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	Cybersecurity5
Contact Name	Brian Rajaram
Contact Title	Penetration Tester

Document History

Version	Date	Author(s)	Comments
001	March 24, 2024	Brian Rajaram	

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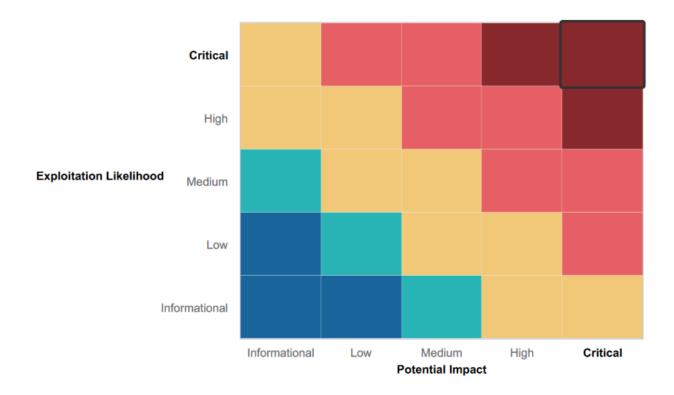
As the following grid shows, each threat is assessed in terms of both its potential impact on the business and the likelihood of exploitation:

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.

- Use of pen-testing to identify weaknesses and vulnerabilities in system

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 and SQL injection vulnerabilities in the web app.
- Apache server in use vulnerable to multiple exploits.
- Open ports allow for access.
- Access to password hashes allow for cracking and credential stealing.
- Physical address for server publicly available.
- Credentials stored in html code.

Executive Summary

The penetration test conducted by Cybersecurity5 was able to reveal multiple weaknesses and vulnerabilities in Rekall's system that could lead to loss of confidential data, downtime, reputational damage and loss of revenues.

We first tested Rekall's web application. We determined that it was susceptible to XSS Reflected, XXS Stored, SQL injection, Local File Inclusion and Command Injection attacks across various pages of your website. All of these attacks allow an attacker to potentially gain access to your system and steal information.

The Linux environment in use at Rekall was tested next. We discovered 5 IP addresses that were publicly available and determined the use of Drupal on one of the hosts - a major vulnerability. Using Meterpreter, we were able to gain access to the root by exploiting vulnerabilities and thereby gain access to confidential system files.

Your Windows OS also has weak points. We discovered that port 21 and 110 was open, the latter of which is used for SLMail service. We exploited this vulnerable mail service and once again gained root privileges.

Ultimately, we were able to find several different ways of gaining a foothold into your system through your Web App, Linux OS and Windows OS. These vulnerabilities need to be addressed, and your system hardened, should you wish to mitigate your chances of a potential hacker gaining confidential, valuable and damaging information about your company.

Summary Vulnerability Overview

Vulnerability	Severity
Nmap Scan	**Critical**
Aggressive Nmap Scan	**Critical**
Shellshock on Web Server	**Critical**
Metepreter Shell RCE	**Critical**
John the Ripper	**Critical**
FTP data exposure	**Critical**
Local File Inclusion	**Critical**
Local File Inclusion Advanced	**Critical**
OSINT data	Medium
Certificate Search Using crt.sh	Medium
Reflected XSS	Medium
XSS Payload in VR Planner page (Choose Your Character field)	Medium
Stored XSS on Welcome Page	Medium
Sensitive Information Exposure	**Low**

The following summary tables represent an overview of the assessment findings for this penetration test:
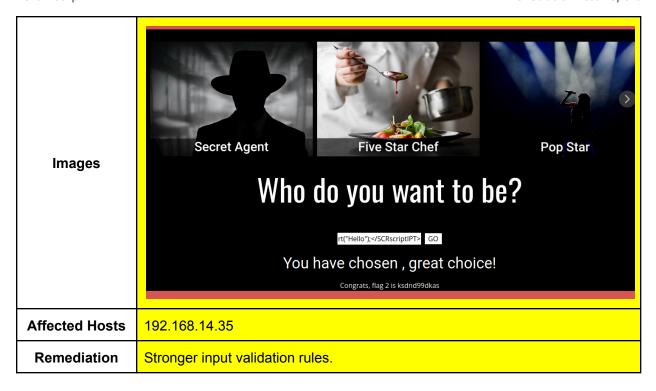
Scan Type	Total
Hosts	172.22.117.20, 172.22.117.10, 192.168.14.35, 192.168.13.10, 192.168.13.11, 192.168.13.12, 192.168.13.13, 192.168.13.14
Ports	21, 22, 80, 106, 110
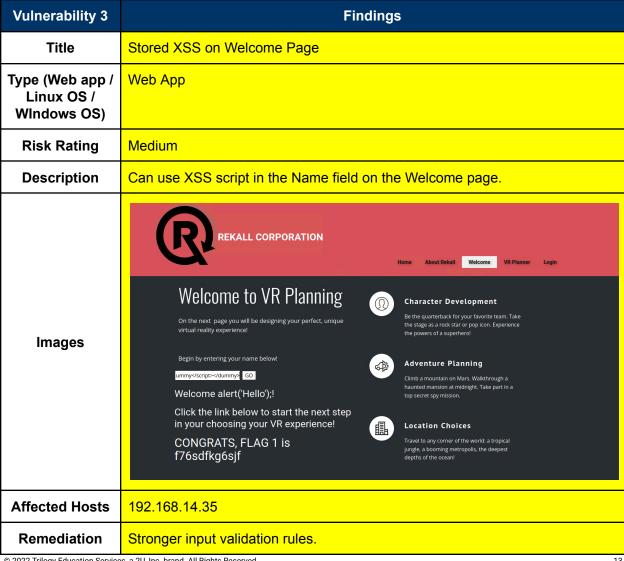
Exploitation Risk	Total
Critical	8
High	0
Medium	5
Low	1

Vulnerability Findings

Vulnerability 1	Findings
Title	Reflected XSS
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Medium
Description	Cross-site scripting on Welcome page.
Images	
Affected Hosts	192.168.14.35
Remediation	Input Validation
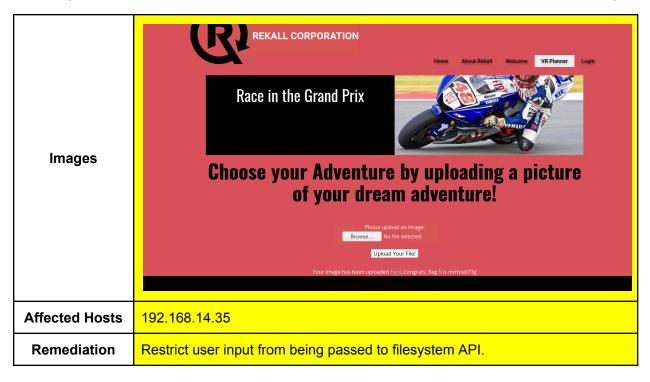
Vulnerability 2	Findings
Title	XSS Payload in VR Planner page (Choose Your Character field)
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Medium
Description	Bypassing input validation may allow for attacker to gain access to system directories.

Images	
	rt("Hello");</SCRscriptIPT> GO
	You have chosen , great choice!
	Congrats, flag 2 is ksdnd99dkas
Affected Hosts	192.168.14.35
Remediation	Stronger input validation rules.

Vulnerability 3	Findings
Title	Stored XSS on Welcome Page
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Medium
Description	Can use XSS script in the Name field on the Welcome page.
Images	
Affected Hosts	192.168.14.35
Remediation	Stronger input validation rules.

Vulnerability 4	Findings
Title	Sensitive Information Exposure
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Low
Description	Easily accessible website and server information by running curl against site IP.
Images	
Affected Hosts	192.168.14.35
Remediation	No remediation.

Vulnerability 5	Findings
Title	Local File Inclusion
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Critical
Description	Uploaded php file where image should be uploaded.

Images	
Affected Hosts	192.168.14.35
Remediation	Restrict user input from being passed to filesystem API.

Vulnerability 6	Findings
Title	Local File Inclusion Advanced
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Critical
Description	Uploaded .php file by including the extension '.jpg' in the file name.
Images	
Affected Hosts	192.168.14.35

Remediation	Restrict user input from being passed to filesystem API.

Vulnerability 7	Findings
Title	OSINT data
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Medium
Description	Found employee information using OSINT tool.

Images	Registrant Contact Information:
	        Name sshUser alice
	        Organization
	        Address h8s692hskasd Flag1
	        City Atlanta
	        State / Province Georgia
	        Postal Code 30309
	        Country US
	        Phone +1.7702229999
	        Email jlow@2u.com
	
	Administrative Contact Information:
	        Name sshUser alice
	        Organization
	        Address h8s692hskasd Flag1
	        City Atlanta
	        State / Province Georgia
	        Postal Code 30309
	        Country US
	        Phone +1.7702229999
	        Email jlow@2u.com
	
	Technical Contact Information:
	        Name sshUser alice
	        Organization
	        Address h8s692hskasd Flag1
	        City Atlanta
	        State / Province Georgia
	        Postal Code 30309
	        Country US
	        Phone +1.7702229999
	        Email jlow@2u.com
	
	Information Updated: 2024-02-25 20:46:51

Affected Hosts	
Remediation	Try to keep publicly available data about the company to a minimum.

Vulnerability 8	Findings
Title	Certificate Search Using crt.sh
Type (Web app / Linux OS / WIndows OS)	Web App

Risk Rating	Medium
Description	Found stored certificate for totalrekall.xyz
Images	
Affected Hosts	
Remediation	Prevent certificates from being stored.

Vulnerability 9	Findings
Title	Nmap Scan
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	Nmap Scan 192.168.13.0/24 provided 5 hosts.
Images	
Affected Hosts	192.168.13.10, 192.168.13.11, 192.168.13.12, 192.168.13.13, 192.168.13.14
Remediation	IP Blocking.

Vulnerability 10	Findings
Title	Aggressive Nmap Scan
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	Using aggressive nmap scan, we were able to determine that the host was running Drupal, which represents a vulnerability.
Images	
Affected Hosts	192.168.13.12
Remediation	Restrict information returned on scan or return intentionally misleading results.

Vulnerability 11	Findings
Title	Shellshock on Web Server
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	Used exploit (multi/http/apache_mod_cgi_bash_env_exec) to gain access to root privileges.

| Images | ```
meterpreter > cat /etc/sudoers
#
# This file MUST be edited with the 'visudo' command as root.
#
# Please consider adding local content in /etc/sudoers.d/ instead of
# directly modifying this file.
#
# See the man page for details on how to write a sudoers file.
#
Defaults        env_reset
Defaults        mail_badpass
Defaults        secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin"

# Host alias specification

# User alias specification

# Cmnd alias specification

# User privilege specification
root    ALL=(ALL:ALL) ALL

# Members of the admin group may gain root privileges
%admin ALL=(ALL) ALL

# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL

# See sudoers(5) for more information on "#include" directives:

#includedir /etc/sudoers.d
flag8-9dnx5shdf5 ALL=(ALL:ALL) /usr/bin/less
meterpreter > █
``` |
|---|---|
| **Affected Hosts** | 192.168.13.14 |
| **Remediation** | Limit Access to Sudo Accounts. |

Vulnerability 12	**Findings**
Title	Metepreter Shell RCE
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	Used tomcat_jsp_upload_bypass exploit to gain system access to 192.168.13.10

Images	

Affected Hosts	192.168.13.10
Remediation	Vendor updates.

Vulnerability 13	**Findings**
Title	John the Ripper
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Critical
Description	Used John the Ripper to crack password for user trivera.
Images	
Affected Hosts	
Remediation	Stronger password policy enforcement; salting hashes.

Vulnerability 14	Findings
Title	FTP data exposure.
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Critical
Description	Used ftp command to pull open port on network hosts.
Images	
Affected Hosts	172.22.117.20
Remediation	Close open ports.

```
  ┌──(root💀kali)-[~]
  └─# ftp 172.22.117.20
Connected to 172.22.117.20.
220-FileZilla Server version 0.9.41 beta
220-written by Tim Kosse (Tim.Kosse@gmx.de)
220 Please visit http://sourceforge.net/projects/filezilla/
Name (172.22.117.20:root): anonymous
331 Password required for anonymous
Password:
230 Logged on
Remote system type is UNIX.
ftp> ls
200 Port command successful
150 Opening data channel for directory list.
-r--r--r-- 1 ftp ftp            32 Feb 15  2022 flag3.txt
226 Transfer OK
ftp> cat flag3.txt
?Invalid command
ftp> download flag3.txt
?Invalid command
ftp> get flag3.txt
local: flag3.txt remote: flag3.txt
200 Port command successful
150 Opening data channel for file transfer.
226 Transfer OK
32 bytes received in 0.00 secs (286.6972 kB/s)
ftp> ls
200 Port command successful
150 Opening data channel for directory list.
-r--r--r-- 1 ftp ftp            32 Feb 15  2022 flag3.txt
226 Transfer OK
ftp>
```