A picture containing symbol, graphics, screenshot, design

Description automatically generated

EXECUTIVE SUMMARY

Produced by Woodman Security Group – 20 May 2023

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

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

TABLE OF CONTENTS

[Overview 2](#_Toc137037167)

[Disclaimer 2](#_Toc137037168)

[Summary of Work 2](#_Toc137037169)

[Findings 3](#_Toc137037170)

[Low or Informational Severity 3](#_Toc137037171)

[Response Headers 3](#_Toc137037172)

[Cookies 3](#_Toc137037173)

[Evaluation 3](#_Toc137037174)

[Conclusion 4](#_Toc137037175)

[Recommendations 4](#_Toc137037176)

[References 5](#_Toc137037177)

# Overview

This executive summary, produced for Copperplate, is part of their ongoing efforts to highlight and remediate security issues. As per the vulnerability assessment, testing has been performed on the site using various tools. This summary outlines the findings of said testing.

This report will outline:

* Summary of work
* Findings
* Evaluation against NIST CSF standard and adherence to GDPR regulation
* Conclusion
* Recommendations

# Disclaimer

Due to the constrained engagement parameters it may be difficult or impossible to provide a factual assessment for several sections and components of the website, since the researchers were not provided access to the website nor to the server.

# Summary of Work

The website was initially assessed with Burp Suite and manual testing. This assessment showed several possible vulnerabilities, some of which are theoretical due to engagement parameters. Social engineering is also included as a theoretical attack vector.

# Findings

Overall, the Copperplate website itself was found to be mostly secure. Assuming that the version in use is the latest one available in the Softaculous Coppermine script, the Copperplate website uses Coppermine Gallery version 1.6.25 (Softaculous, 2023).

The Coppermine development team appears to be voluntary and the project is open-source. This could present a number of issues, including the fact that they appear to be lacking contributors and have been for some time (phill104, 2010). Their public repository on GitHub affirms the lack of contributors (coppermine-gallery, 2023). The Coppermine Gallery website is extremely dated, the last news post is in 2018, although the downloads link correctly links off to the latest version on their GitHub repository. Dependencies can also be out of date, it appears that the latest jQuery version in use is version 1.12.4, published on May 20 2016 (Snyk, 2023).

These are outlined as they are important in assessing issues, both present and theoretical.

# Evaluation

With any system that collects user information, it is paramount to adhere to security standards and applicable regulations. In this section, we will outline Copperplate’s adherence to the NIST Cybersecurity Framework security standard as well as any breaches of the General Data Protection Regulation (GDPR).

Again, without website or server access, this evaluation is only theoretical.

Copperplate should have a robust internal training plan to cover one of the easiest attack vectors, social engineering. According to Gitnux, up to 54% of all ransomware infection was caused by successful phishing attacks (Gitnux, 2023).

## NIST Cybersecurity Framework

The NIST CSF comprises of 5 categories: identify, protect, detect, respond, and recover. These categories mostly revolve around how the company is managing their assets and information, if there are plans in place, how they would respond in a crisis, and how resilient and recoverable their assets are as well as a plan for protecting the company’s reputation (NIST, n.d.).

Copperplate should internally review this standard and ensure they are compliant as it outlines a complete and detailed risk management plan. Given that Copperplate collects user information and stores other data such as images, particular attention should be paid to the protect and recover categories. The other categories should also be reviewed to ensure a holistic approach to security via this well defined standard.

## General Data Protection Regulation (GDPR)

The original GDPR is a regulation enacted by the European Union that applies to any data collected from individuals that reside in the European Economic Area. If a website is public facing and accessible to any country that GDPR applies to, the company must adhere to the GDPR.

The United Kingdom keeps a version of it that applies to UK citizens, called the UK GDPR. The key principles of both are the same. They are clearly summarised by the Information Commissioner’s Office (ICO, n.d.):

* Lawfulness, fairness, and transparency
  + Data processing must be performed in a lawful manner, with fairness and transparency towards the data subject
* Purpose limitation
  + Personal data should only be collected for specific, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes
* Data minimisation
  + Only necessary personal data required for the specific purpose should be collected
* Accuracy
  + Personal data should be accurate and kept up to date. Out of date or inaccurate data should be deleted or rectified
* Storage limitation
  + Personal data should not be stored for longer than necessary for the purpose in which it was collected
* Integrity and confidentiality
  + Organisations are mandated to ensure the security and protection of personal data against unauthorised or unlawful processing, accidental loss, destruction, or damage
* Accountability
  + Organisations responsible with GDPR compliance must be able to demonstrate their compliance by keeping records of data processing activities, conducting data protection impact assessments (DPIAs) where necessary, and implementing measures to protect data subjects’ rights

Whereas the NIST CSF is for ensuring a company is mitigating risk and prepared for a crisis more so in a systems and planning sense, the GDPR ensures that a company is compliant with all data collected from users. It is imperative that a public facing and globally accessible site such as Copperplate be GDPR compliant.

There is not a readily apparent Privacy Policy page available, this is required for GDPR compliance to outline how data collected will be used. This is true even if the only user is yourself if you are living in a country affected by GDPR. If the site uses cookies to collect and/or store personal data, then a cookie disclaimer should be forefront on the website when visiting. Currently, the website is noncompliant with GDPR from these two issues alone.

# Conclusion

# Recommendations

These issues and recommendations are listed in presumed order of priority to the business, taking into account the previous section on evaluation and any non-compliance. The severity column indicates the respective severity, based on the Common Vulnerability Scoring System v3 (CSSv3), an industry standard maintained by the Forum of Incident Response and Security Teams (FIRST, n.d.).

|  |  |  |
| --- | --- | --- |
| SEVERITY | OBJECT | RECOMMENDATION |
| High | Serialized PHP object in HTTP message  The cookie “cpg16x\_data” contains a serialized PHP object.  This object can be re-serialized with a payload and used in a PHP object injection attack if the underlying code is not properly sanitising the object or if unsafe logic is used. | The request is a PHP object, and differs in response depending on the request endpoint. For example, on the homepage this method is used several times to request images and JavaScript files.  These files should not be requested in this manner. This appears to be the way that this software handles fetching of certain things, like icons. This may not be possible to remediate without extensive refactoring of the Coppermine scripts themselves. |
| 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 PHP 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]
* 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]