| 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** | CyberWarrior Security |
| --- | --- |
| **Contact Name** | Mohammed Odeh |
| **Contact Title** | Penetration Tester |

## 

## Document History

| **Version** | **Date** | **Author(s)** | **Comments** |
| --- | --- | --- | --- |
| 001 | 1/7/2024 | Mohammed Odeh |  |

# 

## 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.

* High-level summary of strengths here
* SQL Injection unsuccessful against web page
* Input scripts were unsuccessful on some web pages
* Web Application was well organized

### 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.

* High-level summary of weaknesses here
* Vulnerabilities exposed using Osint tools
* Vulnerable to malicious scripting
* Vulnerabilities were found in both Windows and Linux systems, like Shellshock, SLMail pop3d, and Apache Tomcat Remote Code Execution.
* Cracked passwords using kiwi
* Website vulnerable to different attacks
* Sensitive data is easily accessible when in system
* Multiple open ports

## Executive Summary

## 

Hello, I'm a penetration tester from CyberWarrior Security, here's some details about our most recent Rekall cybersecurity evaluation. Our approach was similar to a scientific investigation of their computer systems, exploring areas of strength, identifying vulnerabilities, and creating tactical improvements for their virtual defenses. Rekall's cybersecurity defense showed impressive qualities, highlighted by its ability to avoid SQL injection attempts, keep its web application structure organized , and show protection against certain types of attacks. These advantages highlight Rekall's dedication to important security procedures and its awareness of possible dangers. We also found vulnerabilities in Rekall's systems during the assessment. These vulnerabilities could be used by malicious actors; they are similar to small gaps in a walled building. There were some windows that were left open and needed to be closed quickly, which highlights how important it is to make changes right away in order to block any entrance points. In order to maintain the organization's security trustworthiness and provide a strong defense against cyber threats, it is essential to address these vulnerabilities. Finding these vulnerabilities is the first strategic step in protecting Rekall's digital environment. During the investigation, important vulnerabilities were found, mostly in Windows and Linux systems. SLMail Exploit through Meterpreter, Access through FTP, and Open Source Data Exposure were three major vulnerabilities that were direct risks to Rekall security. Furthermore, vulnerabilities to Command Injection, Local File Inclusion, and Cross-Site Scripting (XSS) showed the urgent need for repair. For it to strengthen Rekall's security in general and reduce potential threats, these vulnerabilities must be addressed. To improve Rekall's cybersecurity, it is recommended to apply serious input validation as well as security controls to counter Cross-Site Scripting (XSS) vulnerabilities. To reduce the dangers of Local File Inclusion, secure file upload rules must be created. By using customized queries and input validation, vulnerabilities related to command injection can be reduced. Improve access controls in open-source sources to solve Open Source Data Exposure. By limiting FTP access, turning down unused services, and quickly patching vulnerabilities, the risks of service exploitation can be reduced. Important precautions include making sure sensitive data is encrypted, setting up firewalls to restrict external scanning, and keeping SSL certificates updated. Rekall has to have a strong cybersecurity policy which involves protecting DNS records and reviewing firewall rules on a regular basis. In conclusion, Rekall's defenses will be considerably strengthened by implementing the suggested cybersecurity measures. security will be established by addressing vulnerabilities in network protocols, data management, and online applications. This approach guarantees strong defense and consistent security against new cyberthreats. By prioritizing this, Rekall creates the conditions for a safe and reliable security for customers and employees.

Thank you for choosing CyberWarrior Security!

## 

## 

## Summary Vulnerability Overview

| **Vulnerability** | **Severity** |
| --- | --- |
| Cross-Site Scripting XSS Reflected | **Medium** |
| Cross-Site Scripting XSS Reflected Memory Planner | **Medium** |
| Cross-Site Scripting XSS Stored | **Medium** |
| Local File Inclusion | **High** |
| Command Injection | **Critical** |
| Sensitive Data Exposure | **High** |
| Open Source Data Exposure | **Low** |
| Sensitive Data Exposure (searching robots txt in browser) | **High** |
| DNS Info exposed | **Low** |
| SSL Certificate Research | **Low** |
| NMAP Scan 192.168.13.0/24 | **High** |
| Nessus Scanning | **Critical** |
| Remote Code Execution | **Critical** |
| RCE/ShellShock Exploit | **Critical** |
| Sensitive Data Exposure | **Critical** |
| Nmap Scanning 172.22.117.20/24 | **High** |
| Access Through FTP | **High** |
| SLMail Exploit Through Meterpreter | **High** |
| Performed Task Schedule | **Medium** |
| Performed Kiwi | **High** |
| Applying “Type” Command In Meterpreter in C:\Users\Public\Documents Folder | **Critical** |

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

| **Scan Type** | **Total** |
| --- | --- |
| Hosts | 9 |
| Ports | 4 |

| **Exploitation Risk** | **Total** |
| --- | --- |
| **Critical** | 6 |
| **High** | 8 |
| **Medium** | 4 |
| **Low** | 3 |

## Vulnerability Findings

**DAY 1**

| **Vulnerability 1** | **Findings** |
| --- | --- |
| **Title** | Cross-Site Scripting XSS Reflected |
| **Type (Web app / Linux OS / WIndows OS)** | Web app |
| **Risk Rating** | Medium |
| **Description** | The welcome name of totalrekall.xyz included a malicious script on it that read as follows: <script>alert flag1 Is here ) </script> |
| **Images** |  |
| **Affected Hosts** | 192.168.14.35/Welcome.php |
| **Remediation** | Input validation |

| **Vulnerability 2** | **Findings** |
| --- | --- |
| **Title** | Cross-Site Scripting XSS Reflected Memory Planner |
| **Type (Web app / Linux OS / WIndows OS)** | Web App |
| **Risk Rating** | Medium |
| **Description** | Typed “SCcriptRIPT” which divided payload and successfully accessed flag 4 |
| **Images** |  |
| **Affected Hosts** | 192.168.14.35/Memory-Planner.php |
| **Remediation** | Input Validation |

| **Vulnerability 3** | **Findings** |
| --- | --- |
| **Title** | Cross-Site Scripting XSS Stored |
| **Type (Web app / Linux OS / WIndows OS)** | Web App |
| **Risk Rating** | Medium |
| **Description** | Located Comments field and input “<script>alert(flag1)” |
| **Images** |  |
| **Affected Hosts** | 192.168.14.35/comments.php |
| **Remediation** | Input validation |

| **Vulnerability 4** | **Findings** |
| --- | --- |
| **Title** | Local File Inclusion |
| **Type (Web app / Linux OS / WIndows OS)** | Web App |
| **Risk Rating** | High |
| **Description** | Uploading Malicious PHP File to server |
| **Images** |  |
| **Affected Hosts** | 192.168.14.35/Memory-Planner.php |
| **Remediation** | Don’t allow users to upload files into local file system |

| **Vulnerability 5** | **Findings** |
| --- | --- |
| **Title** | Sensitive Data Exposure |
| **Type (Web app / Linux OS / WIndows OS)** | Web App |
| **Risk Rating** | High |
| **Description** | Highlighted webpage and found login credentials which were hidden but in the html |
| **Images** |  |
| **Affected Hosts** | 192.168.14.35/login.php & /networking.php |
| **Remediation** | Remove it! |

| **Vulnerability 6** | **Findings** |
| --- | --- |
| **Title** | Sensitive Data Exposure (Searching robots txt in browser) |
| **Type (Web app / Linux OS / WIndows OS)** | Web App |
| **Risk Rating** | High |
| **Description** | Unrestricted access to robots.txt page |
| **Images** |  |
| **Affected Hosts** | 192.168.14.35/robots.txt |
| **Remediation** | Limit access ! |

| **Vulnerability 7** | **Findings** |
| --- | --- |
| **Title** | Command Injection |
| **Type (Web app / Linux OS / WIndows OS)** | Web App |
| **Risk Rating** | Critical |
| **Description** | In MX record checker field payload command was uploaded at [www.welcometorecall.com](http://www.welcometorecall.com) | cat vendors.txt |
| **Images** |  |
| **Affected Hosts** | 192.168.14.35/networking.php |
| **Remediation** | Input Validation |

**Day 2**

| **Vulnerability 8** | **Findings** |
| --- | --- |
| **Title** | Open Source Data Exposure |
| **Type (Web app / Linux OS / WIndows OS)** | Linux |
| **Risk Rating** | Low |
| **Description** | Using WHOIS for totalrekall.xyz on domain dossier sensitive data was exposed |
| **Images** |  |
| **Affected Hosts** |  |
| **Remediation** | No sensitive data published |

| **Vulnerability 9** | **Findings** |
| --- | --- |
| **Title** | DNS Records published |
| **Type (Web app / Linux OS / WIndows OS)** | Linux |
| **Risk Rating** | Low |
| **Description** | DNS info and other information published |
| **Images** |  |
| **Affected Hosts** | 192.168.14.35 |
| **Remediation** | No possible sensitive data published |

| **Vulnerability 10** | **Findings** |
| --- | --- |
| **Title** | SSL Certificate Research |
| **Type (Web app / Linux OS / WIndows OS)** | Linux |
| **Risk Rating** | Low |
| **Description** | SSL certificate information located after research |
| **Images** |  |
| **Affected Hosts** | <https://crt.sh/?q=totalrekall.xyz> |
| **Remediation** | Do not publish any possible “Sensitive” information!!!! |

| **Vulnerability 11** | **Findings** |
| --- | --- |
| **Title** | Nessus Scanning |
| **Type (Web app / Linux OS / WIndows OS)** | Linux |
| **Risk Rating** | Critical |
| **Description** | We ran a scan to figure out how many hosts and the IPs |
| **Images** |  |
| **Affected Hosts** | All 5 hosts |
| **Remediation** | block ports |

| **Vulnerability 12** | **Findings** |
| --- | --- |
| **Title** | Locating server running “Drupal” |
| **Type (Web app / Linux OS / WIndows OS)** | Linux |
| **Risk Rating** | Medium |
| **Description** | Here we found 192.168.13.13 running on drupal |
| **Images** |  |
| **Affected Hosts** | 192.168.13.13 |
| **Remediation** | . |

| **Vulnerability 13** | **Findings** |
| --- | --- |
| **Title** | Scanning vulnerabilities through Nessus |
| **Type (Web app / Linux OS / WIndows OS)** | Linux |
| **Risk Rating** | Critical |
| **Description** | Nussus scanning against host 192.160.13.12 reveals an Apache Struts 2.3.5 - 2.3.31 vulnerability that permits for remote code execution. |
| **Images** |  |
| **Affected Hosts** | 192.168.13.12 |
| **Remediation** | Patch,update, and test |

| **Vulnerability 14** | **Findings** |
| --- | --- |
| **Title** | Remote Code Execution Vulnerability |
| **Type (Web app / Linux OS / WIndows OS)** | Linux |
| **Risk Rating** | Critical |
| **Description** | On host 192.168.13.10 I performed a Metasploit exploit to gain access to RCE and accessed a reverse shell |
| **Images** |  |
| **Affected Hosts** | 192.168.13.10 |
| **Remediation** | Update Tomcat |

**Day 3**

| **Vulnerability 15** | **Findings** |
| --- | --- |
| **Title** | Username found on GitHub and hashed |
| **Type (Web app / Linux OS / WIndows OS)** | Windows |
| **Risk Rating** | Critical |
| **Description** | The location of the user's credentials and any other relevant data were found using a specific search operator. John helped us decipher the user's password from a text file and provide the password. |
| **Images** |  |
| **Affected Hosts** | https://GitHub.com/totalrekall/site |
| **Remediation** | Remove sensitive information off website |

| **Vulnerability 16** | **Findings** |
| --- | --- |
| **Title** | Nmap Scanning 172.22.117.20/24 |
| **Type (Web app / Linux OS / WIndows OS)** | Windows |
| **Risk Rating** | High |
| **Description** | The host 172.22.117.20/24 was mapped and it was discovered that 172.22.117.20 has an open http port 80. When the browser asked for a login after we typed in the IP address, we used flag1's username and password. |
| **Images** |  |
| **Affected Hosts** | 172.22.117.20 |
| **Remediation** | 2 factor authentication |

| **Vulnerability 17** | **Findings** |
| --- | --- |
| **Title** | Access Through FTP |
| **Type (Web app / Linux OS / WIndows OS)** | Windows |
| **Risk Rating** | High |
| **Description** | On the host 172.22.117.20, an aggressive map scan revealed that the port 21 ftp server was open. We were able to locate the file and gain access after having success. |
| **Images** |  |
| **Affected Hosts** | 172.22.117.20 |
| **Remediation** | Close or limit access of open ports (port 21) |

| **Vulnerability 18** | **Findings** |
| --- | --- |
| **Title** | SLMail Exploit through Meterpreter |
| **Type (Web app / Linux OS / WIndows OS)** | Windows |
| **Risk Rating** | High |
| **Description** | Because port 110 was open, the attack could be effectively exploited within Metasploit. This allowed access to the meterpreter session and revealed the file's location. |
| **Images** |  |
| **Affected Hosts** | 172.22.117.20 |
| **Remediation** | Stop SLMail service and closer port 110 |

| **Vulnerability 19** | **Findings** |
| --- | --- |
| **Title** | Performed Kiwi and hashed |
| **Type (Web app / Linux OS / WIndows OS)** | Windows |
| **Risk Rating** | High |
| **Description** | In the meterpreter session, we accessed the password hashes in a file using Kiwi and copied them to a text file. John was our tool, and he was effective in cracking the password hashes, producing a reverse shell. |
| **Images** |  |
| **Affected Hosts** | 172.22.117.20 |
| **Remediation** | Restrict access to specific files by modifying the permissions and user privileges |

| **Vulnerability 20** | **Findings** |
| --- | --- |
| **Title** | Applying “Type” Command in meterpreter |
| **Type (Web app / Linux OS / WIndows OS)** | Windows |
| **Risk Rating** | Critical |
| **Description** | We used the type command to read the file after locating its location in the meterpreter session. |
| **Images** |  |
| **Affected Hosts** | 172.22.117.20 |
| **Remediation** | Using techniques that work, improving access limits, and applying security patches to fix vulnerabilities found during the Meterpreter session |