MODULE-2

NETWORK SECURITY

Vulnerability Audit and Assessment - Results and Executive Summary

MS-CYBERSECURITY | AMIT PAHUJA

TABLE OF CONTENT

1. Executive Summary

A security assessment was performed on the https://allthegear.org.uk website. This document describes the methodology employed, GDPR requirements for the organization, vulnerabilities analysis, and recommendations summary for addressing these vulnerabilities. The document describes the security criteria (including compliance with the GDPR) and provides advice.

Domain	Ecommerce Website
Type of Penetration Summary	External Testing
Website	https://allthegear.org.uk
Technique	Web Application Penetration Testing (WAPT)
Scope	BlackBox
Testing Methodology	PTES(Penetration Testing and Execution Standard) OWASP Web Testing Framework
Modelling Technique	STRIDE and DREAD

2. Methodology

2.1 Testing Methodologies:

OWASP & PTES (Penetration Testing Execution Framework)

As the OWASP Testing methodology focuses on application security, testing the application against the OWASP Top10 security risks assures that the top 10 most common attacks can be prevented, in addition to keeping the application's CIA intact. PTES is used ,consists of seven different stages, for penetration testing of any environment .

2.2 Threat Modelling and Risk Analysis Methodology

Threat Modelling is the technique used to identify the threats and rate them. In this Audit/assessment, utilized the Microsoft's six-stage threat modelling process.

The threat modelling for the target application has been performed based on the Microsoft's six-stage process –

3. Information Gathering:

3.1. Website protection

Target website is protected using Immunify360 shield found through the “wafw00f” tool in Kali;

3.2. Port Scanning using NMAP

The below tables show the ‘open ports’ which were identified through TCP and UDP scans using -sS and -sU options respectively

PORT	STATE	SERVICE
21/tcp	open	ftp
53/tcp	open	domain
80/tcp	open	http
110/tcp	open	pop3
143/tcp	open	imap
443/tcp	open	https
465/tcp	open	smtps
587/tcp	open	submission
993/tcp	open	imaps
995/tcp	open	pop3s
2525/tcp	open	ms-v-worlds
3306/tcp	open	mysql
5432/tcp	open	postgresql

PORT	STATE	SERVICE
53/udp	open	domain
319/udp	open|filtered	ptp-event
320/udp	open|filtered	ptp-general

3.3. Subdomains

List of Sub-Domains found using “knockpy”, additional targets that can be exploited-

IP ADDRESS	SUB-DOMAINS
69.66.247.187	autodiscover.allthegear.org.uk
69.66.247.187	cpanel.allthegear.org.uk
69.66.247.187	ftp.allthegear.org.uk
69.66.247.187	mail.allthegear.org.uk
69.66.247.187	webmail.allthegear.org.uk
69.66.247.187	www.allthegear.org.uk

4. Security Vulnerabilities

Few different tools (ZAP and OpenVAS) were used to scan the website. The below section summarizes the total number of vulnerabilities found grouped with the severity of the risk:

RISK LEVEL	No.OF ALERTS
HIGH	0
MEDIUM	4
LOW	3
INFORMATIONAL	1
FALSE-POSITIVES	0
TOTAL	8

4.1 High/Medium Risk Vulnerabilities

The section below details the high & medium risk vulnerabilities found in the scan along with the proposed solution.

1. No Anti-CSRF Tokens Present	
RISK RATING	**MEDIUM**
DESCRIPTION	No Anti-CSRF tokens were found in a HTML submission form. Cross-site request forgery is an attack in which a victim is coerced into sending an HTTP request to a target destination without their knowledge or consent in order to conduct an action as the victim.
TARGET	https://allthegear.org.uk
SOLUTION	Utilize a library or framework that prevents or mitigates this vulnerability, such as anti-CSRF packages such as the OWASP CSRFGuard. Ensure that your application is clear of XSS vulnerabilities, as the majority of CSRF safeguards may be circumvented. Check the HTTP Referer header to determine if the request came from a known page.
REFERENCES	http://projects.webappsec.org/Cross-Site-Request-Forgery http://cwe.mitre.org/data/definitions/352.html

2. Content Security Policy (CSP) Header Not Set	
RISK RATING	**MEDIUM**
DESCRIPTION	Content Security Policy (CSP) is an additional security layer that aids in detecting and mitigating certain sorts of threats. These assaults are used for a variety of purposes, including data theft.
TARGET	https://allthegear.org.uk

SOLUTION	Ensure your web server, application server, load balancer, etc. is configured to set the Content-Security header for Firefox 23+, Safari 7+, and Chrome 25+ and the "X-Content-Security-Policy" header for Internet Explorer and Firefox 4.0+ .
REFERENCES	http://www.w3.org/TR/CSP/ http://content-security-policy.com/

3. Multiple Entries in the X-Frame-Options Header	
RISK RATING	**MEDIUM**
DESCRIPTION	If X-Frame-Options (XFO) headers are detected, a response containing multiple XFO header entries may not be interpreted predictably by all user agents.
TARGET	https://allthegear.org.uk
SOLUTION	Ensure there is only one X-Frame-Options header in the response.
REFERENCES	https://tools.ietf.org/html/rfc7034

4. Vulnerable JS Library	
RISK RATING	**MEDIUM**
DESCRIPTION	jQuery : The vulnerable library version is 1.12.4.
TARGET	https://allthegear.org.uk
SOLUTION	Upgrade to the most recent version of jQuery.
REFERENCES	http://blog.jquery.com/2016/01/08/jquery-2-2-and-1-12-released/ https://nvd.nist.gov/vuln/detail/CVE-2019-11358

4.2 Low/Informational Risk Vulnerabilities

The section below details the low & informational risk vulnerabilities found in the scan:

5. Cookie No “HttpOnly” Flag	
RISK RATING	**LOW**
DESCRIPTION	A cookie has been set without the HttpOnly flag, indicating that it can be viewed by JavaScript and transmitted to another site. If this cookie is for a session, session hijacking may be feasible.
TARGET	https://allthegear.org.uk
SOLUTION	Ensure that all cookies have the HttpOnly flag set.
REFERENCES	https://owasp.org/www-community/HttpOnly

6. The "X-Powered-By" HTTP response header field on the server exposes sensitive information (s)	
RISK RATING	**LOW**
DESCRIPTION	Through one or more "X-Powered-By" HTTP response headers, the web/application server is leaking information. Access to such information may aid attackers in locating further frameworks/components upon which your web application relies, and such components may be vulnerable to exploit.
TARGET	https://allthegear.org.uk
SOLUTION	Ensure that the "X-Powered-By" header is suppressed on your web server, application server, load balancer, etc.
REFERENCES	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

7. Timestamp Disclosure “Unix”	
RISK RATING	**LOW**
DESCRIPTION	The application/web server exposed a timestamp.
TARGET	https://allthegear.org.uk
SOLUTION	Verify manually that the timestamp data is not sensitive and cannot be aggregated to reveal exploitable patterns.
REFERENCES	http://projects.webappsec.org/w/page/13246936/Information%20Leakage

8. Content Security Policy (CSP) Report-Only Header Found	
RISK RATING	**INFORMATIONAL**
DESCRIPTION	The response contained a Content-Security-Policy-Report-Only header, this may indicate a work-in-progress Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP approved sources of content that browsers should be allowed to load on that page — covered types are Java applets, ActiveX, audio and video files.
TARGET	https://allthegear.org.uk
SOLUTION	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-for Chrome 25+, Firefox 23+ and Safari 7+, "X-Content-Security-Policy" for Firefox 4.0+ and Internet Explorer
REFERENCES	https://www.w3.org/TR/CSP2/ https://w3c.github.io/webappsec-csp/ http://caniuse.com/#feat=contentsecuritypolicy http://content-security-policy.com/

5. Security Standard Analysis & Compliance Tests

5.1 GDPR

Compliance Tests for GDPR:

The picture below depicts the GDPR compliance tests conducted.

PRIVACY POLICY	Privacy Policy was found on the website.
WEBSITE SECURITY	Website CMS or its components are outdated and contain publicly known security vulnerabilities
TLS ENCRYPTION	HTTPS encryption is present on the web server
COOKIE PROTECTION	Cookies are sent without the secure flag
COOKIE DISCLAIMER	No Cookie Disclaimer text was found

(GDPR Compliance, N.D.)

5.2 Website Security

To secure personal data, Articles 5(1)(f), 24(1), and 32 of the GDPR mandate the implementation, maintenance and testing of appropriate security processes. The following were determined to have outdated software:

- jQuery 1.12.4
- jQuery Mobile

The figures below details the known issues:

jQuery 1.12.4		
CVSSv3.1 Score	**Vulnerability CVE-ID**	**URL**
5.5 Medium	CVE-2020-11022	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-11022
5.3 Medium	CVE-2015-9251	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-9251
4.8 Medium	CVE-2019-11358	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-11358
4.1 Medium	CVE-2020-11023	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-11023

jQuery Mobile		
CVSSv3.1 Score	**Vulnerability CVE-ID**	**URL (References)**
6.2 Medium	Not Assigned	https://snyk.io/vuln/SNYK-JS-JQUERYMOBILE-174599 https://www.cybersecurity-help.cz/vdb/SB2019050912

5.3 PCI-DSS Compliance

Requirement 6 of the PCI security standards addresses the development and maintenance of secure systems and applications.

Some components of Requirement 6.2 are obsolete, and needs to be updated. In addition, Requirement 6.5 is violated because the website contains public CVEs.

REQUIREMENT 6.2	Website CMS or its components are outdated, need to be updated
REQUIREMENT 6.5	Fingerprinted website CMS or its components contain publicly known vulnerabilities

Recommendations:

- Apply vendor provided latest security patches and protect all system and software components, with critical ones as early as possible.
- Secure coding guidelines must be followed while coding applications
- Developers must be trained periodically for secure coding

(Surkay Baykara,2020)

5.4 HTTPS Headers Security

There are some HTTP headers which are related to security and privacy - are missing and/or misconfigured.

X-Powered-BY: Web Server discloses its version and is potentially opened to further attacks.

SERVER	Version is not disclosed
X-POWERED-BY	Web Server discloses its version and is potentially opened to further attacks.
STRICT-TRANSPORT-SECURITY	Header Properly set
X-CONTENT-TYPE-OPTIONS	Header Properly set
X-FRAME-OPTIONS	Header Properly set

(OWASP, N.D.)

6. Timeline

Here is the project timeline:

	Week1	Week2	Week3	Week4	Week5	Week6	Week7
Project Start							
Planning							
Information gathering / Scanning							
Vulnerability Analysis / Mapping							
Design Document Preparation							
Document Delivery							

7. Conclusion Summary

Using the OWASP web testing framework, PTES, Microsoft threat modelling and DREAD model to rate risks, performed a comprehensive penetration testing of the target website. It has also been found that the target website is protected with Immunify360 WAF shield. Identified and documented different types of risks – high risk/medium risk/ low risk/informational.

Threats with high-risk rating pose a great risk to the application and must be addressed as early as possible, followed by medium risks (with less urgency). Security standard analysis has been performed including for GDPR and recommendations have been provided. Vulnerability assessment is a continuous process, and hence the company should ensure the security assessment is done at least once a year to fix the gaps w.r.t the vulnerabilities/weaknesses in the system and the application is always risk-free and updated.

REFERENCES

1. Penetration Testing Methodologies (N.D)
   https://owasp.org/www-project-web-security-testing-guide/latest/3-The_OWASP_Testing_Framework/1-Penetration_Testing_Methodologies

2. PTES Documentation
   https://pentest-standard.readthedocs.io/en/latest/tree.html

3. PTES
   http://www.pentest-standard.org/index.php/Main_Page

4. Larry Conklin, Victoria Drake (N.D.): - Threat Modelling Process
   https://owasp.org/www-community/Threat_Modeling_Process

5. GDPR Compliance[N.D.]
   https://gdpr.eu/compliance/

6. Surkay Baykara [2020]: PCI DSS Requirement 6 Explained
   https://www.pcidssguide.com/pci-dss-requirement-6/

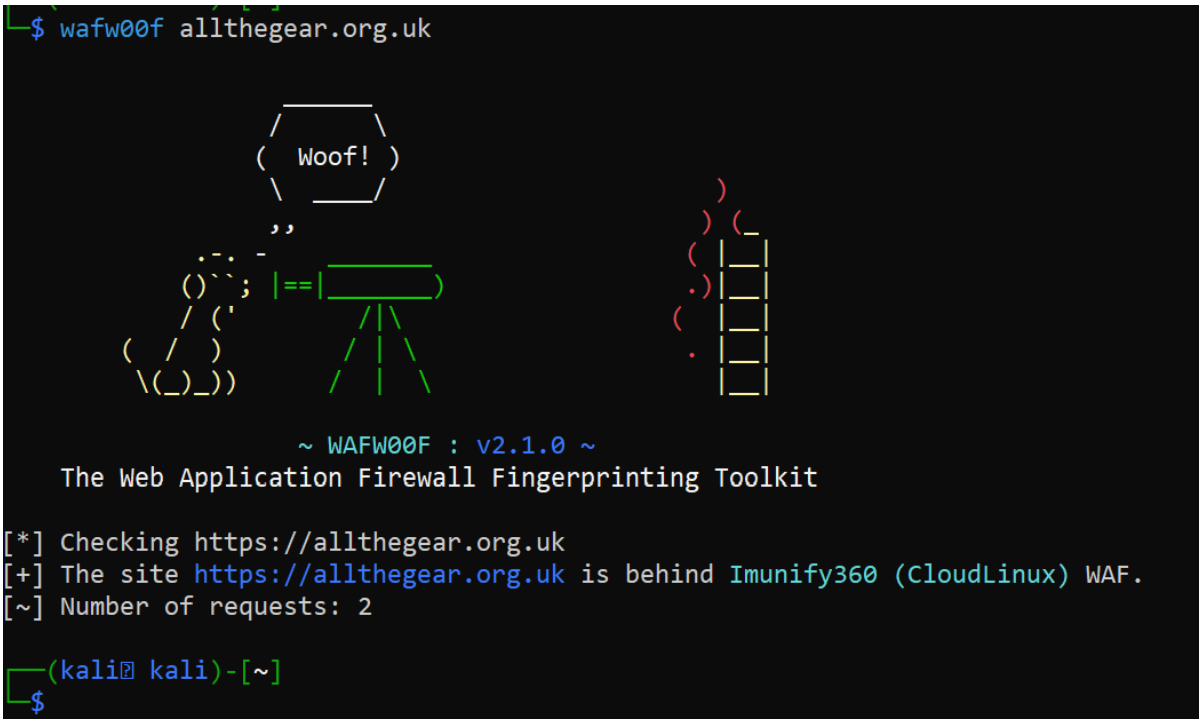
7. OWASP[N.D]: OWASP Secure Headers Project
   https://owasp.org/www-project-secure-headers/#div-technical

SCREENSHOTS:

```
└─$ sudo nmap -O allthegear.org.uk
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-16 05:51 UTC
Nmap scan report for allthegear.org.uk (68.66.247.187)
Host is up (0.088s latency).
rDNS record for 68.66.247.187: 68.66.247.187.static.a2webhosting.com
Not shown: 907 filtered tcp ports (no-response), 9 filtered tcp ports (port-unreach), 1 filtered tcp ports (admin-prohibited), 70
 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
53/tcp   open  domain
80/tcp   open  http
110/tcp  open  pop3
143/tcp  open  imap
443/tcp  open  https
465/tcp  open  smtps
587/tcp  open  submission
993/tcp  open  imaps
995/tcp  open  pop3s
2525/tcp open  ms-v-worlds
3306/tcp open  mysql
5432/tcp open  postgresql
Aggressive OS guesses: Linux 4.4 (92%), Linux 3.10 - 3.12 (91%), Linux 4.9 (90%), Linux 4.0 (90%), Linux 3.10 - 3.16 (89%), Linux
 3.11 - 4.1 (88%), Linux 3.10 (88%), Linux 2.6.32 (88%), Linux 2.6.32 or 3.10 (88%), Linux 3.5 (88%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 17 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.12 seconds

┌──(kali㉿ kali)-[~]
```



```
└─$ knockpy allthegear.org.uk

 _  __                  _
| |/ /                 | |   v5.3.0
| ' / _ __   ___   ___ | | ___ __  _   _
|  < | '_ \ / _ \ / __| |/ / '_ \| | | |
| . \| | | | (_) | (__|   <| |_) | |_| |
|_|\_\_| |_|\___/ \___|_|\_\ .__/ \__, |
                           | |     __/ |
                           |_|    |___/

local: 10757 | google: 0 | duckduckgo: 0 | virustotal: 0

Wordlist: 10757 | Target: allthegear.org.uk | Ip: 68.66.247.187

17:57:46

Ip address      Code Subdomain                                 Server                                    Real hostname
--------------- ---- ----------------------------------------- ----------------------------------------- ----------------------
-----------------
68.66.247.187   400  autodiscover.allthegear.org.uk            Apache

68.66.247.187   200  autoconfig.allthegear.org.uk              Apache

68.66.247.187   401  cpcalendars.allthegear.org.uk             cPanel

68.66.247.187   401  cpcontacts.allthegear.org.uk              cPanel

68.66.247.187   200  cpanel.allthegear.org.uk                  Apache

68.66.247.187   200  ftp.allthegear.org.uk                     Apache                                    allthegear.org.uk
68.66.247.187   200  mail.allthegear.org.uk                    Apache

68.66.247.187   401  webdisk.allthegear.org.uk                 cPanel

68.66.247.187   200  webmail.allthegear.org.uk                 Apache

68.66.247.187        whm.allthegear.org.uk

68.66.247.187   200  www.allthegear.org.uk                     Apache                                    allthegear.org.uk

17:58:10

Ip address: 1 | Subdomain: 11 | elapsed time: 00:00:24


┌──(kali㉿kali)-[~]
└─$
```