| 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](#_30j0zll)

[Contact Information 4](#_1fob9te)

[Document History 4](#_3znysh7)

[Introduction 5](#_2et92p0)

[Assessment Objective 5](#_3dy6vkm)

[Penetration Testing Methodology 6](#_2s8eyo1)

[Reconnaissance 6](#_17dp8vu)

[Identification of Vulnerabilities and Services 6](#_3rdcrjn)

[Vulnerability Exploitation 6](#_26in1rg)

[Reporting 6](#_lnxbz9)

[Scope 7](#_35nkun2)

[Executive Summary of Findings 8](#_44sinio)

[Grading Methodology 8](#_z337ya)

[Summary of Strengths 9](#_3j2qqm3)

[Summary of Weaknesses 9](#_1y810tw)

[Executive Summary Narrative](#_4i7ojhp) 10

[Summary Vulnerability Overview 1](#_2xcytpi)3

Vulnerability Findings [1](#_1ci93xb)4

# 

## Contact Information

| **Company Name** | Beaver Dam Securities 555-555-Beaver1 |
| --- | --- |
| **Contact Name** | David Crane |
| **Contact Title** | Penetration Tester |

## 

## Document History

| **Version** | **Date** | **Author(s)** | **Comments** |
| --- | --- | --- | --- |
| 001 | 12/12/22 | David Crane |  |

# 

## 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:

Chart

Description automatically generated with medium confidence

### 

### 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.

* Multiple fields of input do not accept any sort of command injection.
* The vast majority of fields of input utilize input validation.

### 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.

* Multiple open ports.
* TotalRekall’s website has vulnerabilities including being prone to command injection, cross site scripting, and having poor input protection.

## Executive Summary

After running multiple tests, Beaver Dam Securities was able to determine that Total Rekall has numerous vulnerabilities which require immediate correcting. These vulnerabilities include Command Injection, Cross Site Scripting, Local File Inclusion, and Open Ports. It’s also worth mentioning Total Rekall’s GitHub (https://github.com/totalrekall) contains a vulnerability allowing unauthorized access to sensitive information.   
  
Below, you will find more information on the discovered vulnerabilities, and what Beaver Dam Securities recommends in order to fix these major issues. Should there be any questions or concerns, please reach out to us with the provided contact information above.

## 

## 

## 

## 

## Summary Vulnerability Overview

| **Vulnerability** | **Severity** |
| --- | --- |
| Command Injection | **Critical** |
| Cross Site Scripting | **Critical** |
| Local File Inclusion | **High** |
| GitHub xampp.users contains sensitive hash | **High** |
| Open Ports (80, 21, 110) | **High** |
| SLMail has open port | **High** |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

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

| **Scan Type** | **Total** |
| --- | --- |
| Hosts | 34.102.136.180 - TotalRekall.xyz  192.168.13.0/24 192.168.13.12  172.22.117.0/24 172.22.117.20 |
| Ports | 21 - FTP 80 - HTTP 110 - POP3 |

| **Exploitation Risk** | **Total** |
| --- | --- |
| **Critical** | 2 |
| **High** | 4 |
| **Medium** | 0 |
| **Low** | 0 |

## Vulnerability Findings

| **Vulnerability 1** | **Findings** |
| --- | --- |
| **Title** | Command Injection |
| **Type (Web app / Linux OS / WIndows OS)** | Web App |
| **Risk Rating** | Critical |
| **Description** | Visit ‘who.is’ and entered Totalrekall.xyz |
| **Affected Hosts** | 34.102.136.180 |
| **Remediation** | Set up input validation and create a “white list” of possible inputs. By doing this, the system should only accept the pre-determined inputs. |

| **Vulnerability 2** | **Findings** |
| --- | --- |
| **Title** | Cross Site Scripting |
| **Type (Web app / Linux OS / WIndows OS)** | Web App |
| **Risk Rating** | Critical |
| **Description** | The ‘Comment’ and ‘Welcome’ page allowed script inputs. |
| **Affected Hosts** | 34.102.136.180 |
| **Remediation** | To better sanitize user input to validate/catch user provided data. We also recommend encoding the output to prevent any malicious user provided data from triggering any executables. |

| **Vulnerability 3** | **Findings** |
| --- | --- |
| **Title** | Local File Inclusion |
| **Type (Web app / Linux OS / WIndows OS)** | Web App |
| **Risk Rating** | High |
| **Description** | The Memory Planner webpage allows for malicious file uploads. |
| **Affected Hosts** | 34.102.136.180 |
| **Remediation** | Only allow certain types of files to be uploaded, and sanitize/check all files that are uploaded. |

| **Vulnerability 4** | **Findings** |
| --- | --- |
| **Title** | GitHub ‘xampp.users’ contains PII |
| **Type (Web app / Linux OS / WIndows OS)** | Web App |
| **Risk Rating** | High |
| **Description** | Total Rekall’s GitHub page (<https://github.com/totalrekall>) contains sensitive hash - trivera:$apr1$A0vSKwao$GV3sgGAj53j.c3GkS4oUC0 |
| **Affected Hosts** | Windows OS |
| **Remediation** | Salt Hashes, or remove them all together from the GitHub page. |

| **Vulnerability 5** | **Findings** |
| --- | --- |
| **Title** | SLMail Open Port |
| **Type (Web app / Linux OS / WIndows OS)** | Windows OS |
| **Risk Rating** | High |
| **Description** | Using MSFConsole through Kali Linux, and running exploit/windows/pop3/seattlelab\_pass, we were able to gain access through SLMail port 110 allowing for read/write permissions on sensitive files. |
| **Affected Hosts** | 172.22.117.20 |
| **Remediation** | Close port 110, or discontinue the use of SLMail all together. |