Risk Assessment Report

Max Vilar

---

1. Executive Summary

This risk assessment evaluates the security posture of an Azure-hosted infrastructure that I created running OWASP Juice Shop. The assessment identifies vulnerabilities, assesses risks, and recommends mitigation strategies to improve the overall security of the environment. Key risks include open RDP ports, web application vulnerabilities (e.g., SQL injection), and misconfigured Azure storage.

---

2. Scope and Objectives

Scope

- Azure Virtual Machine (VM) hosting OWASP Juice Shop.
- Networking components (Network Security Groups, Public IPs).
- Application-level security of OWASP Juice Shop.
- Azure Storage Configurations.

Objectives

- Identify potential threats and vulnerabilities.
- Analyze risks using NIST 800-30 guidelines.
- Recommend mitigations aligned with ISO 27001 standards.

---

3. Methodology

The assessment adhered to:

- **NIST 800-30** for identifying and assessing risks.
- **ISO 27001** for implementing security controls.
- Tools used:
    - **OWASP ZAP** for application vulnerability scanning.

- **Nessus Essentials (free for educational purposes)** for network and VM vulnerability scanning.
- **Azure Security Center** for cloud-native recommendations.

---

4. Asset Inventory

Asset	Description	Category
Azure VM	Virtual machine hosting Juice Shop application.	Critical
OWASP Juice Shop	Vulnerable web application for testing.	Critical
Network Security Group	Controls inbound/outbound traffic for the VM.	Supporting
Azure Storage	Stores application data.	Critical

---

5. Threats and Vulnerabilities

Threat	Vulnerability	Affected Asset
Unauthorized Access	Open RDP port (3389)	Azure VM
Unauthorized Access	Weak Admin Passwords	Azure VM
SQL Injection	Unvalidated user input	Juice Shop App
Data Breach	Publicly accessible storage	Azure Storage

---

6. Risk Analysis

Risk	Likelihood	Impact	Risk Level
Open RDP Port	High	High	Critical

Weak Admin Passwords	High	High	Critical
SQL Injection	Medium	High	High
Public Storage Access	High	Medium	High

---

7. Mitigation Plan

Risk	**Mitigation**	**Status**
Open RDP Port	Restrict RDP access to specific IPs or use Azure Bastion.	Mitigated
Weak Admin Passwords	Enforce strong password policies and implement MFA	Pending
SQL Injection	Apply input validation and implement prepared statements.	Pending
Public Storage Access	Remove public access and use SAS tokens for controlled access.	Mitigated

---

8. Residual Risks

- **SQL Injection Vulnerabilities**: Juice Shop is intentionally designed with vulnerabilities for testing purposes. This risk is acceptable in this controlled environment as it aids in learning and development.
- **Open Ports**: RDP access is restricted but still poses a residual risk if IP restrictions are misconfigured.
- **Weak Admin Passwords**: Until MFA and password policies are fully enforced, this remains a potential risk.

---

9. Conclusion and Recommendations

This assessment identified critical risks in the Azure infrastructure and application, including open RDP ports, weak administrative passwords, and web application vulnerabilities. Mitigations were implemented for network and storage risks, reducing the overall risk level. Further actions, such as continuous monitoring and enhanced application security, are recommended.

Future Recommendations

- Enable Multi-Factor Authentication (MFA) for all Azure resources.
- Regularly update and patch the Azure VM and Juice Shop application.
- Conduct periodic vulnerability scans and audits.
- Enforce strong password policies across all administrative accounts.
- Enable advanced logging and monitoring via Azure Monitor and Security Center.

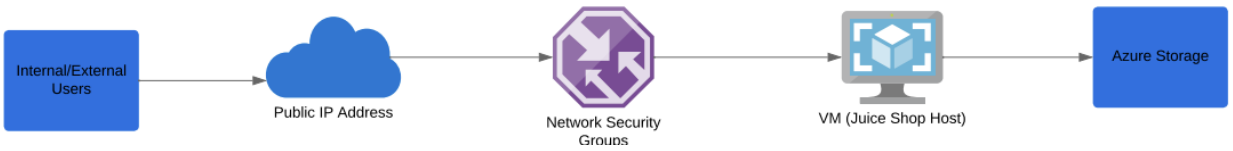
---

10. Appendices

A. Vulnerability Scan Results

- OWASP ZAP: Identified SQL injection and XSS vulnerabilities.
- Nessus Essentials: Found open ports (3389, 80, 443) and outdated software.

B. Azure Architecture Diagram



C. References

- NIST 800-30: Guide for Conducting Risk Assessments.
- ISO 27001: Information Security Management Systems.
- Azure Security Center Documentation.
