



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	MAYURA LLC
Contact Name	SIVAYALINI PARTHIBAN
Contact Title	PENETRATION TESTER

Document History

Version	Date	Author(s)	Comments
001	01/19/2023	SIVAYALINI	

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.

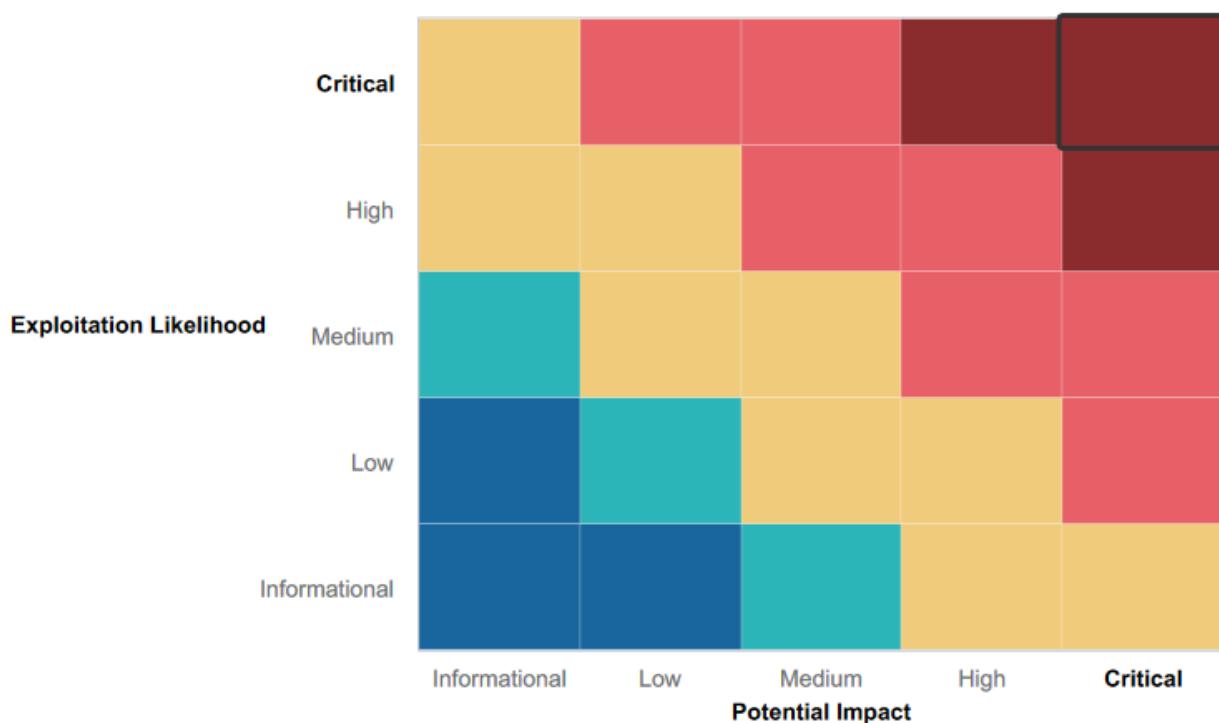
Executive Summary of Findings

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.

- Rekall using Metasploit and nmap that provides good security to prevent unauthorized access.
- No open source data.
- Ensures network availability to mitigate DDoS attack.

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.

- Rekall is vulnerable to XSS and SQL payload injection
- Apache web server is outdated.
- SImail is vulnerable to exploits which allows access to shell.
- Open ports allow for ftp and unauthorized access.
- Password cracking and privilege escalation was very possible due to unauthorized access.
- User Credentials was found publicly in github.

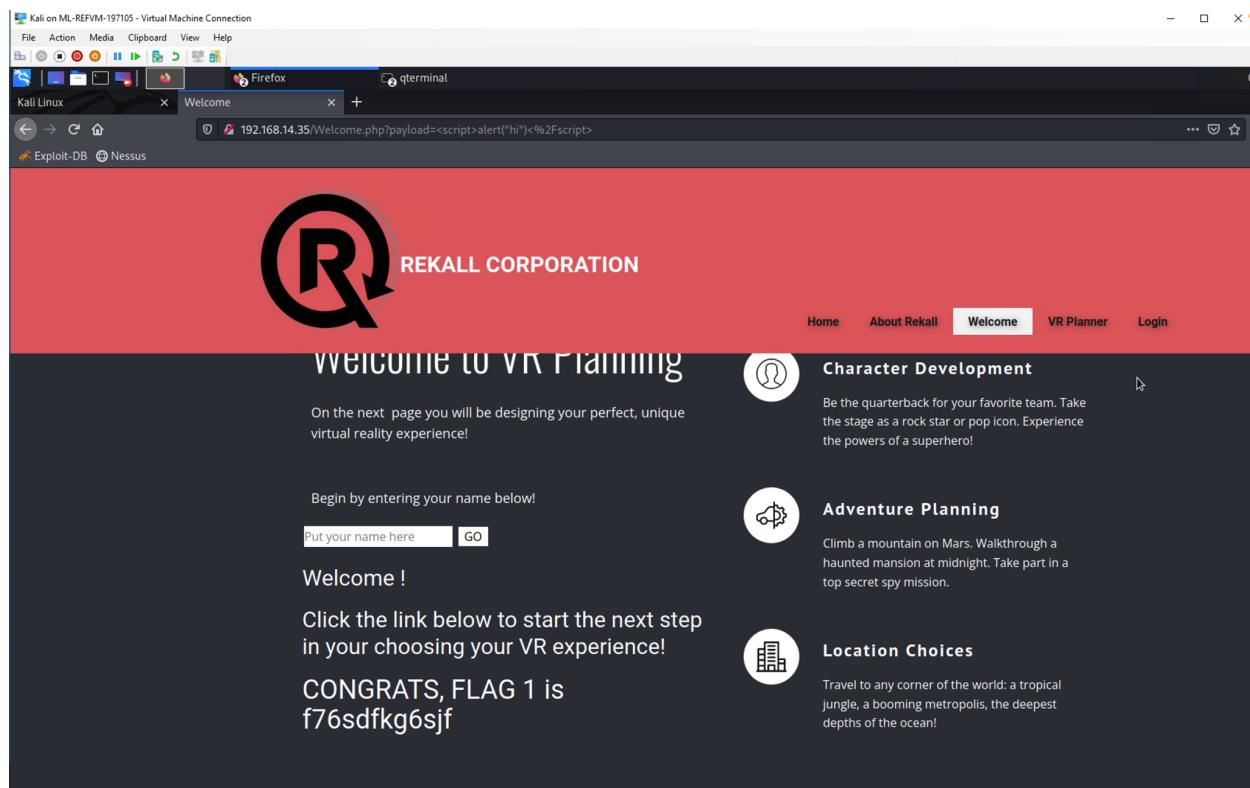
Executive Summary

During the entire Penetration testing for the Rekall's systems, we are able to identify several vulnerabilities that could affect Rekall's financial system and can also be harmful to the long-term stability of an organization. We were able to access Rekall servers/systems, and we were able to exfiltrate sensitive data.

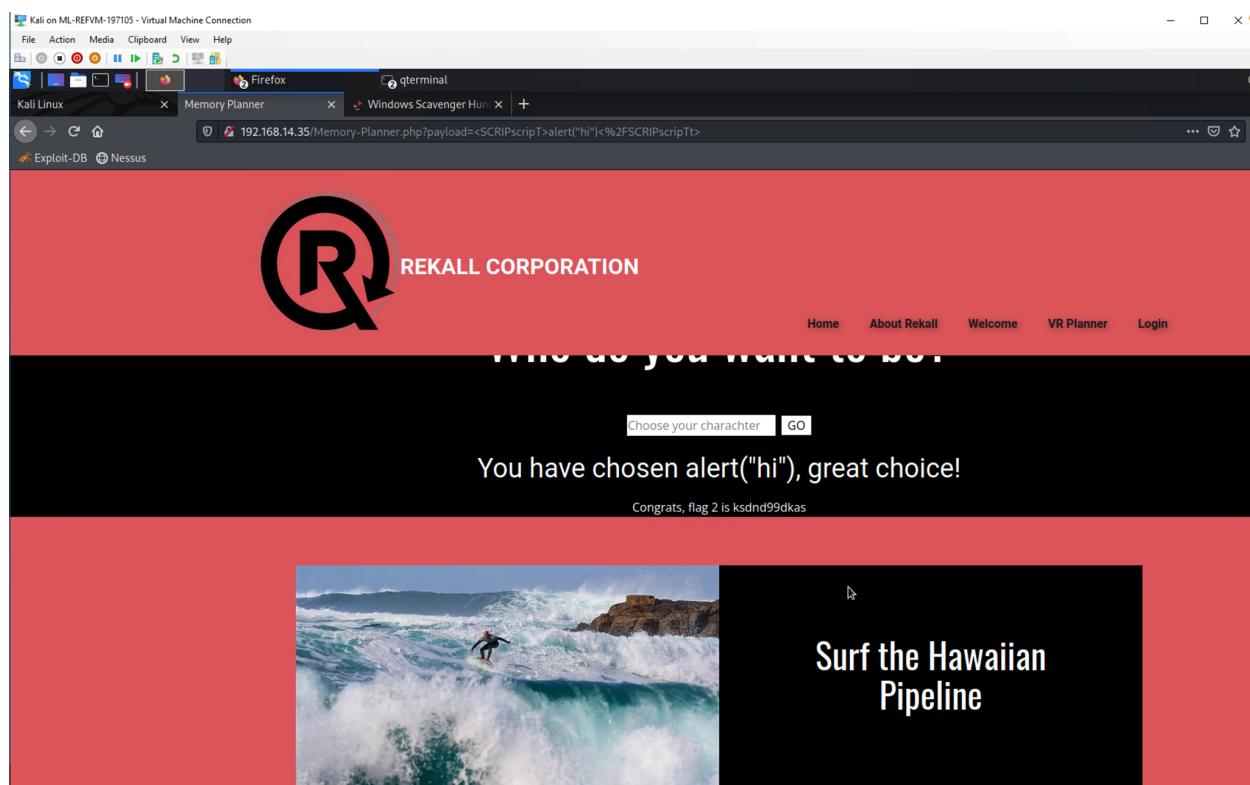
VULNERABLE TO MALICIOUS SCRIPT

- Rekall's site is vulnerable to XSS reflected attack as malicious scripts can run on the Welcome page.php, Memory planner.php page and XSS stored attack on comments.php page.
- Rekall's site is vulnerable to SQL injection attacks on the Login.php and Networking.php pages.
- It is also vulnerable to Local file inclusion on VR planner page.

XSS REFLECTED ATTACK ON WELCOME.PHP PAGE



XSS REFLECTED ATTACK ON MEMORY-PLANNER.PHP



XSS STORED ATTACK ON COMMENTS.PHP PAGE

The screenshot shows a Firefox browser window on a Kali Linux desktop. The address bar shows the URL `192.168.14.35/comments.php`. The page content is from Rekall Corporation's website. A comment box has been modified to display the text "hi". Below the comment box, a success message says "CONGRATS, FLAG 3 is sd7fk1nctx". At the bottom, there is a table of comments:

#	Owner	Date	Entry
1	bee	2023-01-21 13:59:10	hi

LOCAL FILE INCLUSION ON MEMORY-PLANNER.PHP PAGE

The screenshot shows a Firefox browser window on a Kali Linux desktop. The address bar shows the URL `192.168.14.35/Memory-Planner.php?payload=script.jpg.php`. The page content is from Rekall Corporation's website. It features three cards: "Pro Athlete" (a basketball player), "Five Star Chef" (a chef), and "Secret Agent" (a silhouette). Below the cards, a large question asks "Who do you want to be?". At the bottom, there is a form with the text "Choose your character" and a "GO" button, followed by the message "You have chosen .jpg.php, great choice!".

SENSITIVE DATA EXPOSURE ON LOGIN.PHP

Kali on ML-REFVM-197105 - Virtual Machine Connection

File Action Media Clipboard View Help

Kali Linux Windows Scavenger Hunt Login

192.168.14.35/Login.php

Exploit-DB Nessus

REKALL CORPORATION

Enter your Administrator credentials!

Login: [REDACTED]

Password: [REDACTED]

Login

Successful login! flag 8 is 87fsdkf6djf , also check out the admin only networking tools [HERE](#)

SENSITIVE DATA EXPOSURE ON ROBOTS.TXT

Kali on ML-REFVM-197105 - Virtual Machine Connection

File Action Media Clipboard View Help

Kali Linux Windows Scavenger Hunt 192.168.14.35/robots.txt

Exploit-DB Nessus

```
User-agent: GoodBot
Disallow:
User-agent: BadBot
Disallow: /
User-agent: *
Disallow: /admin/
Disallow: /documents/
Disallow: /images/
Disallow: /souvenirs.php/
Disallow: flag:dkdudfkdy23
```

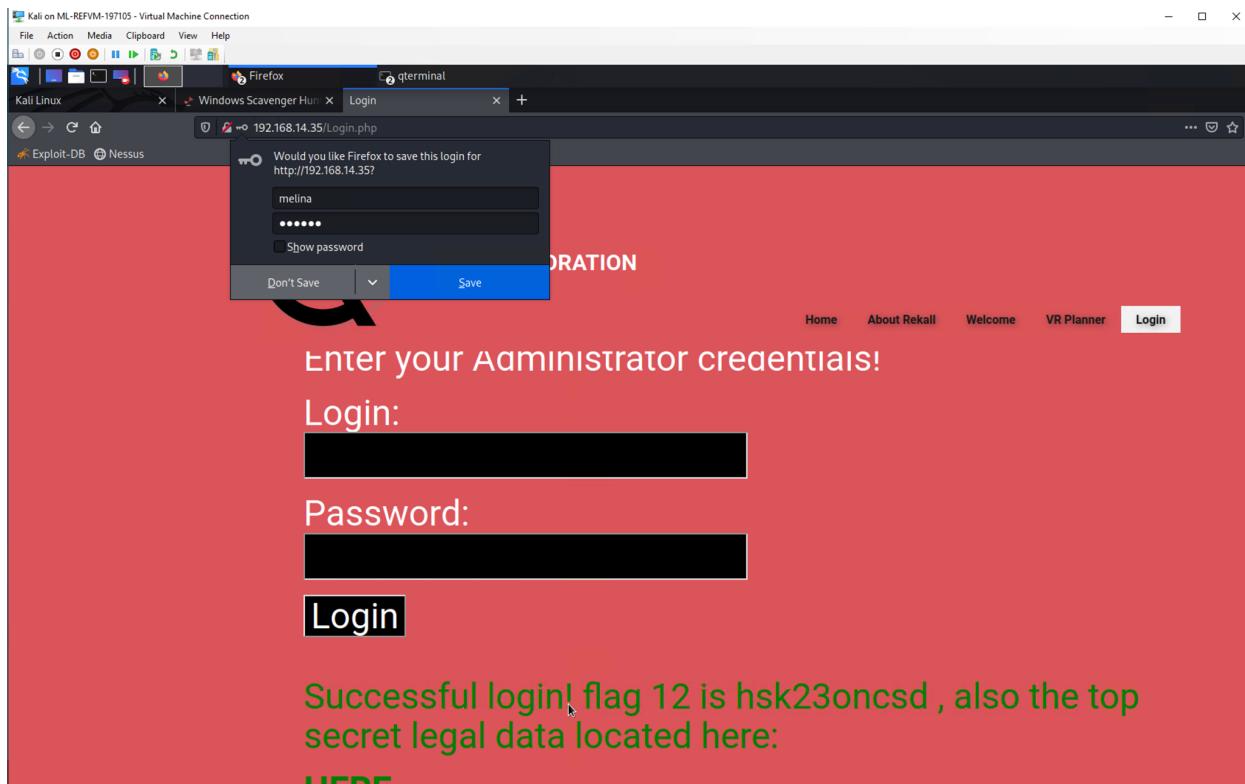
COMMAND INJECTION ON NETWORKING.PHP PAGE

The screenshot shows a Firefox browser window running on a Kali Linux VM. The address bar displays the URL `192.168.14.35/networking.php`. The page content is a red header with the Rekall Corporation logo and navigation links (Home, About Rekall, Welcome, VR Planner, Login). Below the header is a section titled "welcome to Rekall AutmT Networking Tools". A reminder message states: "Just a reminder, the vendor list of our top-secret networking tools are located in the file: vendors.txt". Underneath is a "DNS Check" section with an input field containing "www.example.com" and a "Lookup" button. The response shows: "Server: 127.0.0.11 Address: 127.0.0.11#53 Non-authoritative answer: www.welcometorecall.com canonical name = welcometorecall.com. Name: welcometorecall.com Address: 208.76.82.210 SIEM: splunk Firewalls: barracuda CLOUD: aws Load balancers: F5". A success message "Congrats, flag 10 is ksdnd99dkas" is displayed. Below is an "MX Record Checker" section with an input field containing "www.example.com" and a "Check your MX" button.

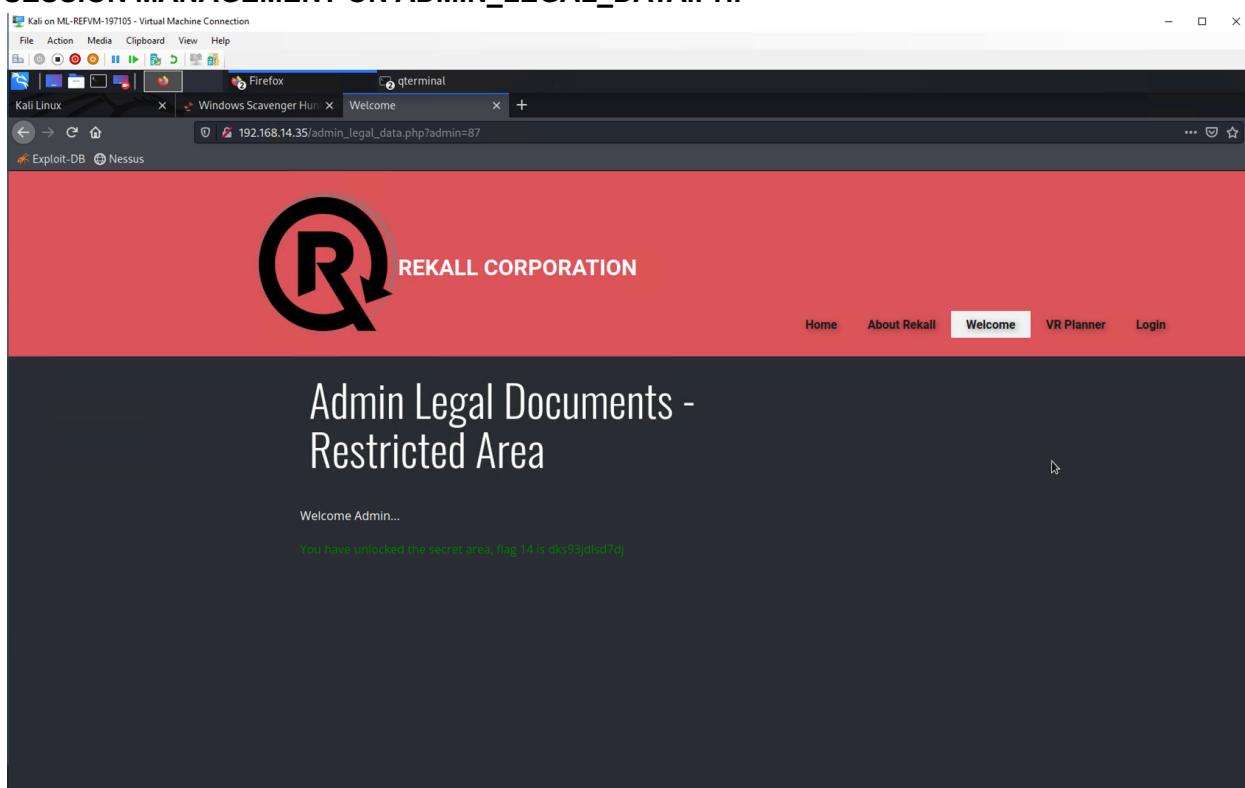
COMMAND INJECTION NETWORKING.PHP PAGE

The screenshot shows a Firefox browser window running on a Kali Linux VM. The address bar displays the URL `192.168.14.35/networking.php`. The page content is identical to the first screenshot, featuring a red header with the Rekall Corporation logo and navigation links. Below the header is a section titled "welcome to Rekall AutmT Networking Tools". A reminder message states: "Just a reminder, the vendor list of our top-secret networking tools are located in the file: vendors.txt". Underneath is a "DNS Check" section with an input field containing "www.example.com" and a "Lookup" button. The response shows: "Server: 127.0.0.11 Address: 127.0.0.11#53 Non-authoritative answer: www.welcometorecall.com canonical name = welcometorecall.com. Name: welcometorecall.com Address: 208.76.82.210 SIEM: splunk Firewalls: barracuda CLOUD: aws Load balancers: F5". A success message "Congrats, flag 10 is ksdnd99dkas" is displayed. Below is an "MX Record Checker" section with an input field containing "www.example.com" and a "Check your MX" button. The response shows: "SIEM: splunk Firewalls: barracuda CLOUD: aws Load balancers: F5". A success message "Congrats, flag 11 is opshdkasy78s" is displayed.

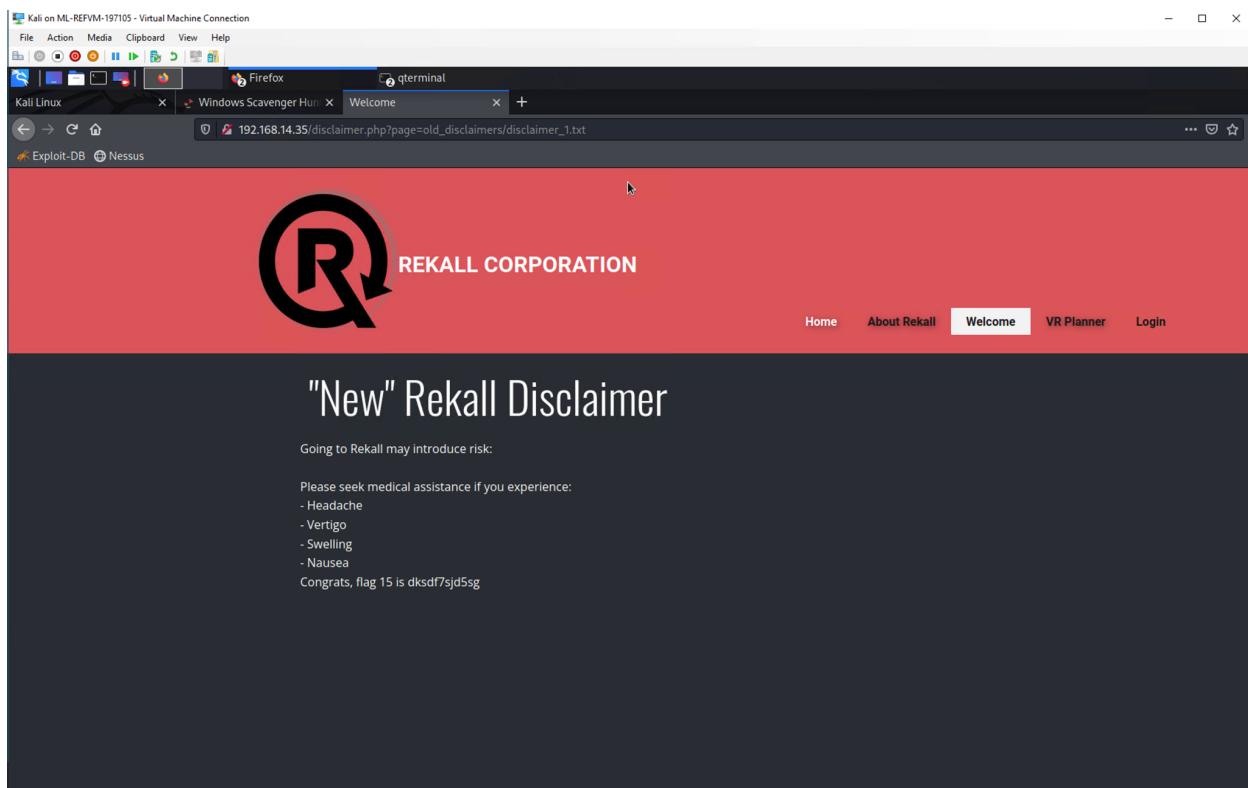
BRUTE FORCE ATTACK ON LOGIN.PHP



SESSION MANAGEMENT ON ADMIN_LEGAL_DATA.PHP



DIRECTORY TRAVERSAL ON DISCLAIMER.PHP



The Linux OS environment was the next testing environment, Mayura Pentesting group was successfully able to reveal the host, and with stolen credentials escalated privileges to root.

- Using OSINT open source data are exposed and using crt.sh stored certificate are exposed.
- By scanning the ports it was determined there are six hosts and one running Drupal.
- Apache Struts(Out of date) - Critical vulnerability was found by running Nessus scan.

OPEN SOURCE EXPOSED DATA on Domain Dossier Webpage

```
Kali on ML-REFVM-197105 - Virtual Machine Connection
File Action Media Clipboard View Help
Firefox qterminal
Kali Linux × Problem loading page × totalrekkal.xyz - Domain + 
https://centralops.net/co/DomainDossier.aspx
Exploit-DB Nessus
canonical name totalrekkal.xyz.
aliases
addresses 34.102.136.180

Domain Whois record
Queried whois.nic.xy with "totalrekkal.xyz"...
Domain Name: TOTALREKKAL.XYZ
Registry Domain ID: D273189417-CNIC
Registrar WHOIS Server: whois.godaddy.com
Registrar URL: https://www.godaddy.com/
Updated Date: 2022-02-02T15:16:02Z
Creation Date: 2022-02-02T15:16:02Z
Registry Expiry Date: 2023-02-02T23:59:00Z
Registrar: Daddy, LLC
Registrar IANA ID: 141
Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Registrant Organization:
Registrant State/Province: Georgia
Registrant Country: US
Registrant Email: Please query the RDNS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name.
Admin Email: Please query the RDNS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name.
Tech Email: Please query the RDNS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name.
Name Server: NS2.DOMAINCONTROL.COM
Name Server: NS3.DOMAINCONTROL.COM
DNSSEC: unsigned
Billing Email: Please query the RDNS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name.
Registrar Abuse Contact Email: abuse@godaddy.com
Registrar Abuse Contact Phone: +1.408.242.5000
URL of the ICANN Whois Accuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of WHOIS database: 2023-01-19T16:16:40.02 <<<

Queried whois.godaddy.com with "totalrekkal.xyz"...
Domain Name: totalrekkal.xyz
Registry Domain ID: D273189417-CNIC
Registrar WHOIS Server: whois.godaddy.com
Registrar URL: https://www.godaddy.com/
Updated Date: 2022-02-02T19:16:02Z
Creation Date: 2022-02-02T19:16:02Z
Registrar Registration Expiration Date: 2023-02-02T23:59:00Z
Registrar: Godaddy.com LLC
Registrant ID: 10000000000000000000
Registrar Abuse Contact Email: abuse@godaddy.com
Registrar Abuse Contact Phone: +1.408.242.5000
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
```

PING totalrecall.xyz

Kali on ML-REFVM-197105 - Virtual Machine Connection

File Action Media Clipboard View Help

Firefox qterminal

```
(root㉿kali:~) ~
└─# ping totalrekkal.xyz
PING totalrekkal.xyz (34.102.136.180) 56(84) bytes of data.
*Connection lookup
--- totalrekkal.xyz ping statistics ---
57 packets transmitted, 0 received, 100% packet loss, time 57346ms
^C
(root㉿kali:~) ~ 100.186

[...]
```

Domain Whois record

Quoted whois.net.vyx whois.totalrekkal.xyz...

```
Domain Name: TOTALREKKAL.NET
Registrant Email: ED-223289317-CNIC
Registrant WHOIS Server: WHOIS-PROD.WHOIS
Registrar WHOIS URL: https://www.godaddy.com/
Updated Date: 2022-02-23T08:12:32-07
Creation Date: 2022-02-23T18:16:00-07
Registrar: GoDaddy, Inc. 223-42-9272-23 [30.02]
Registrar WHOIS Query Delay: 0
Registrar Abuse Contact Email: abuse@godaddy.com
Registrar IANA ID: 240
Registrar Organization: GoDaddy, Inc.
Registrant Country: Georgia
Registrant State/Province: Georgia
Registrant City: Atlanta
Registrant Postcode: 30318
Registrant Phone: +1-404-952-0000
Registrant Email: Please query the ICANN service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name.
Admin Email: Please query the ICANN service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name.
Tech Email: Please query the ICANN service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name.
Name Server: NS01.DYNAMICCONTROL.COM
Name Server: NS02.DYNAMICCONTROL.COM
Name Server: NS03.DYNAMICCONTROL.COM
Name Server: NS04.DYNAMICCONTROL.COM

Billing Email: Please query the ICANN service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name.
Registrar Abuse Contact Email: abuse@godaddy.com
Registrar Abuse Contact Phone: +1-404-952-0000
URL of the ICANN Whois Transparency Complaint Form: https://www.icann.org/wtcf/
... Last update of WHOIS database: 2023-02-19T19:16:40-07
...
```

Quoted whois.godaddy.com whois.totalrekkal.xyz...

```
Domain Name: totalrekkal.NET
Registrant-Domain-ID: B273B9317-CNIC
Registrant WHOIS Server: whois.godaddy.com
Registrant WHOIS URL: https://www.godaddy.com
Updated Date: 2022-02-23T08:12:32
Creation Date: 2022-02-23T18:16:02
Registrar Registration-Expiration Date: 2023-02-23T23:59:59Z
Registrar: GoDaddy.com, LLC
Registrar IANA ID: 240
Registrar Abuse Contact Email: abuse@godaddy.com
Registrar Abuse Contact Phone: +1-404-952-0005
Domain Status: clientTransferProhibited https://icann.org/eppclientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/eppclientUpdateProhibited
```

OPEN SOURCE EXPOSED DATA ON CRT.SH

https://crt.sh/?q=totalrecall.xyz

crt.sh Identity Search Group by Issuer

Criteria Type: Identity Match: ILIKE Search: 'totalrecall.xyz'

Certificates	crt.sh ID	Logged At	Not Before	Not After	Common Name	Matching Identities	Issuer Name
	6095738637	2022-02-02	2022-02-02	2022-05-03	flag3-s7euwehd.totalrecall.xyz	flag3-s7euwehd.totalrecall.xyz	C=AT,O=ZeroSSL,CN=ZeroSSL RSA Domain Secure Site CA
	6095738716	2022-02-02	2022-02-02	2022-05-03	flag3-s7euwehd.totalrecall.xyz	flag3-s7euwehd.totalrecall.xyz	C=AT,O=ZeroSSL,CN=ZeroSSL RSA Domain Secure Site CA
	6095204253	2022-02-02	2022-02-02	2022-05-03	totalrecall.xyz	totalrecall.xyz	C=AT,O=ZeroSSL,CN=ZeroSSL RSA Domain Secure Site CA
	6095204153	2022-02-02	2022-02-02	2022-05-03	totalrecall.xyz	totalrecall.xyz	C=AT,O=ZeroSSL,CN=ZeroSSL RSA Domain Secure Site CA

© Sectigo Limited 2015-2022. All rights reserved.

Sectigo

PORT SCANNING FOUND 6 HOSTS

```
root@kali:~  
File Actions Edit View Help  
└# nmap 192.168.13.0/24  
Starting Nmap 7.92 ( https://nmap.org ) at 2023-01-09 19:18 EST  
Nmap scan report for 192.168.13.10  
Host is up (0.0000080s latency).  
Not shown: 998 closed tcp ports (reset)  
PORT      STATE SERVICE  
8009/tcp  open  ajp13  
8080/tcp  open  http-proxy  
MAC Address: 02:42:C0:A8:0D:0A (Unknown)  
  
Nmap scan report for 192.168.13.11  
Host is up (0.0000080s latency).  
Not shown: 999 closed tcp ports (reset)  
PORT      STATE SERVICE  
80/tcp    open  http  
MAC Address: 02:42:C0:A8:0D:0B (Unknown)  
  
Nmap scan report for 192.168.13.12  
Host is up (0.000010s latency).  
Not shown: 999 closed tcp ports (reset)  
PORT      STATE SERVICE  
8080/tcp  open  http-proxy  
MAC Address: 02:42:C0:A8:0D:0C (Unknown)  
  
Nmap scan report for 192.168.13.13  
Host is up (0.000012s latency).  
Not shown: 999 closed tcp ports (reset)  
PORT      STATE SERVICE  
80/tcp    open  http  
MAC Address: 02:42:C0:A8:0D:0D (Unknown)  
  
Nmap scan report for 192.168.13.14  
Host is up (0.0000080s latency).  
Not shown: 999 closed tcp ports (reset)  
PORT      STATE SERVICE  
22/tcp    open  ssh  
MAC Address: 02:42:C0:A8:0D:0E (Unknown)  
  
Nmap scan report for 192.168.13.1  
Host is up (0.0000080s latency).  
Not shown: 995 closed tcp ports (reset)  
PORT      STATE      SERVICE  
5901/tcp  open       vnc-1  
6001/tcp  open       X11:1  
8080/tcp  filtered   http-proxy  
10000/tcp filtered   snet-sensor-mgmt  
10001/tcp filtered   scp-config  
  
Nmap done: 256 IP addresses (6 hosts up) scanned in 21.61 seconds
```

AGGRESSIVE NMAP SCAN FOUND THE TRACEROUTE

```
Nmap scan report for 192.168.13.13
Host is up (0.000024s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
80/tcp     open  http   Apache httpd 2.4.25 ((Debian))
| http-server-header: Apache/2.4.25 (Debian)
MAC Address: 02:42:C0:A8:0D:0D (Unknown)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe://-
o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.6
Uptime guess: 35.005 days (since Mon Dec 5
19:27:38 2022)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=261 (Good
luck!)
IP ID Sequence Generation: All zeros

TRACEROUTE
HOP RTT      ADDRESS
1    0.02 ms  192.168.13.13
```

APACHE STRUTS - CRITICAL VULNERABILITY

The screenshot shows a Nessus scan result for a host. The top bar indicates the severity as 'CRITICAL'. The title of the result is 'Apache Struts 2.3.5 - 2.3.31 / 2.5.x < 2.5.10.1 Jakarta Multipart Parser RCE (remote)'. The 'Description' section states that the version of Apache Struts running on the remote host is affected by a remote code execution vulnerability in the Jakarta Multipart parser due to improper handling of the Content-Type header. An unauthenticated, remote attacker can exploit this, via a specially crafted Content-Type header value in the HTTP request, to potentially execute arbitrary code, subject to the privileges of the web server user. The 'Solution' section suggests upgrading to Apache Struts version 2.3.32 / 2.5.10.1 or later, or applying the workaround referenced in the vendor advisory. On the right side, there is a 'Plugin Details' panel with the following information:

Severity:	Critical
ID:	97610
Version:	1.24
Type:	remote
Family:	CGI abuses
Published:	March 8, 2017
Modified:	November 30, 2021

NESSUS SCAN FOUND THE HOST IS VULNERABLE TO STRUTS

```
msf6 auxiliary(scanner/http/apache_mod_cgi_bash_env) > run

[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/http/apache_mod_cgi_bash_env) > sessions

Active sessions
-----
No active sessions.

msf6 auxiliary(scanner/http/apache_mod_cgi_bash_env) > ls

Desktop Documents Downloads file2 file3 flagfile flagisinThisfile.7z hash.txt LinEnum.sh Music Pictures Public Scripts Templates Videos
msf6 auxiliary(scanner/http/apache_mod_cgi_bash_env) > cd flagsinThisfile.7z
[-] The specified path does not exist
msf6 auxiliary(scanner/http/apache_mod_cgi_bash_env) > cd flagsinThisfile
[-] The specified path does not exist
msf6 auxiliary(scanner/http/apache_mod_cgi_bash_env) > cd /flagsinThisfile
[-] The specified path does not exist
msf6 auxiliary(scanner/http/apache_mod_cgi_bash_env) > nano flagisinThisfile
[*] exec: nano flagisinThisfile

msf6 auxiliary(scanner/http/apache_mod_cgi_bash_env) > nano flagisinThisfile.7z
[*] exec: nano flagisinThisfile.7z

msf6 auxiliary(scanner/http/apache_mod_cgi_bash_env) > nano flagisinThisfile.7z
[*] exec: nano flagisinThisfile.7z

msf6 auxiliary(scanner/http/apache_mod_cgi_bash_env) >
```

The WINDOWS OS environment was the next testing environment. Mayura Penetration testing team successfully found the user credentials stored within the HTML source code of the Login.php page.

- User credentials were actually stored in the Github repository which can be used for unauthorized access to the system.
 - FTP port 21 was open and vulnerable , port 110 used for SLMail service.
 - Using Metasploit access can be gained to password hash file, which we cracked and helped for reverse shell creation.
 - Meterpreter can display directories on public Windows directories.

Summary Vulnerability Overview

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

Scan Type	Total
Hosts	
Ports	

Exploitation Risk	Total
Critical	0
High	0
Medium	0



Vulnerability Findings

Vulnerability 1	Findings
Title	
Type (Web app / Linux OS / Windows OS)	
Risk Rating	
Description	
Images	
Affected Hosts	
Remediation	

Vulnerability 2	Findings
Title	
Type (Web app / Linux OS / Windows OS)	
Risk Rating	
Description	
Images	
Affected Hosts	
Remediation	

Vulnerability 3	Findings
Title	
Type (Web app / Linux OS / Windows OS)	

Risk Rating	
Description	
Images	
Affected Hosts	
Remediation	

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.