

PWNED LABS

[Assessment type / environment, for example Microsoft Azure and Microsoft 365]

Report of Findings Document

2022

Created by:	Prepared for:
[Tester name]	Client Contact
Pwned Labs	[CLIENT NAME]
[tester email]	[client contact email]

CONFIDENTIALITY STATEMENT: The information contained in this report document is for the exclusive use of the client specified and may contain confidential, privileged, and non-disclosable information. If the recipient of this report is not the client or addressee, such recipient is strictly prohibited from reading, photocopying, distributing or otherwise using this report or its contents in any way.

Table of Contents

Executive Summary 4
- Assessment Overview 4
- Key Findings 4
- Overall Risk Assessment 4
- Remediation & Verification 4
- Summary Table of Findings by Severity 5

Findings, Observations, and Recommendations 6
- Critical Risk Findings 6
  - 1. [Critical finding title] [Category] 6
- High Risk Findings 7
  - 2. [High finding title] [Category] 7
- Medium Risk Findings 7
  - 3. [Medium finding title] [Category] 7
- Low Risk Findings 8
  - 4. [Low finding title] [Category] 8
- Informational / Positive Results 8
  - 5. [Informational or positive result title] [Positive] 8
- Additional Observations 9

Executive Summary

Assessment Overview

[Summarize the engagement: the environment and scope assessed (tenant, subscriptions, workloads or IP ranges), the testing approach (external and unauthenticated, authenticated configuration review, or assumed-breach), and the test window. State what was in and out of scope.]

[Note any second-tester reconciliation, the methodology or technique catalogue applied, and how findings were validated and rated.]

Key Findings

[Tester] identified [N] findings across the [CLIENT NAME] scope, categorized by severity as follows:

1. Critical-Risk Findings: [N] findings. [One-line summary of the most serious issues.]
2. High-Risk Findings: [N] findings. [One-line summary of the High findings.]
3. Medium-Risk Findings: [N] findings. [One-line summary of the Medium findings.]
4. Low-Risk Findings: [N] findings. [One-line summary of the Low findings], plus [N] positive or informational results.

[State the single most significant risk, why it matters, and that it is described in full with reproduction steps and evidence in the findings that follow.]

Overall Risk Assessment

[State the overall posture rating and the reasoning behind it: the most serious exploitable paths and the recommended remediation priority.]

Remediation & Verification

[Tester] has provided remediation recommendations for each finding in this report. [State what post-report support is included, for example a technical readout session and a single retest of each finding after the client has validated the fixes.]

Summary Table of Findings by Severity

The table below lists all findings by risk level. Detailed findings and remediation guidance follow.

Findings	Affected Systems	Risk Level
1. [Critical finding title] [Category]	**[Affected systems, for example a storage account, app registration or subscription.]**	**Critical**
2. [High finding title] [Category]	**[Affected systems.]**	**High**

3. [Medium finding title] [Category]	**[Affected systems.]**	**Medium**
4. [Low finding title] [Category]	**[Affected systems.]**	**Low**
5. [Informational or positive result title] [Positive]	**[Affected systems or scope of the positive result.]**	**Informational**

Findings, Observations, and Recommendations

During the course of our assessment we identified the following issues, listed below by risk level.

Critical Risk Findings

● 1. [Critical finding title] [Category]
Finding [Describe the exposed surface or misconfiguration in plain language: what it is, where it lives, and why it is reachable. Name the affected resource or identity.] [Describe what we did and what we observed, in prose rather than a raw command dump. State the evidence captured in the figure below, for example a successful unauthenticated response or a recovered credential.] [Explain the impact and why it is rated Critical: what an attacker gains that they did not already have, and the chain from this issue to serious compromise. State the CVSS 3.1 base score and vector, for example 9.8 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).] *Figure 1: [Short description of the captured evidence].*
Recommendation [State the specific remediation: the exact setting, role or control to change, named concretely rather than in general terms.]
Affected Systems

[Affected resource or identity, with scope. Endpoint: [URL or resource path].]

High Risk Findings

2. [High finding title] [Category]

Finding

[Describe the surface or weakness and the affected resource or identity.]

[Describe what we did and what we observed, and the evidence captured below.]

[Explain the impact and why it is rated High. State the CVSS 3.1 base score and vector, for example 8.1 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:N).]

Figure 2: [Short description of the captured evidence].

Recommendation

[State the specific remediation.]

Affected Systems

[Affected resource or identity, with scope. Endpoint: [URL or resource path].]

Medium Risk Findings

3. [Medium finding title] [Category]

Finding

[Describe the surface or weakness and the affected resource or identity.]

[Describe what we did and what we observed, and the evidence captured below.]

[Explain the impact and why it is rated Medium. State the CVSS 3.1 base score and vector, for example 5.9 (AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N).]

Figure 3: [Short description of the captured evidence].

Recommendation

[State the specific remediation.]

Affected Systems

[Affected resource or identity, with scope. Endpoint: [URL or resource path].]

Low Risk Findings

● 4. [Low finding title] [Category]
Finding [Describe the hardening gap and where it applies.] [Describe what we did and what we observed, and the evidence captured below.] [Explain the impact and why it is rated Low, including any context that bounds the risk. State the CVSS 3.1 base score and vector, for example 3.1 (AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N).] *Figure 4: [Short description of the captured evidence].*
Recommendation [State the specific remediation.]
Affected Systems [Affected resource or identity, with scope. Endpoint: [URL or resource path].]

Informational / Positive Results

● 5. [Informational or positive result title] [Positive]
Finding [Describe what was tested and the positive or informational result.] [Explain why this is a positive result and what good practice it reflects.]
Recommendation [State the recommendation, for example maintain the current good practice.]
Affected Systems [Affected systems or scope. Endpoint: n/a.]

Additional Observations

[Optional observation heading, for example an area tested and found clean]. [Describe an area that was tested and did not result in a finding, or a note worth recording that does not rise to a finding.]