A picture containing symbol, graphics, screenshot, design

Description automatically generated

EXECUTIVE SUMMARY

Produced by Woodman Security Group – 08 June 2023

**Lead Researcher:** Trevor Woodman **–** <https://essex.trevorwoodman.ca>

**Stakeholder:** Copperplate **–** <https://copperplate.org.uk>

TABLE OF CONTENTS

[Overview 2](#_Toc137135438)

[Disclaimer 2](#_Toc137135439)

[Summary of Work 2](#_Toc137135440)

[Findings 3](#_Toc137135441)

[Evaluation 3](#_Toc137135442)

[NIST Cybersecurity Framework 3](#_Toc137135443)

[Review 3](#_Toc137135444)

[General Data Protection Regulation (GDPR) 4](#_Toc137135445)

[Review 4](#_Toc137135446)

[Conclusion and Recommendations 5](#_Toc137135447)

[GDPR 5](#_Toc137135448)

[NIST CSF 5](#_Toc137135449)

[Technical Remediation 6](#_Toc137135450)

[References 7](#_Toc137135451)

# Overview

As per the vulnerability assessment, testing has been performed on the site using various automated and manual tools. This summary outlines the findings of said testing.

# Disclaimer

Due to the constrained engagement parameters and limited access, it may be difficult or impossible to provide a factual assessment for several sections of the website.

# Summary of Work

The website was assessed with automated and manual reconnaissance and testing. The findings section will outline this, and the technical mitigation section has some recommendations for the software and security teams.

# Findings

The website was found to be predominantly secure.

The Coppermine team is voluntary, and the project open source. This could present issues, including the longstanding lack of contributors (phill104, 2010), their contributors on GitHub affirms this (coppermine-gallery, 2023).

Assuming that the latest version available from Softaculous was used, the website uses Coppermine version 1.6.25 (Softaculous, 2023). Some dependencies are out of date, possibly presenting far more issues; it appears that the latest jQuery version in use is version 1.12.4, published on May 20, 2016 (Snyk, 2023).

# Evaluation

With the collection of user data, it is paramount to adhere to security standards and applicable regulations. This section outlines the NIST Cybersecurity Framework security standard and General Data Protection Regulation (GDPR) with brief reviews.

Again, with limited access, this evaluation is mostly theoretical.

## NIST Cybersecurity Framework

The NIST CSF comprises of 5 categories: identify, protect, detect, respond, and recover. These revolve around managing and planning for a crisis, resiliency, and recovery (NIST, n.d.).

### Review

Copperplate should review this standard and ensure compliance. With collection of user information and storing of data such as images, protect and recover categories should be prioritised. All categories should be reviewed to ensure a holistic approach via this well-defined standard.

Develop or enhance internal training plan to cover the easiest attack vector: social engineering. According to Gitnux, up to 54% of all ransomware infection was caused by successful phishing attacks (Gitnux, 2023).

## General Data Protection Regulation (GDPR)

The GDPR is a regulation enacted by the European Union that applies to any data collected from individuals in the European Economic Area. If an organisation collects user data and they reside in a country that GDPR applies to, that company must be compliant.

The United Kingdom keeps their own version, the UK GDPR. They share key principles, which are neatly summarised by the Information Commissioner’s Office (ICO, n.d.):

* Lawfulness, fairness, and transparency towards the data subject.
* Purpose limitation on data collected, used for specific purposes and not further processed outside of these purposes.
* Data minimisation by only collecting required user data.
* Accuracy of data with deletion or rectification of inaccurate data.
* Storage limitation by only storing data as long as necessary.
* Integrity and confidentiality by securing and protecting data against unauthorised or unlawful processing, loss, or damage.
* Accountability through demonstration of compliance by data processing records, data protection impact assessments (DPIAs), and measures to protect data subjects’ rights.

Where the NIST CSF is more so for ensuring a company is mitigating risk and prepared for a crisis in a systems and planning sense, the GDPR ensures that a company is keeping and using user data in a safe and privacy-focused manner.

### Review

There is no readily apparent privacy policy page available; a privacy policy is required for compliance. If the website uses cookies to collect or store personal data, a disclaimer should be presented when visiting.

# Conclusion and Recommendations

Copperplate is non-compliant. Recommendations are in order of priority. Review the evaluation section for specifics.

## GDPR

Review the regulation and become compliant. The fines for non-compliance can be substantial, with larger offending organisations being made example of via fines, such as Meta recently being fined the largest sum yet at €1.2 billion euros in May of 2023 (Enzuzo, 2023).

## NIST CSF

Review the CSF and begin implementing or covering areas that are not currently compliant and prioritise “protect” and “recover” categories. Secure data and being able to fully recover from a crisis quickly are paramount to the business’ longevity.

# Technical Remediation

These technical issues were found as part of automated and manual testing.

Severity is based on the Common Vulnerability Scoring System v3 (CSSv3), an industry standard maintained by the Forum of Incident Response and Security Teams. It is used to categorise vulnerabilities based on several factors like the level of effort required, if the attacker can do it remotely, and more (FIRST, n.d.).

|  |  |  |
| --- | --- | --- |
| SEVERITY | OBJECT | RECOMMENDATION |
| High | Serialized PHP object in HTTP message  “cpg16x\_data” contains a serialized PHP object, used several times to request images and files.  This object can be re-serialized with a payload and used in a PHP object injection attack if the code is not sanitising the object or if unsafe logic is used. | Files should not be requested in this manner. This appears to be inherent to the software. It may not be possible to remediate without refactoring of the scripts. |
| Low | The cookie “cpg16x\_data” does not have the “secure” flag set, nor does it have the “HttpOnly” flag set. | Set the “secure” flag (Coates et al., n.d.) and the “HttpOnly” flag (Rknell et al., n.d.) |
| Low | “X-Powered-By” response header indicates the exact PHP version in use, PHP/7.4.33 | Remove the “X-Powered-By” header by modifying php.ini or by additional code (ubiq.co, n.d.) |

# References

* Coates, M. et al (n.d.). OWASP: Secure Cookie Attribute. Available at: <https://owasp.org/www-community/controls/SecureCookieAttribute> [Accessed 07 June 2023]
* coppermine-gallery (2023). cpg1.6.x. Available at: <https://github.com/coppermine-gallery/cpg1.6.x> [Accessed 07 June 2023]
* Enzuzo (2023). 51 Biggest GDPR Fines and Penalties So Far (Updated!). Available at: https://www.enzuzo.com/blog/biggest-gdpr-fines
* FIRST (n.d.). Forum of Incident Response and Security Teams – Common Vulnerability Scoring System v3.0: Specification Document. Available at: <https://www.first.org/cvss/v3.0/specification-document> [Accessed 05 June 2023]
* Gitnux (2023). Social Engineering 2023: Statistics And Trends. Available at: <https://blog.gitnux.com/social-engineering-statistics/> [Accessed 07 June 2023]
* ICO (n.d.). A guide to the data protection principles. Available at: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles/> [Accessed 07 June 2023]
* phill104 (2010). Help, the Coppermine project needs you. Available at: <https://forum.coppermine-gallery.net/index.php/topic,66475.0.html> [Accessed 07 June 2023]
* Rknell. et al (n.d.). OWASP: HttpOnly. Available at: <https://owasp.org/www-community/HttpOnly> [Accessed 07 June 2023]
* Snyk (2023). Jquery vulnerabilities. Available at: <https://security.snyk.io/package/npm/jquery> [Accessed 07 June 2023]
* Softaculous (2023). Coppermine. Available at: <http://www.softaculous.com/softwares/galleries/Coppermine> [Accessed 07 June 2023]
* Ubiq.co (n.d.). How to Remove x-powered-by in Apache/PHP. Available at: <https://ubiq.co/tech-blog/how-to-remove-x-powered-by-in-apache-php/> [Accessed 05 June 2023]