ThinThread

Protecting your business from within

Vulnerability Assessment Report

Company: Example

Date: Day/Month/Year

Scope

The project includes the review of the following assets:

NAME	ASSET	TYPE OF TESTS
External Assets	example.co.uk	Automatic and manual
	Webmail.example.co.uk	
	0.0.0.0	

The technical tests were carried out between **/**/**** and **/**/****

Goals

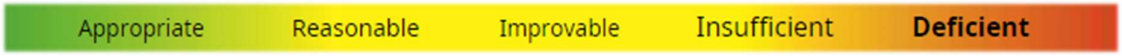
The general objective of the review carried out has been to identify and analyse potentially exploitable vulnerabilities, which could be used to compromise the confidentiality, integrity and/or availability of the data managed and contained by Examples external assets. The review has been carried out following a black, grey or white box approach.

Executive Summary

ThinThread was requested to carry out an External Vulnerability Assessment, which allows evaluating the risks associated with possible configuration and/or implementation errors that may exist.

The purpose of this document is to report the vulnerabilities detected so far, their security risks and the appropriate recommendations to eliminate or reduce them.

After carrying out the review, it is observed that the security level of the web server provided by the application is **Deficient**



A level is considered:

- Deficient, when there is at least 1 critical vulnerability or more than 2 high vulnerabilities
- Insufficient, when there are 1 or 2 high vulnerabilities
- Improvable, when there is at least a medium vulnerability
- Reasonable, when there is at least a low vulnerability
- Appropriate, in the rest of the cases

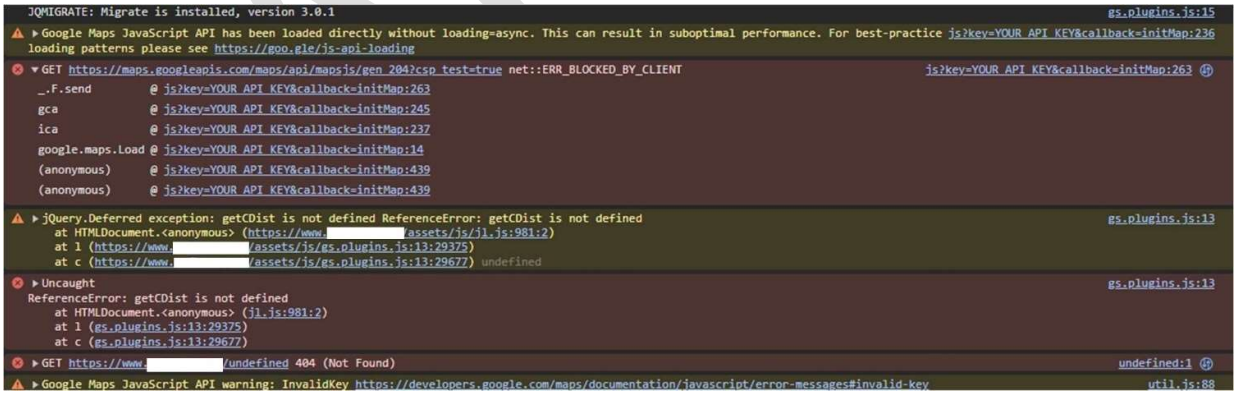
Website Findings

- Does not render well in any browser. Words over the images
- Social Media links do not work
- Strange page lettering at base of screen
- Parish Map, image loads are sometimes slow - the images have not been created as a thumbnail
- Instructions for using the Essex Parish Map, when clicking on 'Alternatively proceed to search our database' it goes to a '404 Not Found error' page
- Some pages have been put in a 'pages' folder so it '404 Not found error' if on the pages URL
- Chapman Codes does not render correctly - outside of page pagination
- The pages/volunteer's page does not go across the screen
- Google Maps JavaScript API errors, these can create latency issues

Mobile Website

- Boxes do not render correctly on mobile phone
- Parish map does not render correctly
- Projects page does not render correctly
- Shop pagination is a mess

Browser Findings



Software Findings

jQuery 3.3.1

The fingerprinted component version is outdated and vulnerable to publicly known vulnerabilities. Urgently update to the most recent version **3.7.1**.

CVSSv3.1 Score	Vulnerability CVE-ID CVE	Vulnerability Type
5.5 Medium	CVE-2020-11022	CWE-79 - Cross-site scripting
4.8 Medium	CVE-2019-11358	CWE-1321 - Prototype pollution
4.1 Medium	CVE-2020-11023	CWE-79 - Cross-site scripting

jQuery UI 1.12.1

The fingerprinted component version is outdated and vulnerable to publicly known vulnerabilities. Urgently update to the most recent version **1.13.3**.

CVSSv3.1 Score	Vulnerability CVE-ID CVE	Vulnerability Type
5.5 Medium	CVE-2021-41184	CWE-79 - Cross-site scripting
5.3 Medium	CVE-2021-41182	CWE-79 - Cross-site scripting
5.3 Medium	CVE-2021-41183	CWE-79 - Cross-site scripting
4.1 Medium	CVE-2022-31160	CWE-79 - Cross-site scripting

Server and Web Server

- Server Software CentOS is EOL (end of life), and is now out of date
- Web Server Software is out of date - Apache/2.4.6, latest is 2.4.62
- PHP is out of date - PHP/7.3.33, latest is 8.2 (the code the pages are written in)
- Cookie PHPSESSID created without the secure flag and Cookie PHPSESSID created without the httponly flag - the default values for the SECURE and HTTPONLY flags of cookies, especially for the PHP session cookie, (PHPSESSID) are not set to true. This opens a hidden vulnerability for serious XSS attacks
- X-Powered-By header describes the technologies used by the webserver. This information exposes the server to attackers - disable or remove
- The X-Frame-Options HTTP response header can be used to indicate whether a browser should be allowed to render a page in a frame, iframe, embed or object - deny
- Strict-Transport-Security HTTP header is not defined - possibly a redirect in place but the missing Strict- Transport-Security header results in communication over HTTP being allowed to the specified domain. That makes the website vulnerable to man-in-the-middle attacks, presenting a fake login page being one of the options
- Without the X-Content-Type-Options header set to 'nosniff', older versions of Internet Explorer and Chrome may perform MIME-sniffing on the response body
- OpenSSL/1.0.2k-fips is out of date, latest version 3.0.8
- HTTP TRACE method is active which suggests the host is vulnerable to XST (cross-site tracing), can be successfully leveraged in some scenarios to steal legitimate users' credentials - disable the TRACE method

Open Ports

PORT	*STATE*	*SERVICE*	*VULNERABILITY*
21/tcp	filtered	ftp	
22/tcp	open	ssh	Remote SSH server is configured to allow / support weak encryption
23/tcp	filtered	telnet	
80/tcp	open	http	
110/tcp	filtered	pop3	
143/tcp	filtered	imap	
443/tcp	open	https	
3389/tcp	filtered	ms-wbt-server	If not required should be closed

CVE and CWE Issues

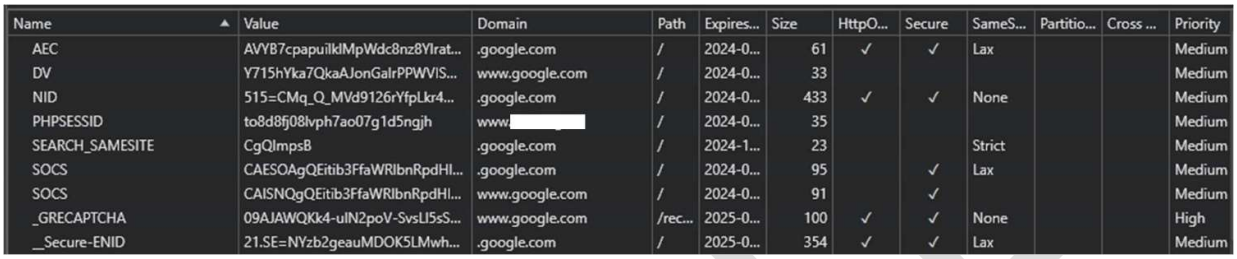
The web server and Operating System server have multiple CVE (common vulnerabilities and exposures) and CWE (common weakness enumeration) vulnerabilities.

- /inc/config.php: Bookmark4U v1.8.3 include files are not protected and may contain remote source injection by using the 'prefix' variable. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1253
- /admin/login.php?action=insert&username=test&password=test: phpAuction may allow user admin accounts to be inserted without proper authentication. Attempt to log in with user 'test' password 'test' to verify. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-0995
- /icons/: Directory indexing found.
- /admin/phpinfo.php: Output from the phpinfo() function was found.
- /admin/phpinfo.php: Immobilier allows phpinfo() to be run. See: https://vulners.com/osvdb/OSVDB:35877
- /webapp/admin/_pages/_bc4jadmin/: Oracle JSP files. See: CWE-552
- /_pages/_demo/: Oracle JSP file. See: CWE-552
- /_pages/_webapp/_jsp/: Oracle JSP file. See: CWE-552
- /_pages/_demo/_sql/: Oracle JSP file. See: CWE-552
- /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to- iconsreadme/
- /admin/login.php: Admin login page/section found.
- /login.php: Admin login page/section found.

- /help.php: A help file was found **CWE 552 - The product makes files or directories accessible to unauthorized actors, even though they should not be*

Cookie Issues and GDPR Compliance

- No Cookie Consent Banner – third party cookie information required
- No copyright information – not essential but good practice



Name	Value	Domain	Path	Expires...	Size	HttpO...	Secure	SameS...	Partitio...	Cross ...	Priority
AEC	AVYB7cpapuiIkIMpWdc8nz8YIrat...	.google.com	/	2024-0...	61	✓	✓	Lax			Medium
DV	Y715hYka7QkaAJonGaIrPPWVIS...	www.google.com	/	2024-0...	33						Medium
NID	515=CMq_Q_MVd9126rYfpLkr4...	.google.com	/	2024-0...	433	✓	✓	None			Medium
PHPSESSID	to8d8fj08lvph7ao07g1d5ngjh	www.[redacted]	/	2024-0...	35						Medium
SEARCH_SAMESITE	CgQImpsB	.google.com	/	2024-1...	23			Strict			Medium
SOCS	CAESOAgQEitib3FfaWRlbnRpdHI...	.google.com	/	2024-0...	95		✓	Lax			Medium
SOCS	CAISNQgQEitib3FfaWRlbnRpdHI...	www.google.com	/	2024-0...	91		✓				Medium
_GRECAPTCHA	09AJAWQKk4-uIN2poV-SvsLI5sS...	www.google.com	/rec...	2025-0...	100	✓	✓	None			High
__Secure-ENID	21.SE=NYzb2geauMDOK5LMwh...	.google.com	/	2025-0...	354	✓	✓	Lax			Medium

Email

- Sender Policy Framework (spf record) in place

```
v=spf1 mx a ip4:[redacted]/32 include:[redacted]eu include:spf.[redacted].com ~all
```

- DKIM Policy not in place
- DMARC Policy not in place

Email Spoofing

Test email sent using host Domain - successful