Web Application Penetration Test: Summary Report

20th December 2023

1.0 Introduction

This report provides the results of the penetration test that was undertaken the 4th and the 20th December of 2023 by Dionach Limited (Dionach) for ASE Corporate Eyecare Limited (EyeMed UK).

The objectives of the test were to find and highlight any potential security threats and vulnerabilities relating to EyeMed's Eyecare Platform from an external viewpoint.

2.0 Methodology

The following checks were completed as part of this penetration test. Any issues that were found during these checks are identified in the penetration test results section 3.0.

- Information gathering, including organisation websites, business social networking and technical websites checked for sensitive information relating to the websites and APIs.
- DNS zone transfer.
- TCP and UDP port scans.
- Network vulnerability scanning.
- Manual tests for network vulnerabilities.
- Web application vulnerability scanning.
- OWASP: Manual tests on input fields, parameters, cookies for injection attacks, cross-site scripting, cross-site request forgery, insecure direct object reference, cryptographic issues, malicious file execution, information leakage, and improper error handling.
- OWASP: Manual tests on pages and links for broken authentication, broken session management, failure to restrict URL access, privilege escalation.
- OWASP: Insecure communications.
- Click-jacking.
- Shared web hosting.
- CAPTCHA bypass.
- Retest of the issues identified in the previous penetration test conducted in February 2023 (reference number 20024-14Q1-1).

3.0 Summary Findings

The penetration test revealed ten low risk issues. Overall, security of the websites represents low risk. The current security infrastructure is sufficient to prevent remote attackers from compromising the websites.

Section	Description	Impact	L'hood	Risk
5.2.1	Insufficient DNS Security Measures	Med	Low	Low
5.2.2	Insufficient Input Validation and Sanitisation	Med	Low	Low
5.2.3	Missing Content Security Policy	Med	Low	Low
5.2.4	Old Versions of PDF Libraries	Med	Low	Low
5.2.5	Old and Unsupported Versions of JavaScript Libraries	Med	Low	Low
5.2.6	Potentially Insufficient Access Control	Med	Low	Low
5.2.7	Potentially Insufficient User Details Protection	Med	Low	Low
5.2.8	Website Functionality Provided by Cross-Domain Includes	Med	Low	Low
5.2.9	Websites Use Predictable IDs	Low	Med	Low
5.2.10	Web Servers Show IIS Version in HTTP Headers	Low	Med	Low

4.0 Response and Remediation Plan

EyeMed is committed to safeguarding the security of the information with which it is entrusted, to complying with relevant data protection legislation, and to meeting the information security requirements of its customers and partners across its people, processes and technology.

EyeMed is pleased that the penetration test identified no critical, high- or medium-risk issues.

EyeMed is committed to continuous improvement and will consider all Low and Informational findings in its regular reviews of information security risk for further action and planning.