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

Contact Information

Company Name	Black Cyberspace
Contact Name	Joy Dada
Contact Title	Pent Tester

Document History

Version	Date	Author(s)	Comments
001			

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.

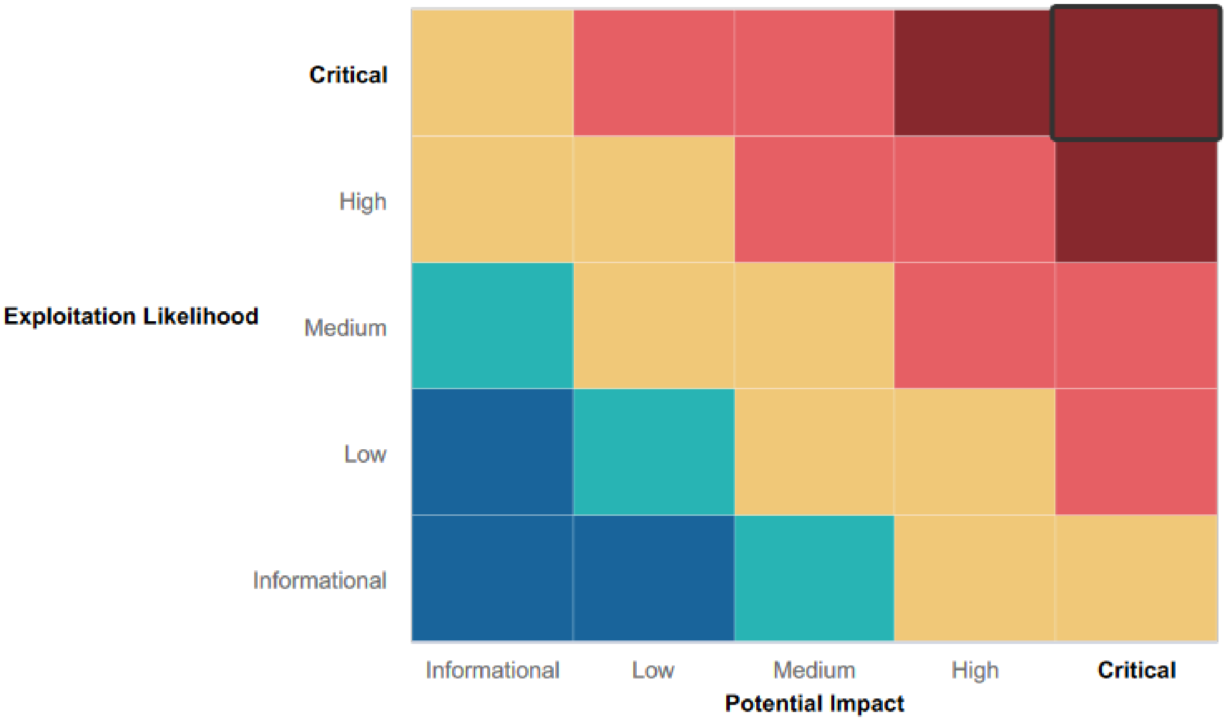
Executive Summary of Findings

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.

- Website was easy to do
- Website was user friendly

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.

- Vulnerable to cross-site scripting
- Vulnerable to command injection
- Vulnerable to credential dumping
- Weak passwords
- Open ports
- Vulnerable to PHP injection

Executive Summary

[Provide a narrative summary of your steps and findings, including screenshots. It’s fine to mention specifics (e.g., used Metasploit to exploit a vulnerable version of DistCC), but do not get too technical in these specifics. This should be an A–Z summary of your assessment.]

I did a penetration test on the environment. I was hired to do penetration testing on the environment and I found a lot of vulnerabilities in the system. I will list down the vulnerabilities along with the remediation below.

Summary Vulnerability Overview

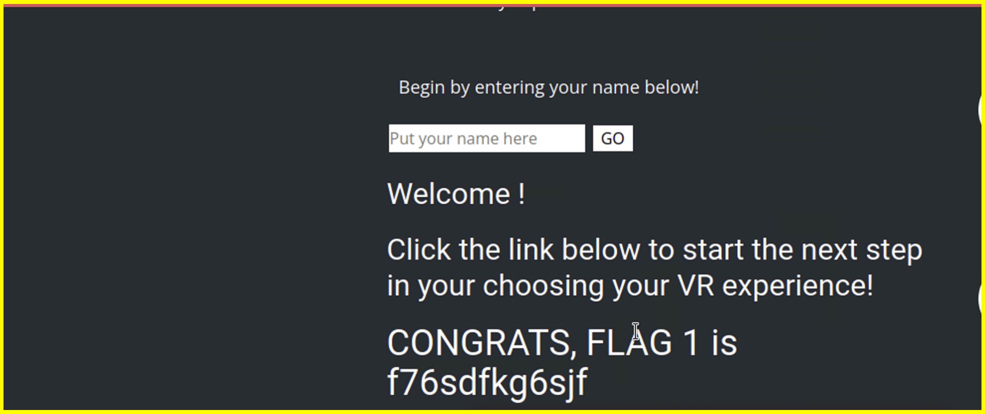
Vulnerability	Severity
Vulnerable to cross-site scripting	**Critical**
Vulnerable to cross-site scripting advanced	**Critical**
Vulnerable to local file inclusion	**Critical**

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

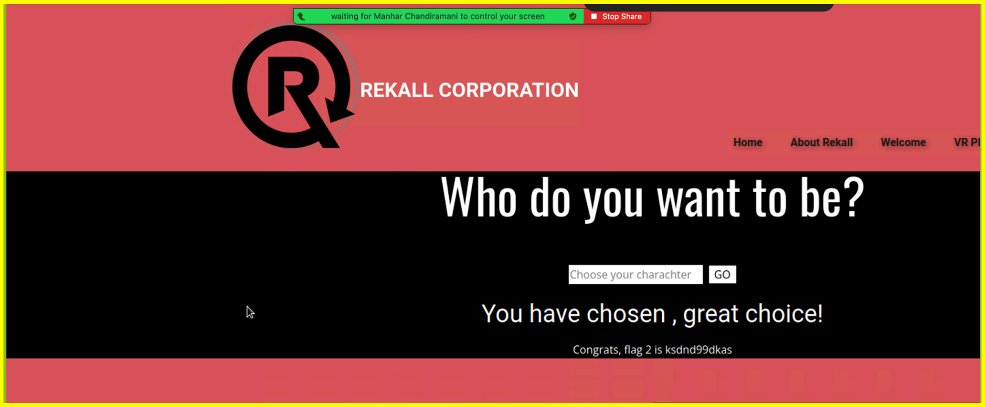
Scan Type	Total
Hosts	192.168.14.35
Ports	21,22,25,80,443,3389,53

Exploitation Risk	Total
Critical	3
High	0
Medium	0
Low	0

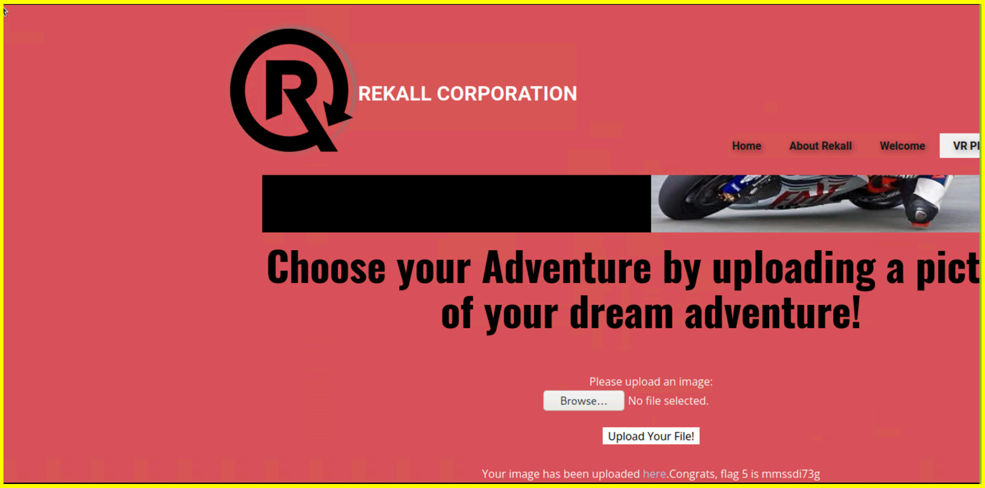
Vulnerability Findings

Vulnerability 1	Findings
Title	Cross-site scripting
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	Critical
Description	They injected the malicious script and said, “Hi.”
Images	 Begin by entering your name below! Put your name here GO Welcome ! Click the link below to start the next step in your choosing your VR experience! CONGRATS, FLAG 1 is f76sdfkg6sjf
Affected Hosts	192.168.14.35
Remediation	Creating and implementing a content security policy (CSP) is an effective way of mitigating Cross-Site Scripting and other vulnerabilities. It prevents XSS by white-listing URLs from which browsers can load and execute scripts. The server prevents the client's browser from executing any script from an untrusted URL. Answer from: https://www.code-intelligence.com/blog/what-is-cross-site-scripting#:~:text=Creating%20and%20implementing%20a%20content,script%20from%20an%20untrusted%20URL.

Vulnerability 2	Findings
Title	Cross-site scripting advanced
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	Critical

Description	Injected an advanced script and said, “Hello.”
Images	 waiting for Manhar Chandiramani to control your screen Stop Share REKALL CORPORATION Home About Rekall Welcome VR Pl Choose your charachter GO Who do you want to be? You have chosen , great choice! Congrats, flag 2 is ksdnd99dkas
Affected Hosts	192.168.14.35
Remediation	Creating and implementing a content security policy (CSP) is an effective way of mitigating Cross-Site Scripting and other vulnerabilities. It prevents XSS by white-listing URLs from which browsers can load and execute scripts. The server prevents the client's browser from executing any script from an untrusted URL. Answer from: https://www.code-intelligence.com/blog/what-is-cross-site-scripting#:~:text=Creating%20and%20implementing%20a%20content,script%20from%20an%20untrusted%20URL.

Vulnerability 3	**Findings**
Title	Local file inclusion
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	Critical
Description	I was able to exploit the vulnerabilities by uploading a PHP script file onto my web application.

Images	 REKALL CORPORATION Home About Rekall Welcome VR Pl Browse... Upload Your File! Choose your Adventure by uploading a pict of your dream adventure! Please upload an image: No file selected. Your image has been uploaded here.Congrats, flag 5 is mmssdi73g
Affected Hosts	192.168.14.35
Remediation	The most effective solution to eliminate file inclusion vulnerabilities is to avoid passing user-submitted input to any filesystem/framework API. Answer from: https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/07-Input_Validation_Testing/11.1-Testing_for_Local_File_Inclusion#:~:text=The%20most%20effective%20solution%20to,to%20any%20filesystem%2Fframework%20API.

Vulnerability 4	Findings
Title	
Type (Web app / Linux OS / WIndows OS)	
Risk Rating	
Description	
Images	
Affected Hosts	
Remediation	

Vulnerability 5	Findings
Title	
Type (Web app / Linux OS / WIndows OS)	

Risk Rating	
Description	
Images	
Affected Hosts	
Remediation	

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.