| 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

[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** | The Almighty Browns |
| --- | --- |
| **Contact Name** | Pellegrino Adu Gyamfi |
| **Contact Title** | Penetration Tester |

## 

## Document History

| **Version** | **Date** | **Author(s)** | **Comments** |
| --- | --- | --- | --- |
| 001 | 4/23/2025 | Pellegrino A. |  |

# 

## 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.

* Some input fields in the web applications resisted basic XSS attacks, requiring more sophisticated probing to bypass protections.
* Basic security measures were present in certain areas, making it more difficult for The Almighty Browns to successfully carry out exploits like Local File Inclusion and, in some cases, XSS attacks.

### 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.

* The web application is vulnerable to Cross-Site Scripting (XSS), Local File Inclusion (LFI), and Command Injection attacks.
* Hardcoded usernames and passwords were found in web page HTML and public files like robots.txt
* GitHub repositories containing hashed (but crackable) passwords were publicly accessible
* Internal files and credentials were easily retrievable through both web and network exploitation.
* Open ports were discovered across multiple hosts without proper protection, exposing services to unauthorized access.
* FTP services were running openly, which can be exploited if not properly secured.
* Machines like SLMail servers were left vulnerable to known exploits.
* We were able to exploited unpatched servers using Metasploit to gain unauthorized shell access, compromising critical Linux hosts.
* Lack of system patching increased vulnerability to known exploits.
* Public WHOIS and SSL certificate data revealed information that could assist attackers during reconnaissance phases.

## Executive Summary

The Almighty Browns LLC conducted an extensive internal and external penetration test of Rekall Corporation’s networks, systems, and web applications. The goal was to identify exploitable vulnerabilities, assess the impact of these flaws, and provide actionable recommendations to bolster Rekall’s cybersecurity posture.

The Almighty Browns LLC began the penetration test with a thorough reconnaissance phase, during which we gathered detailed information about the target systems. This initial step involved identifying and learning about the network, operating systems (O/S), applications, and available user accounts within the environment. By leveraging open-source intelligence (OSINT) techniques, active network scanning, and enumeration tools, we successfully mapped the structure of the network and uncovered valuable details about exposed services and potential points of entry.

Following the reconnaissance phase, The Almighty Browns LLC transitioned into the scanning stage. During this phase, we utilized tools such as Nmap to conduct comprehensive scans for open ports and to monitor network traffic across the environment. The goal was to identify active services, exposed ports, and potential vulnerabilities that could be leveraged in later stages. Based on the information gathered, we cross-referenced the identified services with current CVE (Common Vulnerabilities and Exposures) databases to determine known vulnerabilities associated with the discovered systems. Subsequently, we tested and exploited these vulnerabilities to assess the true extent of the risks, successfully validating many critical security weaknesses.

The final report highlights all identified vulnerabilities and provides a detailed mapping of the findings. Each vulnerability was graded based on its severity using a standardized risk scale—Critical, High, Medium, and Low. This grading reflects both the potential business impact and the likelihood of exploitation. It is our strong recommendation that Rekall Corporation prioritize the remediation of Critical vulnerabilities as a first step, given that these issues pose the highest risk of network compromise if discovered and exploited by threat actors. Addressing these critical vulnerabilities promptly will significantly reduce Rekall’s exposure to potential cyberattacks and safeguard its critical assets.

During our assessment, we employed a wide range of industry-standard tools to identify and exploit vulnerabilities within the Rekall environment. Tools such as Metasploit, Nessus, Burp Suite, and Nmap were extensively utilized to perform network scanning, vulnerability assessments, web application testing, and exploitation activities. The combination of automated scanning and manual verification enabled us to uncover critical weaknesses that might otherwise have gone undetected, ensuring a comprehensive evaluation of Rekall's security posture.

The Rekall environment is currently exposed to a combination of critical technical vulnerabilities, insecure design practices, and publicly available information leaks. Immediate and strategic remediation is required.

## 

## 

## 

## 

## Summary Vulnerability Overview

| **Vulnerability** | **Severity** |
| --- | --- |
| Reflected XSS Payload | **Medium** |
| XSS vulnerability in comments | **Medium** |
| Local File Inclusion (LFI) exploit | **Critical** |
| Sensitive data exposure | **Critical** |
| Sensitive data exposure | **Medium** |
| Command Injection vulnerability | **Critical** |
| Command Injection | **Critical** |
| WHOIS domain for website totalrekall.xyz | **Low** |
| WHOIS lookup for the IP address | **Low** |
| Exposed open source data | **Low** |
| Weak network security (Zenmap scan on Network) | **Medium** |
| Weak network security(Nmap scan against discovered hosts) | **High** |
| Weak network security (Nessus scan against the host that ends with 12) | **Critical** |
| RCE exploit through Metasploit & Server search | **Critical** |
| Exploit Vulnerability | **High** |
| Exploit Vulnerability | **High** |
| GitHub repositories belonging to Totalrekall | **Low** |
| Weak network security (Nmap scan on 172.22.117.20) | **Medium** |
| FTP Enumeration | **Medium** |
| Machine that is running the SLMail service | **Medium** |

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

| **Scan Type** | **Total** |
| --- | --- |
| Hosts | 192.16.13.10, 192.16.13.11, 192.16.13.12, 192.16.13.13, 192.16.13.14, 192.16.13.15 |
| Ports | 21 22 80 110 |

| **Exploitation Risk** | **Total** |
| --- | --- |
| **Critical** | 6 |
| **High** | 3 |
| **Medium** | 7 |
| **Low** | 4 |

## Web Application

| **Vulnerability 1** | **Findings** |
| --- | --- |
| **Title** | Reflected XSS Payload |
| **Type (Web app / Linux OS / WIndows OS)** | Web app |
| **Risk Rating** | Medium |
| **Description** | In the Welcome.php we entered <script>alert(“hello”)</script> in the field where is says “Put your name here” |
| **Images** |  |
| **Affected Hosts** | welcome.php |
| **Remediation** | Input Validation to make sure that the data processed by the application is in the correct form |

| **Vulnerability 2** | **Findings** |
| --- | --- |
| **Title** | XSS vulnerability in comments |
| **Type (Web app / Linux OS / WIndows OS)** | Web app |
| **Risk Rating** | Medium |
| **Description** | We entered a malicious script in the comment section: <script>alert(“Buckeyes”)</script> |
| **Images** |  |
| **Affected Hosts** | comments.php |
| **Remediation** | Input Validation to make sure that the data processed by the application is in the correct form |

| **Vulnerability 3** | **Findings** |
| --- | --- |
| **Title** | Local File Inclusion (LFI) exploit |
| **Type (Web app / Linux OS / WIndows OS)** | Web app |
| **Risk Rating** | Critical |
| **Description** | We used a file from the terminal with the “.php” extension and uploaded it by clicking the “Browse” button in the web page |
| **Images** |  |
| **Affected Hosts** | Memory-Planner.php |
| **Remediation** | Secure a file path where employees can on view their ID |

| **Vulnerability 4** | **Findings** |
| --- | --- |
| **Title** | Sensitive data exposure |
| **Type (Web app / Linux OS / WIndows OS)** | Web app |
| **Risk Rating** | Critical |
| **Description** | We found the username and password in the HTML |
| **Images** |  |
| **Affected Hosts** | login.php |
| **Remediation** | Never put sensitive info into a web page HTML |

| **Vulnerability 5** | **Findings** |
| --- | --- |
| **Title** | Sensitive data exposure |
| **Type (Web app / Linux OS / WIndows OS)** | Web app |
| **Risk Rating** | Medium |
| **Description** | We found the file “robots.txt”. This file has no restriction to web access |
| **Images** |  |
| **Affected Hosts** | robots.txt page |
| **Remediation** | Make sure you put high privileges on private files |

| **Vulnerability 6** | **Findings** |
| --- | --- |
| **Title** | Command Injection vulnerability |
| **Type (Web app / Linux OS / WIndows OS)** | Web app |
| **Risk Rating** | Critical |
| **Description** | After entering the admins username and password we entered the “network tools” page. We entered “[www.](http://www.google.com)splunk.com” as the payload in the DNS Check white box and we were able to get sensitive data |
| **Images** |  |
| **Affected Hosts** | Networking.php |
| **Remediation** | Input Validation to make sure that the data processed by the application is in the correct form |

| **Vulnerability 7** | **Findings** |
| --- | --- |
| **Title** | Command Injection |
| **Type (Web app / Linux OS / WIndows OS)** | Web app |
| **Risk Rating** | Critical |
| **Description** | We entered payloads in the two fields |
| **Images** |  |
| **Affected Hosts** | networking.php |
| **Remediation** | Input Validation to make sure that the data processed by the application is in the correct form |

## 

## 

## 

## 

## 

## 

## 

## 

## 

## 

## 

## 

## 

## Linux Server

| **Vulnerability 8** | **Findings** |
| --- | --- |
| **Title** | WHOIS domain for website totalrekall.xyz |
| **Type (Web app / Linux OS / WIndows OS)** | Web app / Linux OS |
| **Risk Rating** | Low |
| **Description** | We used a Domain Dossier open source tool to find information about the WHOIS domain. |
| **Images** |  |
| **Affected Hosts** | https://centralops.net/co/DamainDossier.aspx |
| **Remediation** | Stronger domain encryptions so that sensitive information isn’t revealed |

| **Vulnerability 9** | **Findings** |
| --- | --- |
| **Title** | WHOIS lookup for the IP address |
| **Type (Web app / Linux OS / WIndows OS)** | Web app / Linux OS |
| **Risk Rating** | Low |
| **Description** | IP address was found through OSINT Framework - Whosis Records - View DNS.info. Then we typed “Totalrekall.yxz” in the IP History lookeup and the following page exposed the IP. |
| **Images** |  |
| **Affected Hosts** | 34.102.136.180 |
| **Remediation** | Hide your IP address |

| **Vulnerability 10** | **Findings** |
| --- | --- |
| **Title** | Exposed open source data |
| **Type (Web app / Linux OS / WIndows OS)** | Web app / Linux OS |
| **Risk Rating** | Low |
| **Description** | We used crt.sh to look up the SSL certificates for totalrekall.xyz |
| **Images** |  |
| **Affected Hosts** | totalrekall.xyz |
| **Remediation** | Make sure that there is no sensitive date found in the WHOIS records |

| **Vulnerability 11** | **Findings** |
| --- | --- |
| **Title** | Zenmap scan on Network |
| **Type (Web app / Linux OS / WIndows OS)** | Linux OS |
| **Risk Rating** | Medium |
| **Description** | We used zenmap to Intense scan to 192.168.13.0/24 and found 6 hosts that responded |
| **Images** |  |
| **Affected Hosts** | 192.16.13.10, 192.16.13.11, 192.16.13.12, 192.16.13.13, 192.16.13.14, 192.16.13.15 |
| **Remediation** | Block the ports |

| **Vulnerability 12** | **Findings** |
| --- | --- |
| **Title** | Nmap scan against discovered hosts |
| **Type (Web app / Linux OS / WIndows OS)** | Linux OS |
| **Risk Rating** | High |
| **Description** | We ran an nmap scan against 192.168.13.0/24 |
| **Images** |  |
| **Affected Hosts** | 192.168.13.0/24 |
| **Remediation** | Block port scans |

| **Vulnerability 13** | **Findings** |
| --- | --- |
| **Title** | Nessus scan against the host that ends with 12 |
| **Type (Web app / Linux OS / WIndows OS)** | Web app / Linux OS |
| **Risk Rating** | Critical |
| **Description** | We ran a Nessus scan on the 192.168.13.12 host |
| **Images** |  |
| **Affected Hosts** | 192.168.13.12 |
| **Remediation** | To reduce errors and vulnerabilities make sure to have the latest patch updated |

| **Vulnerability 14** | **Findings** |
| --- | --- |
| **Title** | RCE exploit through Metasploit & Server search |
| **Type (Web app / Linux OS / WIndows OS)** | Linux OS |
| **Risk Rating** | Critical |
| **Description** | We used Msfconsole through Metasploit to exploit the RCE. Searched for Tomcat We found the exploit then entered 192.168.13.10 and opened a shell |
| **Images** |  |
| **Affected Hosts** | 192.168.13.10 |
| **Remediation** | To reduce errors and vulnerabilities make sure have the latest patch is updated |

| **Vulnerability 15** | **Findings** |
| --- | --- |
| **Title** | Exploit Vulnerability |
| **Type (Web app / Linux OS / WIndows OS)** | Linux OS |
| **Risk Rating** | High |
| **Description** | Used the RCE exploit through the Metasploit and exploited the host 192.168.13.11. Finally we cat /etc/sudoers the file in rhosts 192.168.13.11 |
| **Images** |  |
| **Affected Hosts** | 192.168.13.11 |
| **Remediation** | To reduce errors and vulnerabilities make sure have the latest patch is updated |

| **Vulnerability 16** | **Findings** |
| --- | --- |
| **Title** | Exploit Vulnerability |
| **Type (Web app / Linux OS / WIndows OS)** | Linux OS |
| **Risk Rating** | High |
| **Description** | Through the meterpreter shell we opened /etc/passwd |
| **Images** |  |
| **Affected Hosts** | 192.168.13.11 |
| **Remediation** | To reduce errors and vulnerabilities make sure have the latest patch is updated |

## Windows Server

| **Vulnerability 17** | **Findings** |
| --- | --- |
| **Title** | GitHub repositories belonging to Totalrekall |
| **Type (Web app / Linux OS / WIndows OS)** | Windows |
| **Risk Rating** | Low |
| **Description** | We used OSINT and searched repositories in GitHub that belong to Totalrekall. There are users with hashed passwords. We cracked the passwords with john in the terminal. |
| **Images** |  |
| **Affected Hosts** | 192.168.13.10 |
| **Remediation** | Take the private data out of the public webpage |

| **Vulnerability 18** | **Findings** |
| --- | --- |
| **Title** | Nmap scan on 172.22.117.20 |
| **Type (Web app / Linux OS / WIndows OS)** | Windows OS |
| **Risk Rating** | Medium |
| **Description** | We used nmap on 172.22.117.20. Two servers came up: WinDC01 and Windows10. Went to the browser and entered 172.22.117.20 then a login popup came up and we entered the user and password from flag 1 (tivera - Tanya4life). |
| **Images** |  |
| **Affected Hosts** | 172.22.117.20 |
| **Remediation** | Make sure that critical, sensitive date is kept off of public websites |

| **Vulnerability 19** | **Findings** |
| --- | --- |
| **Title** | FTP Enumeration |
| **Type (Web app / Linux OS / WIndows OS)** | Windows OS |
| **Risk Rating** | Medium |
| **Description** | From the last scan we know that port FTP 21 is open to access. |
| **Images** |  |
| **Affected Hosts** | 172.22.117.20 |
| **Remediation** | Close all ports that are not being used; only open them when they need to be |

| **Vulnerability 20** | **Findings** |
| --- | --- |
| **Title** | Machine that is running the SLMail service |
| **Type (Web app / Linux OS / WIndows OS)** | Windows OS |
| **Risk Rating** | Medium |
| **Description** | Found the machine and used the Metasploit to exploit the vulnerabilities. We used SLMail in port 25 and 110. |
| **Images** |  |
| **Affected Hosts** | 172.22.117.20 |
| **Remediation** | Make sure the Operating System has the latest security patch update |