



Cybersecurity

## Penetration Test Report

**Rekall Corporation**

## Penetration Test Report

**Student Note: Complete all sections highlighted in yellow.**

## 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

Confidentiality Statement	2
Contact Information	4
Document History	4
Introduction	5
Assessment Objective	5
Penetration Testing Methodology	6
Reconnaissance	6
Identification of Vulnerabilities and Services	6
Vulnerability Exploitation	6
Reporting	6
Scope	7
Executive Summary of Findings	8
Grading Methodology	8
Summary of Strengths	9
Summary of Weaknesses	9
Executive Summary Narrative	10
Summary Vulnerability Overview	13
Vulnerability Findings	14

## Contact Information

Company Name	CyberGuard
Contact Name	Evan Boroff
Contact Title	

## Document History

Version	Date	Author(s)	Comments
001	8/3/2023	Evan Boroff	

# 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.

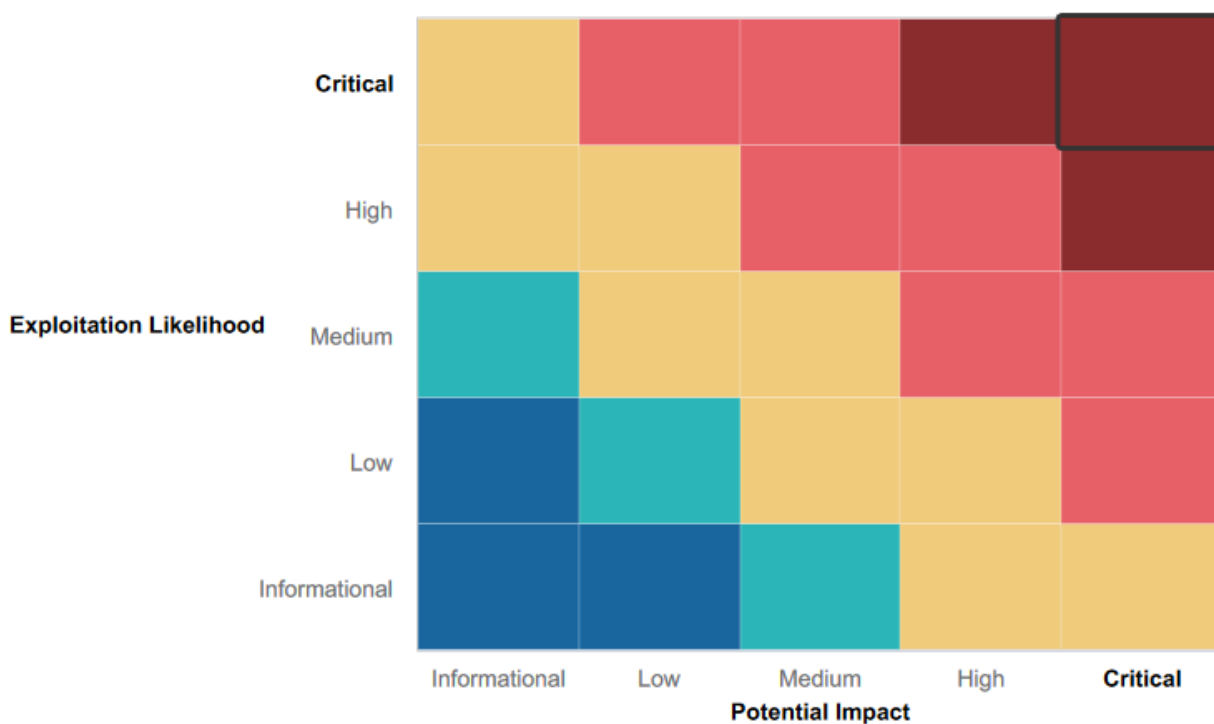
# Executive Summary of Findings

## 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.

- No vulnerable open source data
- Utilization of Metasploit and Nmap to limit access

## 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.

- XSS reflection
- XSS stored
- SQL injection
- Credentials in source code
- Publicly available server address

## Executive Summary

Multiple vulnerabilities were found by CyberGuard upon this penetration test. We were able to identify that Rekall was vulnerable to XSS reflected, SQL injection, and XSS stored attacks. We also found that the server address was stored in publicly available files and users' credentials are located in the source code.

## Summary Vulnerability Overview

[illegible]

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

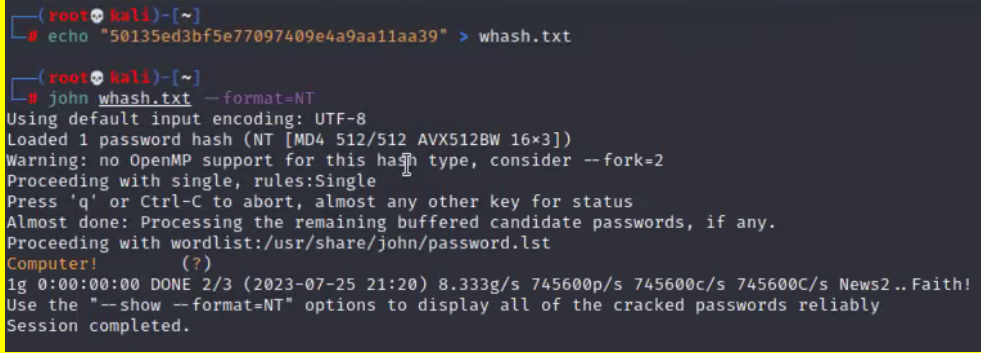
Scan Type	Total
Hosts	172.22.117.20
	172.22.117.10
	192.168.13.10
	192.168.13.11
	192.168.13.12
	192.168.13.13
	192.168.13.14
	192.168.14.35
Ports	21
	22
	80
	106
	110

Exploitation Risk	Total
Critical	2
High	1
Medium	2
Low	0

## Vulnerability Findings

Vulnerability 1	Findings
Title	XSS Reflected
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	Medium
Description	Malicious script successfully reflected on host home page
Images	
Affected Hosts	192.168.14.35
Remediation	Input Validation

Vulnerability 2	Findings
Title	SQL Injection
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	Critical
Description	Payload entered into the toolbar intended for password resulted in an exploit.
Images	
Affected Hosts	192.168.14.35
Remediation	Unable to allow web app to accept direct input and implement character escaping.

Vulnerability 3	Findings
Title	Exposed User Credentials
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	Critical
Description	Easy access to password file through hash dump within post/window/gather/hashdump. Used "john" to crack passwords and successfully gained access to user credentials.
Images	 <pre> (root@kali)~# echo "50135ed3bf5e77097409e4a9aa11aa39" &gt; whash.txt (root@kali)~# john whash.txt --format=NT Using default input encoding: UTF-8 Loaded 1 password hash (NT [MD4 512/512 AVX512BW 16x3]) Warning: no OpenMP support for this hash type, consider --fork=2 Proceeding with single, rules:Single Press 'q' or Ctrl-C to abort, almost any other key for status Almost done: Processing the remaining buffered candidate passwords, if any. Proceeding with wordlist:/usr/share/john/password.lst Computer! (?) 1g 0:00:00:00 DONE 2/3 (2023-07-25 21:20) 8.333g/s 745600p/s 745600c/s 745600C/s News2.. Faith! Use the "--show --format=NT" options to display all of the cracked passwords reliably Session completed. </pre>
Affected Hosts	172.22.117.20
Remediation	Limit access to vulnerable files by restricting permissions and user permissions.

Vulnerability 4	Findings
Title	XSS Stored
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	Medium
Description	<script>alert("Hi")</script> entered on /Commands page
Images	
Affected Hosts	192.168.14.35
Remediation	Implement XSS protection

Vulnerability 5	Findings
Title	Server Address Stored Publicly

Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	High
Description	Unrestricted access
Images	
Affected Hosts	192.168.14.35
Remediation	Restrict access to authorized users

Vulnerability 6	Findings
Title	
Type (Web app / Linux OS / Windows OS)	
Risk Rating	
Description	
Images	
Affected Hosts	
Remediation	

Vulnerability 7	Findings
Title	
Type (Web app / Linux OS / Windows OS)	
Risk Rating	
Description	
Images	
Affected Hosts	
Remediation	

Add any additional vulnerabilities below.