RED CITADEL
CYBER SECURITY

Letter of Attestation



CREST MEMBER

Client: GRW Halo Ltd T/A Halo Benefits
Classification: Public
Issue Date: 20.11.2026

Summary

This letter confirms that on 12 November 2026, Red Citadel Limited conducted a one-day engagement comprising a CREST black box web application penetration test for GRW Halo Ltd T/A Halo Benefits.

The purpose of the assessment was to provide an independent, point-in-time review of the security posture of the in-scope system and to identify security weaknesses that could affect their confidentiality, integrity or availability, or that of the data they store and/or process.

Scope of Engagement

The scope of the assessment was broken down into the following components:

- Web Application: An instance of the Halo Benefits Web Application

No exclusions were agreed for this assessment.

Findings

The penetration test demonstrated that GRW Halo Ltd T/A Halo Benefits had implemented strong and effective security controls, particularly in the areas of authentication, access control and the protection of sensitive information and data. The application presented a very limited attack surface, with no evidence of unauthorised access to protected functionality or compromise of sensitive information.

The assessment identified one medium and three low-risk findings, primarily relating to the disclosure of internal application information, which can be addressed through targeted security improvements.

Addressing the findings documented within the Penetration Test report will further strengthen GRW Halo Ltd T/A Halo Benefits 's existing security posture and support continued alignment with recognised industry standards and security best practice.

Limitations

The following limitations apply:

- Penetration Test was conducted against a specific version of the systems within a defined environment and agreed testing window.
- The results reflect the security posture only at the time of assessment.
- Changes made after the test, including software updates, code changes, infrastructure changes, configuration changes, or newly introduced functionality, fall outside the scope of this letter.
- This attestation does not confirm that all vulnerabilities were identified or that the system is free from weaknesses.
- The engagement did not include remediation or verification of fixes unless explicitly stated.

About Red Citadel

Red Citadel is a CREST Penetration Test company delivering expert security assurance across Penetration Test, cloud security audits, vulnerability assessments and IASME certification services.

Our CREST accreditation provides independent assurance that our Penetration Test services are delivered in line with recognised technical, ethical and quality standards. Testing is carried out by experienced consultants using structured methodologies, agreed Rules of Engagement and a clear focus on genuine risk, business impact and practical remediation.

As an IASME Certification Body, we are also authorised to deliver Cyber Essentials, Cyber Essentials Plus and IASME Cyber Assurance Level 1 and Level 2 certifications.

Our team brings more than 20 years of combined IT and cyber security experience. We work closely with clients throughout each engagement, sharing clear findings, practical guidance and support that helps them strengthen their defences and make informed security decisions.

Appendix A: Web Application Penetration Test Methodology

The following test areas were considered during the web application penetration test. Testing was performed where applicable, based on the functionality, access, configuration, and application behaviour available during the assessment.

The methodology was informed by recognised security testing guidance, including the OWASP Top 10, OWASP Web Security Testing Guide, and relevant industry best-practice approaches.

Information Gathering and Application Mapping

- Search engine discovery and reconnaissance
- Review of publicly available information
- Web server fingerprinting
- Application and framework fingerprinting
- Review of web server metadata and exposed files
- Identification of application entry points
- Mapping of application functionality and execution paths
- Review of application architecture and exposed interfaces

Configuration and Deployment Management

- Review of application and platform configuration
- Testing for insecure HTTP methods
- Review of HTTP security headers
- Testing for missing or misconfigured transport security controls
- Review of file extension handling
- Identification of backup, temporary, or unreferenced files
- Enumeration of administrative interfaces
- Testing for subdomain takeover risks
- Review of cloud storage exposure, where applicable

Identity and Authentication

- Review of user registration and account provisioning processes
- Testing for account enumeration
- Review of username and password policy controls
- Testing for default or weak credentials
- Testing for authentication bypass weaknesses
- Review of password reset and account recovery functionality
- Testing of session persistence and “stay logged in” functionality
- Review of browser caching affecting authenticated content

Authorisation and Access Control

- Unauthenticated data access
- Testing for access control bypass
- Testing for privilege escalation
- Testing for insecure direct object references
- Testing for directory traversal and file inclusion weaknesses
- Review of role-based access controls, where applicable
- Cross-tenant data access

Session Management

- Review of session management controls
- Testing of cookie attributes and security flags
- Testing for session fixation
- Review of exposed session variables
- Testing for cross-site request forgery
- Review of logout functionality
- Review of session timeout behaviour
- Testing for session hijacking risks, where applicable

Input Validation and Injection Testing

- Testing for reflected cross-site scripting
- Testing for stored cross-site scripting
- Testing for DOM-based cross-site scripting
- Testing for HTML injection
- Testing for SQL injection
- Testing for XML injection
- Testing for LDAP injection
- Testing for XPath injection
- Testing for server-side template injection
- Testing for server-side request forgery
- Testing for command injection
- Testing for code injection
- Testing for HTTP parameter pollution
- Testing for HTTP request smuggling or splitting risks
- Testing for host header injection

Business Logic Testing

- Review of business logic controls
- Testing for request forgery and workflow bypass
- Testing for insufficient integrity checks
- Testing for process timing weaknesses
- Testing for abuse of rate limits or usage limits
- Testing for upload of unexpected or malicious file types
- Review of application-specific misuse cases

Client-Side Security Testing

- Testing for client-side injection weaknesses
- Testing for client-side URL redirection
- Testing for client-side resource manipulation
- Review of cross-origin resource sharing controls
- Testing for clickjacking
- Testing of browser storage controls
- Testing for cross-document messaging risks
- Testing for WebSocket security issues, where applicable
- Testing for cross-site script inclusion risks

API Security Testing

- Review of API endpoints identified during testing
- Testing for unauthorised access to API functionality
- Testing for insecure object references within API requests
- Testing for weak API authentication and authorisation controls
- Review of API error handling and information disclosure
- Testing for excessive data exposure
- Testing for GraphQL-specific weaknesses, where applicable

Risk Rating and Validation

- Manual validation of identified issues
- Removal of false positives where possible
- Risk-based prioritisation of findings
- Cross-referencing of findings with CVSS where appropriate
- Documentation of findings within a Penetration Test report

Red Citadel Limited | **Registered Address:** 71-75 Shelton Street, Covent Garden, London, WC2H 9JQ | **Company Number:** 16554117