Cybersecurity

Penetration Test Report

Rekall Corporation

Penetration Test Report

Confidentiality Statement

This document contains confidential and privileged information from Rekall Inc. (henceforth known as Rekall). The information contained in this document is confidential and may constitute inside or non-public information under international, federal, or state laws. Unauthorized forwarding, printing, copying, distribution, or use of such information is strictly prohibited and may be unlawful. If you are not the intended recipient, be aware that any disclosure, copying, or distribution of this document or its parts is prohibited.

Table of Contents

Contact Information

Company Name	Coleman Security Insights (CSI)
Contact Name	Chontele Coleman
Contact Title	Lead Penetration Tester

Document History

Version	Date	Author(s)	Comments
001	04/25/2025	Chontele Coleman	Included comprehensive findings for identified vulnerabilities.

Introduction

In accordance with Rekall policies, our organization conducts external and internal penetration tests of its networks and systems throughout the year. The purpose of this engagement was to assess the networks' and systems' security and identify potential security flaws by utilizing industry-accepted testing methodology and best practices.

For the testing, we focused on the following:

- Attempting to determine what system-level vulnerabilities could be discovered and exploited with no prior knowledge of the environment or notification to administrators.
- Attempting to exploit vulnerabilities found and access confidential information that may be stored on systems.
- Documenting and reporting on all findings.

All tests took into consideration the actual business processes implemented by the systems and their potential threats; therefore, the results of this assessment reflect a realistic picture of the actual exposure levels to online hackers. This document contains the results of that assessment.

Assessment Objective

The primary goal of this assessment was to provide an analysis of security flaws present in Rekall's web applications, networks, and systems. This assessment was conducted to identify exploitable vulnerabilities and provide actionable recommendations on how to remediate the vulnerabilities to provide a greater level of security for the environment.

We used our proven vulnerability testing methodology to assess all relevant web applications, networks, and systems in scope.

Rekall has outlined the following objectives:

Table 1: Defined Objectives

Objective
Find and exfiltrate any sensitive information within the domain.
Escalate privileges.
Compromise several machines.

Penetration Testing Methodology

Reconnaissance

We begin assessments by checking for any passive (open source) data that may assist the assessors with their tasks. If internal, the assessment team will perform active recon using tools such as Nmap and Bloodhound.

Identification of Vulnerabilities and Services

We use custom, private, and public tools such as Metasploit, hashcat, and Nmap to gain perspective of the network security from a hacker's point of view. These methods provide Rekall with an understanding of the risks that threaten its information, and also the strengths and weaknesses of the current controls protecting those systems. The results were achieved by mapping the network architecture, identifying hosts and services, enumerating network and system-level vulnerabilities, attempting to discover unexpected hosts within the environment, and eliminating false positives that might have arisen from scanning.

Vulnerability Exploitation

Our normal process is to both manually test each identified vulnerability and use automated tools to exploit these issues. Exploitation of a vulnerability is defined as any action we perform that gives us unauthorized access to the system or the sensitive data.

Reporting

Once exploitation is completed and the assessors have completed their objectives, or have done everything possible within the allotted time, the assessment team writes the report, which is the final deliverable to the customer.

Scope

Prior to any assessment activities, Rekall and the assessment team will identify targeted systems with a defined range or list of network IP addresses. The assessment team will work directly with the Rekall POC to determine which network ranges are in-scope for the scheduled assessment.

It is Rekall's responsibility to ensure that IP addresses identified as in-scope are actually controlled by Rekall and are hosted in Rekall-owned facilities (i.e., are not hosted by an external organization). In-scope and excluded IP addresses and ranges are listed below.

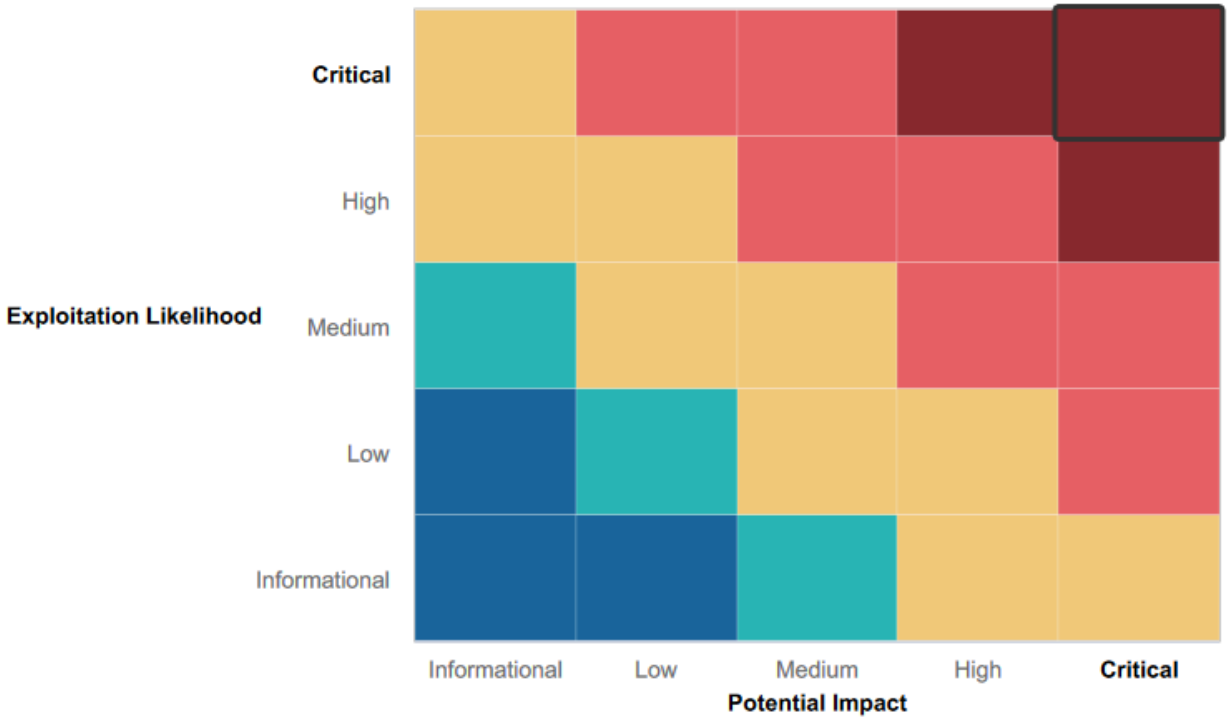
Executive Summary of Findings

Grading Methodology

Each finding was classified according to its severity, reflecting the risk each such vulnerability may pose to the business processes implemented by the application, based on the following criteria:

Critical: Immediate threat to key business processes.
High: Indirect threat to key business processes/threat to secondary business processes.
Medium: Indirect or partial threat to business processes.
Low: No direct threat exists; vulnerability may be leveraged with other vulnerabilities.
Informational: No threat; however, it is data that may be used in a future attack.

As the following grid shows, each threat is assessed in terms of both its potential impact on the business and the likelihood of exploitation:



Summary of Strengths

While the assessment team was successful in finding several vulnerabilities, the team also recognized several strengths within Rekall's environment. These positives highlight the effective countermeasures and defenses that successfully prevented, detected, or denied an attack technique or tactic from occurring.

- **Defense-in-Depth Strategy Applied:** On more than one occasion successful infiltration required the orchestration of a series of steps which highlights a resilient architecture.
- **Security Zoning with Role-Based Permissions:** By Segmenting internal systems while simultaneously enforcing strict access controls, lateral movement was constrained, making sure attackers have to adopt more cultivated enumeration and escalation practices.
- **Tracking and Observation through Logs and Monitoring:** Many activities, such as exploitation and post exploitation steps were captured by system or network monitoring, which shows the potential for real-time monitoring
- **Strategic Use of OSINT-Proof Settings:** Some externally visible services had minimized data indicators and limited response information, reducing the efficiency of passive reconnaissance techniques.
- **Data Encryption for Sensitive Information:** Vital data was encrypted during transmission and while stored. Ensuring that delicate info remains safeguarded even in the event of a security breach.

Summary of Weaknesses

We successfully found several critical vulnerabilities that should be immediately addressed in order to prevent an adversary from compromising the network. These findings are not specific to a software version but are more general and systemic vulnerabilities.

- **Web App Security Flaws:** Encountered multiple injection flaws, including reflected XSS, stored XSS, LFI, and command injection were identified exposing Rekall to the threat of remote code execution and data breaches.
- **Deficient Input Control and Output Encoding Mechanisms:** The highly successful exploitation of cross-site scripting Local File Inclusion showcases the lack of secure coding practices and improper handling of user input.
- **Unauthorized Access to Confidential Information:** A variety of systems leaked sensitive data through disclosure vulnerabilities, certificate transparency logs, and unprotected service banners that supported reconnaissance and exploitation.
- **Vulnerable Authentication and User Credential Management:** obtained credentials were susceptible to hash and password cracking. This enabled credential stuffing and account compromise across services.
- **Insufficient Segregation of Network Zones and User Permissions:** Successful lateral movement, privilege escalation via scheduled tasks, and RCE across systems demonstrate gaps in segmentation and privilege boundaries.
- **Absence of Surveillance and Intrusion:** Detection Systems: Although some logging was displayed, most of the malicious activity including recon, vulnerability scanning, and post exploitation was not flagged during testing.
- **Outdated and Unsecured Services:** Exploitable legacy services (e.g., SLmail via POP3) helped advance remote code execution avenues and accentuates the need for the discontinuation of outdated services.

Executive Summary

Throughout the process of an extensive penetration test, I was able to analyze the Rekall Corp system for security vulnerabilities across web applications, infrastructure, and user access controls. My findings divulged several critical weaknesses that could allow a malicious individual to gain unauthorized access, escalate privileges, and extract sensitive data. Major outcomes included successful exploitation of remote code execution (RCE), command injection and local file inclusion (LFI), as well as reflected and stored cross-site scripting (XSS) vulnerabilities. These issues, coalesced with exposed sensitive information and unsecured configurations, illustrate a high risk to the confidentiality, integrity and availability of the system. This penetration test also exploited passive and active reconnaissance, open-source intelligence (OSINT), and post exploitation techniques such as credential stuffing and password cracking to simulate real-world attack scenarios.

Summary Vulnerability Overview

Vulnerability	Severity
RCE Web Application Exploit via Tomcat, POP3	Critical
Command Injection	Critical
Credential Dumping + Offline Password Cracking	Critical
Privilege Escalation via Scheduled Tasks	Critical
Credential Stuffing, Account Compromise	Critical
Local File Inclusion (LFI)	High
Sensitive Data Exposure / Information Disclosure	High
Network Reconnaissance + File Discovery + Exfiltration	High
Service Discovery and Vulnerable Service Exploitation (e.g., FTP FileZilla FTPd 0.9.41)	High
Reflected Cross-Site Scripting (XSS)	Medium
Web Application Fingerprinting	Medium
Vulnerability Scanning	Medium
Passive Reconnaissance (OSINT, Certificate Transparency, etc.)	Low
Post-Exploitation Enumeration	Low

The following summary tables represent an overview of the assessment findings for this penetration test:

Scan Type	Total
Hosts	18
Ports	12

Exploitation Risk	Total
Critical	6
High	6
Medium	5
Low	4

Vulnerability Findings

Vulnerability 1	Findings
Title	Reflected XSS Payload
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	**Medium**
Description	On the Welcome.php page entered a reflected XSS payload where it says “Put Your Name Here” field. Successful payload made a pop-up appear. success was verified upon closing the pop-up. This maliciou payload is often submerged in a URL.
	Screenshot (133).png, Screenshot (134).png, Screenshot (135).png
Affected Hosts	192.168.14.35/Welcome.php
Remediation	Precisely and reliably apply context aware output encoding on all unauthenticated data before displaying in the HTML. Can be enhanced with a robust Content Security Policy to provide defense-in-depth.

Vulnerability 2	Findings
Title	XSS Payload
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	**Medium**
Description	Although the input value made this exploit slightly more challenging than the above mentioned reflected XSS payload. The outcome was the same.
Images	Screenshot (139).png, group member verified the correct input was entered into the field but did not render the targeted data. The flag was awarded by the Instructor.
Affected Hosts	192.168.14.35/Welcome.php
Remediation	Focusing on prohibiting the browser from administering unreliable code will help prevent this type of exploit.

Vulnerability 3	Findings
Title	XSS Payload
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	**Medium**
Description	Executed a malicious script/code that was administered into the Rekall website. When a victim interacts with this malicious code the browser is interrupted (in this case a pop-up window) leading to a security breach.
Images	Screenshot (141).png, Screenshot (143).png, Screenshot (144).png
Affected Hosts	192.168.14.35/comments.php
Remediation	Focusing on prohibiting the browser from administering unreliable code will help prevent this type of exploit.

Vulnerability 4	Findings
Title	Local File Inclusion Exploit (LFI)
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	**High**
Description	This is a type for web app vulnerability which permits an attacker to incorporate and enact files that already exist on the server's local file system.
Images	Screenshot (148).png,
Affected Hosts	192.168.14.35/Memory-Planner.php
Remediation	By ensuring the authorizing of approved files and paths, secure input validation, utilizing secure file processing methods, limiting file system access, preventing directory browsing,ongoing security assessments and testing

Vulnerability 5	Findings
Title	Information Disclosure Vulnerability
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	High
Description	This exploit pertains to a more broad category of security flaws. Where an application unintentionally exposes sensitive data to unauthorized users.
Images	Screenshot (150).png, Screenshot (151).png,
Affected Hosts	192.168.14.35/login.php
Remediation	Requires a multifaceted approach with the emphasis on secure, strong coding practices, robust encryption, stringent access controls, and continuous security awareness and testing.

Vulnerability 6	Findings
Title	Sensitive Data Exposure / reconnaissance technique
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	High
Description	When an attacker obtains data about a targeted system to reveal where sensitive information might be unintentionally shown through misconfigurations, unreliable practices, or weaknesses.
Images	Screenshot (153).png,
Affected Hosts	192.168.14.35/robots.txt
Remediation	Minimize data footprint by storing only essential sensitive data. Using Secure configurations will harden servers, apps, and network devices. Vigorous access controls will implement strict login verification.

Vulnerability 7	Findings
Title	Command Injection
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	**Critical**
Description	Attackers exploit vulnerabilities to execute unrestricted operating system commands on a server, often by injecting malicious commands into application inputs.
Images	Screenshot (156).png, Screenshot (157).png
Affected Hosts	192.168.14.35/Network.php
Remediation	Accepting pre-approved input only will allow predefined and safe values. Thoroughly clean input to erase all potentially malicious characters (can be prone to errors). Implementation of Principle of Least Privilege by giving users only access to information they need to complete their specific tasks.

Vulnerability 8	Findings
Title	Passive Information Gathering / Reconnaissance
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	**Low**
Description	Gathering Data about an objective without directly engaging with its systems. Is dependant on public resources such as search engines, DNS records, and even social media
Images	Screenshot (176).png
Affected Hosts	https://osintframework.com/ and totalrekall.xyz
Remediation	Curtail public data to reduce the amount of sensitive or revealing information available online (see description).

Vulnerability 9	Findings
Title	reconnaissance technique
Type (Web app / Linux OS / WIndows OS)	Web App Linux OS
Risk Rating	**Low**
Description	Are methods used to collect data about a target system or organization to identify potential vulnerabilities or attack surfaces.
Images	Screenshot (177).png
Affected Hosts	76/223.105.230 totalrekall.xyz
Remediation	Intrusion detection to identify and block scanning probing efforts. Network segmentation will reduce the scope of info accessible from one point. Implement some kind of security awareness training to educate employees and other users on social engineering and data security.

Vulnerability 10	Findings
Title	Certificate Transparency using OSINT (Open Source Intelligence)
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	**Low**
Description	Leverages publicly available Certificate Transparency logs as OSINT technique to disclose information about a target.
Images	Screenshot (178).png
Affected Hosts	https://crt.sh and totalrekall.xyz
Remediation	Limit certificate issuance to only necessary domains/subdomains. Track issued CT's to identify potential unauthorized publication.

Vulnerability 11	Findings
Title	Network Reconnaissance
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	**Low**
Description	Method used to reveal information about a target network's framework, active hosts, services, and potential weaknesses by scanning and probing its backend.
Images	Screenshot (160).png
Affected Hosts	192.168.13.14
Remediation	Implementation of strong firewall rules to restrict inbound and outbound traffic. Disable unnecessary network protocols to limit potential attack vectors. Routinely audit network configurations will assist with identifying and closing data leaks.

Vulnerability 12	Findings
Title	Service Enumeration, Web Application Fingerprinting
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	When done separately the risk rating would be **Medium** but combined I would give this a rating of **High**.
Description	Service Enumeration is the finding of active services and their versions on a running targeted system. Web Application Fingerprinting is Identifying the precise tech, architecture, and versions used by a web app.
Images	Screenshot (162).png, Screenshot (161).png
Affected Hosts	192.168.13.10, www.drupal.org
Remediation	Reinforce service configurations by removing banners and unwarranted info. Restrict who can connect to services. Use non-standard ports but not as a primary use of security.

Vulnerability 13	Findings
Title	Vulnerability Scanning
Type (Web app / Linux OS / WIndows OS)	Linux OS Web App
Risk Rating	**Medium**
Description	A programmed process of identifying known security vulnerabilities in systems, networks, and apps by contrasting their properties against a database of deficiencies.
Images	Screenshot (163).png
Affected Hosts	192.168.13.12
Remediation	Regularly scan systems to identify vulnerabilities quickly. Prioritize findings to focus on critical and high-risk issues. Fix and resolve to apply vendor-sourced updates to manage unidentified weaknesses. Validate remediation efforts by rescaning to confirm vulnerabilities are resolved.

Vulnerability 14	Findings
Title	Remote Code Execution (RCE), Web Application Exploit, Payload Delivery, Post-exploitation (via Apache Tomcat/Coyote JSP engine 1.1)
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	**Critical**
Description	RCE is the ability for an attacker to execute arbitrary code on a remote system. Web Application Exploit is a method to take advantage of a vulnerability in a web application to achieve unauthorized actions
Images	Screenshot (166).png, Screenshot (172).png, Screenshot (173).png, Screenshot (174).png
Affected Hosts	192.168.13.10
Remediation	Patch immediately to update vulnerable software (Apache Tomcat/Coyote JSP engine). Input validation will sanitize all user-supplied data rigorously. Web Application Firewall (WAF) to implement a filter for malicious requests. Isolate compromised systems to help prevent further network spread. Use forensic analysts to understand the extent of the compromise.

Vulnerability 15	Findings
Title	Post Exploitation Enumeration
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	**Medium**
Description	Measures an attacker takes on a compromised system to gather further information about the internal network, users, files, and running processes to facilitate lateral movement, privilege escalation, and data exfiltration.
Images	Screenshot (185).png
Affected Hosts	192.168.13.10
Remediation	Implement robust authentication and authorization for accessing resources. Monitor internal system activity for malicious behavior via host-based intrusion detection systems(HIDS). Endpoint detection and response (EDR) to help identify and bring awareness to suspicious post-exploitation activity.

Vulnerability 16	Findings
Title	Credential Dumping + Offline Password Cracking
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	**High**
Description	Credential Dumping attack is when a username and password are repeatedly performed abroad on numerous websites or services to achieve unauthorized access to accounts. Offline Password Cracking is the procedure to recover plaintext passwords from hashes that have been retrieved without directly interacting with the authentication system. Specialized software on the attackers own system to crack these hashes
Images	Screenshot (186).png, Screenshot (195).png, Screenshot (196).png
Affected Hosts	github.com/totalrekall/site
Remediation	Implement strong access controls to limit who can access systems and memory. Enable Credential Guard (Windows) that Isolate and protect LSASS processes. Harden LSASS to prevent unauthorized process access. Disable programs that store plaintext credentials. Monitor for suspicious process access that detect tools used for credential dumping.

Vulnerability 17	Findings
Title	Vulnerability Scanning, Enumeration, Credential Harvesting
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	High
Description	A programmed process of identifying known security vulnerabilities in systems, networks, and apps by contrasting their properties against a database of deficiencies. Digging into services for useful information and being successful.
Images	Screenshot (202).png, Screenshot (203).png, Screenshot (210).png
Affected Hosts	172.22.117.20
Remediation	Routinely scan to swiftly identify weaknesses. Patch diligently to apply updates for identified vulnerbilities. Reduce exposed data by limiting visible services and details. Practice secure credential storage to safeguard databases and memory.

Vulnerability 18	Findings
Title	Network Reconnaissance followed by File Discovery and Information Exfiltration. Service Discovery + File Retrieval (via ftp FileZilla FTPd 0.9.41)
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Critical
Description	Discovered network framework, hosts, and services. Recognizing sensitive files on compromised systems. Prohibited transfer of data from compromised systems. Unauthorized copying of files from compromised systems. Identified running services on compromised hosts.
Images	Screenshot (206).png, Screenshot (208).png, Screenshot (209).png
Affected Hosts	172.22.117.20
Remediation	Closure of all unnecessary ports. Robust firewall rules to restrict traffic. Data loss prevention to oversee and prevent sensitive data from leaving . Block unauthorized outbound connections. Reduce data exposure. Encryption at rest will help protect information. Observe file access to detect prohibited file access.

Vulnerability 19	Findings
Title	Remote Code Execution (RCE) via POP3
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	**Critical**
Description	Ability for an attacker to perform malicious code on a remote system.
Images	Screenshot (187).png, Screenshot (188).png, Screenshot (189).png, Screenshot (190).png
Affected Hosts	172.22.117.20
Remediation	Keep software updated. Implement input validation. Use a Web application firewall (WAF) to filter malicious requests.

Vulnerability 20	Findings
Title	Post-Exploitation Enumeration, Privilege Escalation via Scheduled Tasks
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	**Critical**
Description	Compiled interior system information after the initial breach. Manipulated the faulty setup that made the scheduled tasks vulnerable to achieve escalated access.
Images	Screenshot (211).png, Screenshot (212).png, Screenshot (213).png
Affected Hosts	172.22.117.20
Remediation	Practice Principle of Least Privilege to limit user and service account permissions. Continuously monitor for suspicious activity.

Vulnerability 21	Findings
Title	Post-Exploitation Enumeration
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	**Critical** (this exploit by itself would have a rating of **low-medium**. Because **Remote Code Execution** was already achieved it elevated the risk to critical).
Description	Collected internal platform data after the initial compromise.
Images	Screenshot (191).png, Screenshot (192).png
Affected Hosts	172.22.117.20
Remediation	Network segmentation to restrict internal transparency. Endpoint detection and response to spot and react to suspicious events in real time.