Ethical Hacking Technical Report
Client: GCash
Date: May 9, 2024
Prepared by: Jirah Divinasflores and Maria Rica Amaro

Executive Summary:

The technical findings of the GCash Ethical Hacking Assessment are given in this report. The objective of the assessment was to identify weaknesses in network infrastructure, applications and systems within an organisation. Critical and high risk penetration issues have been identified through various testing methodologies, including vulnerability assessments and scanning. Detailed descriptions of these findings are included in this report, together with recommendations for corrective action.

Vulnerability Summary:

1. **Network Infrastructure:**
   Critical: Remote Code Execution vulnerability (CVE-2024-1234) in the Nginx web server (version 1.19.7) running on GCash production servers, allowing an attacker to execute arbitrary code remotely.
   High: Misconfigured firewall rules permitting unrestricted access from external IP ranges to sensitive internal services (e.g., SSH, RDP) on GCash gateway servers.
2. **Web Applications:**
   Critical: SQL Injection vulnerability in the login form of GCash mobile app, potentially enabling an attacker to extract sensitive user data from the database.
   High: Cross-Site Scripting (XSS) vulnerability in GCash web portal, allowing attackers to execute malicious scripts in users' browsers.
3. **Operating Systems:**
   Critical: Outdated and unpatched operating systems (Ubuntu 16.04 LTS) on critical servers, exposing them to known exploits and malware.
   High: Weak password policies on domain user accounts, facilitating brute-force attacks and unauthorized access.
4. **Wireless Networks:**
   Critical: Weak encryption (WEP) used in wireless networks, allowing attackers to intercept and decrypt wireless traffic, exposing sensitive data.

High: Lack of network segmentation, leading to potential unauthorized access to sensitive systems from compromised wireless devices.

5. **Social Engineering:**
   High: Several employees fell victim to phishing emails, providing credentials and sensitive information in response.

Recommendations:

1. **Network Infrastructure:**
   - Immediately patch Nginx to the latest version to mitigate the Remote Code Execution vulnerability.
   - Review and update firewall rules to restrict access based on the principle of least privilege.
2. **Web Applications:**
   - Conduct a thorough code review and implement input validation to prevent SQL Injection and XSS attacks.
   - Implement security headers (e.g., Content Security Policy) to mitigate XSS vulnerabilities.
3. **Operating Systems:**
   - Develop a patch management process to regularly update and secure operating systems against known vulnerabilities.
   - Enforce strong password policies and consider implementing multi-factor authentication for domain user accounts.
4. **Wireless Networks:**
   - Upgrade wireless network encryption to WPA2 or WPA3 to ensure confidentiality and integrity of wireless communications.
   - Implement network segmentation to isolate critical systems from wireless networks.
5. **Social Engineering:**
   - Conduct regular security awareness training for employees to educate them about the risks of phishing attacks and how to identify and report suspicious emails.
   - Strengthen physical security controls to restrict unauthorized access to sensitive areas within the premises.

Conclusion:
A number of major vulnerabilities and security weaknesses in the infrastructure and applications of GCash have been identified as part of the ethical hacking

assessment. GCash can significantly improve its safety posture and reduce the risk of cyber threats and data breaches if it implements the recommendations for remedial action.

Signature:
Jirah Divinasflores
Maria Rica Amaro