ThinThread
Cyber Security

Security Audit

Client: example.co.uk
Date: 10/03/2025

Scope

The project includes the review of the following assets:

NAME	ASSET	TYPE OF TESTS
External Assets	example.co.uk / 92.0.0.0	Automatic and manual
	example.org / 15.0.0.0	

The technical tests were carried out between 03/03/2025 and 12/03/2025

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 EXAMPLE external assets. The review has been carried out following a **black-box** approach.

Black-box vulnerability testing assesses a system's security from an external perspective, simulating a real-world attacker's approach, without knowledge of its internal workings or code

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 site and 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

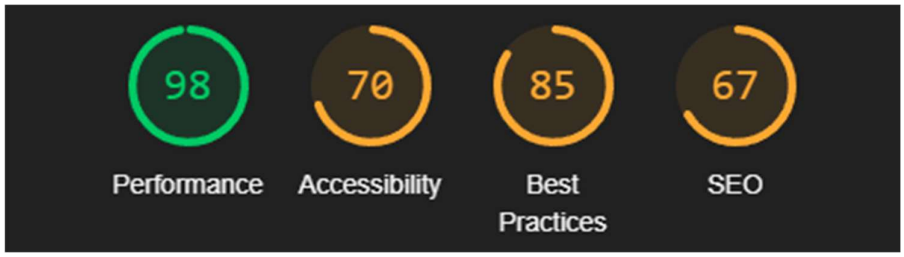
Multiple vulnerabilities were found and as such must be actioned. The majority are due to updates not being installed in a timely fashion; the rest are due to incorrect code issues that need to be closed by a developer.

Vulnerability Summary Table

HIGH	MEDIUM	LOW

Website Findings

- The Lighthouse performance score based on the home page showed a **98%** performance rating



- A website redirect is in place for EXAMPLE.org to send http and https traffic to EXAMPLE.co.uk
- **The site https://EXAMPLE.co.uk is not behind a WAF**
  Further Reading: https://www.cloudflare.com/en-gb/learning/ddos/glossary/web-application-firewall-waf
- The site https://EXAMPLE.org is behind the AWS Elastic Load Balancer (Amazon) WAF
- **The site is using HTTP/2.0** – this is preferred over HTTP/1.1 due to multiplexing and header compression
- **Dead Links** – two links found that return 404 errors

EXAMPLE Domain	Dead Link
EXAMPLE.co.uk/pages/events.php	familyhistory.com/2024/04/golden-j
EXAMPLE.co.uk/pages/links.php	surreycc.gov.uk/reigate

SSL/TLS Findings

- There are **four Weak cipher suites** supported in TLS 1.2

```
Accepted  TLSv1.2  64 bits   DHE-RSA-AES256-CCM8          DHE 2048 bits
Accepted  TLSv1.2  64 bits   DHE-RSA-AES128-CCM8          DHE 2048 bits
Accepted  TLSv1.2  64 bits   AES256-CCM8
Accepted  TLSv1.2  64 bits   AES128-CCM8
```

Further reading: https://convesio.com/knowledgebase/article/the-dangers-of-weak-cipher-suites-what-you-need-to-know

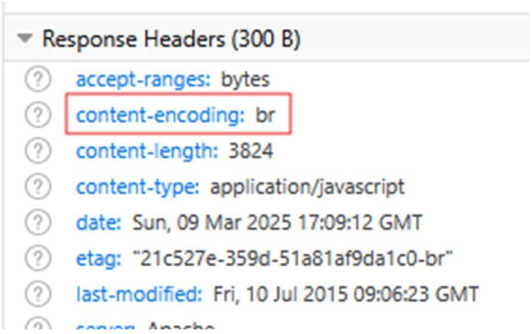
- **TLSv1.2 enabled** with **SSLv2/SSLv3/TLSv1.0/TLSv1.1/TLSv1.3 disabled** – this is the correct setup

- TLS/SSL **not vulnerable** to:

SSL/TLS	Heartbleed / CCS Injection
SSL/TLS	Ticketbleed / ROBOT
SSL/TLS	Secure Renegotiation
SSL/TLS	CRIME / POODLE /BEAST
SSL/TLS	SWEET32 / FREAK / Winshock
SSL/TLS	DROWN / RC4

- The web server SSL/TLS is showing the **possibility of BREACH (CVE-2013-3587)** being possible but this looks to be a possible false positive. The BREACH attack exploits gzip compression, the EXAMPLE.co.uk site uses .br compression as the default. Worth noting that the Twitter/X widget plugged into the site uses .gzip compression

```
BREACH (CVE-2013-3587)                potentially NOT ok, "br gzip" HTTP compression detected
```



Server and Web Server Findings

- **No DNSSEC found** – leaves DNS records vulnerable to manipulation and spoofing attacks
  Further reading: https://www.icann.org/resources/pages/dnssec-what-is-it-why-important-2019-03-05-en
- The server has no **Permissions Policy** – recommended for extra security depending on web resources
  Further reading: https://developer.mozilla.org/en-US/docs/Web/HTTP/Permissions_Policy
  Further reading: https://www.w3.org/TR/permissions-policy
- The server has no **Content Security Policy** – recommended as an extra layer of security for preventing vulnerabilities such as XSS
  CWE ID: 693
  Further reading: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Content-Security-Policy
- **Cookie No HttpOnly Flag** - A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript
  CWE ID: 1004
  Further reading: https://docs.stackhawk.com/vulnerabilities/10010
- **Cookie Without Secure Flag** - A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections
  CWE ID: 614
  Further reading: https://docs.stackhawk.com/vulnerabilities/10011

- **Cookie without SameSite Attribute** - which means that the cookie can be sent as a result of a 'cross-site' request
  CWE ID: 1275
  Further reading: https://docs.stackhawk.com/vulnerabilities/10054
- **Cross-Domain JavaScript Source File Inclusion** - The page includes one or more script files from a third-party domain
  CWE ID: 829
  Further reading: https://docs.stackhawk.com/vulnerabilities/10017
- **Missing Anti-clickjacking Header** - the response does not protect against 'ClickJacking' attacks. It should be included in Content-Security-Policy
  CWE ID: 1021
  Further reading: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
- **x-powered-by header exposed** - the X-Powered-By header reveals information about specific technology used on the server, the server is displaying **PHP/5.6.40**
  CWE ID: 200
  Further reading:
  https://docs.stackhawk.com/vulnerabilities/10037/#:~:text=It%20is%20important%20to%20address,attack%20surface%20of%20the%20application.
- **X-Content-Type-Options Header Missing** - this could allow the user agent to render the content of the site in a different fashion to the MIME type and should be set to 'nosniff'
  CWE ID: 693
  Further reading: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header
- **HTTPS redirect not supported** - All redirects should be performed over HTTPS
  Further reading: https://blog.dnsimple.com/2016/08/https-redirects
- **Absence of Anti-CSRF Tokens** – No Anti-CSRF tokens were found in a HTML submission form
  CWE ID: 352
  Further reading: https://www.iothreat.com/blog/absence-of-anti-csrf-tokens
- Directory EXAMPLE.co.uk/webmail/blank.html is showing: **IlohaMail 0.8.10 contains an XSS vulnerability** – the server is showing this product installed but it could be non-deleted legacy files if the webmail has been upgraded. Ask hosting company
- /img-sys/: **Default image directory should not allow directory listing** – the directory is showing blank but directory listing should be disabled if enabled

Software Findings

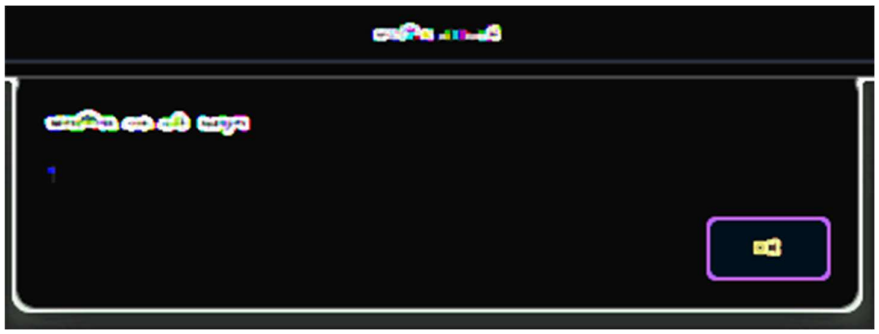
- **A critical XSS (Cross Site Scripting) vulnerability was found in pages that require user input and should be looked at and fixed**

  URL: https://EXAMPLE.co.uk/pages/login.php?

  URL: https://EXAMPLE.co.uk/pages/login.php?source=cp&filename=services.php?

  URL: https://www.EXAMPLE.co.uk/pages/certificates.php?btn=Search&surname=?

By appending a test script to the URL (**"><scrIpt>alert(1);</scRipt>**) we can test to see if the browser returns the alert message '1'. If the alert message '1' is returned it validates the possible existence of a reflected XSS vulnerability. This was difficult to categorically prove or disprove due to the legalities with the hosting company but the reflect indicates a positive answer. Please use the further reading to ensure the code is correct and re-test. Upgrading to the latest PHP version would remediate.



As shown in the diagram '1' is returned

Further reading:

https://cwe.mitre.org/data/definitions/79.html

https://cheatsheetseries.owasp.org/cheatsheets/Cross_Site_Scripting_Prevention_Cheat_Sheet.html

- **JavaScript files were found on the site and were publicly readable** - could disclose sensitive information and version highlighting any relevant CVE's and CWE's. This also allows indirect access to the Assets directory
  - https://www.EXAMPLE.co.uk/calendar_eu.js
  - https://www.EXAMPLE.co.uk/pagereload.js
  - https://www.EXAMPLE.co.uk/slideshow.js
  - https://www.EXAMPLE.co.uk/tcal.js
- **PHP/5.6.40 which has multiple known vulnerabilities and should be upgraded immediately**
  Further reading: https://www.tenable.com/plugins/nessus/121602

Open Ports on shared Server

PORT	*SERVICE*	
21	ftp	FTP Unencrypted cleartext (insecure)
22	ssh	Secure Shell
25	*smtp*	email
80	http	browser
110	pop3	email
143	imap	email
443	https	browser
465	smtps	Now deprecated by the Internet Engineering Task Force
587	mail	email
993	secure imap	email

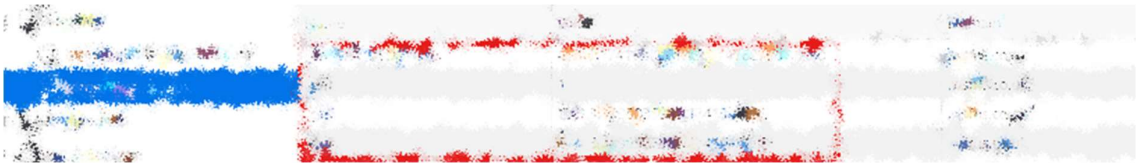
995	Secure pop3	email
3306	mysql	MySQL

Cookie Issues and GDPR Compliance

- **No Cookie Consent Banner**
- **Google cookies are being used on the site** – the _ga cookie requires a cookie consent policy

Privacy Disclosures Policy

When you use Google Analytics on your site or application, you must disclose the use of Google Analytics and how it collects and processes data.



Email

Sender Policy Framework (spf record) in place and securely locked to the email vendor

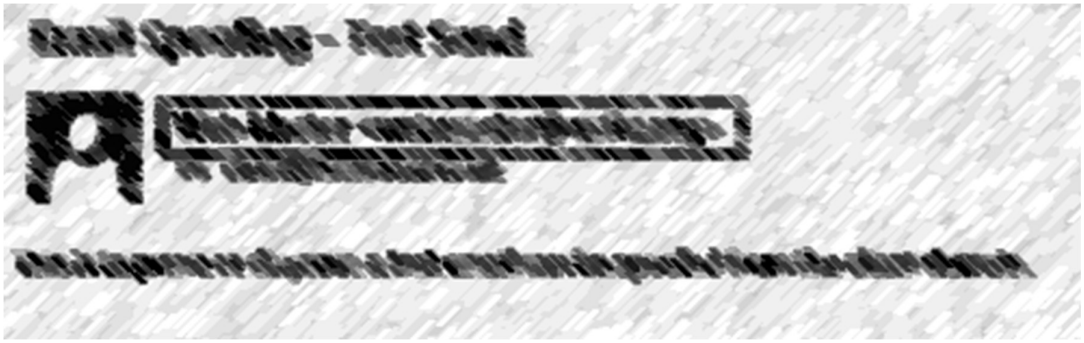
DKIM **Policy not in place**
DMARC - **No DMARC Record found**
MTA-STS – **No MTA-STS Record found**

MX Records found for EXAMPLE.org and EXAMPLE.co.uk

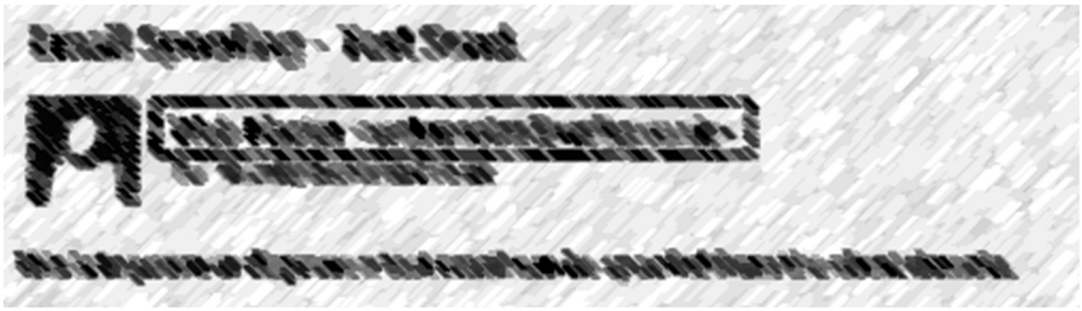
smtp.example.net 216.0.0.0
mailstore1.example.net 216.0.0.0

Email Spoofing

Test email sent from host Domain EXAMPLE.org to thinthread.co.uk – **successful**
Further reading: https://www.proofpoint.com/us/blog/email-and-cloud-threats/prevent-email-spoofing-with-dmarc



Test email sent from host Domain EXAMPLE.co.uk to thinthread.co.uk – **successful**



Dark Web

A tool was used to see if stealer logs or combo-list information has been leaked on the Dark Web. No stealer logs were found but references to a combo-list leak were found. It is unknown as to what level the data is available or being used but does indicate leakage from either a site or server.

Further reading:
https://flare.io/learn/resources/blog/combo-lists-the-dark-web-understanding-leaked-credentials
https://www.breachsense.com/blog/dark-web-combo-list

Recommendations

Thinthread would recommend that where possible all '**HIGH**' and '**MEDIUM**' findings are rectified with an emphasis on '**HIGH**'. The key findings are the XSS script used to prove reflected XSS within the browser. If these are not fixed an attacker could use a carefully crafted email with the EXAMPLE domain to point a member to an erroneous website for downloading malicious scripts. The Server and Web Server findings highlight many server-side issues which may not be possible to fix if using shared hosting due to in place restrictions. Each one of the findings has an associated CWE (Common Weakness Enumeration) number with it which can be viewed at https://cwe.mitre.org for a full description. We would also recommend the creation of a 'Content Security Policy' which helps mitigate XSS vulnerabilities at the Server level and can be used in parallel with the PHP/5.6.40 upgrade preventing XSS vulnerabilities from being performed.

As part of the test, we were able to send spoofed emails from the @EXAMPLE.org and @EXAMPLE.co.uk domains. We would recommend putting a DMARC Record in place to prevent this from being executed.

We would also recommend signing up to the NCSC https://www.ncsc.gov.uk/section/active-cyber-defence/sign-in-register, a government website that monitors for certain key vulnerabilities in websites and email. This can be completed by the EXAMPLE as a DNS entry is required and associated email address to set up.

END