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

[Table of Contents 1](#_Toc136866323)

[Overview 2](#_Toc136866324)

[Disclaimer 2](#_Toc136866325)

[Summary of Work 2](#_Toc136866326)

[Findings 3](#_Toc136866327)

[Critical Severity 3](#_Toc136866328)

[High Severity 3](#_Toc136866329)

[Medium Severity 3](#_Toc136866330)

[Low or Informational Severity 3](#_Toc136866331)

[Header Response 3](#_Toc136866332)

[Evaluation 3](#_Toc136866333)

[Conclusion 4](#_Toc136866334)

[Recommendations 4](#_Toc136866335)

[References 5](#_Toc136866336)

# 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

This section will go into detail on our findings, which indicated a number of issues after assessing the website with Burp Suite and manual testing. This section is grouped based on the severity of the issue, from high to low, based on the CVSS (Common Vulnerability Scoring System) v3 standard (FIRST, n.d.).

## Critical Severity

??

## High Severity

??

## Medium Severity

This level of severity includes vulnerabilities that could be disruptive or cause damage, but would require an extraordinary level of effort or expertise, or both, to exploit.

## Low or Informational Severity

This level indicates that the vulnerabilities found are typically little to no impact, and any exploitation would require extraneous circumstance such as the attacker monitoring public WiFi during website usage, or the attacker having local or physical access to a system in use by the website.

### Response Headers

The response headers from the website server contain information that could assist an attacker.

### Cookies

Cookies are a piece of text data that resides in the client’s browser and contains website-related information, these issues here indicate a possible vector of attack on users of the website.

* TLS cookie doesn’t have secure flag set, allowing trivial intercept by an attacker that is monitoring the network traffic
* Cookie doesn’t have HttpOnly flag set, same issue as above

# 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).

# Conclusion

# Recommendations

These recommendations are listed in recommended order of priority to the business, taking into account the previous section on evaluation and any non-compliance.

## High Priority

## Medium Priority

## Low Priority

* ‘X-Powered-By’ header indicates the exact PHP version in use, PHP/7.4.3
  + Remove the header (ubiq.co, n.d.)

# References

* 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]
* 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]