



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

<b>Company Name</b>	RogueSecurity
<b>Contact Name</b>	Tyler Mills Aailyah Lockett
<b>Contact Title</b>	Security Specialist.

## Document History

<b>Version</b>	<b>Date</b>	<b>Author(s)</b>	<b>Comments</b>
001	01/25/2023	Aailyah Lockett Tyler Mills	First Draft

# 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.

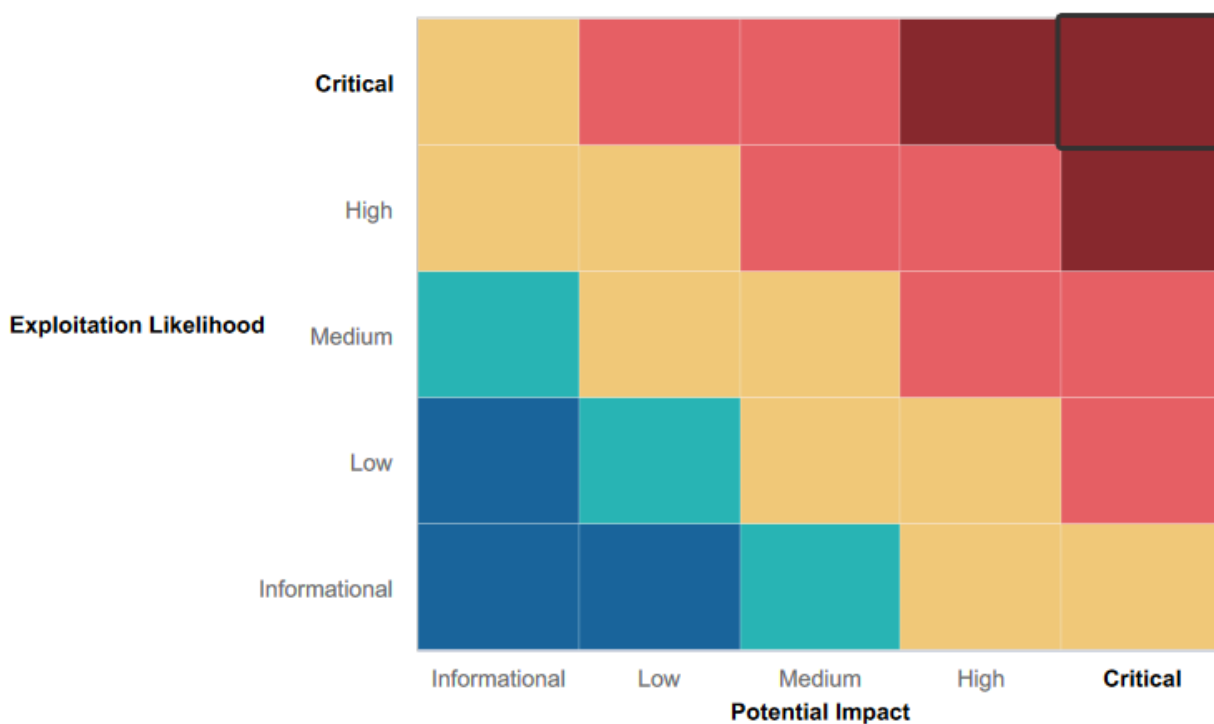
# Executive Summary of Findings

## 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.

- Mitigation strategy in place for denial of DDOS Attacks to ensure network availability
- No vulnerable open source data penetration due to mapping network architecture
- Tools like Metasploit/Hashcat/Nmap are utilized to prevent unauthorized access
- Forward-thinking defensive and offensive strategy
- Current and continuing penetration testing to identify vulnerabilities for mitigation

## 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 is vulnerable to XSS and SQL payload injection
  - Credentials are being stored in HTML source code
  - Apache web server is outdated and vulnerable to multiple exploits
  - SLMail server is vulnerable to exploits which allow access to shell
  - Unauthorized access to password hashes allow for password cracking and privilege escalation
  - Rekall's server physical address is publicly available
  - Credentials are displayed when doing a IP lookup
  - IP addresses within Rekall's IP range display potential vulnerabilities (open ports, IP addresses, etc.) when scanned
  - Open ports allow for file enumeration and unauthorized access
- High-level summary of weaknesses here

## Executive Summary

RogueSecurity, LLC conducted a security assessment on Rekall Corporation network infrastructure to identify any existing vulnerabilities and risks. The assessment employed penetration testing methods to give Rekall Corporation management insight into the risks and security of their current corporate environment. The internal network infrastructure was tested by using reconnaissance and host discovery tools, such as Zenmap and OSINT, to identify the operating systems, software, and services running on each target host.

Vulnerability enumeration was then used to find all potential vulnerabilities on each host and develop a list of attack vectors. Many vulnerabilities were discovered during testing, which put Rekall Corporation resources at risk of compromise. The assessment revealed that Rekall Corporation is not adequately prepared to defend against an attack and should take immediate steps to address the findings in this report.

Critical, High, and Medium severity issues were found impacting Rekall Corporation internal network, requiring immediate action to secure the company against potential threats. These issues included poor password management practices, open ports that may have potentially vulnerable applications running, and lack of security measures on the Cisco AnyConnect configuration file.

In light of the findings, RogueSecurity recommended that Rekall Corporation take immediate steps to address these vulnerabilities and implement security measures to protect against potential threats. This may include implementing password policies, patching vulnerable systems and applications, and implementing security controls on the Cisco AnyConnect configuration file. It is important for Rekall Corporation to regularly conduct security assessments to identify and address any new vulnerabilities that may arise in the future.

## Summary Vulnerability Overview

Vulnerability	Severity
XSS Exploit (Cross-site scripting)	Critical
Local File Inclusion	Critical
SQL Injection	Critical
Command Injection	Critical
FTP Enumeration	Critical
SLMail Exploit	Critical
Open Source exposed data	Medium
Certificate Search via crt.sh	Medium
Nmap Results	Critical
Nessus Scan	Medium
Privilege Escalation	Critical
Port scan Of Subnet	Critical
Machine Task Scheduler	Medium
Public Directory Search	Medium


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

Scan Type	Total
Hosts	192.168.14.35 127.0.0.11 172.22.117.10 172.22.117.20 192.168.13.11 192.168.13.12 192.168.13.13 192.168.13.14
Ports	21- ftp 22- ssh 80- http 106-smb 110-

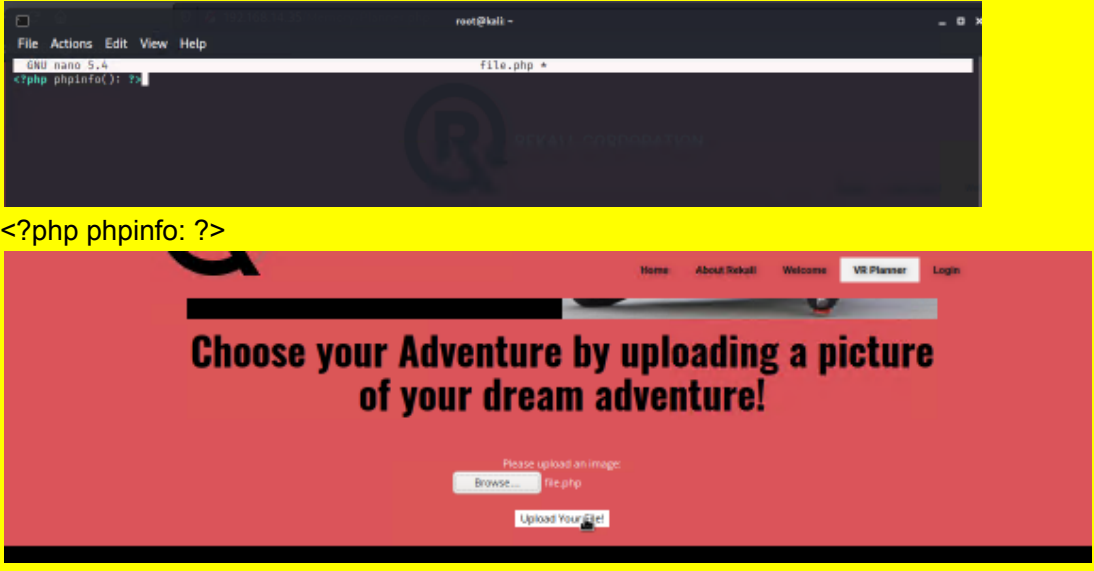
Exploitation Risk	Total
Critical	14
High	5
Medium	3
Low	0

## Vulnerability Findings

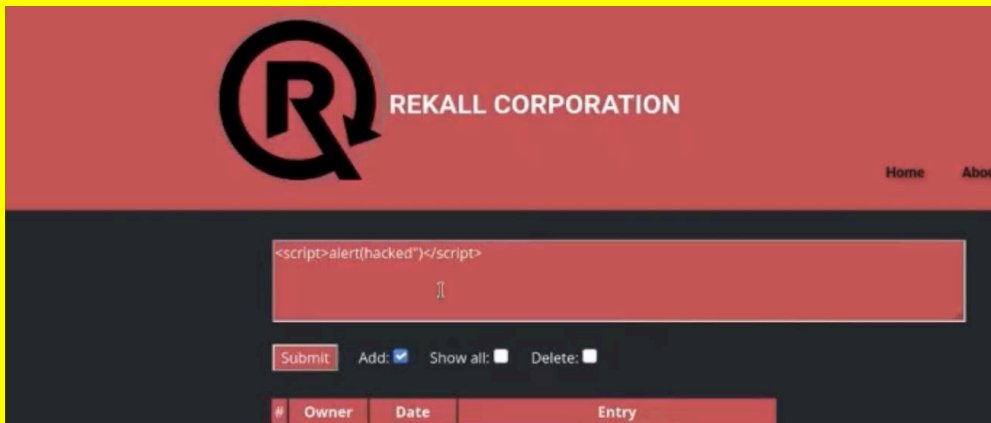
Vulnerability 1	Findings
Title	XSS Exploit (Cross-Site Scripting)
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	Medium
Description	<p>The report titled "XSS Reflected Type Web App Risk Rating Medium" details the findings of a security vulnerability within a web application. The vulnerability in question is known as a cross-site scripting (XSS) attack of the reflected type. This type of attack occurs when a malicious script is executed on the host's home page, in this case, the script being <code>&lt;script&gt;alert(Document.cookie)&lt;/script&gt;</code>.</p> <p>The impact of this vulnerability is rated as medium, as the malicious script is able to successfully reflect on the host's home page, potentially exposing sensitive information such as cookies. The affected host in this instance is identified as 192.168.14.35. To remediate this vulnerability, it is recommended that input validation is implemented as a means to prevent malicious scripts from being executed. This could include using sanitization techniques, such as encoding user input, to ensure that any malicious scripts are rendered harmless before they are processed by the web application.</p>

<p><b>Images</b></p>	
<p><b>Affected Hosts</b></p>	<p>192.168.14.35</p>
<p><b>Remediation</b></p>	<p>Input Validation to be required</p>

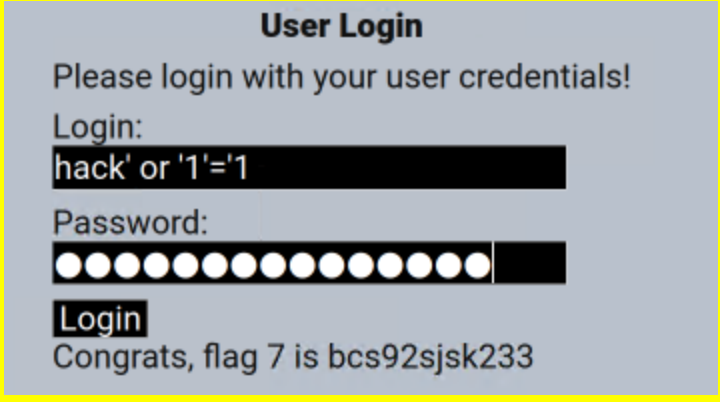
Vulnerability 2	Findings
<p><b>Title</b></p>	<p>Local File Inclusion</p>
<p><b>Type (Web app / Linux OS / Windows OS)</b></p>	<p>Web App</p>
<p><b>Risk Rating</b></p>	<p>Critical</p>
<p><b>Description</b></p>	<p>The findings from this report indicate a critical vulnerability in a web application, specifically a Local File Inclusion (LFI) vulnerability. This type of vulnerability allows an attacker to access sensitive files on the affected system by manipulating the file paths in the web application. In this case, the attacker was able to successfully upload a .php file from the toolbar located on the VR Planner page.</p> <p>The vulnerability has been identified as having a critical risk rating, as the ability to upload files can lead to a variety of malicious actions such as data exfiltration, server takeover, and code execution. The affected hosts in this case have been identified as being located at the IP address 192.168.14.35. To remediate this vulnerability, it is recommended to prevent file paths from being able to be appended directly.</p> <p>Additionally, if possible, restrict the API to allow file inclusion only from a specific directory and the directories below it. This will help to limit the attacker's ability to access sensitive files on the system and will greatly reduce the risk of a successful attack.</p>

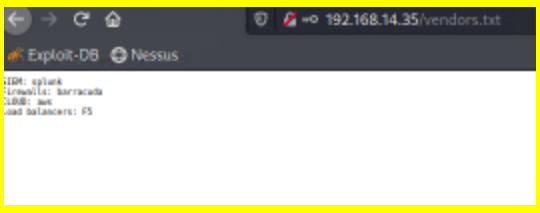
<p><b>Images</b></p>	 <p>&lt;?php phpinfo: ?&gt;</p> <p>Browse: file.php</p>
<p><b>Affected Hosts</b></p>	<p>192.168.14.35</p>
<p><b>Remediation</b></p>	<p>Prevent file paths from being able to be appended directly</p>

Vulnerability 3	Findings
<p><b>Title</b></p>	<p>XSS Stored Type</p>
<p><b>Type (Web app / Linux OS / Windows OS)</b></p>	<p>Web App</p>
<p><b>Risk Rating</b></p>	<p>Critical</p>
<p><b>Description</b></p>	<p>The findings report titled "XSS Stored Type" highlights a critical risk for a web application. The report states that a malicious script, specifically an alert message with the text "Hi", was successfully entered and stored while accessing the /Comments page. This action revealed a flag 3 image on the affected host with an IP address of 192.168.14.35. This type of vulnerability is known as Cross-Site Scripting (XSS) and can allow attackers to inject malicious scripts into web pages viewed by other users. These scripts can steal user data, such as cookies and session tokens, and can also be used to perform actions on behalf of the victim.</p> <p>To mitigate this type of vulnerability, it is important to implement proper input validation and sanitization on all user input. This can include encoding user input to prevent the execution of malicious scripts, and also limiting the types of characters that can be inputted. Additionally, it is important to regularly scan and test the web application for any vulnerabilities, and to also keep all software and libraries up-to-date to ensure that any known vulnerabilities are patched. Overall, a multi-layered approach to security is the best way to prevent XSS attacks and to protect the web application and its users from harm.</p>

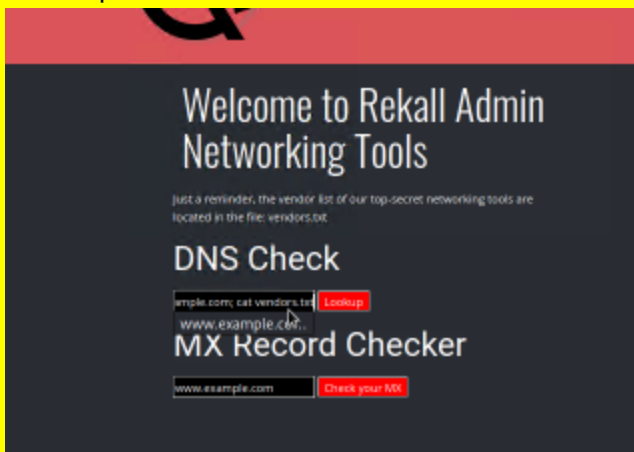
Images	 <script>alert(hacked)</script>
Affected Hosts	192.168.14.35
Remediation	Implement XSS protection to disallow injection of script code

Vulnerability 4	Findings
Title	SQL Injection Type
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	Critical
Description	<p>The findings of a recent security review have revealed a critical vulnerability in a web application, specifically, an SQL Injection. This type of attack occurs when an attacker is able to input malicious code into a web application's SQL statement, allowing them to gain unauthorized access to sensitive information. In this case, the vulnerability was discovered while accessing the /Login.php page, where a payload was entered into the toolbar intended for the password. The exploit was successful and the affected hosts were identified as 192.168.14.35.</p> <p>To remediate this issue, it is important to disallow the web application from accepting direct input and/or implement character escaping. This will prevent attackers from being able to inject malicious code into the SQL statement and limit their ability to gain unauthorized access to sensitive information. Additionally, regular security audits and penetration testing should be conducted to ensure that any future vulnerabilities are quickly identified and addressed. Overall, this vulnerability highlights the importance of implementing robust security measures to protect web applications from potential attacks.</p>

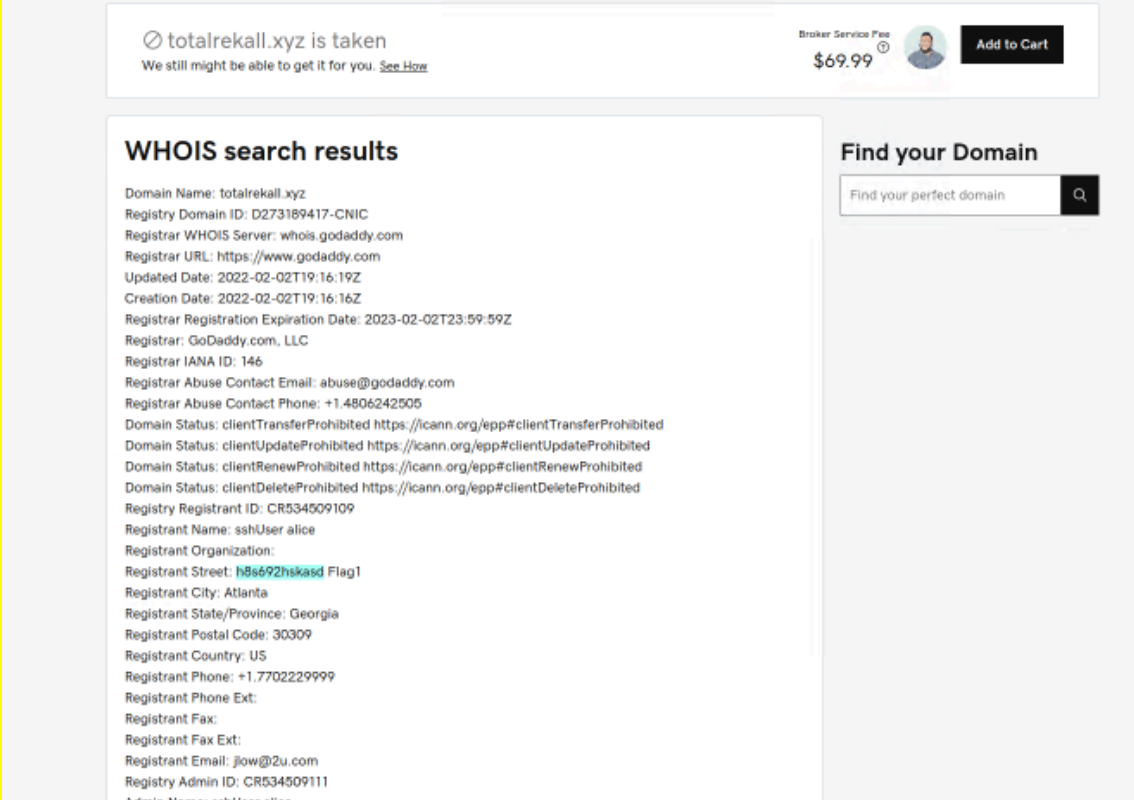
Images	
Affected Hosts	192.168.14.35
Remediation	Disallow the web application from accepting direct input and/or implement character escaping

Vulnerability 5	Findings
Title	Command Injection (Flag 5)
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	Critical
Description	<p>The findings title "Command Injection" highlights a critical vulnerability present in the web application being reviewed. This type of vulnerability, also known as "shell injection" or "OS command injection," allows an attacker to execute arbitrary commands on the host operating system via the web application. In this specific case, the vulnerability was discovered while navigating from the /Networking.php page to the 192.168.14.35/disclaimer.php?page=vendors.txt page via the 192.168.14.35/networking.php page. It was found that an attacker could input "splunk" inside of the toolbar intended for DNS Check, which would allow them to execute arbitrary commands on the host operating system. The affected host in this case is IP address 192.168.14.35.</p> <p>This vulnerability is particularly dangerous because it allows an attacker to gain full control of the host operating system, potentially leading to the theft of sensitive information or the installation of malware. It is important that remediation steps are taken immediately to address this vulnerability. One potential solution would be to validate user input and sanitize any potentially dangerous characters or commands. Another option would be to restrict the capabilities of the web application so that it is unable to execute arbitrary commands on the host operating system.</p>
Images	 <p>192.168.1.35/vendors.txt</p>

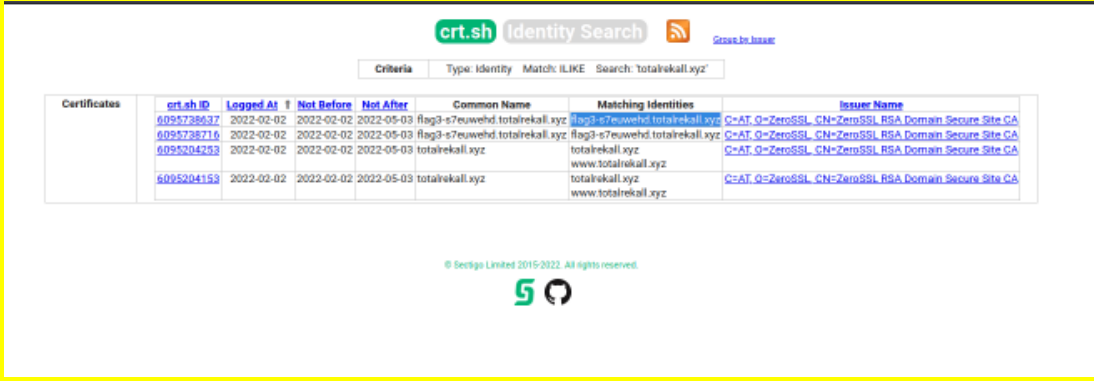


	<p>SIEM: splunk</p>  <p><a href="http://www.example.com">www.example.com</a>; cat vendors.txt</p>
<b>Affected Hosts</b>	192.168.14.35
<b>Remediation</b>	Implement Input Validation

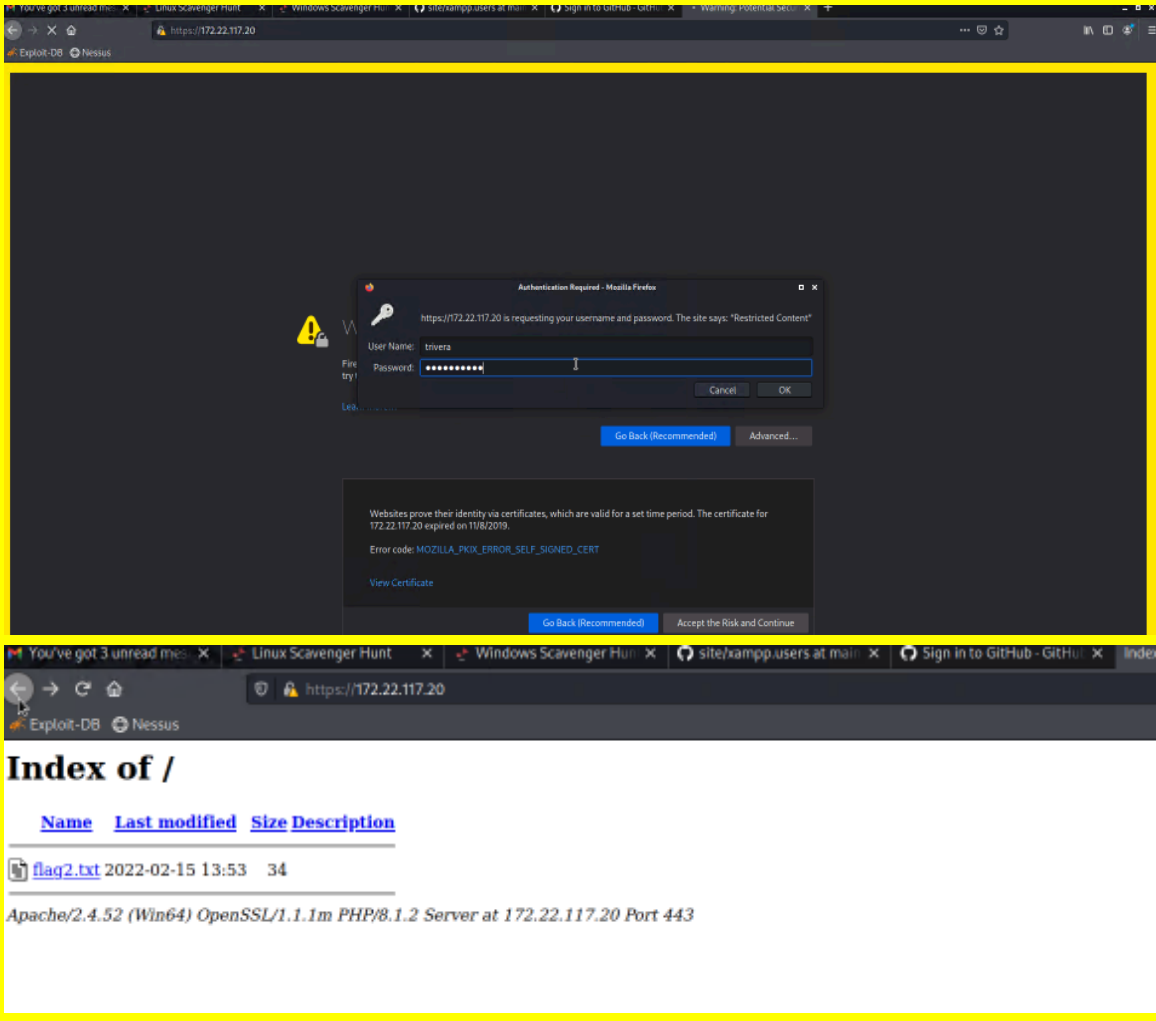
Vulnerability 6	Findings
<b>Title</b>	Open Source Exposed Data (Flag 1)
<b>Type (Web app / Linux OS / Windows OS)</b>	Web App
<b>Risk Rating</b>	Medium
<b>Description</b>	<p>The finding titled "Open source exposed data" highlights a potential risk in the web app with a risk rating of medium. The vulnerability was discovered while viewing WHOIS data on the Domain Dossier webpage, which exposed sensitive information for the domain Total rekall.xyz. The affected host for this vulnerability is <a href="https://centralops.net/co/DomainDossier.aspx">https://centralops.net/co/DomainDossier.aspx</a>.</p> <p>To remediate this vulnerability, it is important to ensure that no sensitive data is being shared publicly. This can be achieved by cleaning up WHOIS records and verifying that all information being shared is appropriate for public viewing. Additionally, regular monitoring of public data sources should be conducted to identify and address any future instances of exposed data. It's also important to note that if the sensitive data exposed is critical enough, it can be used by attackers to launch targeted attacks.</p>

<p><b>Images</b></p>	
<p><b>Affected Hosts</b></p>	<p>rekall.xyz</p>
<p><b>Remediation</b></p>	<p>Ensure no sensitive data is being shared publicly and clean WHOIS records</p>

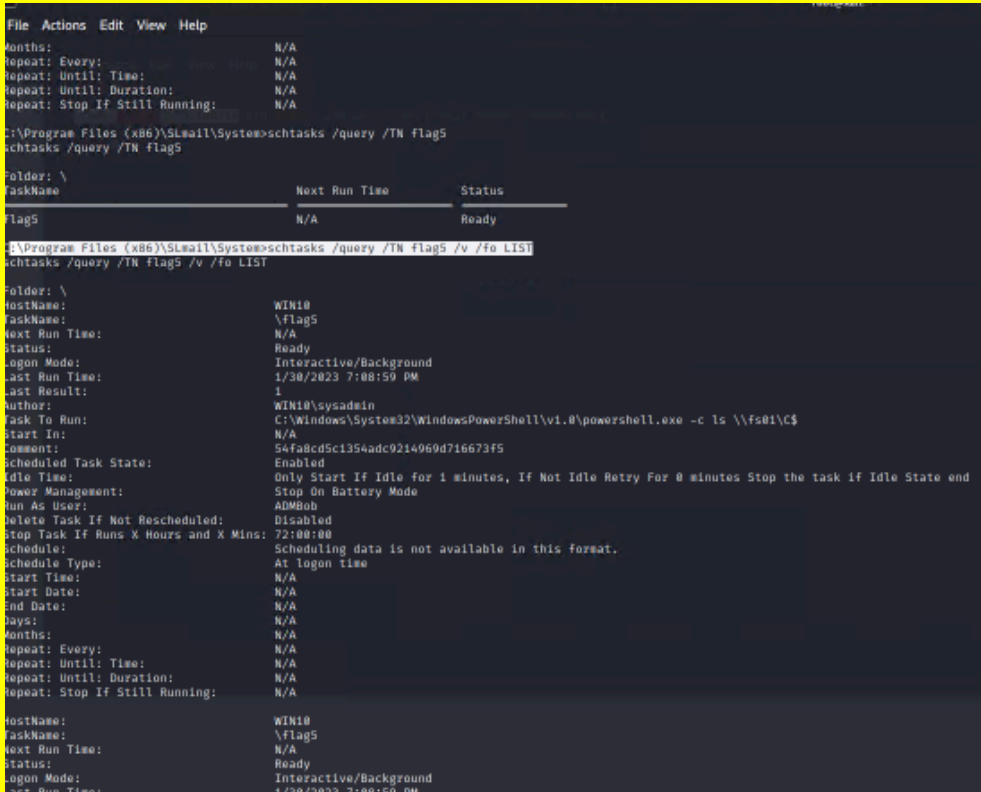
Vulnerability 7	Findings
<p><b>Title</b></p>	<p>Certificate Search (Flag 3)</p>
<p><b>Type (Web app / Linux OS / Windows OS)</b></p>	<p>Web App</p>
<p><b>Risk Rating</b></p>	<p>Medium</p>
<p><b>Description</b></p>	<p>The information provided describes a vulnerability found in a web application through the use of a tool called crt.sh. This tool, known as a certificate search tool, allows users to search for specific certificates stored on a particular domain. In this case, the domain searched for was totalrekall.xyz, and a stored certificate was found.</p> <p>This vulnerability, rated as medium risk, could potentially expose sensitive information stored within the certificate. To mitigate this risk, it is important to ensure that no sensitive information is shared publicly, and to clean up any WHOIS records that may contain sensitive information. Additionally, steps should be taken to protect information from being exposed by the crt.sh site, such as implementing stricter access controls for those who have the ability to search for certificates on the site.</p>

<p><b>Images</b></p>	 <p>The screenshot shows the crt.sh Identity Search interface. The search criteria are set to 'Identity' with a match of 'LIKE' and a search term of 'totalrekill.xyz'. The results table lists certificates with columns for crt.sh ID, Logged At, Not Before, Not After, Common Name, Matching Identities, and Issuer Name. The certificates listed are for 'flag3-s7euwehd.totalrekill.xyz' and 'totalrekill.xyz', all issued by 'C=AT, O=ZeroSSL, CN=ZeroSSL, RSA Domain Secure Site CA'.</p>
<p><b>Affected Hosts</b></p>	<p>34.102.136.180</p>
<p><b>Remediation</b></p>	<p>Protect Information from Being exposed by the crt.sh site.</p>

Vulnerability 8	Findings
<p><b>Title</b></p>	<p>Title Port Scan Of Subnet</p>
<p><b>Type (Web app / Linux OS / Windows OS)</b></p>	<p>Web App</p>
<p><b>Risk Rating</b></p>	<p>Critical</p>
<p><b>Description</b></p>	<p>The information provided describes a critical vulnerability in a web application that allows an attacker to gain access to sensitive information. The vulnerability is related to the use of weak credentials, which can be easily obtained from a Github repository. Once the attacker has gained access to the system, they are able to navigate to a specific file, flag2.txt, which contains the flag. This vulnerability is particularly concerning because it allows an attacker to gain access to sensitive information without needing to go through the usual authentication process.</p> <p>In order to remediate this vulnerability, it is recommended to implement stronger credentials and or 2-factor authentication. This can help to prevent unauthorized access to the system and protect sensitive information from being exposed. Additionally, organizations should also monitor and review their Github repositories for any sensitive information that may be inadvertently exposed. This can help to ensure that credentials and other sensitive information is not being shared publicly, and to take action to remove or restrict access to it if necessary.</p>

<p>Images</p>	 <p>The screenshot shows a web browser window with the address bar displaying 'https://172.22.117.20'. The page content is divided into two sections. The top section shows an 'Authentication Required - Mozilla Firefox' dialog box. The dialog box contains the text: 'https://172.22.117.20 is requesting your username and password. The site says: "Restricted Content"'. Below this, there are input fields for 'User Name' (containing 'trivern') and 'Password' (containing masked characters). There are 'Cancel' and 'OK' buttons. Below the dialog box, there are two buttons: 'Go Back (Recommended)' and 'Advanced...'. The bottom section of the browser window shows a directory listing for 'Index of /'. The listing has columns for 'Name', 'Last modified', 'Size', and 'Description'. There is one entry: 'flag2.txt' with a last modified date of '2022-02-15 13:53' and a size of '34'. Below the listing, there is a text line: 'Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/8.1.2 Server at 172.22.117.20 Port 443'.</p>
<p>Affected Hosts</p>	<p>172.22.117.20</p>
<p>Remediation</p>	<p>Require stronger credentials and or 2-factor authentication</p>

Vulnerability 9	Findings
Title	Machine task scheduler
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	Medium
Description	<p>The following information describes a security vulnerability within a Windows 10 operating system. The risk rating of this vulnerability is medium and it allows for unauthorized access to view details of scheduled tasks. The affected host is identified as 172.22.117.20.</p> <p>One way to address this vulnerability is to change the permissions of accounts to restrict unauthorized access. This could include implementing stricter access controls or limiting the number of accounts that have access to the scheduled tasks feature. Additionally, regular monitoring and auditing of the</p>

	scheduled tasks feature can help detect any unauthorized access attempts and take appropriate action to prevent further breaches.
Images	 <p>The screenshot shows the Windows Task Scheduler interface. A task named 'flag5' is selected. The task is configured to run every day at 7:00 PM. The task is in an 'Enabled' state and is set to run as the user 'WIN10\sysadmin'. The task's logon mode is 'Interactive/Background'. The task's comment is '54fa8cd5c1354adc0214969d716673f5'. The task's scheduled task state is 'Enabled'. The task's idle time is 'Only Start If Idle for 1 minutes, If Not Idle Retry For 0 minutes Stop the task if Idle State end'. The task's power management is 'Stop On Battery Mode'. The task's run as user is 'ADMIN\Bob'. The task's delete task if not rescheduled is 'Disabled'. The task's stop task if runs X hours and X mins is '72:00:00'. The task's schedule is 'Scheduling data is not available in this format.'. The task's schedule type is 'At logon time'. The task's start time is 'N/A'. The task's start date is 'N/A'. The task's end date is 'N/A'. The task's days are 'N/A'. The task's months are 'N/A'. The task's repeat: every is 'N/A'. The task's repeat: until: time is 'N/A'. The task's repeat: until: duration is 'N/A'. The task's repeat: stop if still running is 'N/A'.</p>
Affected Hosts	172.22.117.20
Remediation	Change Permissions of Account to restrict unauthorized access

Vulnerability 10	Findings
Title	Public Directory Search
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	Medium
Description	<p>The Windows OS Risk Rating is Medium, which means that while the vulnerability is not severe, it could still potentially lead to security breaches. The vulnerability is described as being able to navigate to the Users\Public\Documents directory and use the ls command in Meterpreter to display files. The affected host is identified as 172.22.117.20.</p> <p>The remediation for this vulnerability is to move sensitive files to more secure areas and/or restrict unauthorized access. This will prevent attackers from being able to access these files and potentially steal sensitive information. Additionally, it is important to keep the operating system and all software up to date to ensure that any known vulnerabilities are patched and that the system is as secure as possible.</p>

## Images

```
msf5 (root) > shell
msf5preter > shell
Process 4776 created.
Channel 2 created.
Microsoft Windows [Version 10.0.19044.1526]
(c) Microsoft Corporation. All rights reserved.

C:\Program Files (x86)\SLmail\System>cd c:\
cd c:\

c:\>dir
dir
Volume in drive C has no label.
Volume Serial Number is 0014-DB02

Directory of c:\

12/07/2019  01:14 AM    <DIR>          PerfLogs
02/15/2022  05:58 PM    <DIR>          Program Files
03/17/2022  07:22 AM    <DIR>          Program Files (x86)
02/15/2022  02:11 PM    <DIR>          Users
03/07/2022  09:26 AM    <DIR>          Windows
02/15/2022  02:13 PM    <DIR>          xampp
               0 File(s)              0 bytes
               6 Dir(s)  3,416,408,064 bytes free

c:\>cd Users
cd Users

c:\Users>dir
dir
Volume in drive C has no label.
Volume Serial Number is 0014-DB02

Directory of c:\Users

02/15/2022  02:11 PM    <DIR>          .
02/15/2022  02:11 PM    <DIR>          ..
07/13/2022  09:08 AM    <DIR>          ADMINBob
02/15/2022  10:15 AM    <DIR>          Public
03/17/2022  07:13 AM    <DIR>          sysadmin
               0 File(s)              0 bytes
               5 Dir(s)  3,416,408,064 bytes free

c:\Users>cd Public
cd Public

c:\Users\Public>ls
ls
'ls' is not recognized as an internal or external command,
operable program or batch file.

c:\Users\Public>dir
dir
Volume in drive C has no label.
Volume Serial Number is 0014-DB02

Directory of c:\Users\Public
```

	<pre>cd Users c:\Users&gt;dir dir Volume in drive C has no label. Volume Serial Number is 0014-DB02  Directory of c:\Users  02/15/2022  02:11 PM  &lt;DIR&gt;          . 02/15/2022  02:11 PM  &lt;DIR&gt;          .. 07/13/2022  09:08 AM  &lt;DIR&gt;          ADMBob 02/15/2022  10:15 AM  &lt;DIR&gt;          Public 03/17/2022  07:13 AM  &lt;DIR&gt;          sysadmin                0 File(s)              0 bytes                5 Dir(s)  3,416,408,064 bytes free  c:\Users&gt;cd Public cd Public  c:\Users\Public&gt;ls ls 'ls' is not recognized as an internal or external command, operable program or batch file.  c:\Users\Public&gt;dir dir Volume in drive C has no label. Volume Serial Number is 0014-DB02  Directory of c:\Users\Public  02/15/2022  10:15 AM  &lt;DIR&gt;          . 02/15/2022  10:15 AM  &lt;DIR&gt;          .. 02/15/2022  02:02 PM  &lt;DIR&gt;          Documents 12/07/2019  01:14 AM  &lt;DIR&gt;          Downloads 12/07/2019  01:14 AM  &lt;DIR&gt;          Music 12/07/2019  01:14 AM  &lt;DIR&gt;          Pictures 12/07/2019  01:14 AM  &lt;DIR&gt;          Videos                0 File(s)              0 bytes                7 Dir(s)  3,416,399,872 bytes free  c:\Users\Public&gt;cd Documents cd Documents  c:\Users\Public\Documents&gt;dir dir Volume in drive C has no label. Volume Serial Number is 0014-DB02  Directory of c:\Users\Public\Documents  02/15/2022  02:02 PM  &lt;DIR&gt;          . 02/15/2022  02:02 PM  &lt;DIR&gt;          .. 02/15/2022  02:02 PM                32 flag7.txt                1 File(s)              32 bytes                2 Dir(s)  3,416,399,872 bytes free  c:\Users\Public\Documents&gt;</pre>
Affected Hosts	172.22.117.20
Remediation	Move sensitive files to more secure areas and/or restrict unauthorized access