ASSESSMENT DASHBOARD

Target Details

Service Name	Locus Cell Co., Ltd.
Target	https://www.locus-cell.com
Technology Stack	
Service Type	Penetration Testing
User Roles	None

Technical Findings

The assessment identified severity vulnerabilities.

Refer to **Appendix A: Informational Issues** to view the informational risk issue details.

No	Finding	Criticality Rating	Current Status as on 30 October 2023
WEB-1	LACK OF HTTP SECURITY HEADER	MEDIUM	Risk Accepted
WEB-2	CLICKJACKING: LACK OF X-FRAME-OPTIONS IN HTTP HEADERS	LOW	Risk Accepted
WEB-3	CROSS-DOMAIN SCRIPT INCLUDE	INFO	Risk Accepted
WEB-4	WEB SERVER MISCONFIGURATION SCAN RESULT	INFO	Risk Accepted
WEB-5	SUBDOMAIN ENUMERATION	INFO	Risk Accepted
WEB-6	APPLICATION VULNERABILITY SCAN RESULT	INFO	Risk Accepted
WEB-7	HTML USES UNRECOGNIZED CHARSET	INFO	Risk Accepted
WEB-8	USER AGENT-DEPENDENT RESPONSE	INFO	Risk Accepted
WEB-9	INPUT RETURNED IN RESPONSE (REFLECTED)	INFO	Risk Accepted
WEB-10	GENERAL SSL/TLS INFORMATION	INFO	Risk Accepted
WEB-11	OPEN PORTS & SERVICES	INFO	Risk Accepted

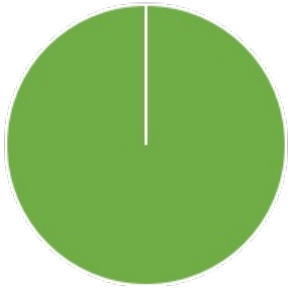
SUMMARY OF FINDINGS

Blacklock adopts OWASP Risk Rating methodology that uses simple and practical approach to calculating overall risk. Each identified vulnerability is measured against threat agent, business impact and likelihood.

Vulnerability Overview

Risk Level	Risks Found	Current Status
Critical	0	0
High	0	0
Medium	1	0
Low	1	0
Info	9	0
Total	11	0

Vulnerabilities Summary



OWASP TOP 10 MAPPING

ID	Web Application Security Risks	Status	Responsible Finding
A1	Broken Access Control	COMPLIANT	-
A2	Cryptographic Failures	COMPLIANT	-
A3	Injection	COMPLIANT	-
A4	Insecure Design	COMPLIANT	-
A5	Security Misconfiguration	COMPLIANT	-
A6	Vulnerable and Outdated Components	COMPLIANT	-
A7	Identification and Authentication Failures	COMPLIANT	-
A8	Software and Data Integrity Failures	COMPLIANT	-
A9	Security Logging and Monitoring Failures	COMPLIANT	-
A10	Server Side Request Forgery (SSRF)	COMPLIANT	-