MOP Cyber Risk Assessment

CHAMELEON

FOR OUR SMARTER WORLD

LEON NETTO

Purpose

This Cyber Risk Assessment aims to meticulously pinpoint potential risk events that could disrupt the MOP web application which is hosted in the Google Cloud Platform (GCP). It delves into the likelihood of each risk occurrence, its potential repercussions, and the existing measures deployed to counter these risks. Moreover, it delineates the residual risk associated with each event, accepted risks, and requisite actions to curtail them.

Leon Netto from the Chameleon organisation spearheaded this comprehensive risk assessment. The threat landscape confronting the MOP web application, identified vulnerabilities, and employed effective risk mitigation techniques were thoroughly examined. The analysis encompasses various threats, including cyberattacks, data breaches, risks from third-party integrations, insider threats, and external threats. Additionally, it covers vulnerabilities such as poor backup procedures, misconfigured resources, inadequate vulnerability management, weak encryption, and inadequate authentication and authorisation practices.

The assessment outlines diverse strategies for risk mitigation, encompassing secure coding, quality assurance protocols, fault tolerance mechanisms, government audits, threat detection tools, testing, and proactive vulnerability management.

Each risk is meticulously evaluated in the specific context of the implemented controls within the MOP web application. Moreover, potential enhancements to bolster the application's resilience are identified, along with corresponding treatments and necessary controls.

Summary of Findings

Risk Rating							
Acute	Very High	High	Medium	Low	Very Low	Negligible	Total
			3	2	2		7

Risk Context

The primary aim of this risk assessment is to precisely identify and outline strategies for managing the risks associated with the MOP web application. It's imperative for security and compliance standards to thoroughly evaluate the security implications of information and communications technology (ICT) systems. This necessitates conducting a risk assessment to document the security measures and potential vulnerabilities within the system.

Each identified risk and mitigation measures will follow the principles outlined in ISO 27001, NIST 800-30, and CISA risk assessment and management guidelines.

Risk Assessment Parameters

Risk identification, assessment criteria, and parameters are integral components of the risk assessment process.

Risks categorised with a residual level of VERY LOW or LOW may be deemed acceptable without requiring supplementary mitigation measures. Risks evaluated with a residual level of MEDIUM should be actively addressed by the Chameleon MOP development team.

Risks appraised as ACUTE, VERY HIGH, or HIGH necessitate mitigation efforts. If post-mitigation, risk levels persist above MEDIUM, explicit acceptance by Chameleon is mandatory.

Risk Register

Risk ID	Potentional Risk Events	Cause/Source of Risk of Vulnerability	Existing Controls	Likelihood	Consequence	Residual Risk (Risk Rating)	Treatments	Likelihood after Treatment
R01	MOP web app is exploited, and the User is manipulated into clicking a link or button that they perceive to be legitimate	Attacker conducts clickjacking attack.	None	Possible	Moderate	Medium	Apply X-Frame-Options HTTP response header to each webpage	Unlikely
R02	Unauthorised user accesses the web application	Poor authorisation mechanisms applied	Password required to login to GCP	Unlikely	Moderate	Low	Apply MFA to access GCP resources	Rare
R03	Lack of availability due to GCP outage	Caused by natural or man-made disasters.	None	Possible	Moderate	Medium	Ensure application is deployed in various regions and zones.	Unlikely
R04	Targeted attacks causes disruptions.	DDoS attacks are conducted	WAF enabled which protects	Rare	Moderate	Very Low	N/A	N/A

			the application from such attacks					
R05	Data integrity is at risk due to weak encryption methods.	1. Attacker can sniff network packets in transit 2. Poor encryption protocls used to encrypt data at rest.	1. TLS used to encrypt data in transit and certificate issued by GCP. 2. GCP used AES-256 to encrypt data at rest as default	Rare	Moderate	Very Low	N/A	N/A
R06	Vulnerabilities in the web application go unnoticed.	Poor vulnerability management and weaknesses are exploited	Code reviews are carried out before	Possible	Moderate	Medium	Use SAST tools such as GitHub Code Scanning and DAST tools such as OWASP ZAP.	Unlikely

		by attackers.	being pushed into the main branch					
R07	Malicious scripts can be inserted into the Search Field	Cross-Site Scripting (XSS) attacks is conducted.	1. Google WAF enabled. 2. User inputs are sanitized.	Unlikely	Moderate	Low	1. Implement Content Security Policy header for each page 2. Implement X-XSS-Protection header for each page	N/A