from Step 1 - Social Engineering Recon

N/A

Findings from Step 2 - Allthegear.org.uk Website Recon

This phase utilized both Nessus and ZAP scanners to cross reference each other and improve the chances of discovering a vulnerability which may have been missed by a single scanner. As a result, the two scanners discovered different vulnerabilities and improved discovery.

Table.4. Represents the 'individual' and 'Total' sum of vulnerability discoveries from the two scanners. It illustrates that Nessus did not report 'Low' vulnerabilities but ZAP did. However, ZAP did not report 'High' vulnerabilities but Nessus had.

Risk Level	Tool - Nessus	Tool - ZAP	Total
Critical	0	N/A	0
High	4	0	4
Medium	15	3	18
Low	0	5	5
Info	151	4	155

Table.4 cross reference of scanner findings.

Nessus Findings

Summary

A vulnerability scan of the website using Nessus had returned 4 'HIGH' vulnerabilities (Table.6) and 15 'MEDIUM' Vulnerabilities (Table.7). 151 'INFO' findings have not been presented due to having a vulnerability rating of Zero.

Although a combined number of 19 vulnerabilities are being reported, these vulnerabilities are spread over just 6 ports (Table.5).

Port	Quantity of Vulnerabilities
21	4
124	4
993	4
995	4
2080	1
2083	2

Table.5 Nessus scan results

HIGH			
	Vulnerability and synopsis (Nessus)	CVE	Plugin output (Where)
	42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)	CVE 2016-2183	tcp/21/ftp
	The remote service supports the use of medium strength SSL ciphers.		
	42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)	CVE 2016-2183	tcp/143/imap
	The remote service supports the use of medium strength SSL ciphers.		
	42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)	CVE 2016-2183	tcp/993/imap
	The remote service supports the use of medium strength SSL ciphers.		
	42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)	CVE 2016-2183	tcp/995/pop3
	The remote service supports the use of medium strength SSL ciphers.		

Table.6 High risk vulnerabilities discovered via a Nessus scan

MEDIUM

	Vulnerability and synopsis (Nessus)	CVE	Plugin Output
	142960 - HSTS Missing From HTTPS Server (RFC 6797)		tcp/2080/www
	The remote web server is not enforcing HSTS, as defined by RFC 6797.		
	142960 - HSTS Missing From HTTPS Server (RFC 6797)		tcp/2083/www
	The remote web server is not enforcing HSTS, as defined by RFC 6797.		
	31705 - SSL Anonymous Cipher Suites Supported	CVE-2007-1858	tcp/21/ftp
	The remote service supports the use of anonymous SSL ciphers.		
	45411 - SSL Certificate with Wrong Hostname		tcp/21/ftp
	The SSL certificate for this service is for a different host.		
	45411 - SSL Certificate with Wrong Hostname		tcp/143/imap
	The SSL certificate for this service is for a different host.		
	45411 - SSL Certificate with Wrong Hostname		tcp/993/imap
	The SSL certificate for this service is for a different host.		
	45411 - SSL Certificate with Wrong Hostname		tcp/995/pop3
	The SSL certificate for this service is for a different host.		
	65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah)	CVE 2015-2808	tcp/21/ftp
	The remote service supports the use of the RC4 cipher (Which is flawed)		
	104743 - TLS Version 1.0 Protocol Detection		tcp/143/imap
	The remote service encrypts traffic using an older version of TLS.		
	104743 - TLS Version 1.0 Protocol Detection		tcp/993/imap
	The remote service encrypts traffic using an older version of TLS.		
	104743 - TLS Version 1.0 Protocol Detection		tcp/995/pop3
	The remote service encrypts traffic using an older version of TLS.		
	157288 - TLS Version 1.1 Protocol Deprecated		tcp/143/imap
	The remote service encrypts traffic using an older version of TLS.		
	157288 - TLS Version 1.1 Protocol Deprecated		tcp/993/imap
	The remote service encrypts traffic using an older version of TLS.		
	157288 - TLS Version 1.1 Protocol Deprecated		tcp/995/pop3
	The remote service encrypts traffic using an older version of TLS.		
	85582 - Web Application Potentially Vulnerable to Clickjacking	CWE:693	tcp/2083/www
	The remote web server may fail to mitigate a class of web application vulnerabilities.		

Table.7 Medium risk vulnerabilities discovered via a Nessus scan

ZAP Findings

Summary

A vulnerability scan of the website using ZAP had returned 3 ‘MEDIUM’ vulnerabilities (Table.8) and 5 ‘LOW’ Vulnerabilities (Table.9). 4 ‘INFO’ findings have not been presented due to having a vulnerability risk rating of Zero.

	Vulnerability and Brief description (ZAP)	CWE
	Absence of Anti-CSRF Tokens	CWE - 352
	Risk of information disclosure because the w eb application can not verify a request correctly	
	HTTP to HTTPS Insecure Transition in Form Post	CWE - 319
	Insecure HTTP page can easily be hijacked through MITM and the secure HTTPS form can be replaced or spoofed.	
	Content Security Policy (CSP) Report-Only Header Found	CWE - 693
	Could allow data theft via cross-site scripting and data injection attacks	

Table.8 Medium risk vulnerabilities discovered via a ZAP scan

	Vulnerability and Brief description (ZAP)	CWE
	Application Error Disclosure	CWE - 200
	May disclose sensitive information to an actor w ho is not authorize to have access	
	Cookie No HttpOnly Flag	CWE - 1004
	If the HttpOnly flag is not set, then sensitive information stored in the cookie may be exposed to unintended parties	
	Cookie Without Secure Flag	CWE - 614
	could cause the user to send plaintext over an HTTP session.	
	Server Leaks Information via "X-Pow ered-By" HTTP Response Header Field(s)	CWE - 200
	May disclose sensitive information to an actor w ho is not authorize to have access	
	Timestamp Disclosure - Unix	CWE - 200
	May disclose sensitive information to an actor w ho is not authorize to have access	

Table.9 Low risk vulnerabilities discovered via a ZAP scan

Findings from Step 3 - List of Technology

Summary

Analysis of the technology stack behind allthegear,org.uk has revealed three potential vulnerabilities (Table.10), 1 ‘Critical’ vulnerability and 2 ‘High’ vulnerabilities which should be addressed immediately due to the possibility of leaking confidential data and breaching GDPR compliance.

Category	Technology	Technology	Technology	Technology	CVE
Analytics & Tracking	Adobe dynamic tag management				
Widgets	Authorize.Net				
Ecommerce	Magento 2				CVE-2023-23617
Framew orks	PHP 7.3.44				CVE-2022-31630
Mobile	View point meta tag	Iphone mobile compatible			
Payment	Cardinal commerce (Payment authenticator)	Braintree (Payment Processor)	PayPal (Payment acceptance)		
Javascript	Require JS	Knockout JS	MatchMedia	Underscore JS	
SSL Certificates	CPanel SSL (Cert)	SSL by default (Re-direct to https/SSL)	HSTS (forces brow ser comms w ith htpps only)		
Web Hosting	Oracle Cloud (Email and/or w ebsite Cloud hosting)	A2 Hosting (VPS, US, Dedicated)			
Email Hosting Providers	SPF (Sender address forgery prevention)				
Name Servers	Apache				CVE-2022-31813
Copyright	2013				

Table.10 Low risk vulnerabilities discovered via a ZAP scan

Findings from Step 4 - Cross Reference with CVSS/NVD

Summary

A cross reference of the findings from steps two and three have indicated that GDPR and PCI-DSS is at risk of being breached due to several vulnerabilities.

4 - Recommendations

The following order of priority, as illustrated below (Table.11) should be followed to ensure that business priorities and mitigation by risk levels are addressed to reduce vulnerabilities and risk to Confidentiality of customers data, Integrity of pricing/stock and Availability of business operations remain.

Priority	Vulnerability / Technology	Port	CVE/CWE
1	Apache Name Server	N/A	CVE-2022-31813
2	PHP 7.3.44	N/A	CVE-2022-31630
3	Magento 2	N/A	CVE-2023-23617
4	42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)	21	CVE 2016-2183
5	42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)	143	CVE 2016-2183
6	42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)	993	CVE 2016-2183
7	42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)	995	CVE 2016-2183
8	142960 - HSTS Missing From HTTPS Server (RFC 6797)	2080	
9	142960 - HSTS Missing From HTTPS Server (RFC 6797)	2083	
10	31705 - SSL Anonymous Cipher Suites Supported	21	
11	104743 - TLS Version 1.0 Protocol Detection	143	
12	104743 - TLS Version 1.0 Protocol Detection	993	
13	104743 - TLS Version 1.0 Protocol Detection	995	
14	157288 - TLS Version 1.1 Protocol Deprecated	143	
15	157288 - TLS Version 1.1 Protocol Deprecated	993	
16	157288 - TLS Version 1.1 Protocol Deprecated	143	
17	85582 - Web Application Potentially Vulnerable to Clickjacking	2083	CWE 693
18	Absence of Anti-CSRF Tokens	N/A	CWE 352
19	HTTP to HTTPS Insecure Transition in Form Post	N/A	CWE 319
20	Content Security Policy (CSP) Report-Only Header Found	N/A	CWE 693
21	Application Error Disclosure	N/A	CWE 200
22	Cookie No HttpOnly Flag	N/A	CWE 1004
23	Cookie Without Secure Flag	N/A	CWE 614
24	Server Leaks Information via "X-Pow ered-By" HTTP Response Header Field(s)	N/A	CWE 200
25	Timestamp Disclosure - Unix	N/A	CWE 200

Table.11 order of priority for mitigating risk

5 - Security Standards Evaluation

(Important Business Requirement)

A search using 'immuniweb.com' had highlighted an issue with both GDPR and PCI-DSS compliance within allthegear.org.uk, as illustrated in figure 2.

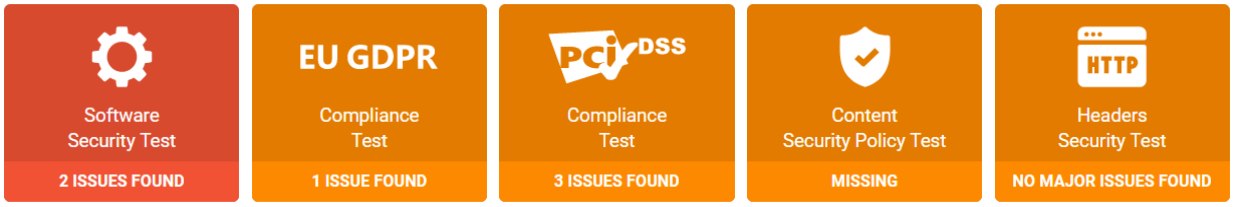

Figure.2. Results of GDPR and PCI-DSS compliance issues from immuniweb.com

UK GDPR (General Data Protection Regulation)

The ICO (2021) has stated that "The EU GDPR is an EU Regulation and it no longer applies to the UK. If you operate inside the UK, you need to comply with the Data Protection Act 2018". However, if the UK company is processing customer data from the EU, then EU GDPR needs to be followed (ICO, 2021)

Breaching GDPR can cost the business 4% of global turnover Or up to 20 Million Euros (European Commission, 2018).

Mitigation and risk reduction approaches.

CWE 352 could leak data and possibly cause a GDPR compliance issue. To reduce the risk of breaching Section 2(1)(c)(ii) of the Data Protection Acts 1988 and 2003, the business could implement and enforce procedures and policies to ensure confidentiality of customer data (Legislation, 2022). If Financially viable, this could be achieved by implementing an ISMS via ISO27001 (ISO, 2022).

PCI-DSS Standards

Staying compliant to meet payment card vendors standards is important and can be guided by mapping it to the NIST cybersecurity framework (PCI-DSS, 2019).

According to PCI-DSS (2022), standards will need to be implemented if the amount of card transactions exceed 20k transitions within a year.

Mitigation and risk reduction approaches.

Vulnerability number 104743 in the recommendation section at priority number 11,12 and 13 needs to be mitigated to ensure PCI-DSS compliance.

6 - Conclusions

To Conclude, the website has very few vulnerabilities but does next to update and patch versions to ensure improved security. EU GDPR, UK GDPR and PCI-DSS compliance needs to be implemented to avoid a breach of regulations. A consideration also needs to be made for The CCPA (California Consumer Privacy Act) due to the website asking for customer details of the United States of America during the checkout process and including an opt out ability. Staff should also be enrolled in a cyber awareness training package.

7 - References

European Commission (2018) Data Protection: Better rules for small businesses. Available from: https://ec.europa.eu/justice/smedataprotect/index_en.htm [Accessed on 04 March 2023]

ICO (2021) Information commissioner's office. Available from: https://ico.org.uk/ [Accessed on 04 March 2023]

ISO (2022) 27001 Information security management systems. Available from: https://www.iso.org/standards.html [Accessed on 26 February 2023].

Legislation (2022) The data protection, privacy and electronic communications (Amendments etc) (EU Exit) Regulations 2019. Available from: https://www.legislation.gov.uk/uksi/2019/419/regulation/2 [Accessed on 27 February 2023]

PCI-DSS (2019) Mapping PCI DSS to the NIST Cybersecurity Framework. Available from: https://docs-prv.pcisecuritystandards.org/Guidance%20Document/PCI%20DSS%20General/Mapping-PCI-DSS-to-NIST-Framework-At-a-Glance.pdf [Accessed on 05 March 2023]

PCI-DSS (2022) Understanding the Payment Card Industry Data Security Standard version 4.0. Available from: https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Supporting%20Document/PCI_DSS-QRG-v4_0.pdf [Accessed on 04 March 2023]