A picture containing symbol, graphics, screenshot, design

Description automatically generated

VULNERABILITY ASSESSMENT

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](#_Toc135512379)

[Engagement Parameters and Site Information 2](#_Toc135512380)

[Parameters 2](#_Toc135512381)

[Site Information 2](#_Toc135512382)

[Visual Summary 3](#_Toc135512383)

[Security Challenges 3](#_Toc135512384)

[Tools and Methods 4](#_Toc135512385)

[Analysis Timeline 4](#_Toc135512386)

[References 5](#_Toc135512387)

# Overview

This assessment, produced for Copperplate, is part of their ongoing efforts to highlight and remediate security issues. It will provide an overview of the target and outline the subsequent testing and executive summary portions of this engagement.

This report will outline:

* engagement parameters and target information
* a visual summary and assumptions
* security challenges both common and target-specific
* the tools to be used to assess the target and their impact, including limitations and assumptions
* recommendations for risk mitigation
* a timeline of work to be undertaken

# Engagement Parameters and Site Information

## Parameters

|  |  |
| --- | --- |
| Parameter | Notes |
| Disallowed | Testing out-of-scope: domains or subdomains other than copperplate.org.uk disallowed |
| Disallowed | Client explicitly requested for pinging and IP-based testing to be avoided |
| Disallowed | DoS/DDoS disallowed |
| Ambiguous | Login credentials are not provided, but testing on authentication was not explicitly disallowed |

## Site Information

The site is built with Softaculous Coppermine script, a PHP-based image gallery with MySQL backend (Softaculous, 2023), and resides on shared hosting.

# Visual Summary

The target contains a login that uses username and password, implying user data is stored in a database. There is a publicly available search function for images. The overall design of the website is quite dated and could indicate security issues if the client-side, server-side, or security design are similarly dated.

# Security Challenges

|  |  |
| --- | --- |
| Challenge | Potential Risk |
| Malicious file upload | Payloads that infect the server:   * spread to other devices * allow unauthorized access or data breach   If the payload is sophisticated, could be used to target users of the site without their knowledge. |
| Denial of Service attacks (DoS) | Attackers could attempt to overwhelm the site’s resources by DoS attack, making it inaccessible to users. |
| Privacy and/or data leakage | Could lead to disclosure of:   * personal information * server information used to launch more targeted attacks |
| Cross-site scripting (XSS) | Can compromise user accounts, steal information, or deliver malicious payloads to users. |
| Insecure authentication | * gain unauthorized access to user accounts * perform account takeovers * impersonate other users |
| Misconfigured or weak server-side security design | Exploitation of server-side vulnerabilities can result in:   * unfettered access to files and possibly to database(s) * unauthorized modification of the website or data to further compromise systems |
| Social engineering | If the site contains contact or support information, social engineering is one of the easiest vectors of attack. |

# Tools and Methods

|  |  |
| --- | --- |
| Tool | Notes |
| sqlmap | Could reveal SQL-injection vulnerabilities on user-input fields |
| Manual Testing | * PHP code injection * OS command injection testing |
| Burp Suite | * Better visual of the structure of the site * Burp Suite’s built-in scanner can automatically detect possible vulnerabilities |

These items have the potential to cause downtime, but used correctly should not cause issues with the site or its use.

# Analysis Timeline

Following review of this document, testing will be conducted on the site to determine any vulnerabilities that may be present.

The executive summary, to be reviewed 12 June 2023, will outline the results of testing utilising graphics, charts, and other easily communicable data points. It will review Copperplate’s adherence to two security standards: GDPR and NIST Cybersecurity Framework. If vulnerabilities are found, Proof of Concepts (PoC) will be provided, if relevant.

# References

OWASP. (2021) OWASP Top Ten. Available from <https://owasp.org/www-project-top-ten/> [Accessed 19 May 2023]

Softaculous. (2023) Coppermine. Available from <https://www.softaculous.com/softaculous/apps/galleries/Coppermine> [Accessed 20 May 2023]

Information Commissioner’s Office. (n.d.) A guide to data security. Available from <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/security/a-guide-to-data-security/> [Accessed 20 May 2023]

GDPR.EU. (n.d.) General Data Protection Regulation. Available from <https://gdpr.eu/tag/gdpr/> [Accessed 20 May 2023]

NIST. (2023) NIST Cybersecurity Framework Quick Start Guide. Available from <https://www.nist.gov/cyberframework/getting-started/quick-start-guide> [Accessed 20 May 2023]