Bibliophile Library Penetration Testing Report

Prepared by:
Team 12
5/3/2025

CONFIDENTIAL

Table of Contents

Table of Contents 2
Finding Classifications 3
Business Impact 3
CVSS Score 3
Critical Risk Findings 4
Title of Finding 4
High Risk Findings 6
Title 6
Moderate Risk Findings 7
Title 7
Low Risk Findings 8
Title 8
Informational Findings 9
Title 9
Appendix B: Tools Used 10

Finding Classifications

Team 12 utilized a two-dimensional matrix, see below, consisting of the business impact and Common Vulnerability Scoring System v4.0 (CVSS)[1] score of each finding to categorize it within one of five overall security risk categories: informational, low, moderate, high, and critical. These categories were organized to prioritize the remediation of findings that would cause RAKMS financial loss, non-compliance with governance requirements, and reputational impact.

	Business Impact				
CVSS Score	**N/A (1)**	**Low (2)**	**Moderate (3)**	**High (4)**	**Critical (5)**
N/A – 0.0 (a)	1a	2a	3a	4a	5a
0.1 – 3.9 (b)	1b	2b	3b	4b	5b
4.0 – 6.9 (c)	1c	2c	3c	4c	5c
8.0 – 8.9 (d)	1d	2d	3d	4d	5d
9.0 – 10.0 (e)	1e	2e	3e	4e	5e

Overall Risk Key: Informational Low Moderate High Critical

Business Impact

Team 12 incorporates business impact into the result for the categorization of a finding to help prioritize mitigation efforts and allocate resources effectively to address the most critical issues. We base our qualitative measurement on the ability of a finding to impact RAKMS's ability to conduct business, ensure public safety and security, protect customer information, or stay in compliance with government regulations and business standards. As TEAM 12 is operating under limited knowledge of the business operations of RAKMS, we would recommend RAKMS to review the business impact of these findings to provide a better understanding of the overall risk of said findings.

CVSS Score

The Common Vulnerability Scoring System (CVSS) is a widely recognized industry standard used to evaluate and communicate the severity of security vulnerabilities in computer systems and software. It provides a structured framework for assessing a vulnerability's potential impact, exploitability, complexity, and privileges required for exploitation, assigning it a numeric score from 0 to 10, with higher scores indicating greater risk. CVSS assists organizations in prioritizing and addressing security flaws by considering their impact on confidentiality, integrity, and availability. In our security assessments, we adhere to the CVSS framework, which allows us to accurately gauge the severity of vulnerabilities and effectively communicate their potential risks.

[1] https://www.first.org/cvss/v4.0/specification-document

Critical Risk Findings

	Title of Finding		
Findings Categorization			
Business Impact	Compromised FTP server	**CVSS v4.0 Score**	3c

Description

Explain what the vulnerability is in plain English. Don't assume the reader knows technical details.

- What is the weakness or misconfiguration?
- Why is it a problem?

Using a credential found in a simple network scan, the attacker was able to bypass password requirements and access a file transfer server. Businesses typically manually block the ability for the scan to be conducted, which would hide the username credentials from any unauthorized users,

Business Impact

Explain how this vulnerability could harm the organization.

Although operations would not be halted in the event of this attack occurring, customer data would be accessible to cybercriminals looking to leak data to sell or for personal use. Additionally, any sensitive data regarding internal network information, systems or passwords are vulnerable to being stolen by an attackers. Furthermore, any files needing to be transferred are at risk of being stolen.

With a vulnerability of this size, customers will lose trust in the confidentiality of their data which is stored and collected by the company. Customers may choose a different company that provides the same service as ours, who has robust security measures.

Affected Systems

List IPs, URLs, or specific systems that are vulnerable.
Format like:

TCP port 21 – FTP

Mitigations

Our recommendation to fix the issue is to close FTP and to implement SFTP for organizational use. Furthermore, requiring username passwords credentials to access the ftp server. Lastly, the firewall needs to block traffic from NMAP to reduce the risk of attackers discovering open ports.

Explain how the issue can be fixed or reduced.

What should the organization do to stop this from happening?

Be practical — authentication, patching, access control, etc.

References

Include links to CVEs, OWASP, blogs, or docs that help explain the issue.

Steps for Reproduction

Write clear, step-by-step instructions that show how you found or tested this vulnerability. Include screenshots where possible
Format example:

1. Navigate to http://10.0.0.1/login
2. Enter credentials: admin:admin
3. Observe access to restricted dashboard

High Risk Findings

	Title		
Findings Categorization			
Business Impact		**CVSS v4.0 Score**	

Description

Business Impact

Affected Systems

Mitigations

References

Steps for Reproduction

Moderate Risk Findings

	Title		
Findings Categorization			
Business Impact		**CVSS v4.0 Score**	

Description

Technical Impact

Affected Systems

Mitigations

References

Steps for Reproduction

Low Risk Findings

	Title		
Findings Categorization			
Business Impact		**CVSS v4.0 Score**	
CVSS Attack Vector			

Description

Technical Impact

Affected Systems

Potential Compliance Violations

Mitigations

References

Steps for Reproduction

Informational Findings

	Title		
Findings Categorization			
Business Impact		**CVSS v4.0 Score**	

Description

Affected Systems

Potential Compliance Violations

Mitigations

References

Steps for Reproduction

Appendix B: Tools Used

Tool name	
Description	
Use Case	
Source	

Tool Name	
Description	
Use Case	
Source	

Tool Name	
Description	
Use Case	
Source	