VULNERABILITY SCANNING & PENETRATION TESTING REPORT

FOR

SAMPLE COMPANY LLC

REPORT NUMBER: [R2026010125]
REPORT DATED: [2026/01/05]

CONFIDENTIAL

Important Disclaimer

This report has been prepared only for the client named above and only for the purpose of the security testing described in this document.

No other person or organisation may rely on this report for any reason.
Afritech Computing does not accept responsibility or liability for:

- Any third party who gains access to this report, or
- Any systems, services, or activities that were not included in the agreed testing scope.

The testing performed reflects the agreed scope, timing, and methods based on recognised industry standards and Afritech Computing's professional judgement. This report does not guarantee that the systems tested are free from all vulnerabilities, nor does it provide a warranty on system performance or security.
Afritech Computing reserves the right to withdraw or amend this report if material issues are later identified.

Confidentiality Notice

This document contains confidential and commercially sensitive information belonging to Afritech Computing and its client. It may not be shared, copied, or disclosed to any third party without prior written approval from Afritech Computing.

Table of Contents

General Information

Purpose of the Report

This report presents the results of a Vulnerability Scanning and Penetration Testing engagement conducted by Afritech Computing for Sample Company LLC. The purpose of this report is to provide an independent, objective assessment of the security posture of the systems, applications, and infrastructure included within the agreed scope of work.

The assessment was performed to:

- Identify security vulnerabilities, weaknesses, and misconfigurations
- Evaluate the effectiveness of existing security controls
- Support regulatory, compliance, and governance requirements
- Assist management in understanding and prioritising security risks

Engagement Context

Afritech Computing was formally appointed by Sample Company LLC to perform third-party security testing in accordance with the agreed engagement terms, scope definition, and testing window.

Testing Period: 2026/01/05 to 2026/01/09

The testing activities were conducted in a controlled manner designed to minimise operational impact. Testing methods and depth were aligned with recognised industry standards, regulatory expectations, and Afritech Computing's professional judgement.

Scope Limitations and Assumptions

The scope of this engagement was limited to the systems, applications, and assets explicitly agreed upon and documented prior to commencement of testing. Any systems, environments, integrations, or services not expressly listed as in scope were excluded from testing and are not covered by this report.

Certain testing techniques (including denial-of-service or stress testing) may have been excluded where such activities posed an unacceptable risk to system availability or business operations.

Accordingly, while reasonable efforts were made to identify material security weaknesses, this assessment cannot guarantee the identification of all possible vulnerabilities.

Use and Reliance on This Report

This report has been prepared exclusively for:

- Sample Company LLC, and
- Relevant regulators, auditors, or oversight bodies where disclosure is required or permitted

No other party may rely on this report without the prior written consent of Afritech Computing.

Professional Standards and Methodology

All testing activities were conducted by suitably qualified security professionals and aligned with recognised best practices, including but not limited to:

- Industry-standard vulnerability assessment and penetration testing methodologies
- The Common Vulnerability Scoring System (CVSS v4) for risk rating
- Afritech Computing's internal quality assurance and review processes

The conclusions and findings presented in this report are based on the information available at the time of testing and reflect Afritech Computing's professional judgement.

Statement of Independence

Afritech Computing confirms that the assessment was performed independently and objectively. Afritech Computing has no operational responsibility for, or management control over, the systems assessed, beyond the activities required to perform this engagement.

Report Approval and Sign-Off

This report has been reviewed and approved by Afritech Computing's authorised representative as a true and accurate reflection of the testing performed and the findings identified.

Signed for and on behalf of Afritech Computing:

_____

Name: Innocent B. Maluka
Title: Director
Date:

Client & Report Details

Client Trading Name: Sample Company LLC
Report Number: R2026010125
Report Date: 2026/01/12

Afritech Computing Information

Legal Entity: Afritech Computing PTY LTD
Address: 9340 Forest Tea, Centurion, Pretoria, South Africa
Contact Email: cybersecurity@afriteq.co.za

Afritech Computing is an independent cybersecurity services provider delivering vulnerability assessments, penetration testing, and security assurance services across multiple industries, including financial services, cloud platforms, enterprise IT, healthcare, e-commerce, and gaming.

All testing is conducted by qualified security professionals holding recognised certifications such as OSCP, CEH, and equivalent industry credentials.

Review & Testing Overview

Engagement Request Date: 2025/11/21
Testing Start Date: 2026/01/05
Testing End Date: 2026/01/09

Testing Team:

Name	Role	Experience	Key Certifications
Tumelo Lesiba	Lead Tester	8+ Years	Certified Ethical Hacker, Certified Penetration Testing Engineer. eLearn Junior Penetration Tester. Practical Network Penetration Tester.
Donovan Naicker	Tester	3 Years	Certified Ethical Hacker, Certified Penetration Testing Engineer,

Scope of Work Summary

The testing scope may include one or more of the following areas, as agreed with the client:

Internal Network Security Assessment

- Identify configuration weaknesses and vulnerabilities on internal systems
- Review exposed services, protocols, and access controls
- Validate findings using manual testing where appropriate

External Network Security Assessment

- Assess public-facing infrastructure for exploitable weaknesses
- Identify exposed services and misconfigurations

Web Application Security Assessment

- Identify vulnerabilities in internet-facing web applications
- Test authentication, access control, session handling, and configuration issues

Mobile Application Security Assessment

- Assess Android and/or iOS applications
- Review application behaviour, data storage, communications, and API usage

Firewall Security & Vulnerability Assessment

- Review firewall rule sets and configurations
- Identify weaknesses that could allow unauthorised access

Anything not explicitly listed above is considered out of scope.

Summary of Testing Performed

Testing was conducted using a combination of automated tools and manual techniques aligned with industry best practices, including:

- Reconnaissance and information gathering
- Vulnerability identification and validation
- Exploitation attempts (where safe and permitted)
- Post-exploitation analysis
- False-positive reduction

Summary of Findings

Severity Rating Model

Afritech Computing uses the Common Vulnerability Scoring System (CVSS v4) to rate the severity of identified issues.

Severity	CVSS v4 Score Range	Description
Critical	9.0 – 10.0	Immediate and severe risk requiring urgent remediation
High	7.0 – 8.9	Serious security risk that should be addressed promptly
Medium	4.0 – 6.9	Moderate security risk requiring planned remediation
Low	Below 4.0	Low risk (tracked but not reported by default)

A risk-based remediation approach is recommended, starting with the highest severity findings.

Detailed Findings

The testing scope may include one or more of the following areas, as agreed with the client:

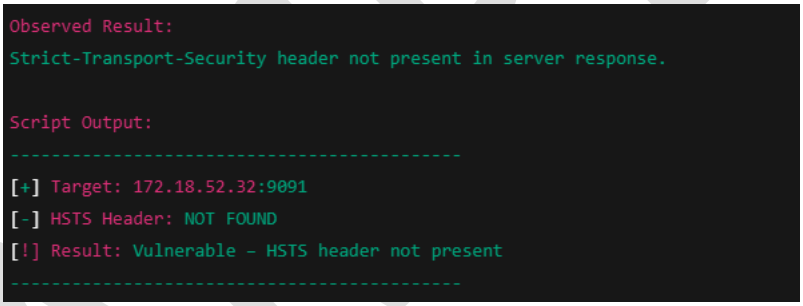
Internal Network Security Assessment Findings

Finding 1: Grafana Privilege Escalation via Data Source UID Misconfiguration	
Affected Asset(s):	172.18.52.32 (9091/tcp)
CVSS Score:	8.9
Severity Rating:	High
Description:	[The Grafana instance running on the affected host is vulnerable to a privilege escalation issue caused by improper access control enforcement in data source management. This issue affects Grafana versions prior to the following patched releases: 10.0.12 10.1.8 10.2.5 10.3.4 9.5.7 A user with permissions to create data sources can exploit the Grafana API by assigning a wildcard (*) value to the data source UID. Due to insufficient validation, this configuration results in the user being granted unrestricted access to all data sources within the Grafana organization. This behavior effectively bypasses intended authorization controls and grants privileges far beyond those assigned to the user role. Impact • Successful exploitation allows an attacker to: • Escalate privileges within the Grafana environment • Read and query all configured data sources • Modify or delete existing data source configurations • Access potentially sensitive data from connected back-end systems • Disrupt monitoring, alerting, and analytics operations This vulnerability poses a significant risk to the confidentiality and integrity of monitored data and may facilitate further lateral movement within the environment.
CVE Reference	CVE-2024-1442
Recommendation:	Upgrade Grafana to **version 10.3.4 or later** (or the latest stable release) to ensure proper access control enforcement and prevent abuse of the data source UID mechanism.
Evidence	

```
Script Output:
------------------------------------------------
[+] Target: 172.18.52.32:9091
[+] Grafana Version: 9.4.3 (Vulnerable)
[+] Wildcard UID accepted
[!] Privilege Escalation Confirmed
[!] Result: Vulnerable – Data Source UID Access Control Bypass
------------------------------------------------
```

Management Comments	Date of Resolution
Name and surname: Title: Date:	Response: Date for fix to be implemented:

Finding 2: HSTS Missing From HTTPS Server	
Affected Asset(s):	172.18.52.32 (9091/tcp)
CVSS Score:	6.5
Severity Rating:	Medium
Description:	The remote web server is not enforcing HSTS, as defined by RFC 6797. HSTS is an optional response header that can be configured on the server to instruct the browser to only communicate via HTTPS. The lack of HSTS allows downgrade attacks, SSL-stripping man-in-the-middle attacks, and weakens cookie-hijacking protections.
CVE Reference	No CVE Applicable
Recommendation:	Configure the remote web server to use HSTS.
Evidence	



Management Comments	Date of Resolution
Name and surname: Title: Date:	Response: Date for fix to be implemented:

External Network Security Assessment Findings

Finding 1: SSL Certificate Cannot Be Trusted	
Affected Asset(s):	Samplecompanyllc.com
CVSS Score:	6.5
Severity Rating:	Medium
Description:	The X.509 certificate presented by the server is not trusted due to a break in the certificate chain of trust. This condition may occur under several circumstances, including: The certificate chain does not terminate at a trusted public Certificate Authority (CA). This can result from the use of a self-signed root certificate or from missing intermediate certificates required to establish a valid trust path. One or more certificates in the chain are not valid at the time of assessment, either because they are not yet active (notBefore) or have expired (notAfter). The certificate chain contains an invalid or unverifiable digital signature. This may be caused by an incorrectly signed certificate or by the use of a signing algorithm that is unsupported or not recognized by the validation engine. If the affected system is a publicly accessible production host, any disruption in the certificate trust chain undermines a client's ability to verify the server's authenticity and identity. As a result, users may be exposed to an increased risk of man-in-the-middle (MITM) attacks, potentially allowing an attacker to intercept or manipulate encrypted communications.
CVE Reference	No CVE Applicable
Recommendation:	Ensure that the server presents a valid and trusted X.509 certificate by configuring a complete and correct certificate chain. The certificate must be issued by a recognized public Certificate Authority (CA) and include all required intermediate certificates. Verify that all certificates in the chain are within their validity period and that digital signatures are correctly generated using supported and secure cryptographic algorithms.
Evidence	

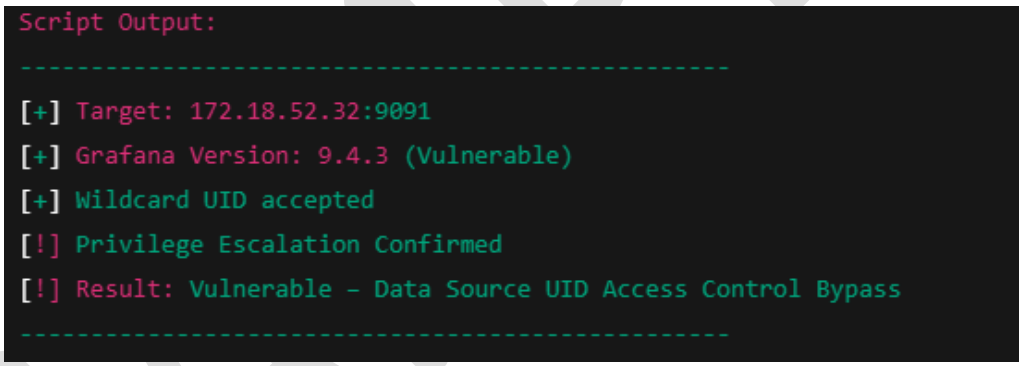
Management Comments	Date of Resolution

Name and surname: Title: Date:	Response: Date for fix to be implemented:

Web Application Security Assessment Findings

Finding 1: Grafana Labs Incorrect Permission	
Affected Asset(s):	Grafana.samplecompanylcc.com
CVSS Score:	4.7
Severity Rating:	Medium
Description:	The version of Grafana Labs installed on the remote host is prior to 10.3.10, 10.4.9, 11.0.5, 11.1.6, or 11.2.1. It is, therefore, affected by a vulnerability as referenced in the cve-2024-8118 advisory. - In Grafana, the wrong permission is applied to the alert rule write API endpoint, allowing users with permission to write external alert instances to also write alert rules. (CVE-2024-8118)
CVE Reference	CVE-2024-8118
Recommendation:	Upgrade to Grafana Labs version 10.3.10 / 10.4.9 / 11.0.5 / 11.1.6 / 11.2.1 or later.

Evidence



Management Comments	Date of Resolution
Name and surname: Title: Date:	Response: Date for fix to be implemented:

Mobile Application Security Assessment Findings

Finding 1: Call to dangerous WebView settings API	
Affected Asset(s):	Package: com.samplecompanyllc.android.samplecompany Status: Open Domain: Security
CVSS Score:	6.2
Severity Rating:	High
Description:	List of WebView API calls.
CVE Reference	OWASP Mobile Security Testing Guide (MSTG) Android Developers: WebView & WebSettings OWASP MSTG - WebView platform guidance
Recommendation:	Review all WebView settings and disable risky options by default (e.g., file access, universal file URL access). Only enable JavaScript for trusted content; block javascript: and file: schemes where possible. Avoid addJavascriptInterface with untrusted content; enforce a strict URL allowlist in shouldOverrideUrlLoading().

Evidence

```
Application Package:
com.samplecompanyllc.android.samplecompany

File Analyzed:
app/src/main/java/com/samplecompany/webview/SampleWebViewActivity.java

Relevant Code Snippet:
--------------------------------------------------
WebView webView = findViewById(R.id.webView);
WebSettings settings = webView.getSettings();

settings.setJavaScriptEnabled(true);
settings.setAllowFileAccess(true);
settings.setAllowContentAccess(true);
settings.setAllowUniversalAccessFromFileURLs(true);
settings.setAllowFileAccessFromFileURLs(true);
```

Management Comments	Date of Resolution
Name and surname: Title: Date:	Response: Date for fix to be implemented:

Firewall Security & Vulnerability Assessment Findings

Finding 1: Overly Permissive Firewall Rule Allowing Unrestricted Remote Access	
Affected Asset(s):	Perimeter Firewall – FW-PROD-01 (203.0.113.10)
CVSS Score:	7.5
Severity Rating:	High
Description:	The perimeter firewall is configured with an overly permissive inbound access rule that allows unrestricted traffic from any source to a sensitive internal service. Specifically, TCP port 3389 (Remote Desktop Protocol) is exposed to the internet without source IP restrictions or additional security controls. This configuration significantly increases the attack surface and may allow unauthorized users to attempt brute-force attacks, exploit known vulnerabilities, or gain unauthorized access to internal systems protected by the firewall.
CVE Reference	N/A (Configuration weakness)
Recommendation:	Restrict inbound access to TCP port 3389 by applying strict source IP allowlists or disabling external access entirely if not required. Where remote administrative access is necessary, enforce access through a secure VPN solution and implement additional controls such as multi-factor authentication, logging, and rate limiting. Review all firewall rules to ensure compliance with the principle of least privilege.

Evidence

```
Firewall Device: FW-PROD-01
Rule ID: 104
Direction: Inbound
Source: Any
Destination: Internal Network (10.10.0.0/16)
Service: TCP/3389
Action: Allow
Status: Enabled

Observation:
Inbound RDP traffic is permitted from any external IP address without restriction.
Timestamp: 2026-01-16
```

Management Comments	Date of Resolution
Name and surname: Title: Date:	Response: Date for fix to be implemented:

Annexures

Annexure A: In-Scope IP Addresses

IP Address(es)			
10.60.10.106	10.60.10.108	10.60.10.141	10.60.10.202
10.60.10.107	10.60.10.109	10.60.10.201	10.60.12.103

Annexure B: In-Scope URLs / Domains

Web Address	Services
www.samplecompany.co.za	HTTP / HTTPS
cash.samplecompany.co.za	HTTP / HTTPS
api.samplecompany.co.za	HTTP / HTTPS
bet.samplecompany.co.za	HTTP / HTTPS
net.samplecompany.co.za	HTTP / HTTPS
media.samplecompany.co.za	HTTP / HTTPS

Annexure C: Open Ports & Services (Internal)

IP Address (Port/Protocol)		
10.60.11.2 (2000/tcp)	10.60.10.106 (3389/tcp	10.60.10.107 (22/tcp
10.60.10.108 (443)	10.60.10.141 (22)	10.60.10.201 (80)
10.60.10.202 (80)	10.60.10.202 (8050)	10.60.10.202 (8055)

Annexure D: Open Ports & Services (External)

IP Address (Port/Protocol)		
185.133.76.2 (2000/tcp)	185.133.76.3 (179	185.133.76.5 (443
185.133.76.25 (179	185.133.76.26 (179	185.133.76.27 (179

Annexure E: Mobile Applications in Scope

Mobile Application	Package Kit File Name
Mobile App (Android)	samplewallet-release-2.1.0.apk
Mobile App (iOS)	SampleCompany-iOS-1.4.2.ipa

Annexure F: Firewall Rules Reviewed

Finding 1: Overly Permissive Firewall Rule Allowing Unrestricted Remote Access								
Table header								
Rule	**Active**	**Action**	**Protocol**	**Source**	**Src Port**	**Destination**	**Dst Port**	**Log**
FW-001	FW-001	FW-001	FW-001	FW-001	FW-001	FW-001	FW-001	FW-001