Cybersecurity

Penetration Test Report

Rekall Corporation

Penetration Test Report

Confidentiality Statement

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

Table of Contents

Contact Information

Company Name	MongoFlow Incorporated
Contact Name	Robert Russell
Contact Title	Project Manager

Document History

Version	Date	Author(s)	Comments
001	01/11/2024	Robert Russell	Logging screenshots during the web browser vulnerability testing
002	01/17/2024	Robert Russell	Logging screenshots during the Linux OS vulnerability testing
003	01/18/2024	Robert Russell	Logging screenshots during the Windows OS vulnerability testing
004	01/20/2024	Robert Russell	Executive Summary + Vulnerability Findings
005	01/21/2024	Robert Russell	Executive Summary + Vulnerability Findings
006	01/22/2024	Robert Russell	Executive Summary + Vulnerability Findings
007	01/23/2024	Robert Russell	Revision

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 a perspective of the network's 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 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.

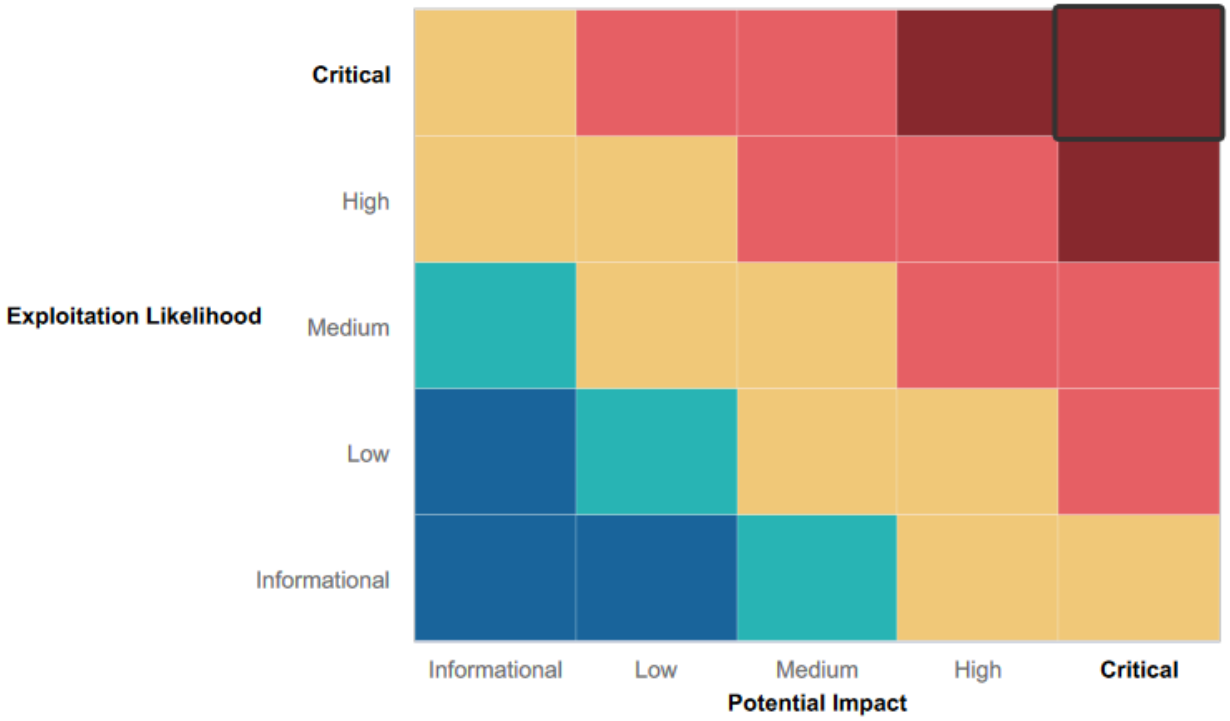
Executive Summary of Findings

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.

- Credentials to the Linux OS were well protected outside the one leaked on GitHub.
- Some input validation was already in place on the web server.
- An Nmap scan showed most ports to be closed.

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.

- XXS Scripting appeared when successfully attempting to exploit the free-text entry fields on all qualifying web browser pages. Notably Reflected XXS and Stored XXS were found.
- Sensitive information in a PHP file can be read publicly by simply retrieving the information through a command line.
- Sensitive information can be discovered in the public HTML source code of the login page.
- Sensitive information can be accessed by typing the correct file name into the URL entry field.
- Malicious PHP scripts can be uploaded on the page "Memory-Planner.php".
- The admin's username and password are internet-facing on the page which gives the option to login as an admin.
- Input validation and sanitization are feeble to a breadth of malicious characters that can be utilized in a command injection for various purposes.
- Sessions can be hijacked through free tools like BurpSuite. There appears to be no time-out or maximum user limits to a single session.
- The server can be initially hacked via port 80 of the Drupal Server linked to 192.168.13.12.
- Drupal is running on an outdated version of Apache Struts making it vulnerable to an RCE in the Jakarta Multipart Parser OGNL Injection.
- Apache Tomcat is outdated. Making it vulnerable to RCE.
- Apache Struts is outdated.
- Drupal is outdated.
- A sudo exploit allows any admin with lower privileges to access root commands. Refer to CV-2019-14287 for more information.

Executive Summary

MongoFlow uncovered a significant amount of vulnerabilities to the Rekall Corporation’s network security, which compromises its confidentiality, integrity, and availability of sensitive information. The following were of most importance, but do not encapsulate the breadth of vulnerabilities uncovered: admin credentials and user credentials exposed, weak input validation, serer exploitation, remote code execution exploitation, local file inclusion, sudo exploit, and session hijacking. Many critical threats are live and exposed, but the good news is multiple can be remediated through updating to the current versions of the respective software. Others merely require buffering access security and transferring sensitive information to more secure locations. Failure to address these issues swiftly and immediately could expose Rekall Corporation to compromising risks and loss of company assets.

Summary Vulnerability Overview

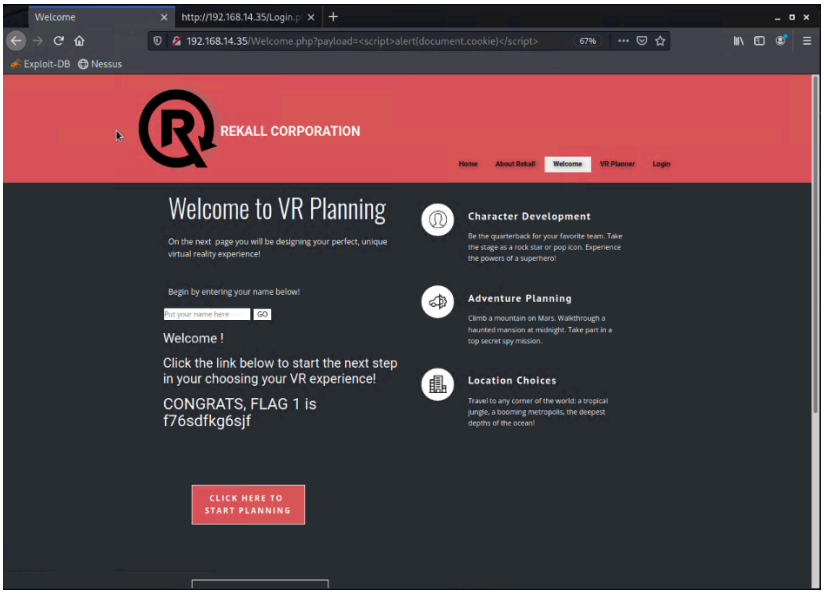
	Vulnerability	Severity
1	XXS Reflected	Medium
2	XXS Stored	Medium
3	Sensitive Data Exposure (Command Line ‘curl’)	Critical
4	Local File Inclusion	High
5	Sensitive Data Exposure (HTML)	Critical
6	Sensitive Data Exposure (URL)	Critical
7	Command Injection	High
8	Brute Force Attack	Medium
9	PHP Injection	High
10	Session Management	High
11	Apache Tomcat Remote Code Execution	Critical
12	Apache Struts Remote Code Execution	Critical
13	Drupal Remote Code Execution	Critical
14	Sudo Security Vulnerability	Medium
16	Exposed Credentials	High
17	Anonymous FTP Session Open	Critical
18	Emails Accessible	Medium

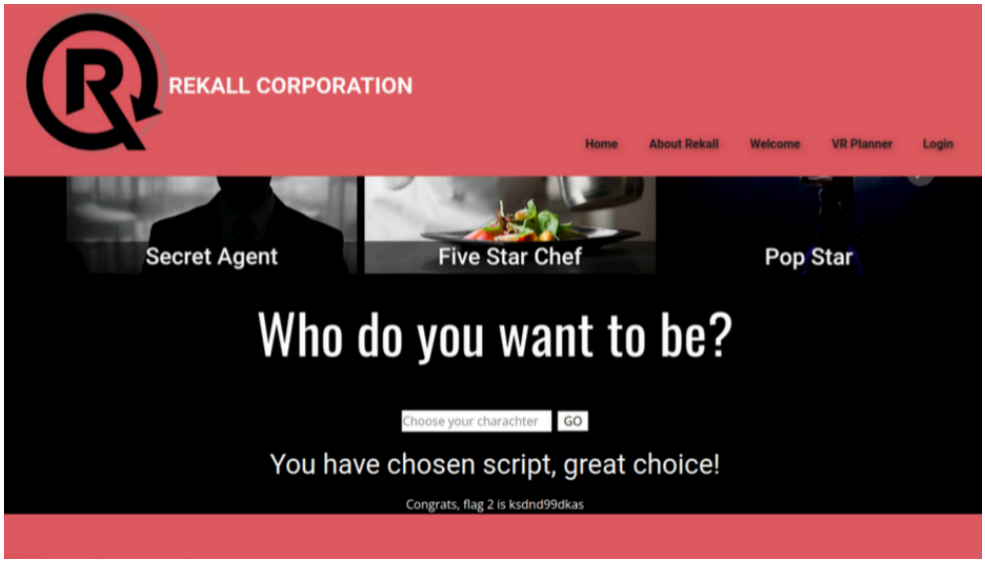
The following summary tables represent an overview of the assessment findings for this penetration test:

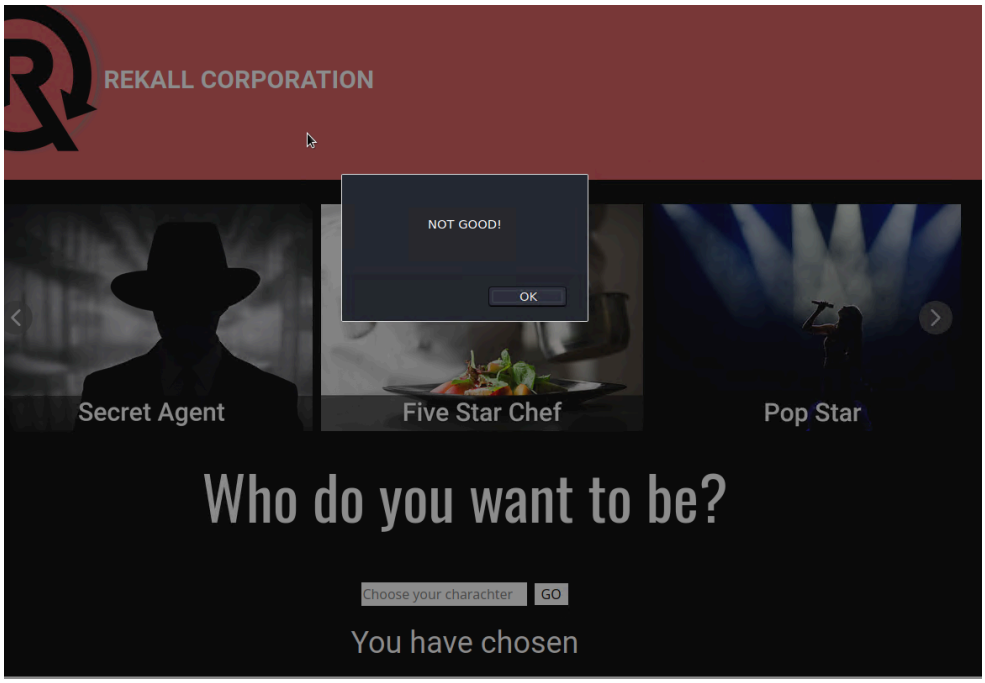
Scan Type	Total
Hosts	7
Ports	5

Exploitation Risk	Total
Critical	7
High	5
Medium	5
Low	0

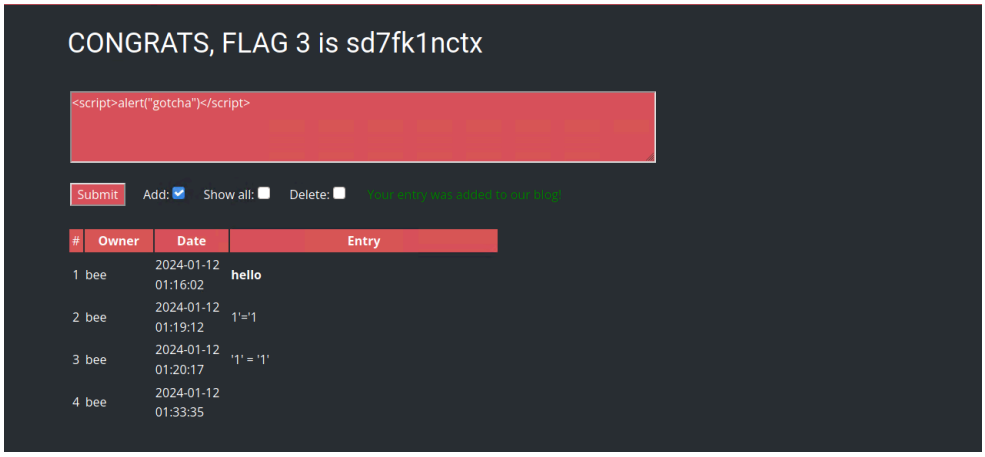
Vulnerability Findings

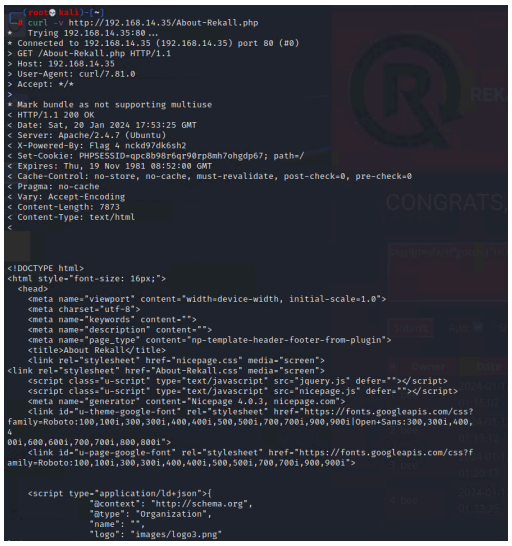
Vulnerability 1	Findings
Title	XXS Reflected
Type (Web app / Linux OS / WIndows OS)	Web Application
Risk Rating	Medium
Description	Picture 1: Type in '<script>alert("hi")</script>' to the free-text entry search box. The prompt triggers an unintended response from the web browser. Picture 2: Type in '<SCRIPscriptT>alert("NOT GOOD!")</SCRIPscriptT>' to the free-text entry search box. The prompt triggers an unintended pop-up.
Images	



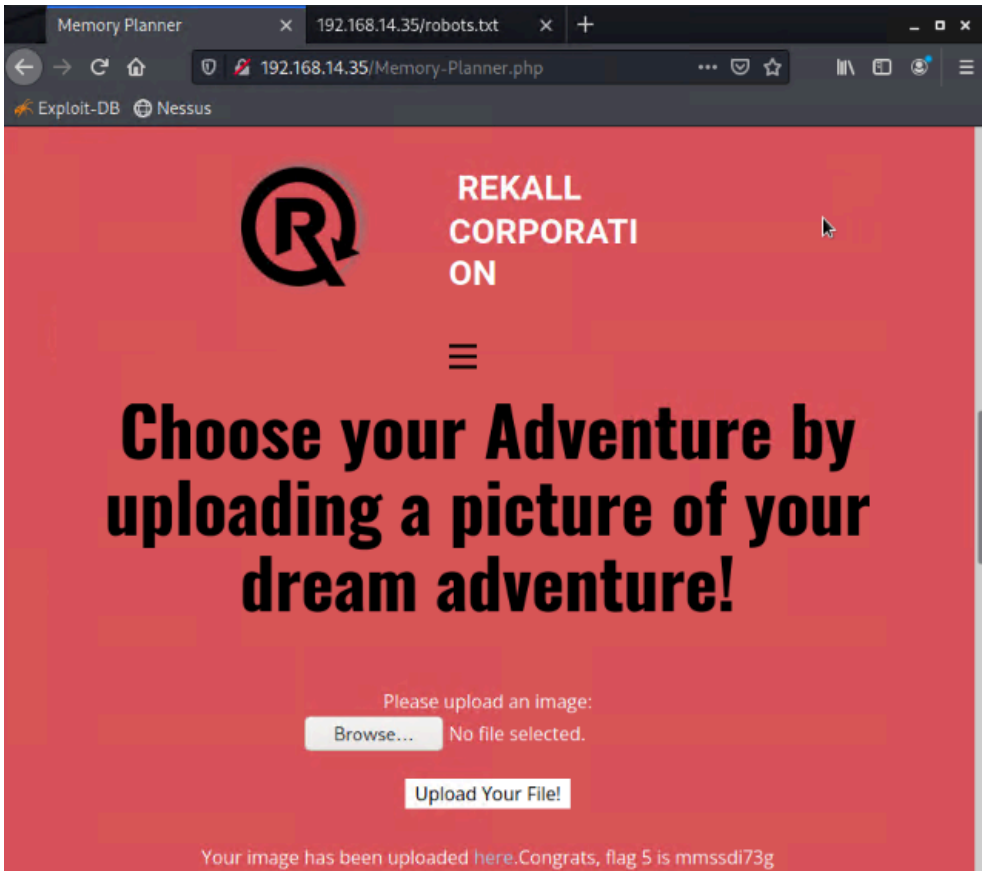


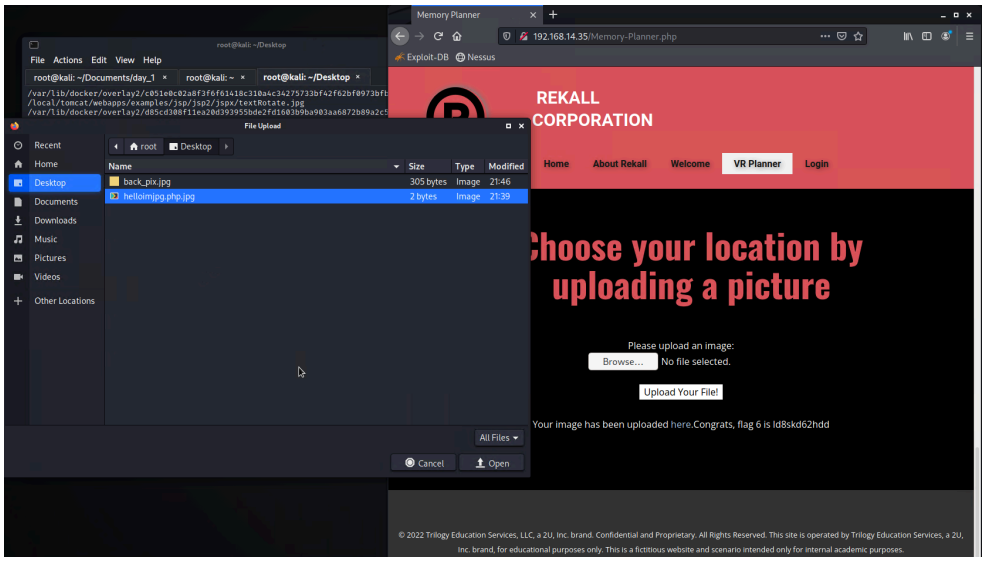
Affected Hosts	192.168.14.35
Remediation	Input Validation and Output Coding

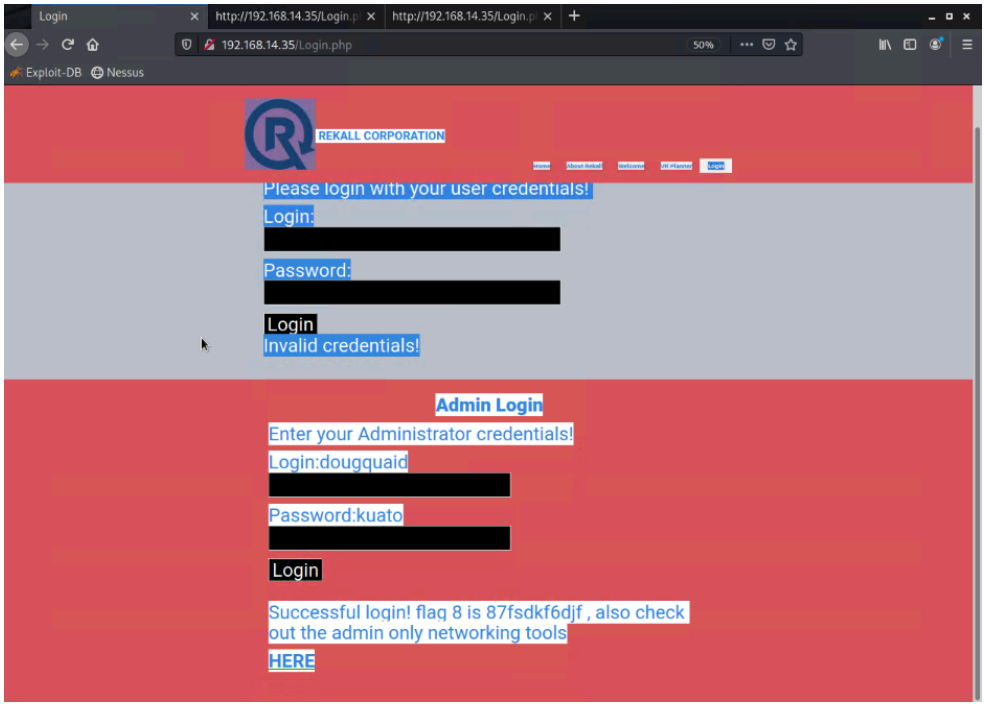
Vulnerability 2	Findings
Title	XXS Stored
Type (Web app / Linux OS / WIndows OS)	Web Application
Risk Rating	Medium
Description	Malicious script can be stored inside the target database from where a comment submission retrieves data.
Images	
Affected Hosts	192.168.14.35
Remediation	Output Encoding

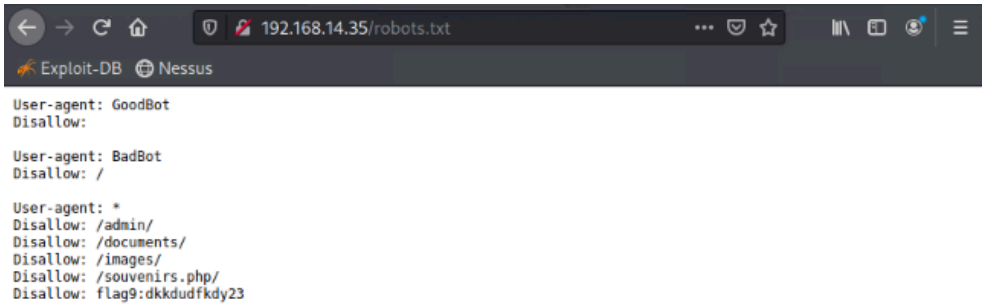
Vulnerability 3	Findings
Title	Sensitive Data Exposure Through ‘Curl’
Type (Web app / Linux OS / WIndows OS)	Web Application
Risk Rating	Critical
Description	The client can read the server-side script by simply curling the .php script through port 80 on the command line. ‘curl -v http://192.168.14.35/About-Rekall.php’
Images	 

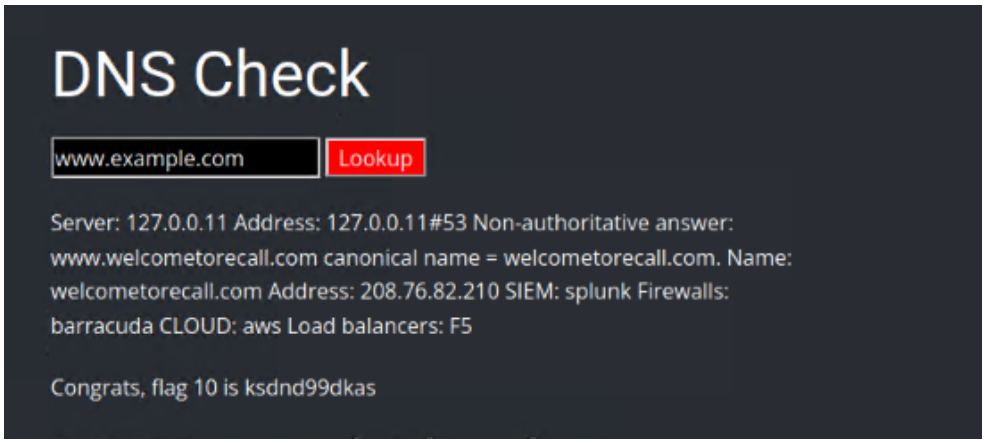
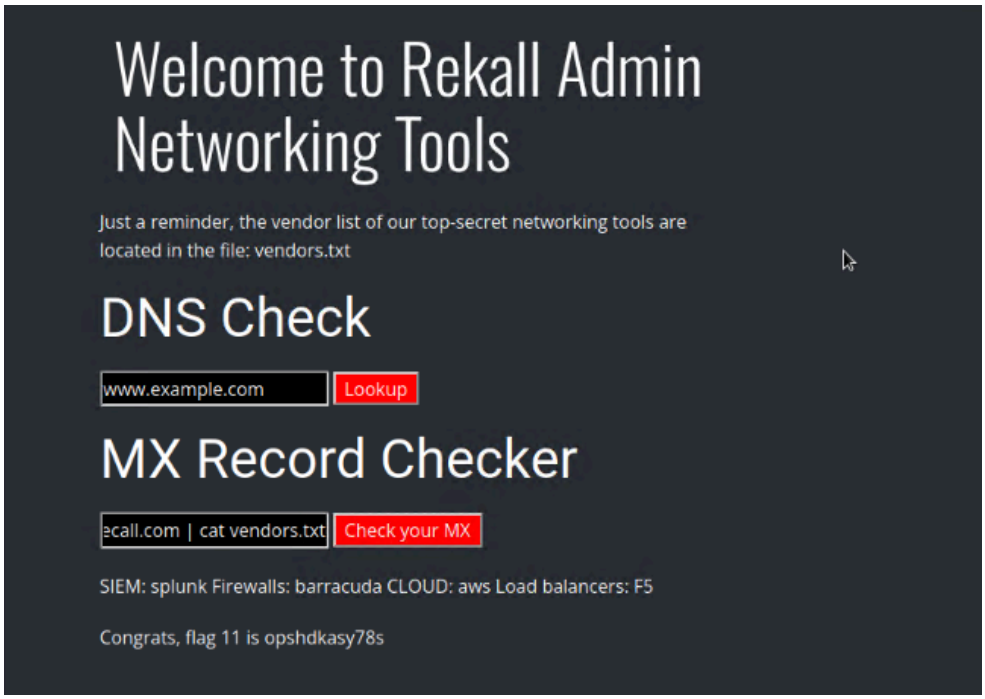
Affected Hosts	192.168.14.35
Remediation	Update API keys to control access to the sensitive information

Vulnerability 4	Findings
Title	Local File Inclusion
Type (Web app / Linux OS / WIndows OS)	Web Application
Risk Rating	High
Description	A PHP file can be uploaded into the first text input field A PHP file can be uploaded into the second text input field by including ".jpg" in the file's name.
Images	

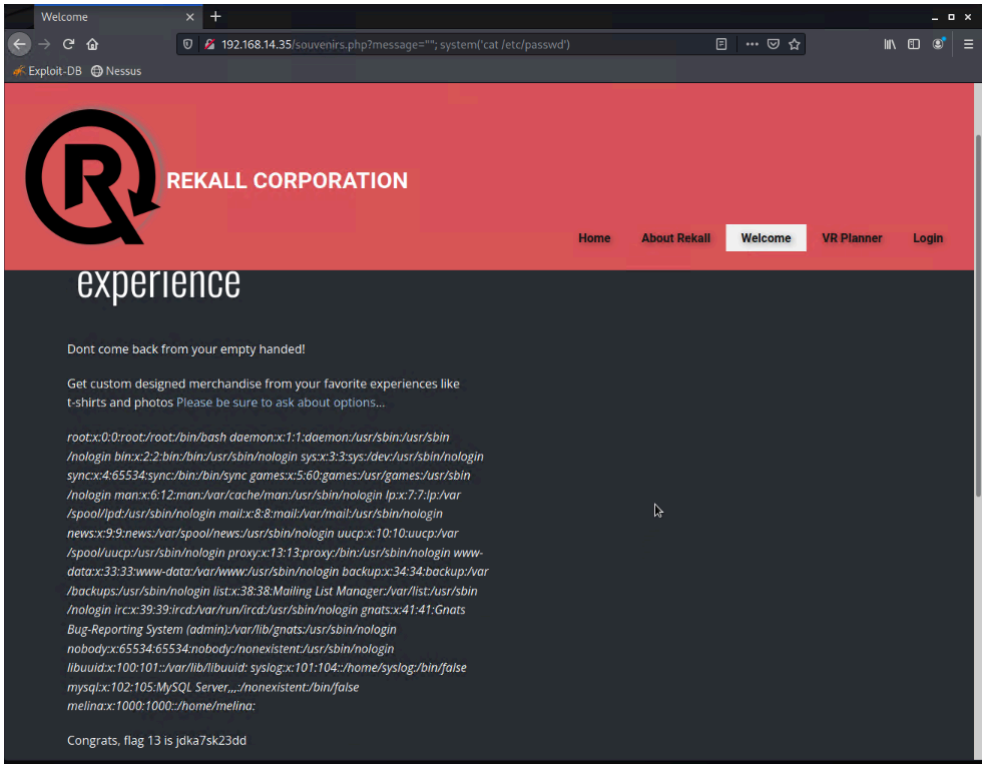
	
Affected Hosts	192.168.14.35
Remediation	File Upload Validation

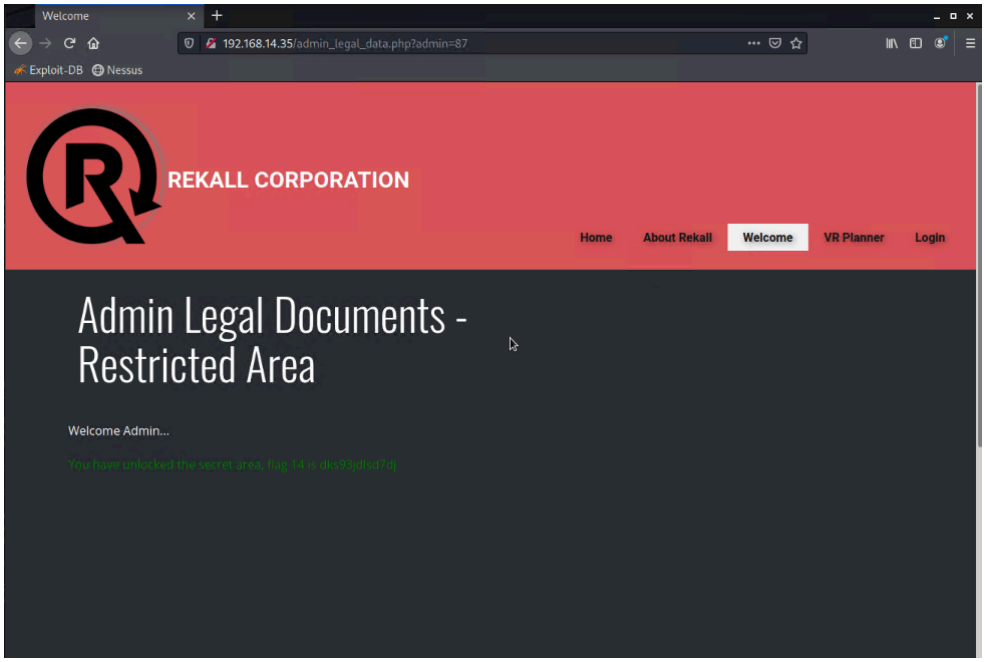
Vulnerability 5	Findings
Title	Sensitive Data Exposure through HTML Source Code
Type (Web app / Linux OS / WIndows OS)	Web Application
Risk Rating	Critical
Description	The admin username and password are visible within the internet-facing HTML code.
Images	
Affected Hosts	192.168.14.35
Remediation	Remove the text from the internet-facing HTML code

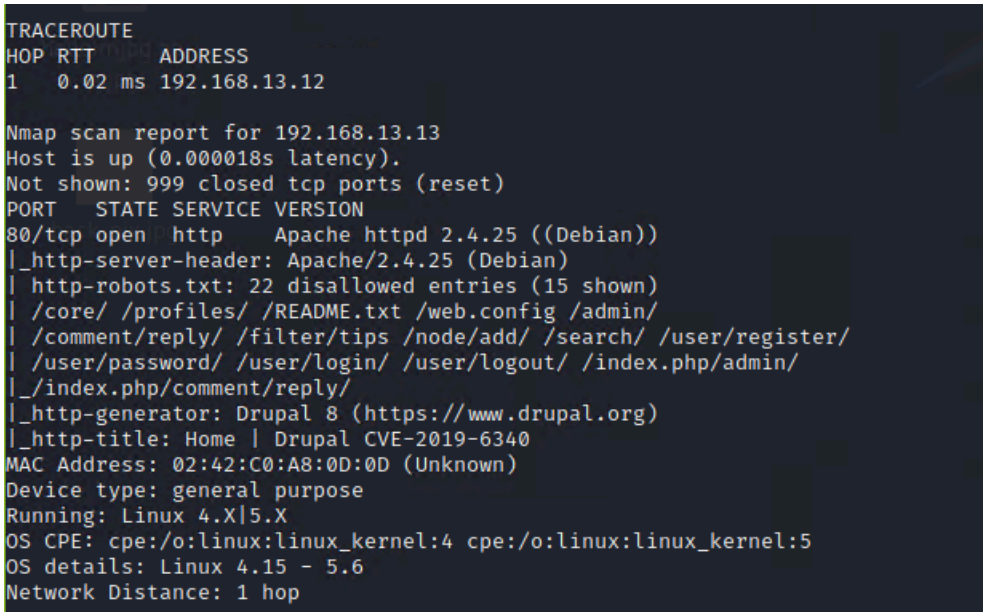
Vulnerability 6	Findings
Title	Sensitive Data Exposure through the URL
Type (Web app / Linux OS / WIndows OS)	Web Application
Risk Rating	Critical
Description	Access to ‘robots.txt’ file by typing the name into the URL
Images	
Affected Hosts	192.168.14.35
Remediation	Remove Sensitive Files from Internet-Facing Data Storage

Vulnerability 7	Findings
Title	Command Injection
Type (Web app / Linux OS / WIndows OS)	Web Application
Risk Rating	High
Description	No input validation restrictions. ‘www.welcometorecall.com && cat vendors.txt’ and ‘www.welcometorecall.com ; cat vendors.txt’ both gain access to the vendors.txt file. In the MX Record Checker, input validation denies “&” and “;”, but “|” can still be used. ‘www.welcometorecall.com | cat vendors.txt’
Images	 
Affected Hosts	192.168.14.35
Remediation	Stronger Input Validation To Remove All Known Malicious Characters

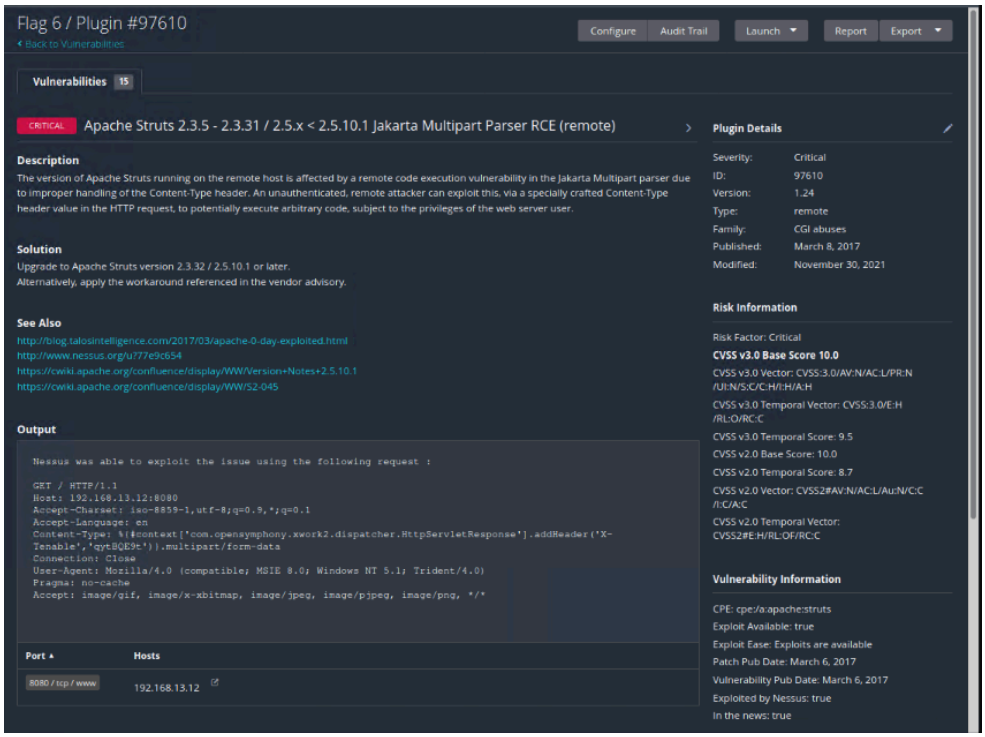
Vulnerability 8	Findings
Title	Brute Force Attack
Type (Web app / Linux OS / WIndows OS)	Web Application
Risk Rating	Medium
Description	The command injection '.... | cat '/etc/vendors.txt' summons sensitive information, such as the username and password of a user.
Images	
Affected Hosts	192.168.14.35
Remediation	Input Validation and Deescalate User Privilege

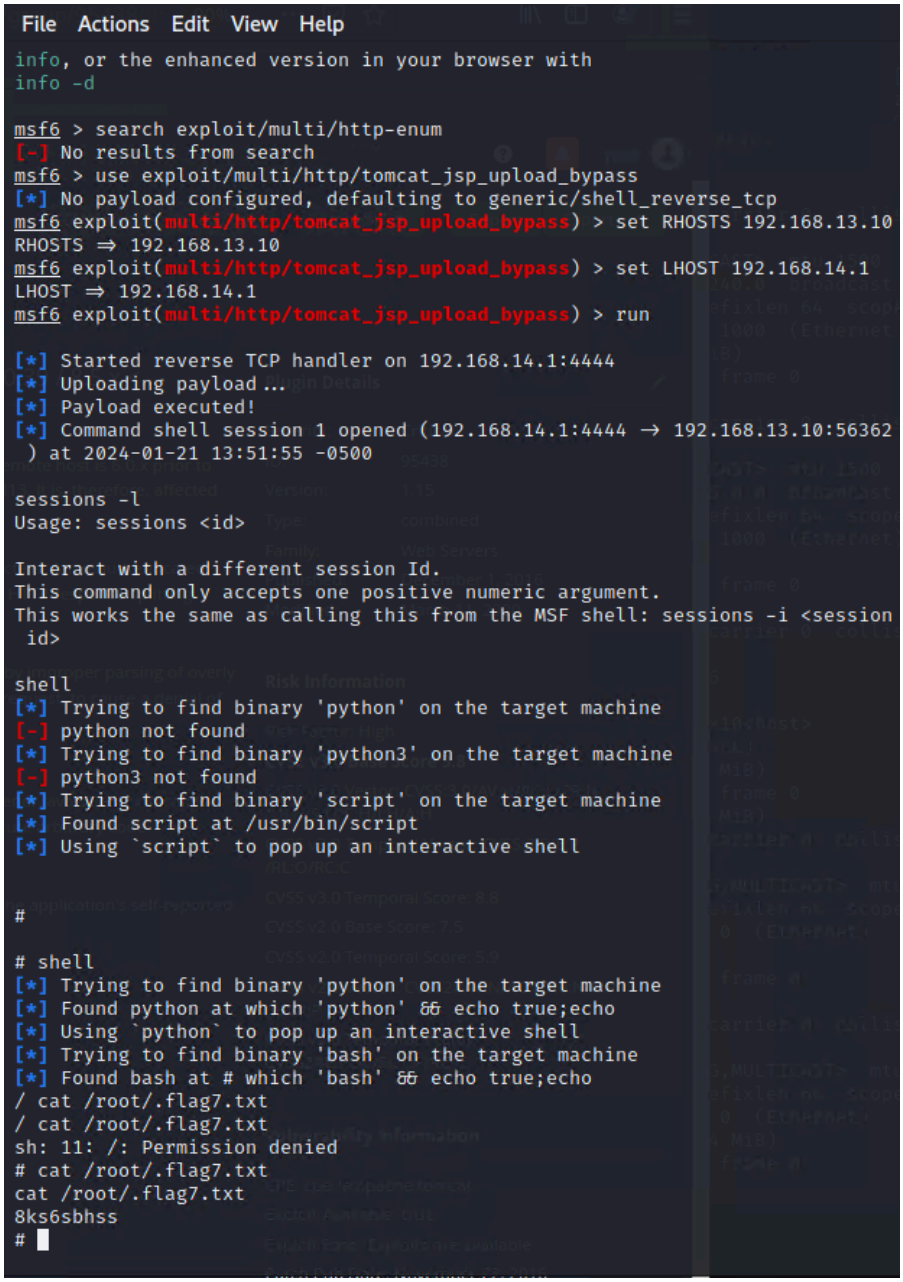
Vulnerability 9	Findings
Title	PHP Injection
Type (Web app / Linux OS / WIndows OS)	Web Application
Risk Rating	High
Description	The aforementioned exposed robots.txt file exposed a hidden PHP file called souvenirs.php. Throa command injection in the URL, the /etc/vendors.txt file can be summoned.
Images	
Affected Hosts	192.168.14.35
Remediation	Input Validation and Sanitation. Remove Backend Files From The Internet-Facing Database.

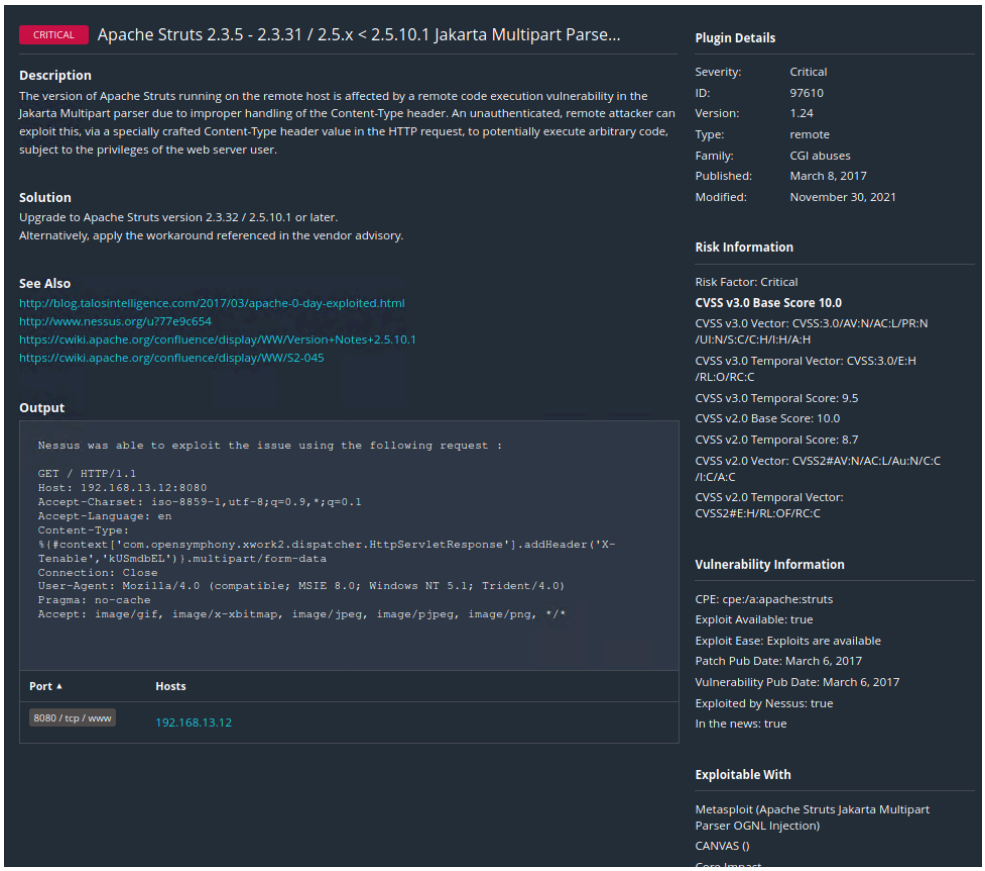
Vulnerability 10	Findings
Title	Session Managment
Type (Web app / Linux OS / WIndows OS)	Web Application
Risk Rating	High
Description	Sessions Can Be Hijacked
Images	
Affected Hosts	192.168.14.35
Remediation	Sessions Adherence Policies.

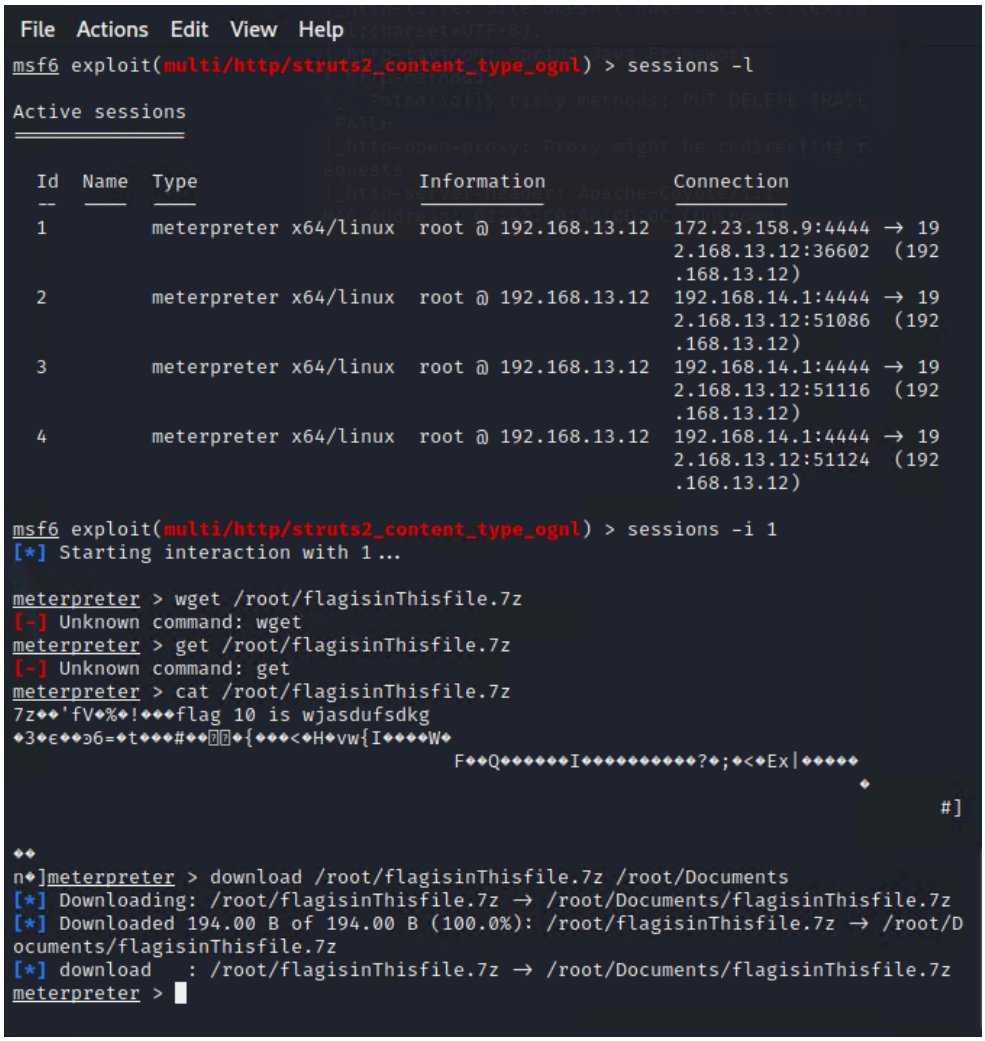
Vulnerability 11	Findings
Title	Remote Code Execution
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	According to the Nessus Scan Report, “The version of Apache Struts running on the remote host is affected by a remote code execution vulnerability in the Jakarta Multipart parser due to improper handling of the Content-Type header. An unauthenticated, remote attacker can exploit this, via a specifically crafted Content-Type header value in the HTTP request, to potentially execute arbitrary code, subject of the privileges of the web server user.”
Images	

```
TRACEROUTE
HOP RTT     ADDRESS
1   0.02 ms 192.168.13.12

Nmap scan report for 192.168.13.13
Host is up (0.000018s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.25 ((Debian))
|_http-server-header: Apache/2.4.25 (Debian)
| http-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
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
```

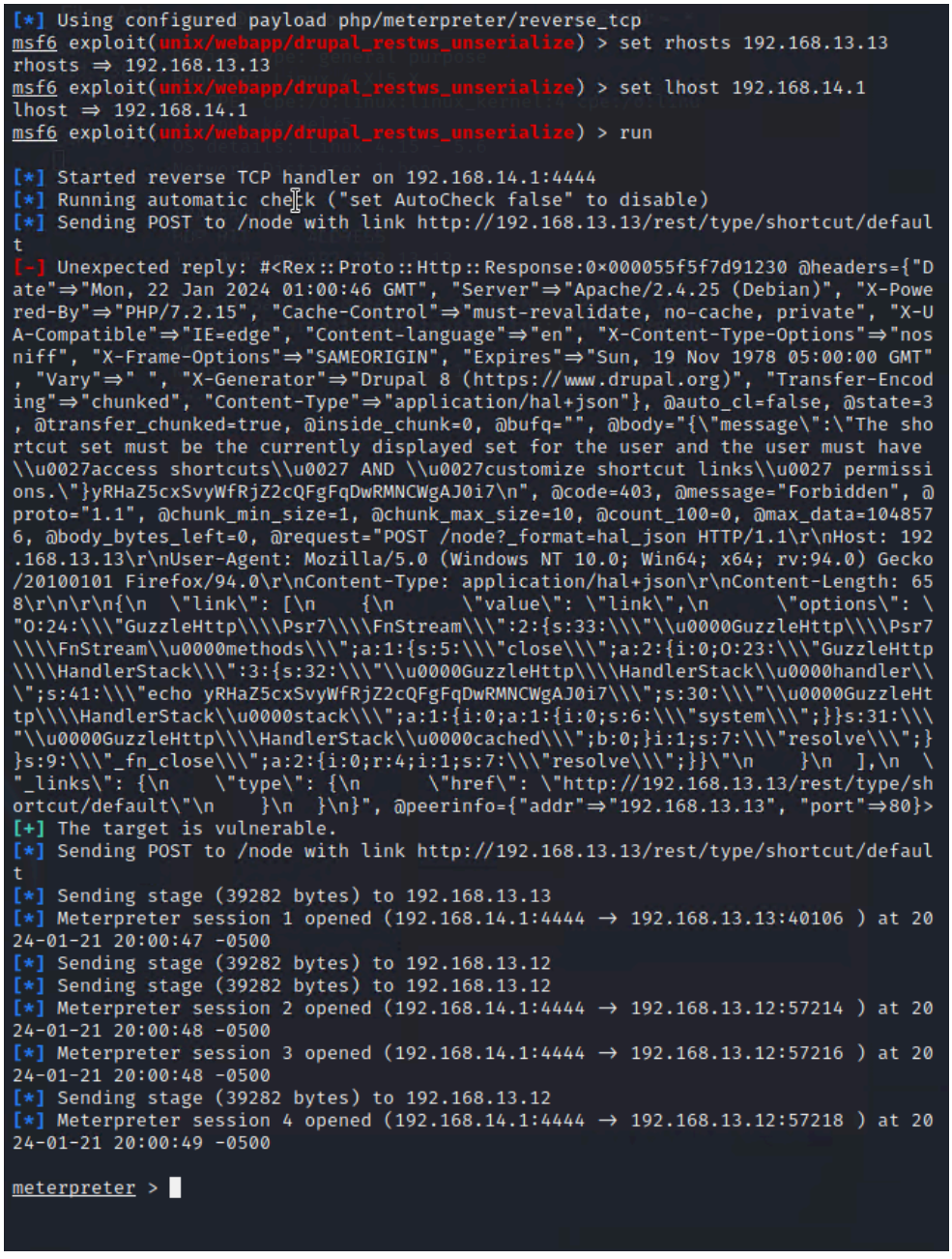
	
Affected Hosts	192.168.13.12
Remediation	Upgrade to the Latest Software Version an Secure Permissions.

Vulnerability 12	Findings
Title	Apache Tomcat Remote Code Execution Vulnerability (CVE-2017-12617)
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	Apache Tomcat Is Outdated. Making it Vulnerable to a JSP (JavaServer Pages) payload to hijack a session.
Images	
Affected Hosts	Apache Tomcat
Remediation	Upgrade to Apache Tomcat Version 8.5.68 or Later

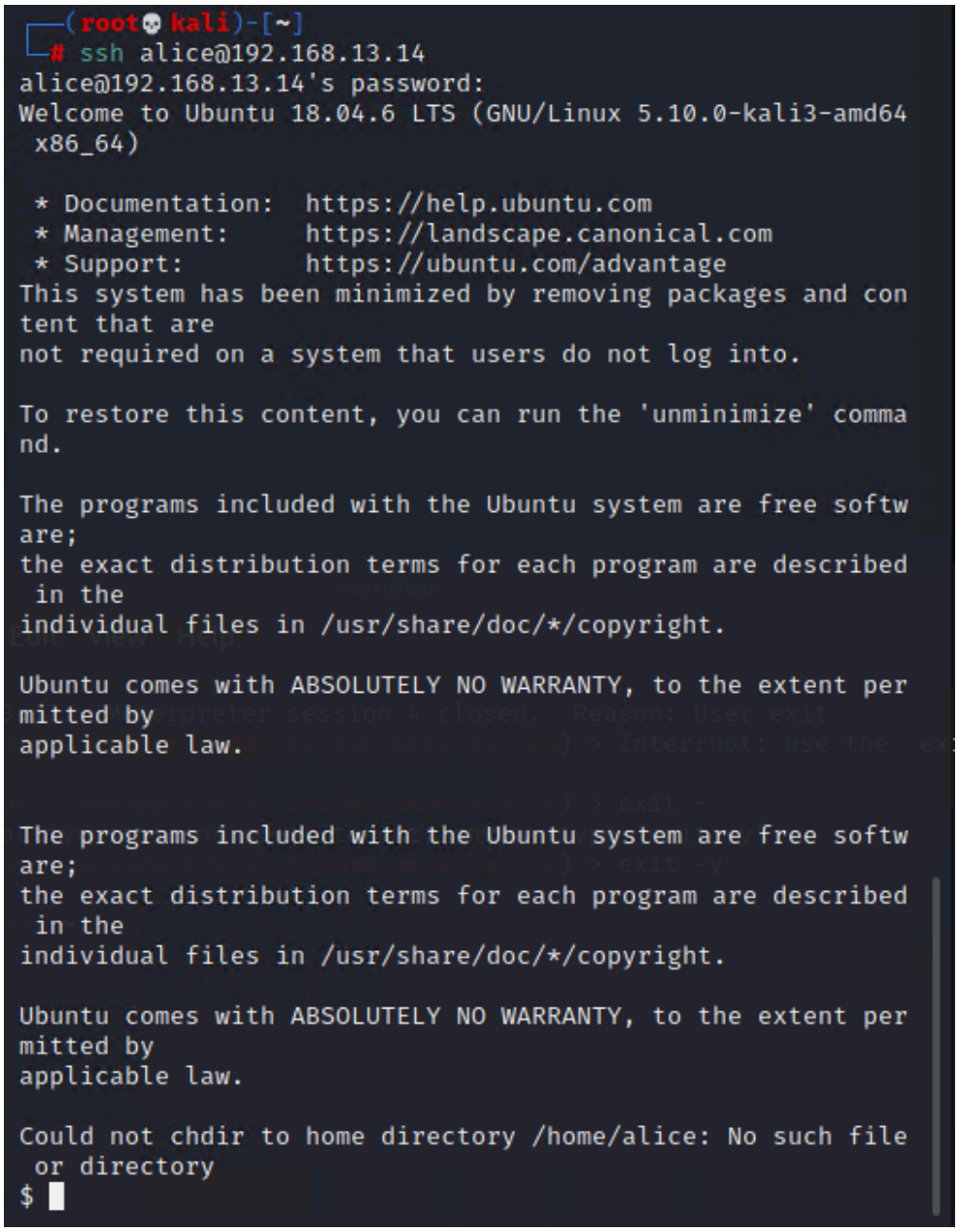
Vulnerability 14	Findings
Title	Struts Remote Code Execution Vulnerability (CVE-2017-5638)
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	The current version of Apache Struts is outdated. A specially crafted Content-Type header in the HTTP request can potentially execute malicious code.
Images	

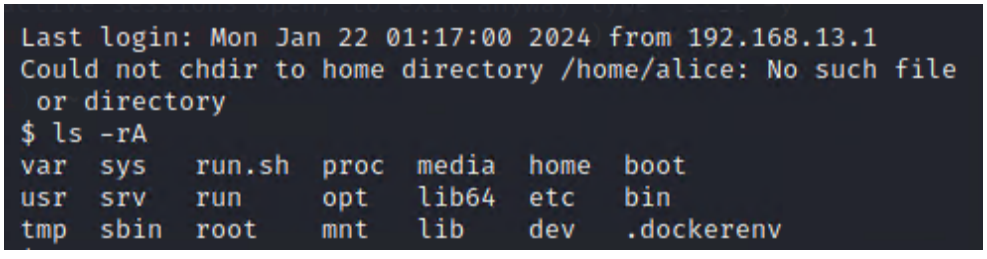


Affected Hosts	192.168.13.12
Remediation	Upgrade to Apache Struts Version 2.3.32/2.5.10.1 or Later

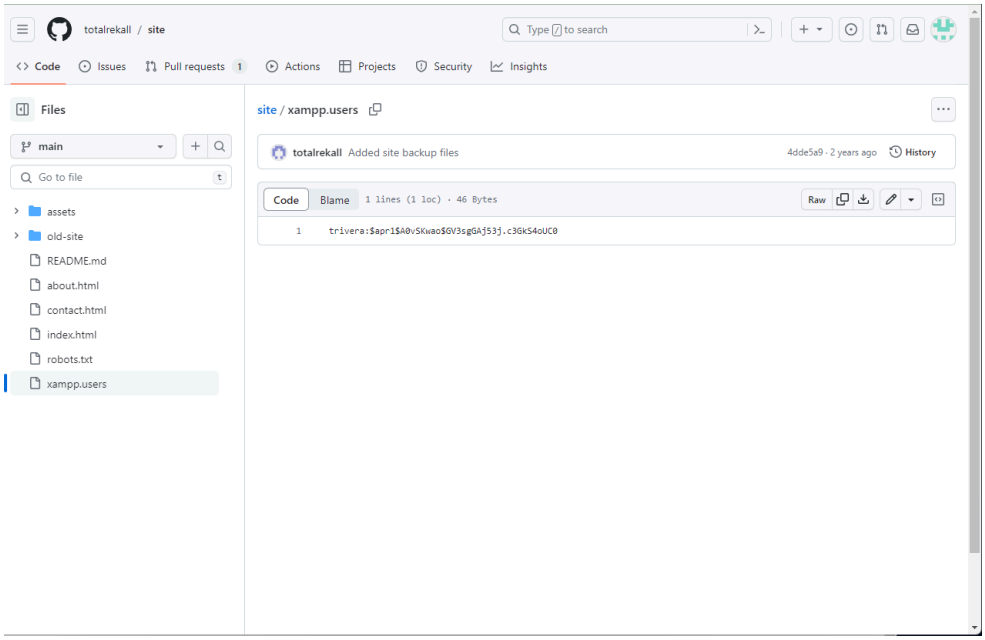
Vulnerability 15	Findings
Title	Drupal Through Port 80 (CVE-2019-6340)
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	Arbitrary Remote Code Execution on The Drupal Server.
Images	
Affected Hosts	192.168.13.12
Remediation	Upgrade to Drupal 8.6.10 or Later

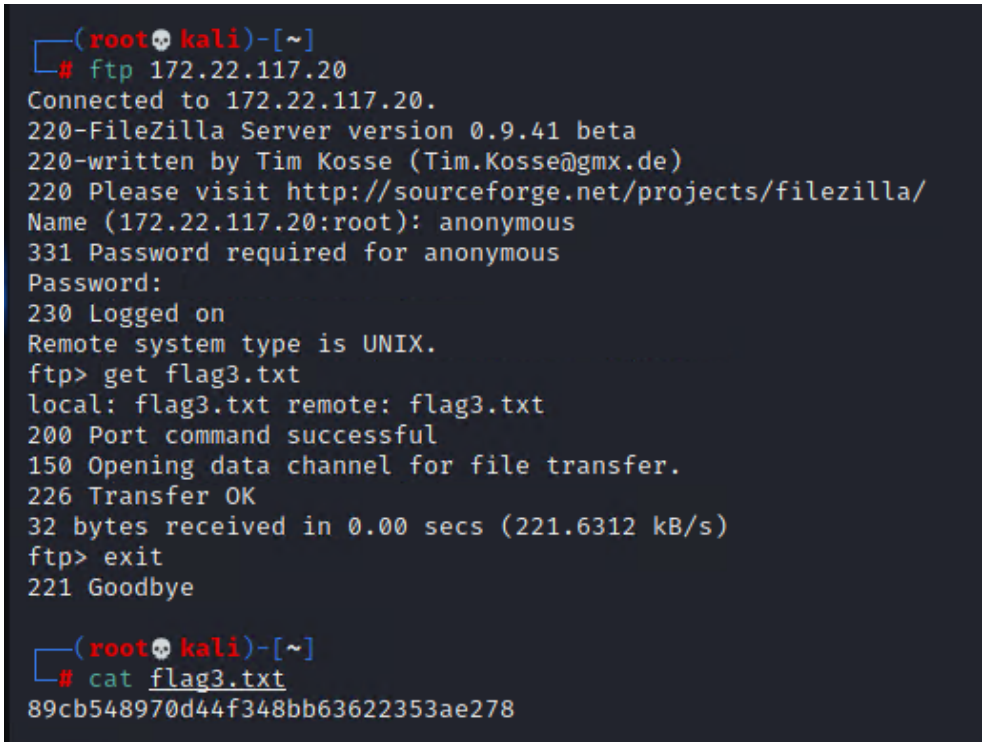
Vulnerability 16	Findings
Title	Sudo Vulnerability (CV-2019-14287)
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Medium
Description	A sudoer issue when the sysadmin enters something into the sudoer's file. All values then parse incorrectly; exposing a command to run as root.
Images	

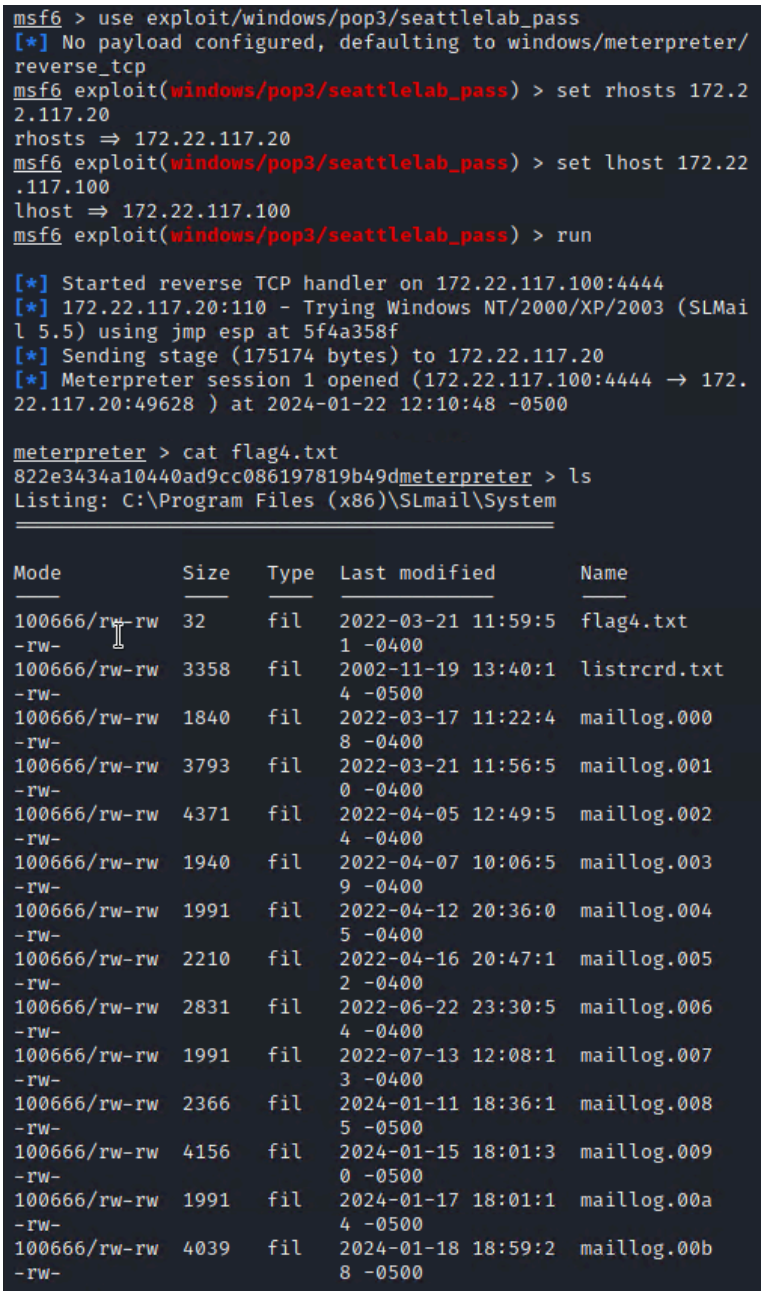


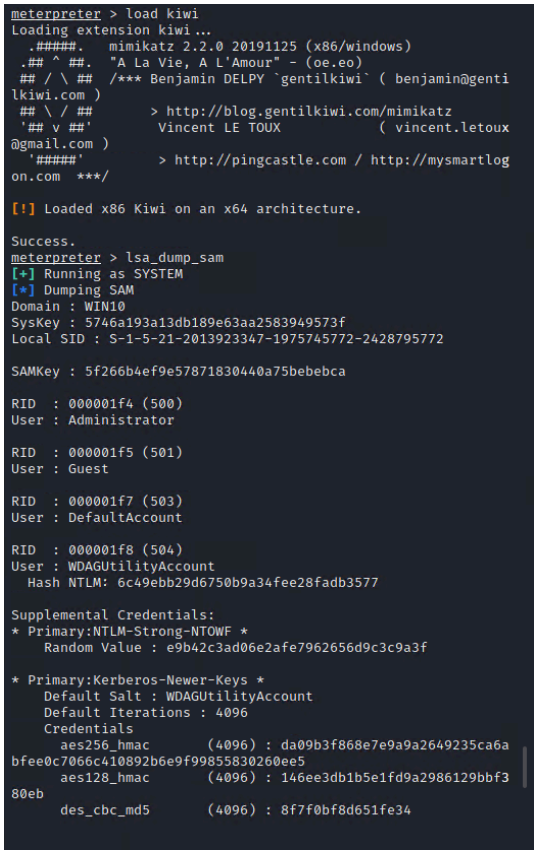


Affected Hosts	Linux OS User and Root
Remediation	Examine each sudoer entry in etc/sudoers and /etc/sudoers.d with a ‘!’ character in the “runas” specification.

Vulnerability 17	Findings
Title	Exposed Credentials
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	High
Description	A user hash was discovered publicly on the GitHub repository path “totalrekall/site/blob/main/xampp.users”
Images	 
Affected Hosts	172.22.117.20
Remediation	Remove the hash from a public repository.

Vulnerability 18	Findings
Title	Anonymous FTP Session Open
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Critical
Description	An Nmap scan of 172.22.117.20 shows port 21 FTP to be open and accessible through an anonymous session.
Images	
Affected Hosts	172.22.117.20 Port 21
Remediation	Disable Anonymous FTP Access

Vulnerability 20	Findings
Title	Email Logs Accessible
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Medium
Description	Email Logs can be accessed through port 110.
Images	
Affected Hosts	172.22.117.20 Port 110
Remediation	Use Port 995 to Securely Deliver Emails.

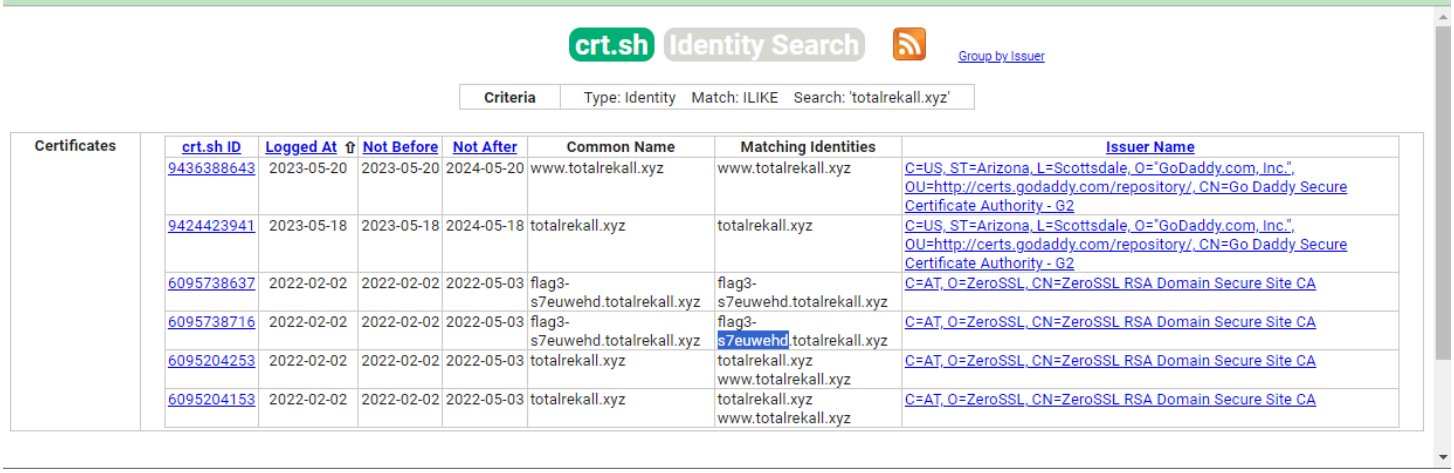
Vulnerability 21	Findings
Title	Credentials Exposed
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Critical
Description	Credentials can be accessed through port 110 on a Meterpreter shell via Kiwi.
Images	
Affected Hosts	SYSTEM 172.22.117.10
Remediation	Secure Sensitive Files

```
Registrant Contact Information:
        Name                            sshUser alice
        Organization
        Address                         h8s692hskasd Flag1
        City                            Atlanta
        State / Province                Georgia
        Postal Code                     30309
        Country                         US
        Phone                           +1.7702229999
        Email                           jlow@2u.com

Administrative Contact Information:
        Name                            sshUser alice
        Organization
        Address                         h8s692hskasd Flag1
        City                            Atlanta
        State / Province                Georgia
        Postal Code                     30309
        Country                         US
        Phone                           +1.7702229999
        Email                           jlow@2u.com

Technical Contact Information:
        Name                            sshUser alice
        Organization
        Address                         h8s692hskasd Flag1
        City                            Atlanta
        State / Province                Georgia
        Postal Code                     30309
        Country                         US
        Phone                           +1.7702229999
        Email                           jlow@2u.com

Information Updated: 2024-01-17 04:58:45
```

Figure 1: Reconnaissance: WHOISXMLAPI of totalrekall.xyz

```
┌──(root💀kali)-[~]
└─# dig TXT totalrekall.xyz

; <<>> DiG 9.16.11-Debian <<>> TXT totalrekall.xyz
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 26943
;; flags: qr rd ad; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0
;; WARNING: recursion requested but not available

;; QUESTION SECTION:
;totalrekall.xyz.               IN      TXT

;; ANSWER SECTION:
totalrekall.xyz.        0       IN      TXT     "flag2 is 7sk67cjsdbs"

;; Query time: 8 msec
;; SERVER: 172.17.16.1#53(172.17.16.1)
;; WHEN: Wed Jan 17 19:27:17 EST 2024
;; MSG SIZE  rcvd: 81

┌──(root💀kali)-[~]
└─#
```

Figure 2: Reconnaissance: ‘dig TXT totalrekall.xyz’



crt.sh Identity Search Group by Issuer

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

Certificates

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

Figure 3: Reconnaissance: SSL Certificate via crt.sh

```
    00c0 - 93 65 bc 84 1f 19 9f 0c-a7 35 ca 4f 57 f3 1e 58   .e.......5.OW..X
    00d0 - 81 bf 9d 19 34 78 a3 b3-1f b1 49 1d ed cf 93 c3   ....4x....I.....
    00e0 - 7a b4 f5 5e 75 0e a3 24-04 b1 e1 0e 21 c4 24 19   z..^u..$....!.$.

    Start Time: 1705537936
    Timeout   : 7200 (sec)
    Verify return code: 0 (ok)
    Extended master secret: no
    Max Early Data: 0
---
read R BLOCK
---
Post-Handshake New Session Ticket arrived:
SSL-Session:
    Protocol  : TLSv1.3
    Cipher    : TLS_AES_256_GCM_SHA384
    Session-ID: B706A902196301D83792033F93D3177F3BB96DC9F723498840A62C55E3EF7229
    Session-ID-ctx:
    Resumption PSK: 834A825C3F57C0164C61D5269A1E34329AA07201E4BDC5FB32E2274DDCE6759
5622F85935A517BE84ABCA518015EE3A4
    PSK identity: None
    PSK identity hint: None
    SRP username: None
    TLS session ticket lifetime hint: 300 (seconds)

MAC Address: 02:42:C0:A8:0D:0D (Unknown)

Nmap scan report for 192.168.13.14
Host is up (0.0000070s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
MAC Address: 02:42:C0:A8:0D:0E (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 192.168.13.1
Host is up (0.0000070s latency).
Not shown: 996 closed tcp ports (reset)
PORT      STATE    SERVICE          VERSION
5901/tcp  open     vnc              VNC (protocol 3.8)
6001/tcp  open     X11              (access denied)
10000/tcp filtered snet-sensor-mgmt
10001/tcp filtered scp-config

Service detection performed. Please report any incorrect results at https://nmap.or
g/submit/ .
Nmap done: 16 IP addresses (6 hosts up) scanned in 47.60 seconds
```

Figure 4: Reconnaissance: NMap scan shows 6 hosts up

```
TRACEROUTE
HOP RTT     ADDRESS
1   0.02 ms 192.168.13.12

Nmap scan report for 192.168.13.13
Host is up (0.000018s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.25 ((Debian))
|_http-server-header: Apache/2.4.25 (Debian)
| http-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
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
```

Figure 6: Reconnaissance: exploitable IP address identified

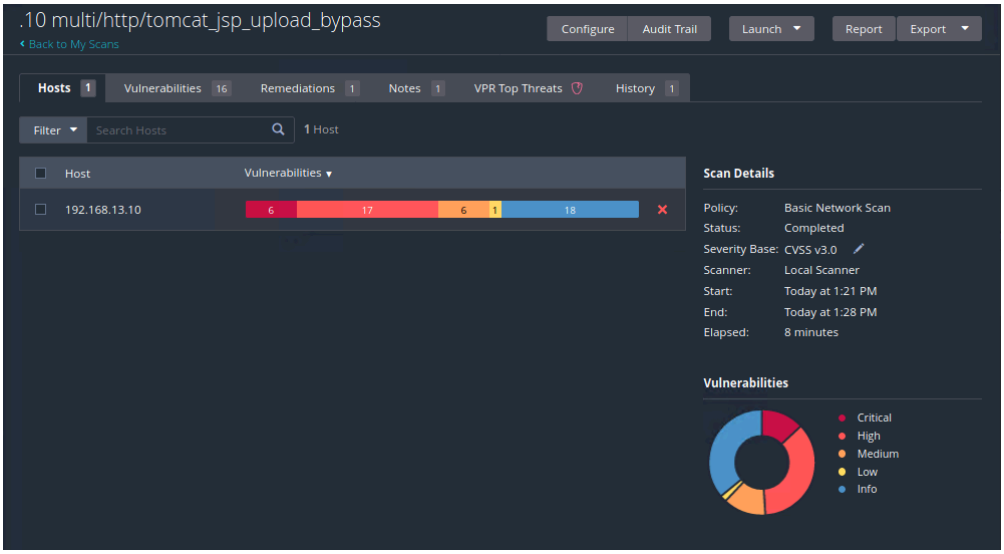


Figure 6: Nessus scan of the IP address vulnerable to RCE through Apache Tomcat

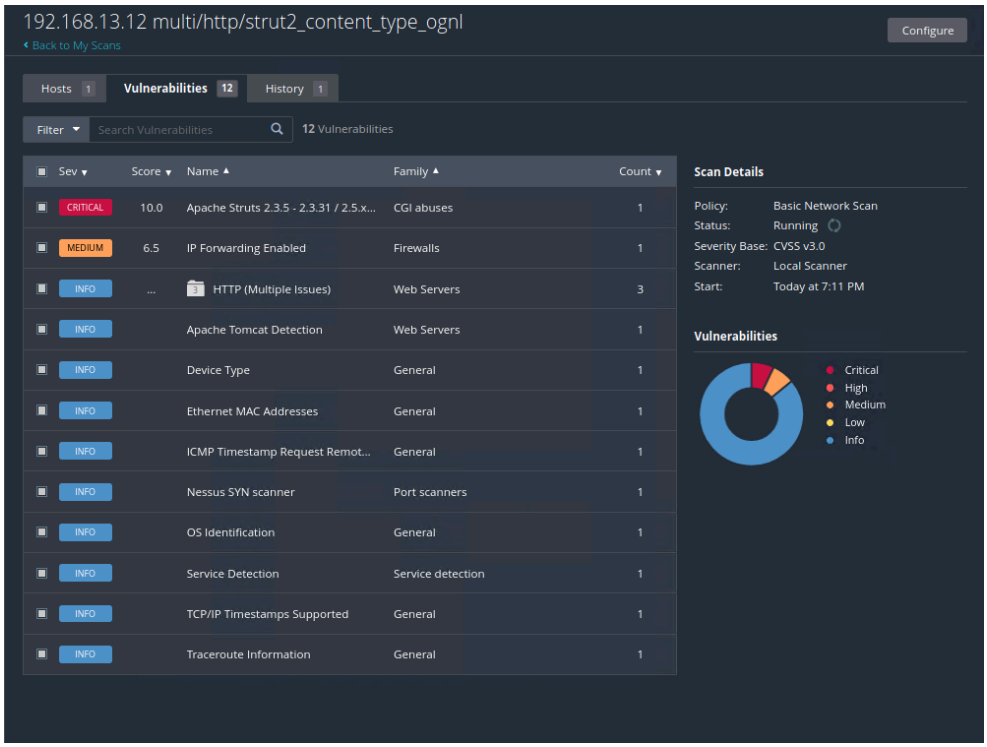


Figure 7: Nessus Report on IP address running Apache Tomcat/Coyote JSP

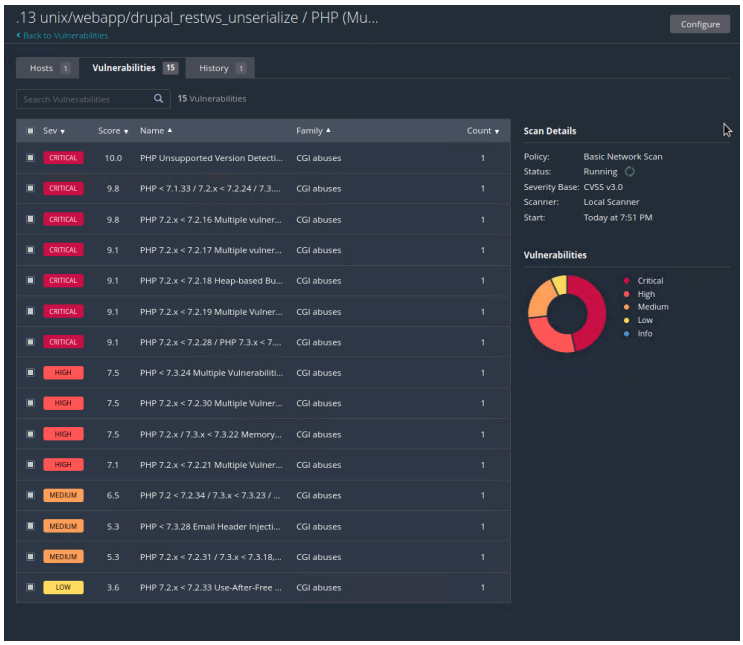


Figure 8: Nessus Report critical findings on IP address running Drupal.