Cybersecurity

Penetration Test Report

Rekall Corporation

Penetration Test Report

Student Note: Complete all sections highlighted in yellow.

© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

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.

© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

Table of Contents

© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

Contact Information

Company Name	Ace's Guard
Contact Name	Alonzo Diaz
Contact Title	Penetration Tester

Document History

Version	Date	Author(s)	Comments
001	03/10/2024	Alonzo Diaz	Findings from the Penetration Testing

© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

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.

© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

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.

© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

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.

© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

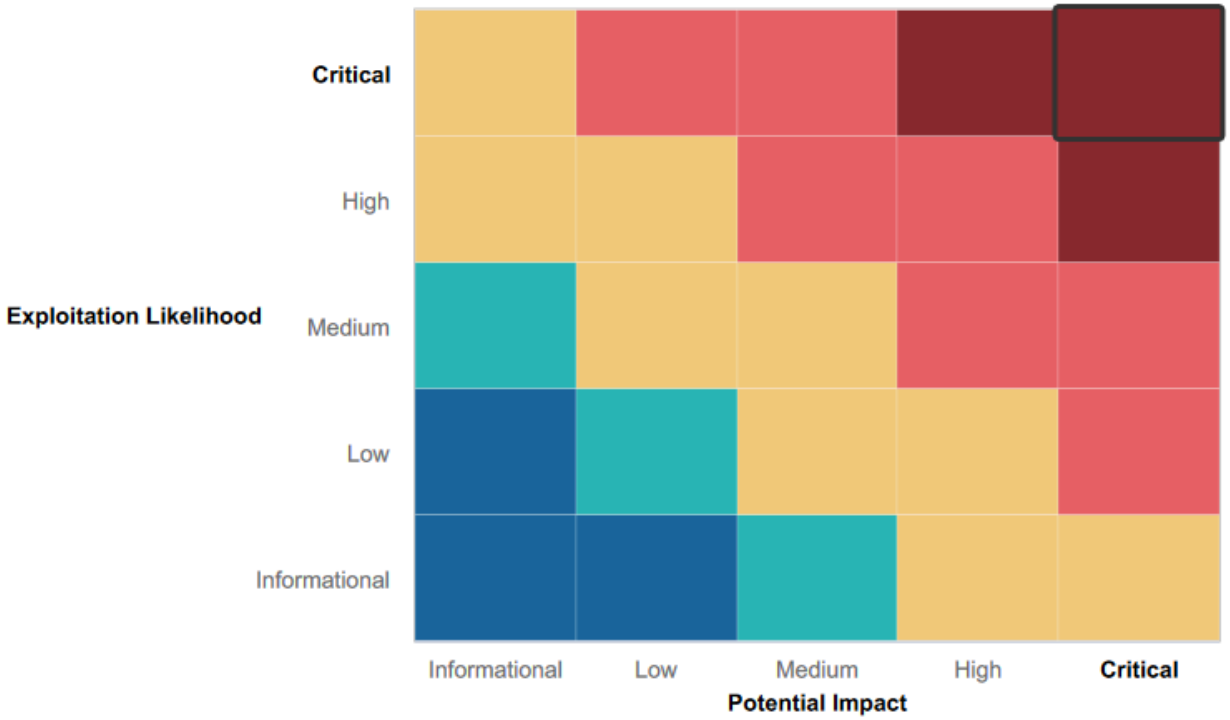
Executive Summary of Findings

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:



© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

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.

Web Application

- For this system it demonstrated strong resilience against command and PHP injections attempts, effective password security to a certain degree and some session management practices which overall minimizes the risk of unauthorized access and exploitation. Additionally it showcases a solid defence against directory traversal and local file vulnerabilities. The web application also has the ability to withstand brute force attacks and the system also has a high awareness of potential risk, highlighting an ongoing commitment to strengthening defenses and improving overall cybersecurity resilience.

Linux OS

- Linux OS shows some resilience to remote code and lowering the risk of post-exploitation threats. It as well has Strong password guessing measures especially handling ShellShock exploits and keeping it to a minimum. Linux OS as well responds nicely to attempts in network scanning by conducting SSL certificate research and reinforcing environmental security. Its provocative approach to OSINT and network scanning highlights a continuous threat assessment and risk mitigation.

Windows OS

- Windows OS system gives good defense against SL mail service exploitation and mitigates any risk of escalating access making it very difficult to obtain admin credentials. It uses its scheduled tasks to reduce high risk activities / vulnerabilities while at the same time preventing unauthorized access. Windows OS has a great identity of identifying and mitigating potential security risks with OSINT and FTP.

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.

Web Application

- The web application has several security weaknesses, including vulnerabilities to command and SQL injection, which could lead to significant data exposure and system compromise. Weak session management and brute force attack risks threaten user authentication and access control. Directory traversal and local file inclusion vulnerabilities present additional security concerns, though their impact may vary. Sensitive data exposure, remote code execution risks, and PHP injection further highlight critical weaknesses. Additionally, XSS vulnerabilities and inconsistencies in impact assessment suggest areas requiring improved security measures and clearer risk evaluation.

Linux OS

- The Linux OS has critical security weaknesses, including remote code execution vulnerabilities that pose a significant risk of system compromise. Post-exploitation risks allow high-level access and control, further escalating security concerns. Persistent vulnerabilities identified by Nessus scans suggest ongoing network security gaps. Additionally, weaknesses in access escalation, network scanning, and

© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

aggressive Drupal scans indicate potential attack vectors, though their impact remains unclear. While OSINT and SSL certificate research expose some low-risk findings, the overall security posture requires improvements to mitigate these threats effectively.

Windows OS

- The Windows OS has several security weaknesses, including a critical vulnerability in the SLMail service, posing a significant risk of exploitation. Post-exploitation tasks on Windows 10 indicate potential high-risk activities, while user enumeration and access escalation vulnerabilities could facilitate unauthorized access and lateral movement. Attempts to compromise administrative credentials further highlight security concerns. Additionally, OSINT, FTP, and HTTP enumeration expose medium-risk findings, while file enumeration presents a lower-risk activity. These weaknesses suggest the need for stronger access controls and improved system monitoring.

Executive Summary

Web Application

This security vulnerabilities of the target system at 192.168.14.15. The assessment uncovered multiple weaknesses, including cross-site scripting (XSS), SQL injection, file upload vulnerabilities, improper access control, and information disclosure. Each issue was successfully exploited to demonstrate potential risks and retrieve security flags.

The test revealed that XSS vulnerabilities allowed script injections on various pages, exposing sensitive information. Command injection and file upload exploits enabled the execution of unauthorized commands and the bypassing of restrictions. SQL injection and authentication bypass flaws provided access to administrator credentials. Additionally, unprotected files exposed sensitive data, while weak input validation in network interfaces allowed the extraction of critical network records. Automated attacks using Burp Suite further demonstrated credential exposure and unauthorized access. Finally, command execution through web interfaces revealed user data vulnerabilities.

© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

Linux OS

This security posture of various systems associated with totalrekall.xyz, identifying multiple vulnerabilities through ping, network scanning, exploitation, and privilege escalation. The findings revealed critical weaknesses that enabled unauthorized access, privilege escalation, and exposure of sensitive data.

Information gathering efforts used tools like centralops.net and crt.sh to extract domain registration details and SSL certificate data. Network scanning with ping tests and Nmap helped map active IP addresses and services. A Nessus scan uncovered an Apache Struts vulnerability, which was exploited alongside other weaknesses in Tomcat, Shellshock, Struts, and Drupal using Metasploit, granting unauthorized access to multiple hosts. Further analysis led to the discovery of SSH credentials, allowing lateral movement between systems. Privilege escalation techniques ultimately provided root access, exposing sensitive files and system vulnerabilities.

Windows OS

This security of the totalrekall.xyz environment by targeting credential harvesting, network enumeration, exploit execution, and privilege escalation. The test uncovered critical weaknesses in password storage, authentication mechanisms, and network service configurations, enabling unauthorized access and privilege escalation across multiple systems.

The test began with credential discovery, where a username and hashed password were found on a public GitHub repository. The hash was cracked using John the Ripper, revealing a user’s password. Network scanning revealed two accessible hosts, leading to successful logins and flag retrievals across both systems. Exploitation of services like SLMail and scheduled tasks allowed further access, and Metasploit was used to gain meterpreter access and escalate privileges. Password cracking and cached credential extraction enabled root-level access and the discovery of multiple flags, further highlighting vulnerabilities in the system’s security.

© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

Summary Vulnerability Overview

Vulnerability	Severity
1 - XSS Reflected (Web Application)	Critical
2 - XSS Reflected Advanced (Web Application)	Critical
3 - XSS Stored Vulnerability (Web Application)	Critical
5 - Local File Inclusion (Web Application)	Critical
6 - Local File Inclusion Advanced (Web Application)	Critical
7 - SQL Injection Login.php (Web Application)	Critical
8 - Sensitive Data Exposure (Web Application)	Critical
10 - Command Injection (Web Application)	Critical
11 - Command Injection (Web Application)	Critical
22 - Apache Tomcat exploit (Linux OS)	Critical
23 - ShellShock Exploiting (Linux OS)	Critical
24 - Escalating Access (Linux OS)	Critical
26 - Drupal Exploiting (Linux OS)	Critical
31 - SLMail Service Exploitation (Windows OS)	Critical
35 - Win 10 to Server2019 Exploit (Windows OS)	Critical
36 - Escalating Access (Windows OS)	Critical
4 - Sensitive Data Exposure (Web Application)	High
9 - Sensitive Data Exposure (Web Application)	High
25 - Struts Exploiting (Linux OS)	High
27 - (.14) exploiting (Linux OS)	High
32 - Scheduled Task on Win10 Exploitation (Windows OS)	High
33 - SLmail exploit on Windows 10 (Windows OS)	High
37 - Compromising Admin (Windows OS)	High
12 - Burp Suite/Brute Force Attack (Web Application)	Medium
13 - Php injection (Web Application)	Medium
14 - Session Management (Web Application)	Medium
19 - Network Scanning (Linux OS)	Medium
20 - Aggressive Scan for Drupal (Linux OS)	Medium
21 - Nessus Scan and Vulnerability ID (Linux OS)	Medium
28 - Github Repository OSINT (Windows OS)	Medium
29 - HTTP Network (Windows OS)	Medium
30 - FTP (Windows OS)	Medium
15 - Directory Traversal (Disclaimers) (Web Application)	Low
16 - Domain Open Source Exposure (Linux OS)	Low
17 - IP Address Ping (Linux OS)	Low

© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

18 - SSL Certification Research (Linux OS)	Low
34 - File Enumeration (Windows OS)	Low

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

Scan Type	Total
Hosts	172.22.117.10 172.22.117.20 192.168.13.10 192.168.13.11 192.168.13.12 192.168.13.13 192.168.13.14 192.168.13.35 192.168.14.35
Ports	8080 8081 SMTP 25 POP3 110 21

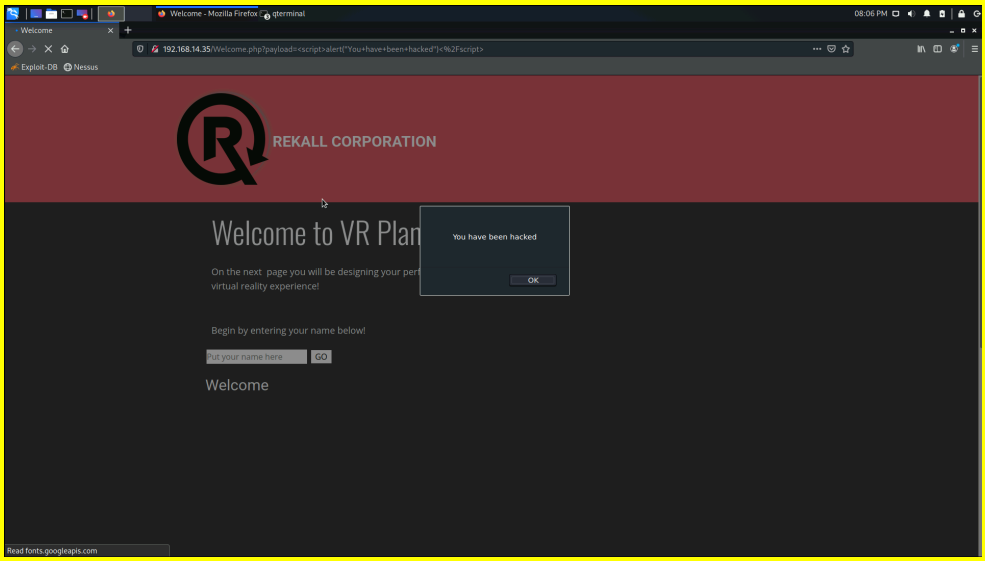
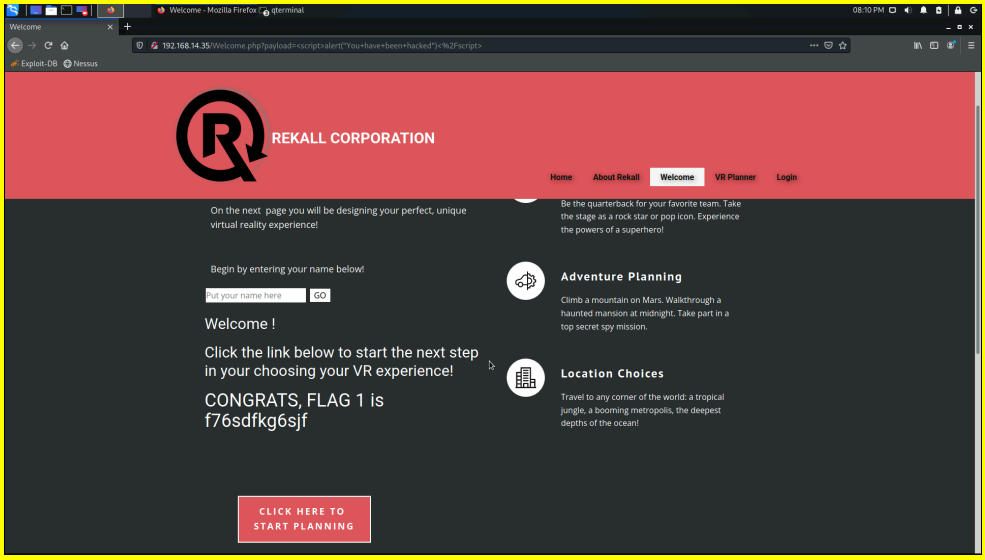
Exploitation Risk	Total
Critical	16
High	7
Medium	9
Low	5

Vulnerability Findings

Web Application

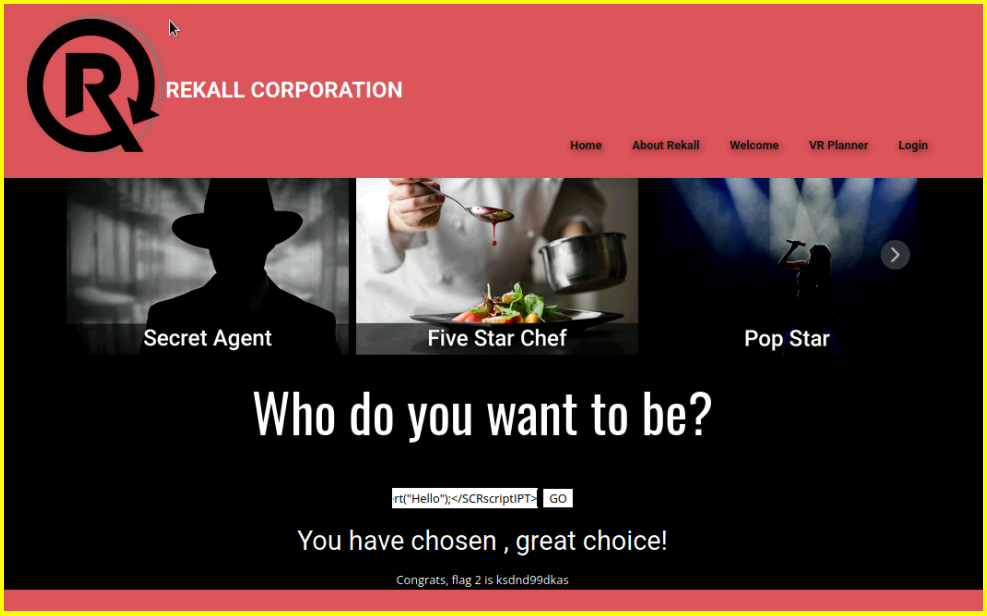
Vulnerability 1	Findings
Title	Flag 1 - reflected XSS payload
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Critical
Description	Wrote in the “enter name below” a payload that will create a pop up (the payload used was <script>alert(“you have been hacked”)</script>

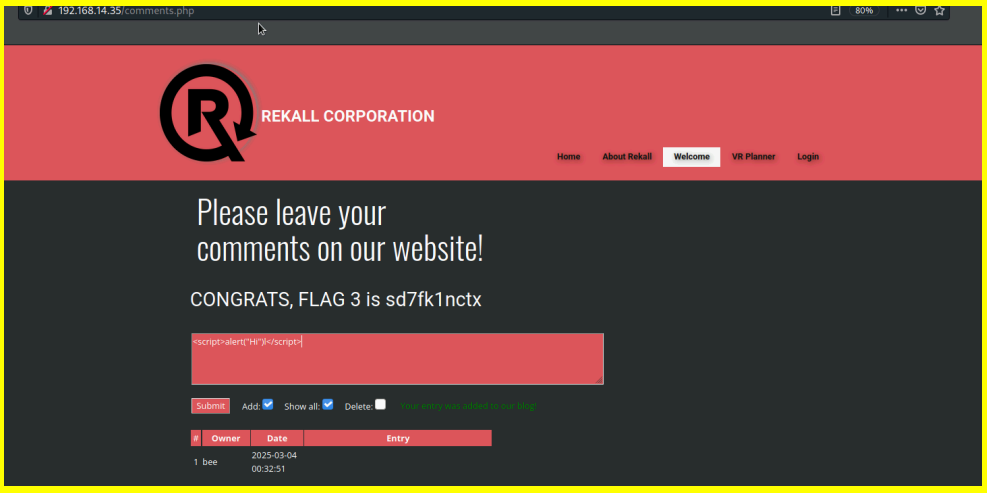
© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

Images	 
Affected Hosts	192.168.14.35
Remediation	Input validation, change back end architecture to sanitize user input

Vulnerability 2	Findings
Title	Flag 2 Reflected XSS
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Critical
Description	using the same method of Flag 1 using a sequence injector creating an Alert notification for the user.

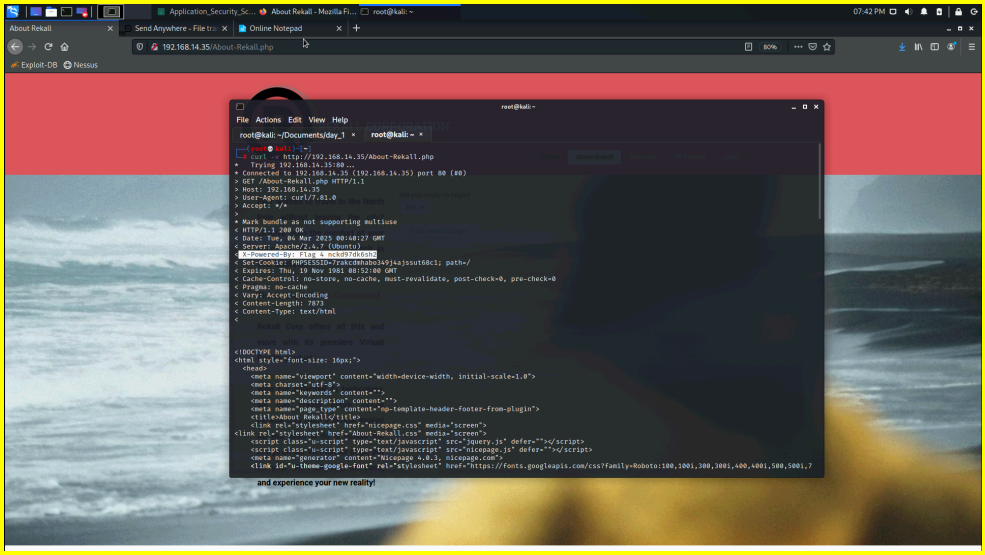
© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

Images	
Affected Hosts	192.168.14.35
Remediation	input validation to prevent advanced scripts to be put into the blank box for the user.

Vulnerability 3	Findings
Title	flag 3 - XSS
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Critical
Description	using the same method of Flag 1 using a sequence injector creating an Alert notification for the user but this time by entering it in the Comment box
Images	
Affected Hosts	192.168.14.35

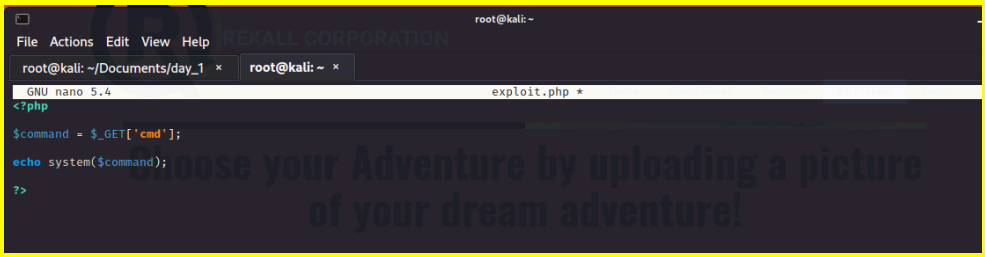
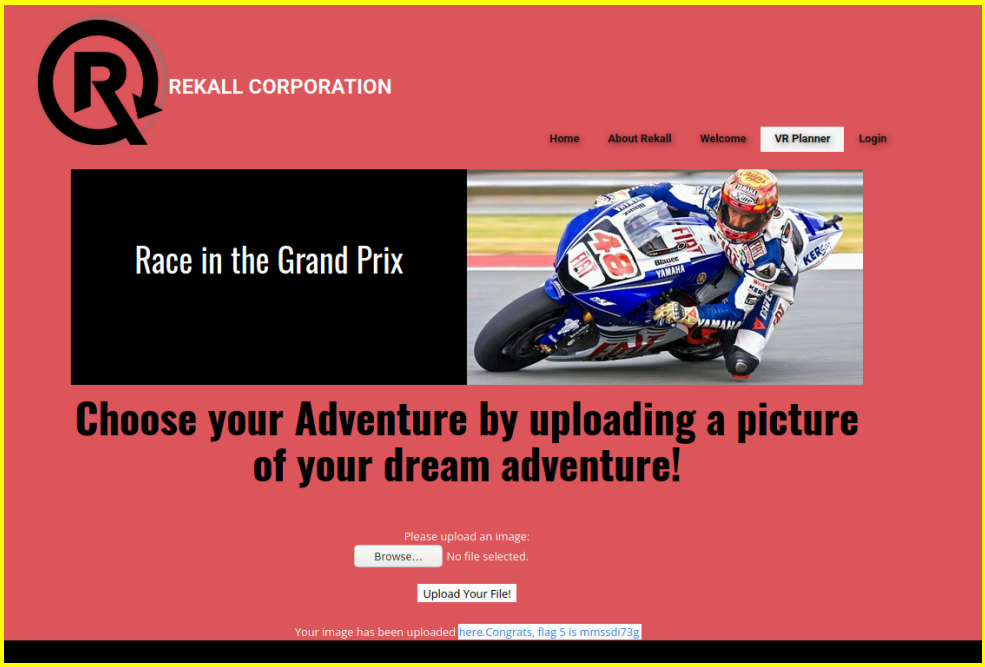
© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

Remediation	input validation from user.

Vulnerability 4	Findings
Title	Flag 4 Data exposure
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	high
Description	used the curl command of the about page for Rekall's website and was able to obtain sensitive data.
Images	
Affected Hosts	192.168.14.35
Remediation	Proper clean up of data on server side

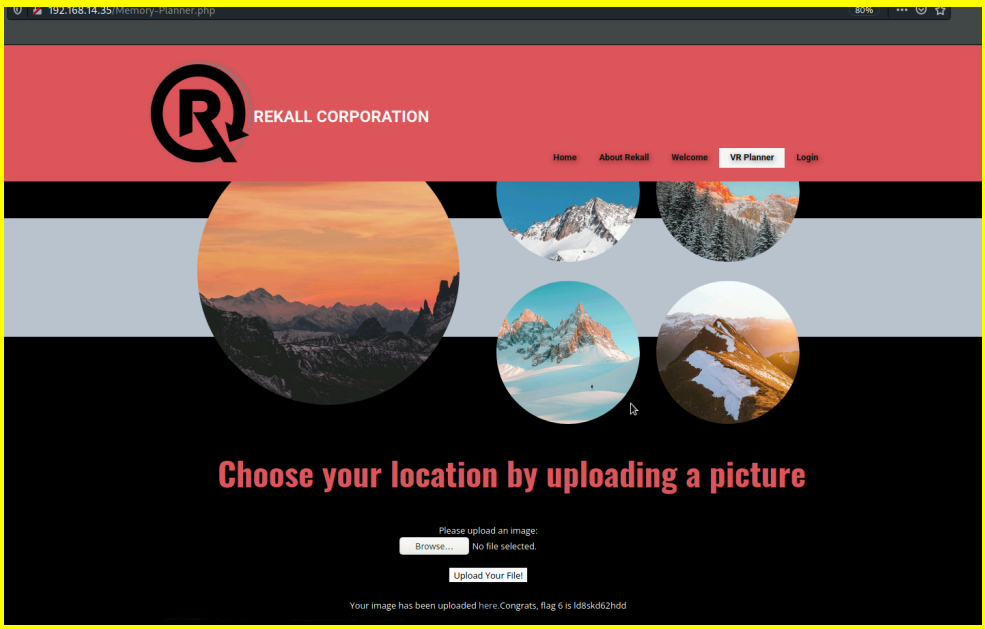
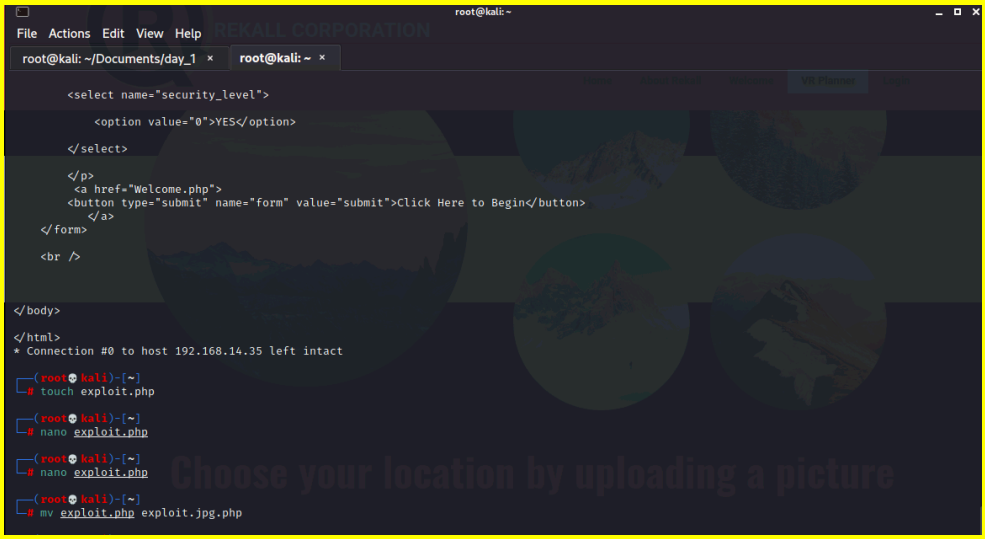
Vulnerability 5	Findings
Title	flag 5 LFI exploit
Type (Web app / Linux OS / WIndows OS)	web app
Risk Rating	Critical
Description	Created a php file that would be accepted and cause an exploit on the web app.

© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

Images	 
Affected Hosts	192.168.14.35
Remediation	File Validation making sure that whatever file is uploaded is the actual file such as jpg for example.

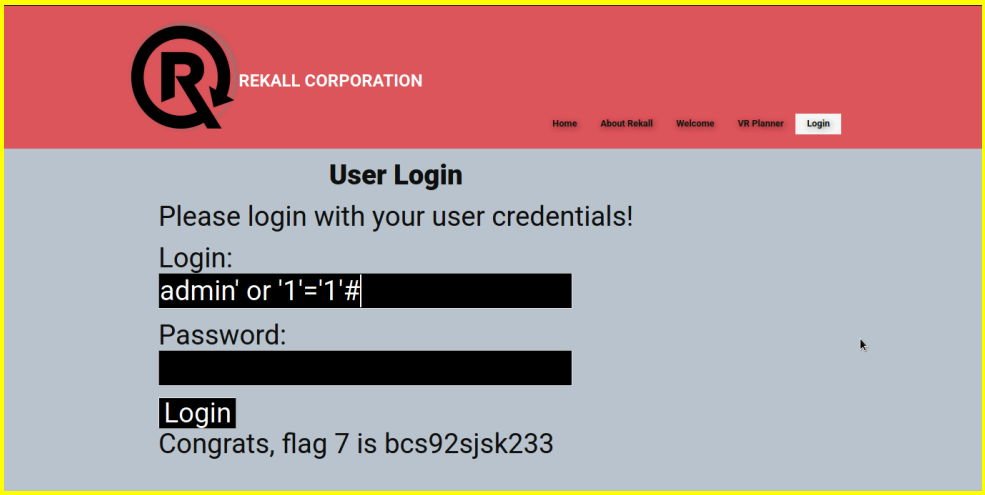
Vulnerability 6	Findings
Title	flag 6 LFI advanced exploit
Type (Web app / Linux OS / WIndows OS)	web app
Risk Rating	critical
Description	when trying to upload the original file of just PHP it was not accepted, however all i did to the file was add an additional jpg to it and was able to submit the file successfully giving me back sensitive data.

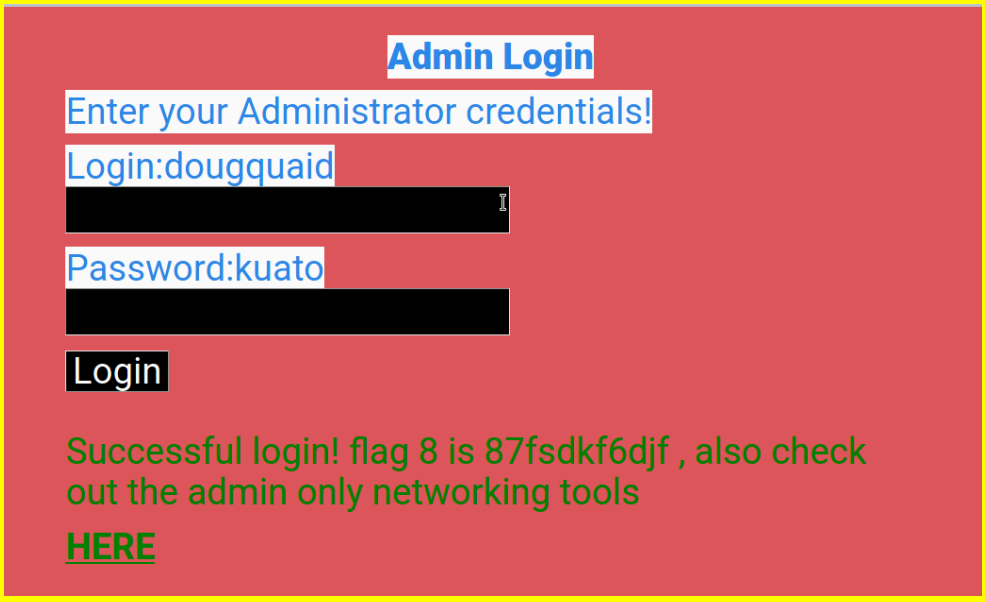
© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

Images	 
Affected Hosts	192.168.14.35
Remediation	File upload validation making sure only jpg file are uploaded

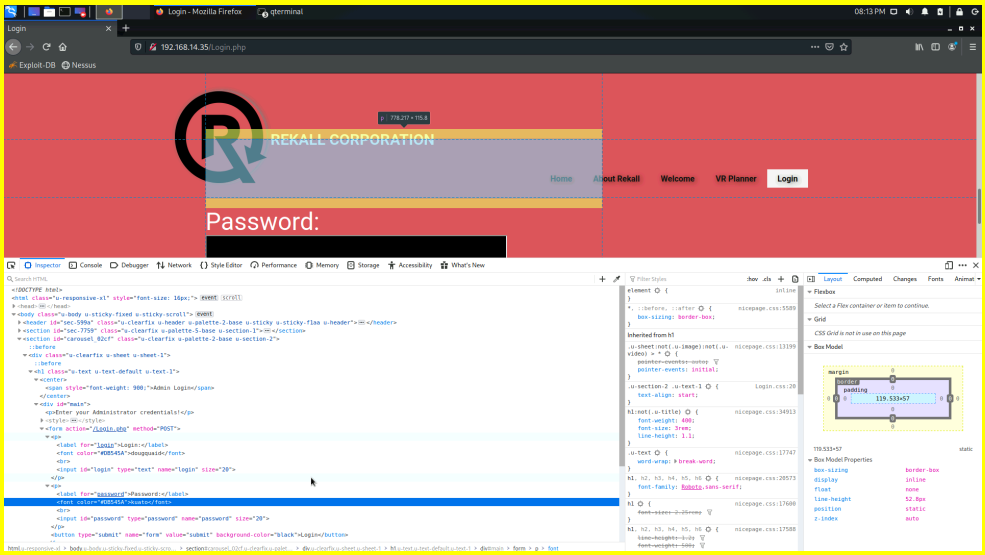
Vulnerability 7	Findings
Title	Flag 7 sql injection
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Critical
Description	using a basic sql injection of admin' or '1'='1' to be able to enter the user login page which ended with obtaining the flag 7

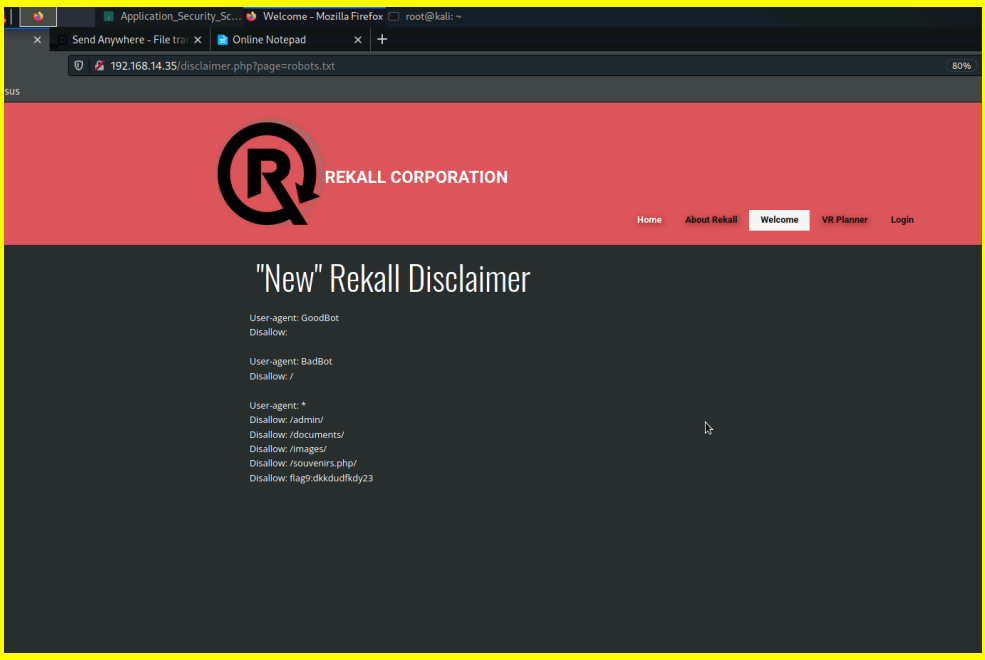
© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

Images	
Affected Hosts	192.168.14.35
Remediation	Do not allow the web application to accept special character combinations

Vulnerability 8	Findings
Title	Flag 8 - Sensitive data Exposure
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Super Critical
Description	Just by looking at the web source code you are able to discover the user name and password for the admin login
Images	

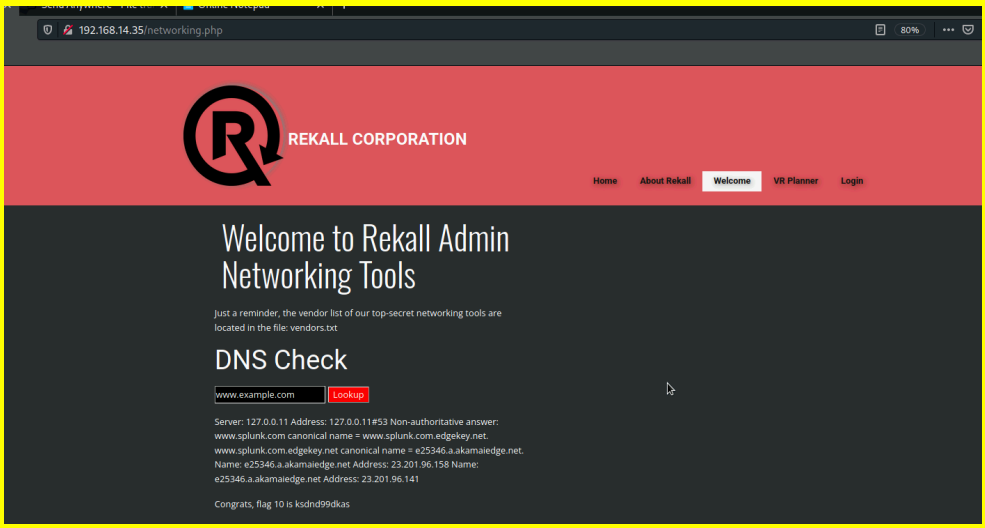
© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

	
Affected Hosts	192.168.14.35
Remediation	remove the user name and password from the web app source code.

Vulnerability 9	**Findings**
Title	Flag 9 - Directory Traversal Attack
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	High
Description	used directory traversal to discover a robots.txt file while using the wildcard rule to allow unrestricted directory movement
Images	

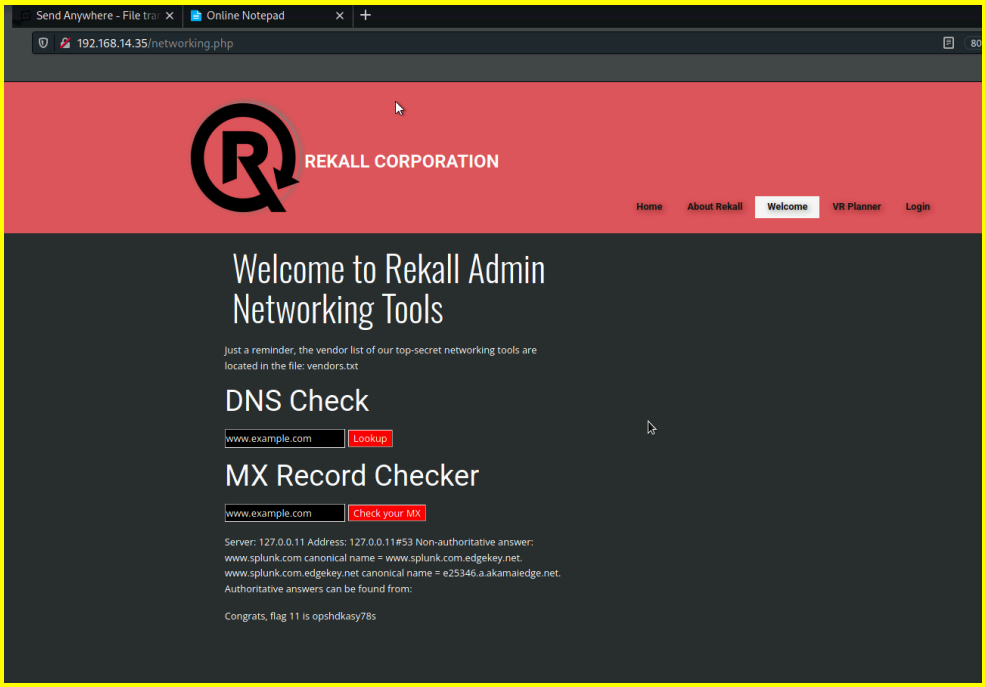
© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

Affected Hosts	192.168.14.35
Remediation	Enable restriction from user to allow any user from obtaining sensitive files and data

Vulnerability 10	**Findings**
Title	flag 10- command injection
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	Critical
Description	by manually navigating to the networking php directory and entering in the DNS check www.splunk.com I was able to obtain sensitive information
Images	
Affected Hosts	192.168.14.35
Remediation	Reset Passwords and all logins for accounts compromised as well needing to get rid of any compromised systems from the network to resolve.

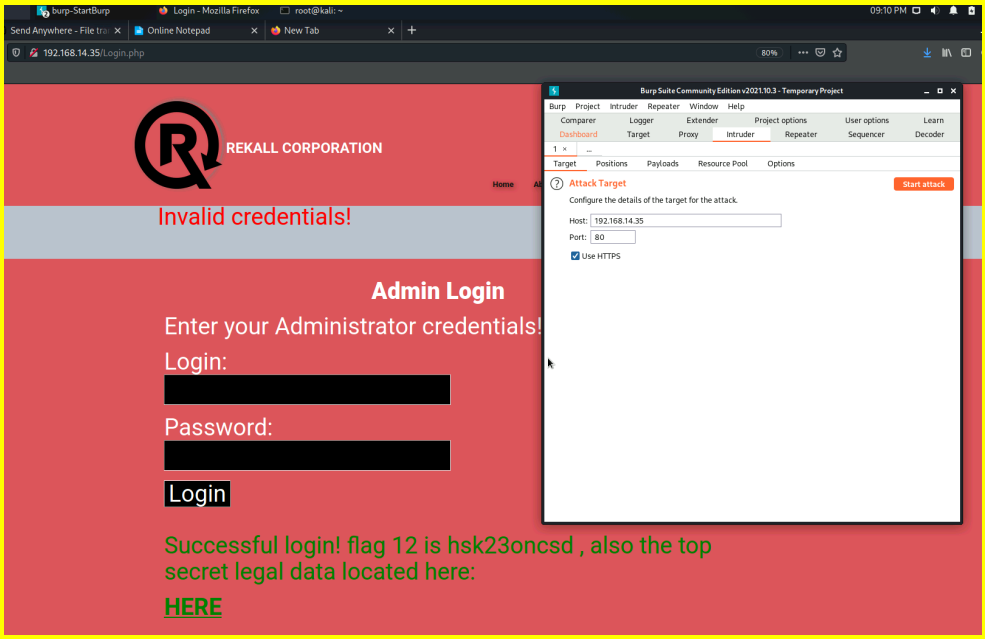
Vulnerability 11	**Findings**
Title	Flag 11 - advanced command injection
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	Critical
Description	by Mimicking the same actions for the pervious vulnerability I entered www.splunk.com in the MX Record Checker and was able to obtain the same information

© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

Images	
Affected Hosts	192.168.14.35
Remediation	Reset Password as well and then implement a password policy to make the password more encrypted which overall makes it very difficult to obtain any sensitive information.

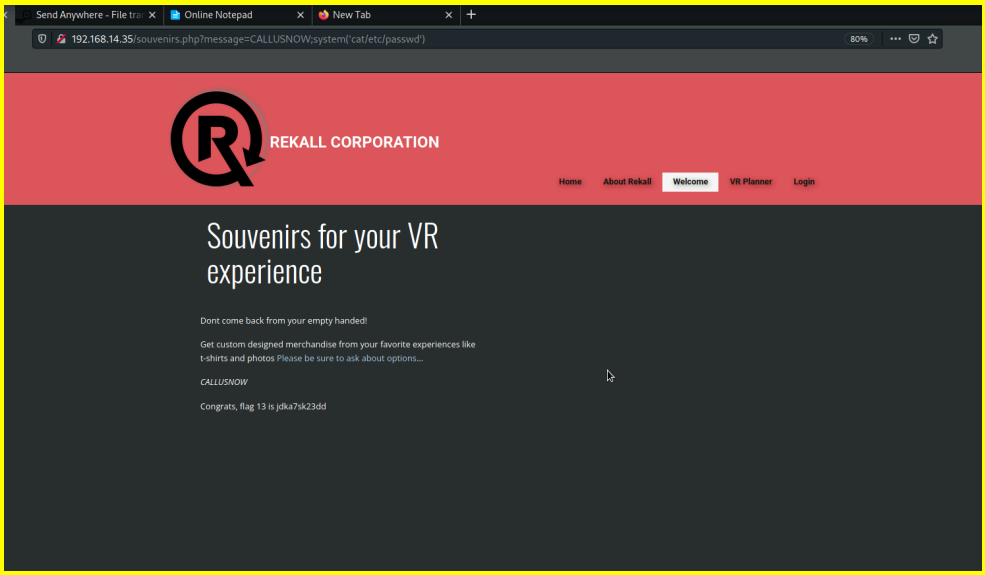
Vulnerability 12	Findings
Title	Flag 12- Brute Force attack
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	Medium
Description	using a burp intruder and setting the parameters I was able to obtain the login information of a user who had admin login credentials allowing me to successful complete my brute force attack.

© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

Images	
Affected Hosts	192.168.14.35
Remediation	For this one as well enforce a stronger password policy the username and password should never match and be identical to one another. As well bringing in a second factor for long in or giving employees a yubi key (for example) that regularly changes the password for the accounts.

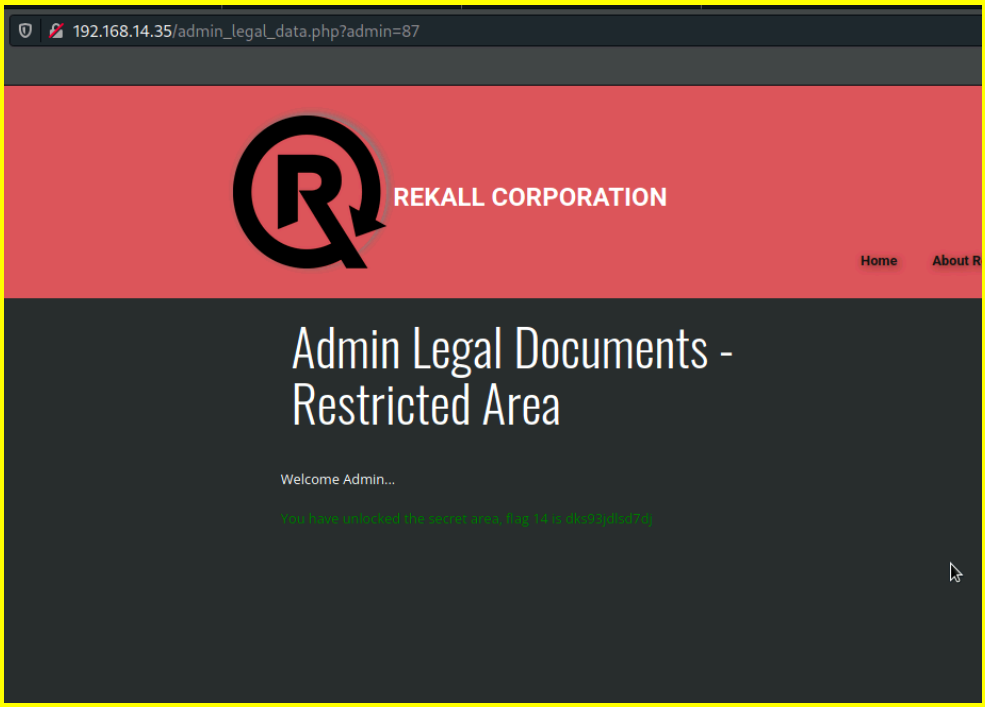
Vulnerability 13	Findings
Title	Flag 13 Php injection
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	medium
Description	with the help of finding other vulnerabilities i was able to navigate to the souvenirs page and by implementing a payload of ;system('cat/etc/passwd') to the end of CALLUSNOW i was able to discover the flag information

© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

Images	
Affected Hosts	192.168.14.35
Remediation	Make sure all user inputs are validated and sanitized before entering in the URL making sure nobody can be able to access any page while using special character scripts.

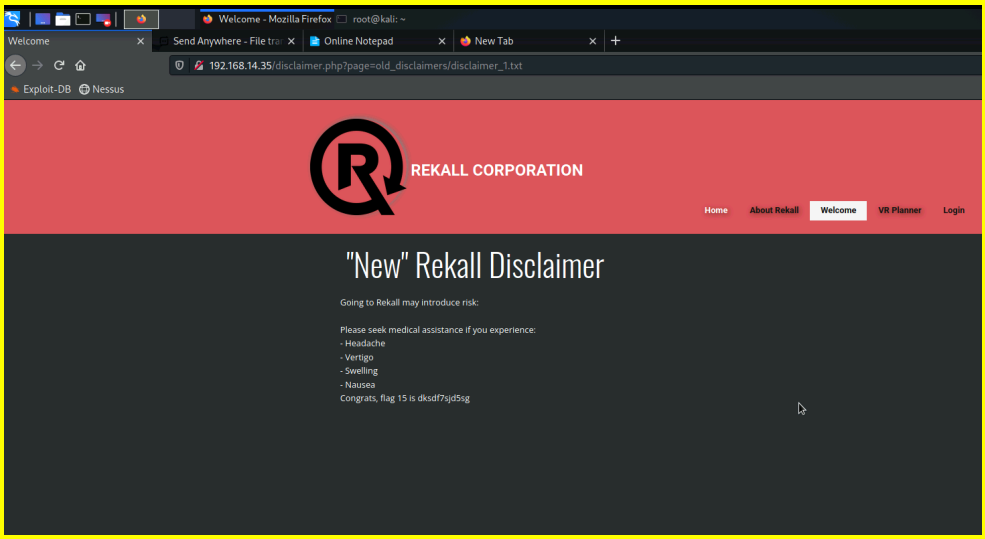
Vulnerability 14	Findings
Title	Flag 14 - Session management
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Medium
Description	By using burp I was able to discover port 87 was vulnerable to access and when changing the url from 1 to 87 I was able to discover the next page of welcome admin giving me the flag information.

© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

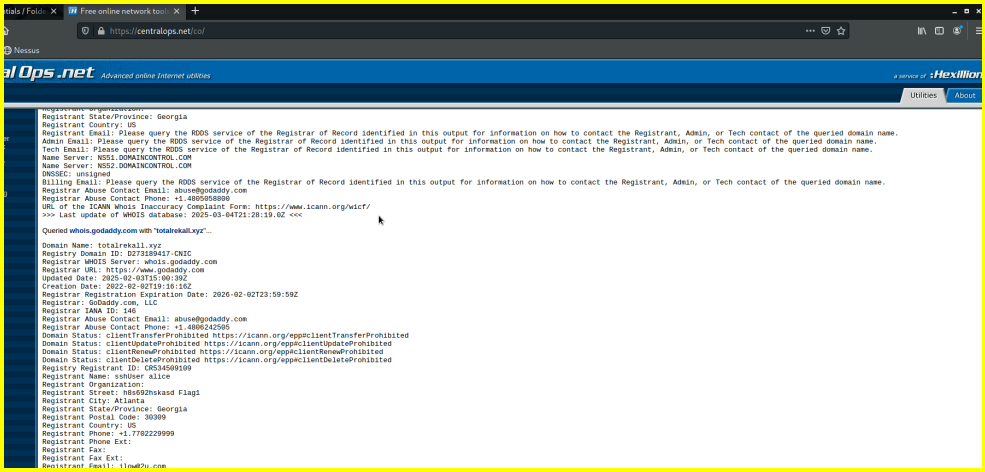
Images	
Affected Hosts	192.168.14.35
Remediation	Using Strong and unique sessions ID align with implementing proper session management would be a good start as well making sure to regularly monitor and audit the session management.

Vulnerability 15	Findings
Title	Flag 15 Directory Traversal (Disclaimers)
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Low
Description	using Directory traversal i was able to make changes to the url to “page=old_disclaimers/disclaimer_1.txt” which in result giving me the sensitive information as well giving me the flag code.

© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

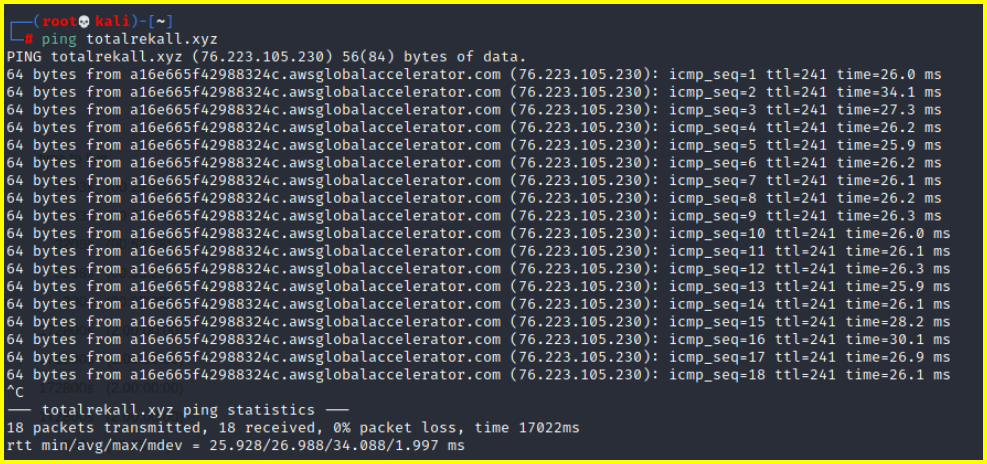
Images	
Affected Hosts	192.168.14.35
Remediation	using absolute paths to prevent any “../” from being used as well as other sequences in order to prevent Directory Traversal

Linux OS

Vulnerability 16	Findings
Title	Domain Data Exposure
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Low
Description	I navigated to centralops.net to use the Domain Dossier and by entering in the totalrekall.xyx under the “Registrant Street” the code for Flag 1 was entered in that space.
Images	
Affected Hosts	

© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

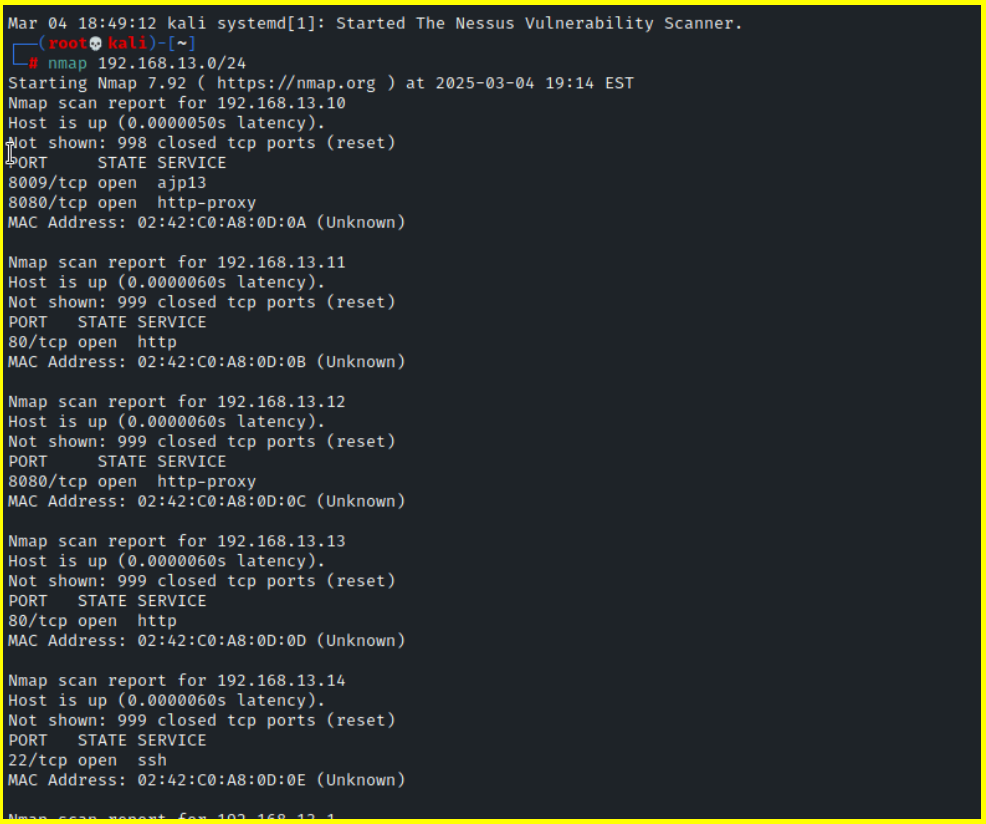
Remediation	To remediate the domain data exposure vulnerability identified through centralops.net, implement WHOIS privacy protection (domain privacy) services to shield sensitive registrant information, and conduct a comprehensive audit of all domain registration details to ensure no sensitive data or credentials are exposed in any registration fields.

Vulnerability 17	Findings
Title	IP Address Ping
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Low
Description	Using the linux terminal and using the ping command i was able to obtain the IP for Flag 2
Images	
Affected Hosts	34.102.136.180
Remediation	Implement network segmentation and proper firewall rules as well as deploy a reverse proxy to mask actual server IP addresses, preventing direct discovery of internal infrastructure through ping commands.

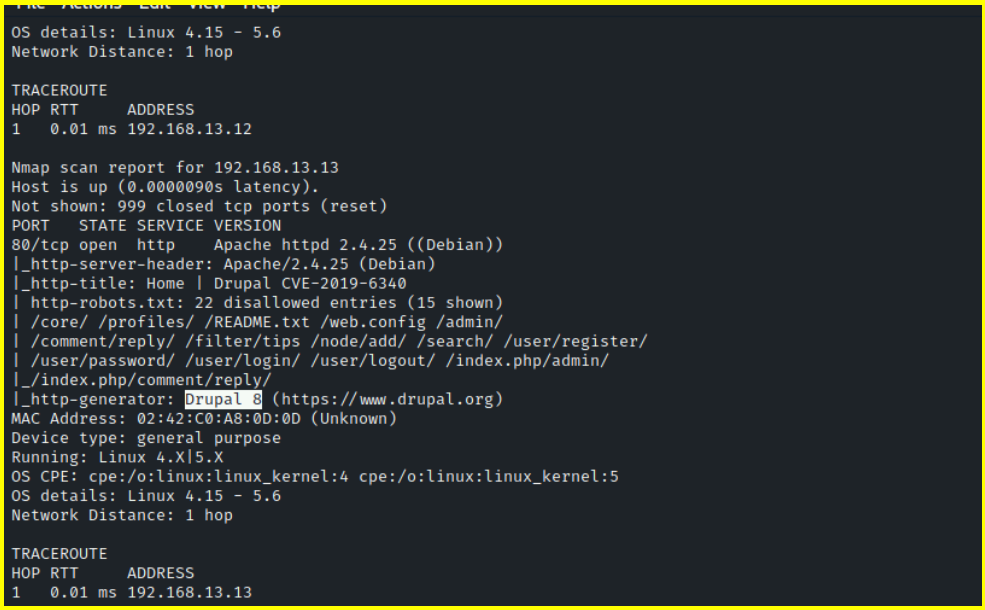
Vulnerability 18	Findings
Title	SSL Certification Research
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Low
Description	I went to crt.sh and by entering totalrekall.xyz I was able to notice Flag 3's code in the results provided.

© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

Images	
Affected Hosts	crt.sh
Remediation	Proper Management of the certification, as well making sure to renew it before expiration.

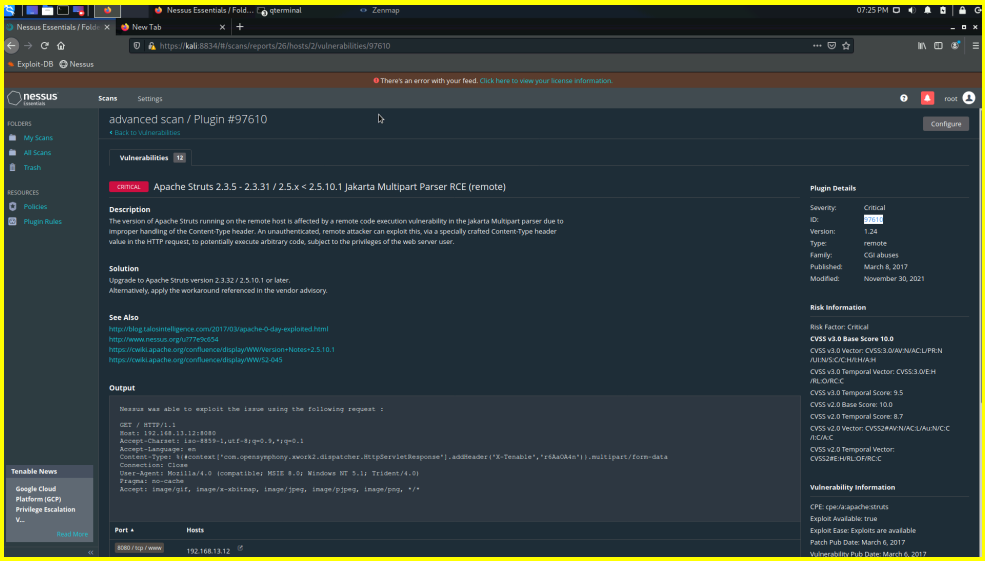
Vulnerability 19	**Findings**
Title	Network Scanning
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Medium
Description	On linux terminal I ran the command nmap on the IP to see the amount of hosts while excluding the one used to run the nmap scan.
Images	
Affected Hosts	192.168.13.0/24
Remediation	Audit the ports to make sure all open ports are actually closed and not being used.

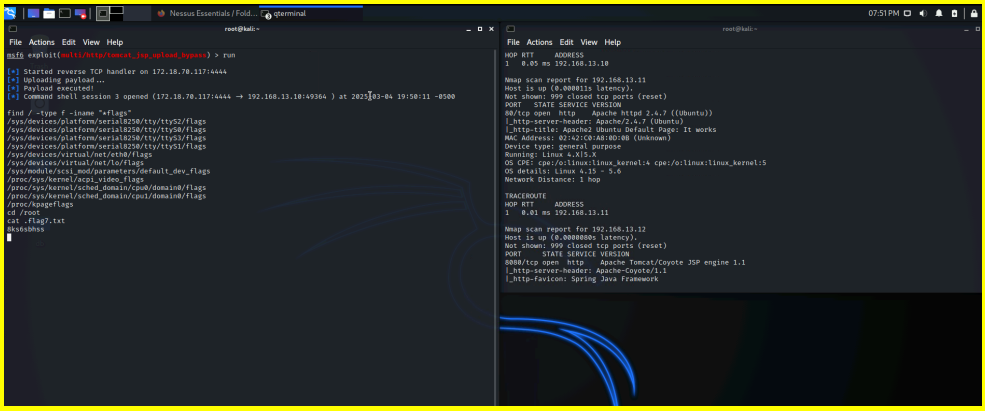
© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

Vulnerability 20	Findings
Title	Aggressive Scan for Drupal
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Medium
Description	On the linux terminal I ran another nmap scan but made it an aggressive scan to run me the IP host needed for Drupal.
Images	
Affected Hosts	192.168.13.13,
Remediation	Overall a simple OS version update would be the best case scenario to avoid this situation from expanding.

Vulnerability 21	Findings
Title	Nessus Scan and Vulnerability ID
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Medium
Description	Ran a Nessus Scan on 192.168.13.12 to give me the Apache Struts Critical Risk. Flag 6 was the ID number under the Plugin Details.

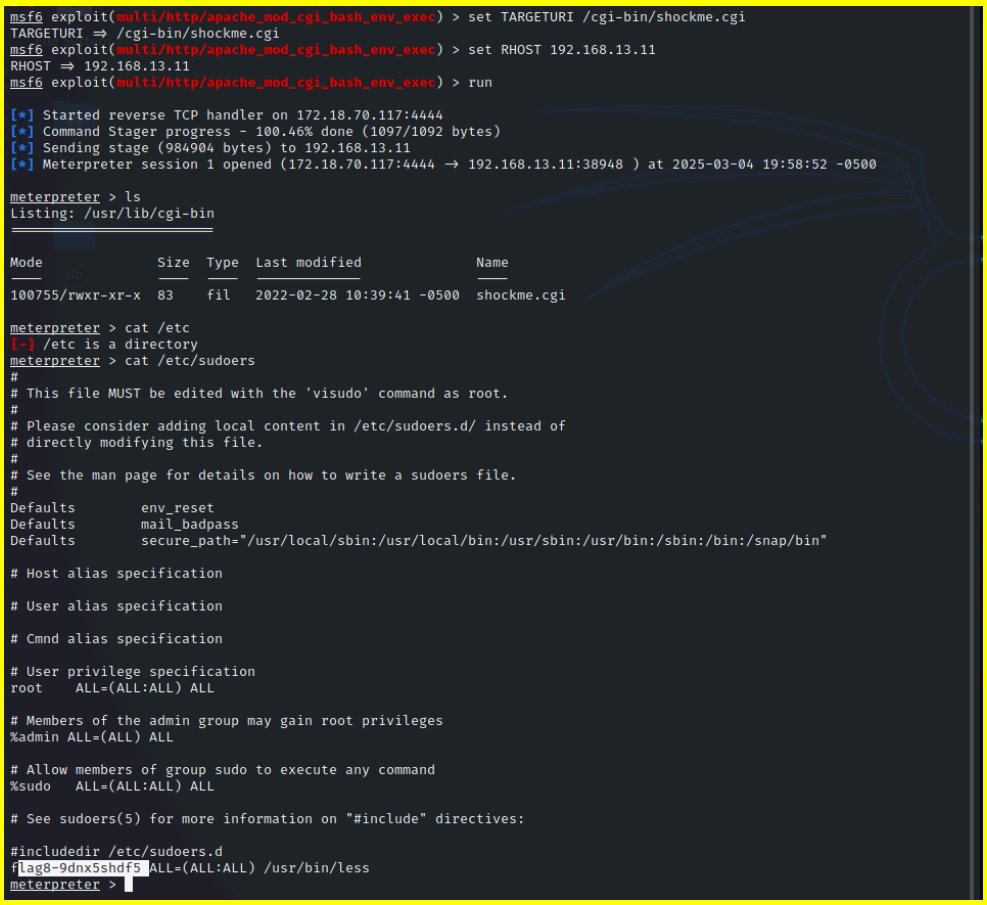
© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

Images	
Affected Hosts	Nessus
Remediation	Auditing all the potential risk with the nessus scan and having employees actively resolve the issue because the longer the risk is active the easier it becomes to hack into.

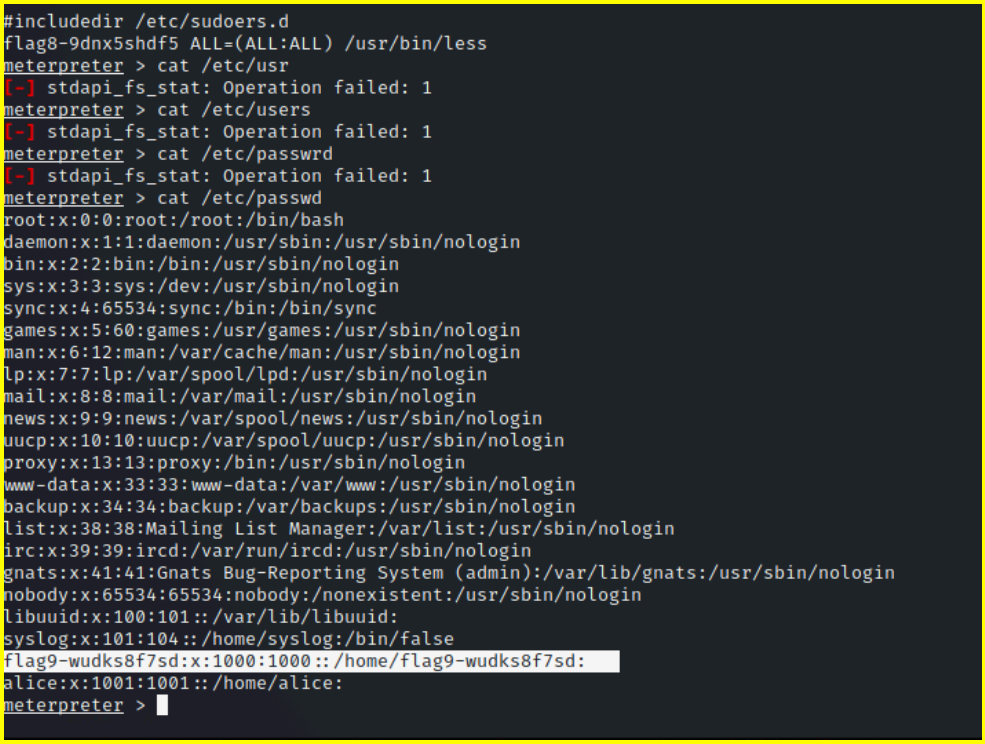
Vulnerability 22	**Findings**
Title	Apache Tomcat exploit
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	used the MSFconsole along with an exploit for Tomcat and JSP under the Rhost of 192.168.13.10…Once in a meterpreter and creating a command line with shell. I used the find command to find the location of Flag 7 and followed the path to obtain the code.
Images	
Affected Hosts	192.168.13.10
Remediation	Limiting user privileges to reduce the risk of exploitation as well as activating a

© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

	firewall to reduce the network traffic to a level that is easier to manage and monitor.

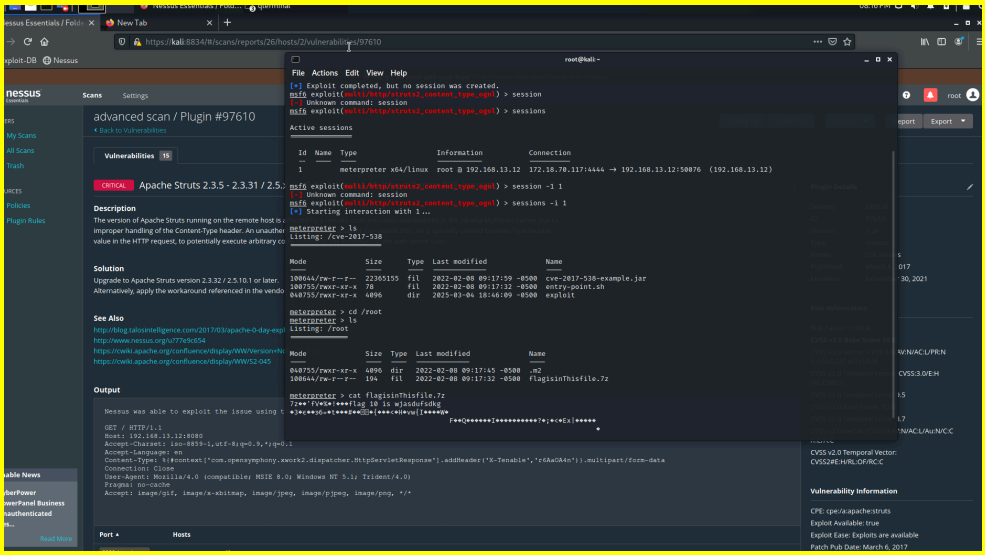
Vulnerability 23	Findings
Title	ShellShock Exploiting
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	Ran MSFconsole with a Shellshock exploit and by changing the parameters with TARGETURI set to /cgi-bin/shockme.cgi and RHOST to 192.168.13.11 Then on the exploited machine I navigated using /etc/sudoers.d to obtain Flag 8
Images	
Affected Hosts	192.168.13.11
Remediation	Limiting User privileges again but as well limiting access to files along with them. On top of repeating the use of a firewall from the previous vulnerability due to this exploit being done onto each layer would as well gradually increase your chance of protecting from hack attempts

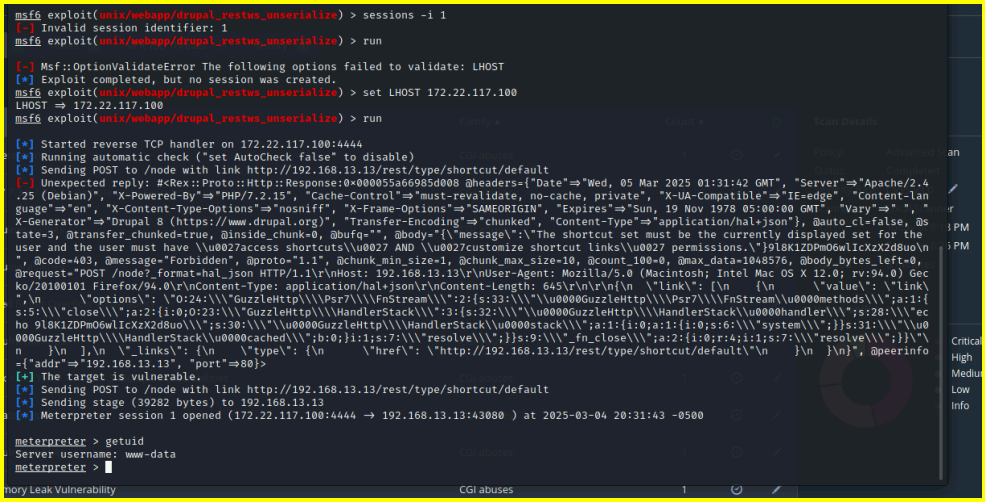
© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

Vulnerability 24	Findings
Title	Escalating Access
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	On the same machine I ran cat /etc/passwd for Flag 9's code
Images	
Affected Hosts	192.168.13.11
Remediation	Limiting User privileges again but as well limiting access to files along with them. On top of repeating the use of a firewall from the previous vulnerability due to this exploit being done on the same machine/server.

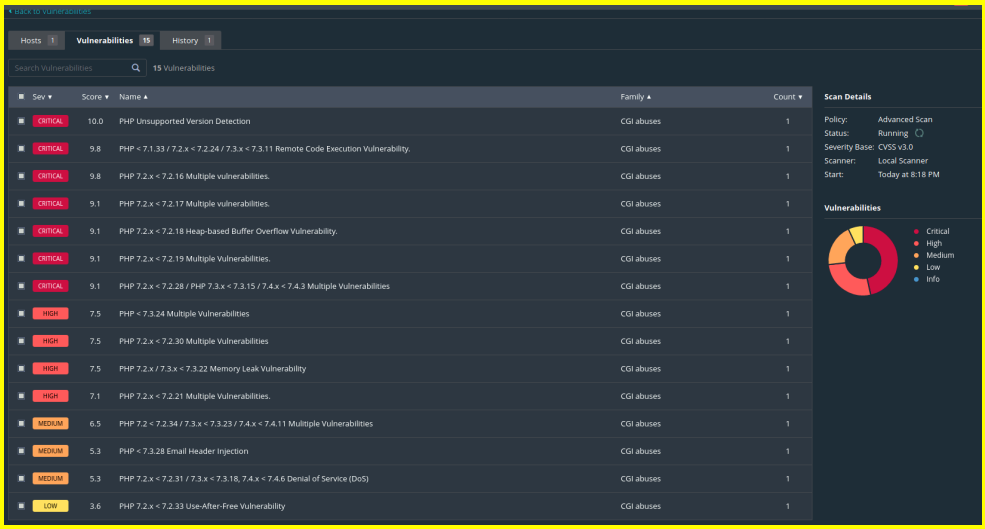
Vulnerability 25	Findings
Title	Struts Exploiting
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	High
Description	Ran another MSFconsole with a Struts exploit instead under the IP 192.168.13.12, then under the exploited machine I used the command cat to make flag 10's code appear.

© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

Images	
Affected Hosts	192.168.13.12
Remediation	Immediately upgrade Apache Struts to version 2.3.32+ or 2.5.10.1+ to patch this critical remote code execution vulnerability, and implement a web application firewall with rules to detect exploitation attempts targeting the Content-Type header.

Vulnerability 26	Findings
Title	Drupal Exploiting
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	Ran another MSFconsole but with an exploit for Drupal and after getting the Meterpreter shell from making the RHOST to 192.168.13.13 and the LHOST 172.22.117.100. I used the command getuid in the exploited shell to give me Flag 11
Images	

© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

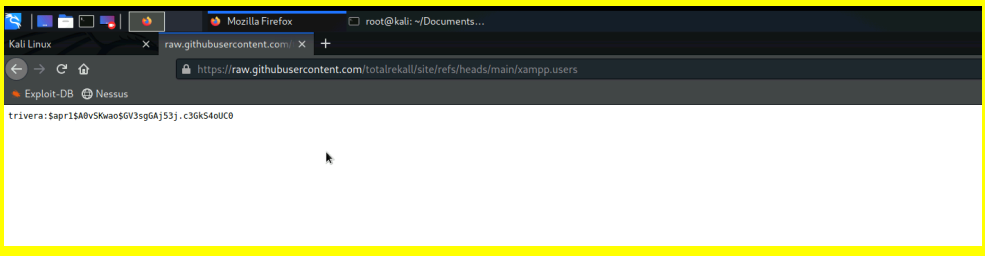
	
Affected Hosts	192.168.13.13
Remediation	Update Drupal core to version 8.6.10/8.5.11 or later to patch the critical remote code execution vulnerability in REST API, and disable the REST API service if not essential for site functionality until patching is complete.

Vulnerability 27	Findings
Title	(.14) exploiting
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	High
Description	In Flag 1 I noticed a sshuserAlice. In the linux terminal I ran ssh alice@192.168.13.14 and trying different passwords I was able to gain access to their server and after I ran a privilege escalation command with cat /root/flag12.txt which resulted in me obtaining Flag 12's code

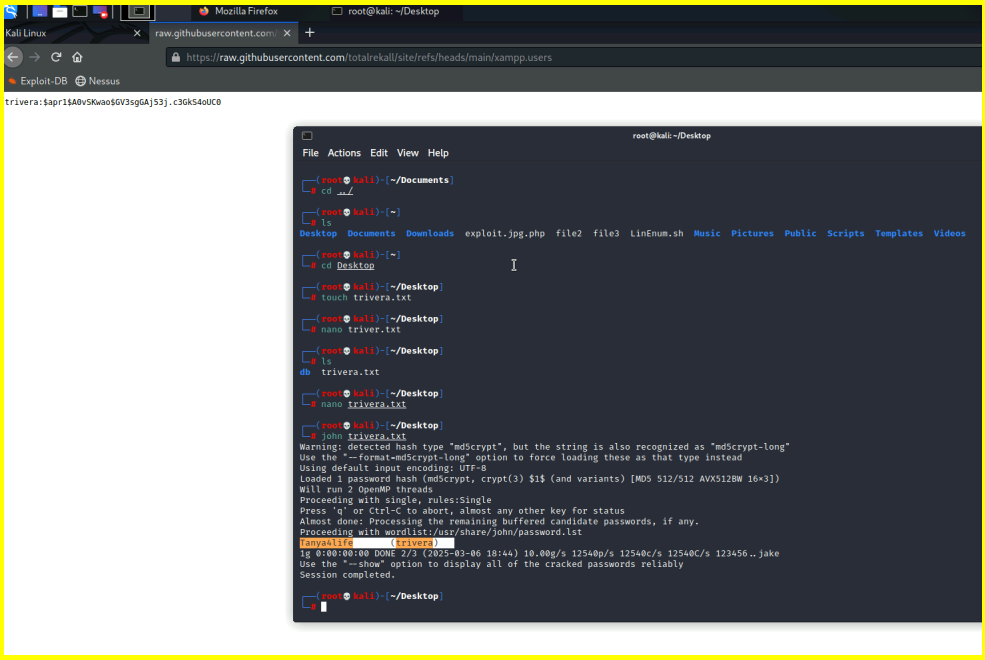
© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

Images	
Affected Hosts	192.158.13.14
Remediation	Update version 1.8.28 or later to patch the privilege escalation vulnerability that allowed users to run commands as root by specifying user ID -1 or 4294967295, and conduct a security audit to identify any potential exploitation attempts through system logs.

Windows OS

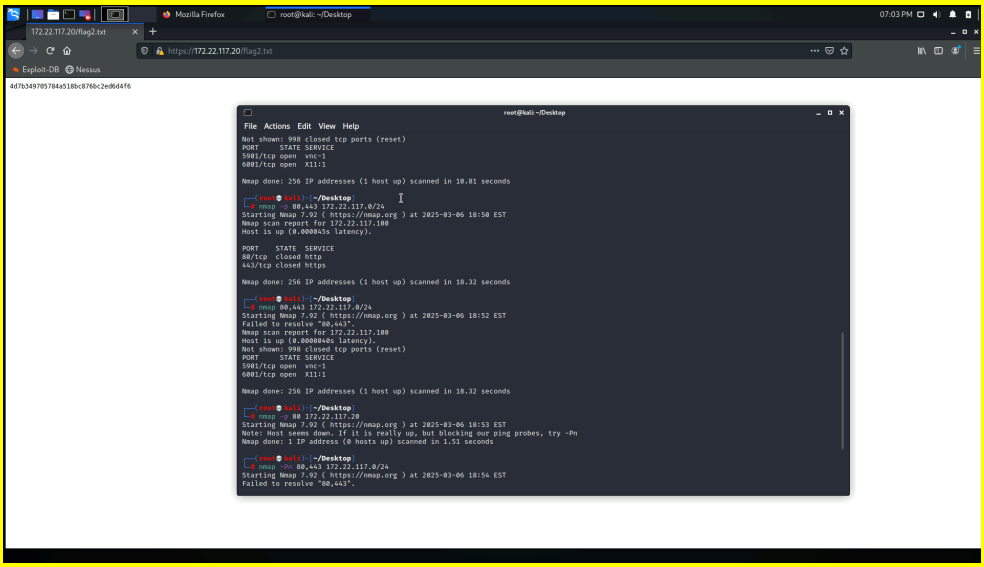
Vulnerability 28	Findings
Title	Github Repository OSINT
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Medium
Description	Using the google search engine by searching totalrekall github page it lead me to a github where it contained an xampp.users.page that had a username and a hashed password. Transferring that hash password into a file and by using john i was able to decipher the hash to Tanya4life which is the password for the username trivera.
Images	

© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

	
Affected Hosts	Github (Website Data)
Remediation	removing the data that is online would be a good start as well to encrypt the data even more to prevent it from being stolen.

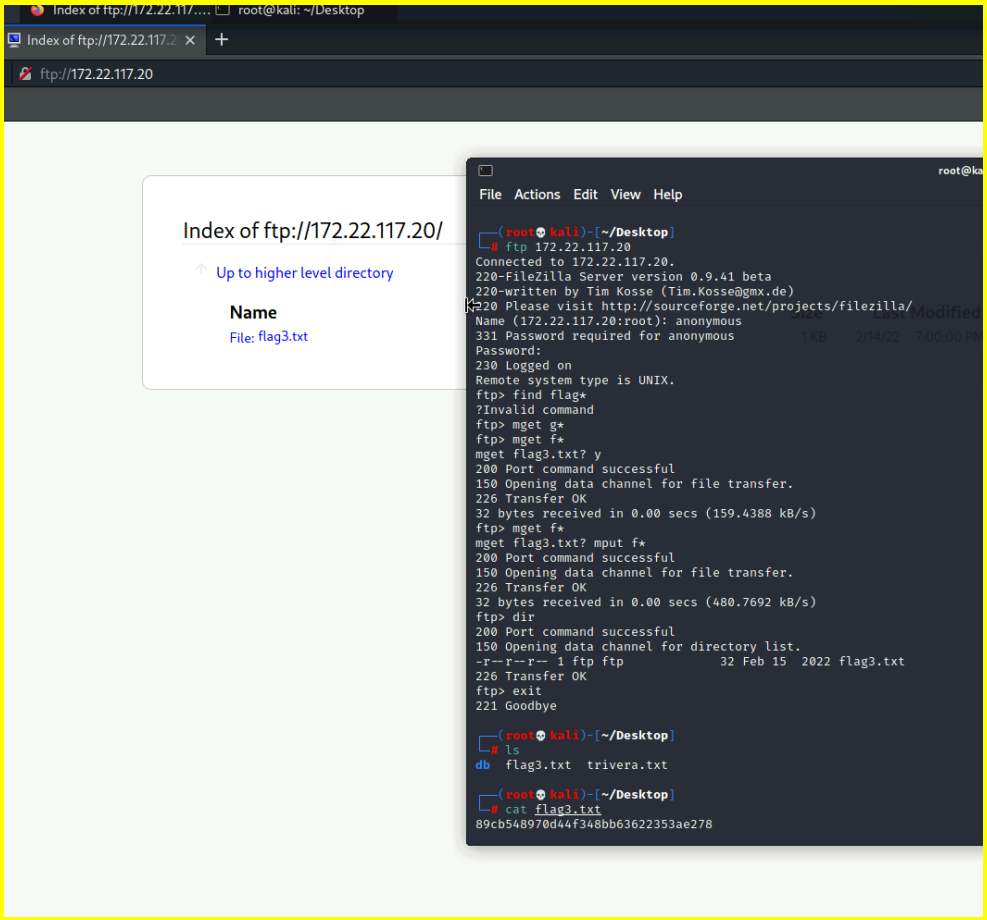
Vulnerability 29	Findings
Title	HTTP Network
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Medium
Description	On the linux terminal using the IP 172.22.117.0/24 I ran a port scan which revealed to me that two machines were open ending in .10 (Win10) and .20(Server2019). When using the Win10 IP ending in .10 I was prompted with a login screen and when entering Flag 1 credentials I was given access and was able to discover flag2.txt which contained the code

© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

Images	
Affected Hosts	172.22.117.20
Remediation	Implement proper network segmentation with firewall rules to restrict unauthorized port scanning activities and limit exposed services to only those necessary for business operations.

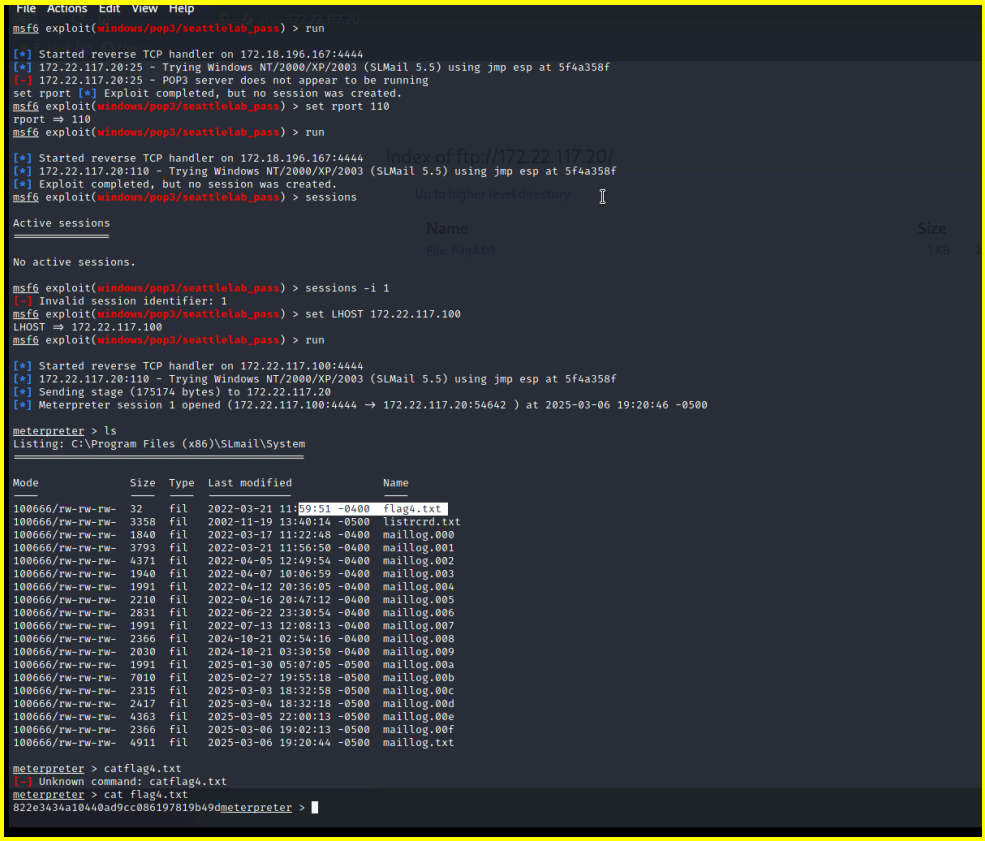
Vulnerability 30	Findings
Title	FTP
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Medium
Description	Using FTP on IP 172.22.117.20 due to the port scan. After logging in with anonymous I was able to retrieve flag3.txt and after downloading it by using the command cat I was able to reveal the code for Flag 3.

© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

Images	
Affected Hosts	172.22.117.20
Remediation	Turn off FTP server access from anonymous users but as well making sure the FTP server makes it required to provided encrypted username and passwords for access.

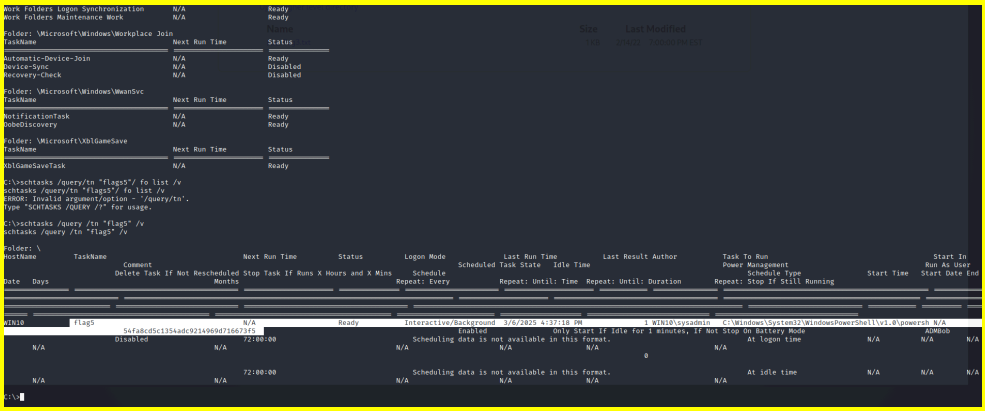
Vulnerability 31	Findings
Title	SLMail Service Exploitation
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Critical
Description	For Flag 4 I ran a MSFconsole with an exploit for SLMail which as well gave me the parameters that SMTP port is 25 and POP3 port is 110. Once setting the RHOST to 172.22.117.20 and rport to 110. I was able to get access to a Meterpreter and after using commands LS I was able to discover the flag4.txt file then by using cat I was able to gain access to the code.

© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

Images	
Affected Hosts	172.22.117.20
Remediation	Implement antivirus for SLmail servers to prevent executable exploits while generating consistent backup profiles with all the necessary data.

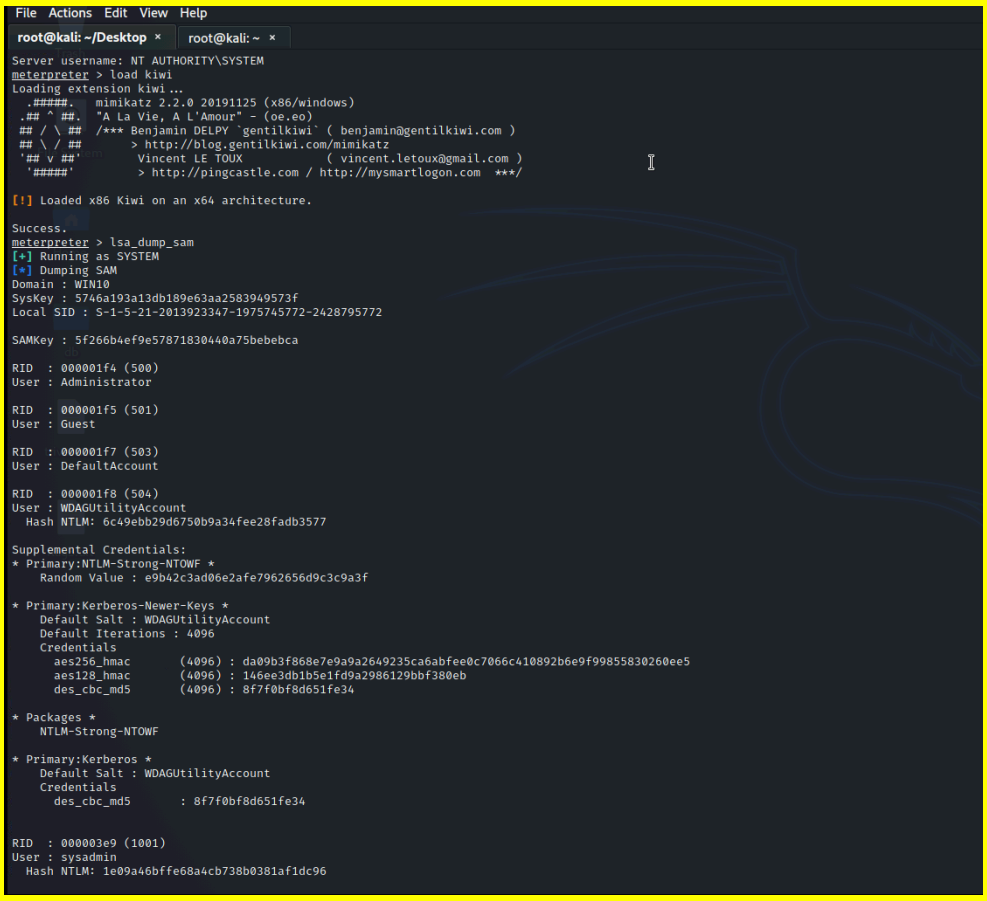
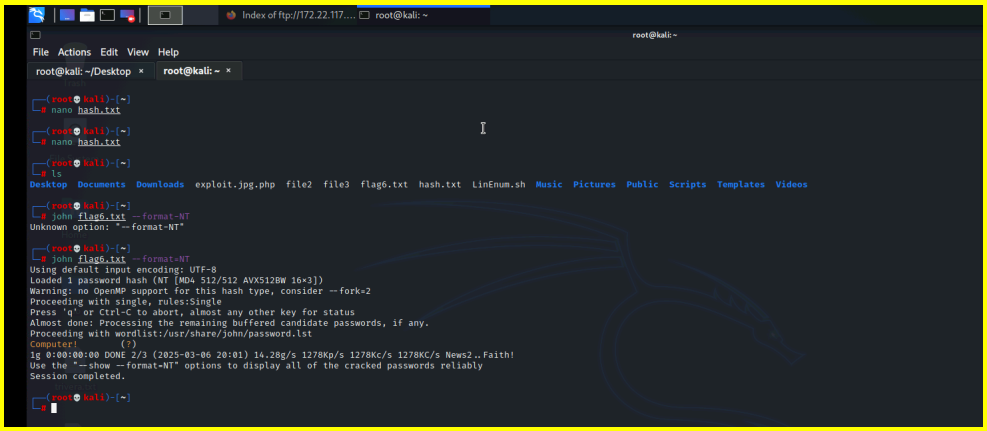
Vulnerability 32	Findings
Title	Scheduled Task on Win10 Exploitation
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	High
Description	I searched for Flag 5 by using the Search Task command which was schtasks / query /tn *flag5* /v this ended up providing me the code I needed to complete Flag 5.

© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

Images	
Affected Hosts	172.22.117.20
Remediation	Audit the scheduled task to figure out tasks that need to be updated or changed entirely while implementing a software to prevent any user having executables without the proper authorization.

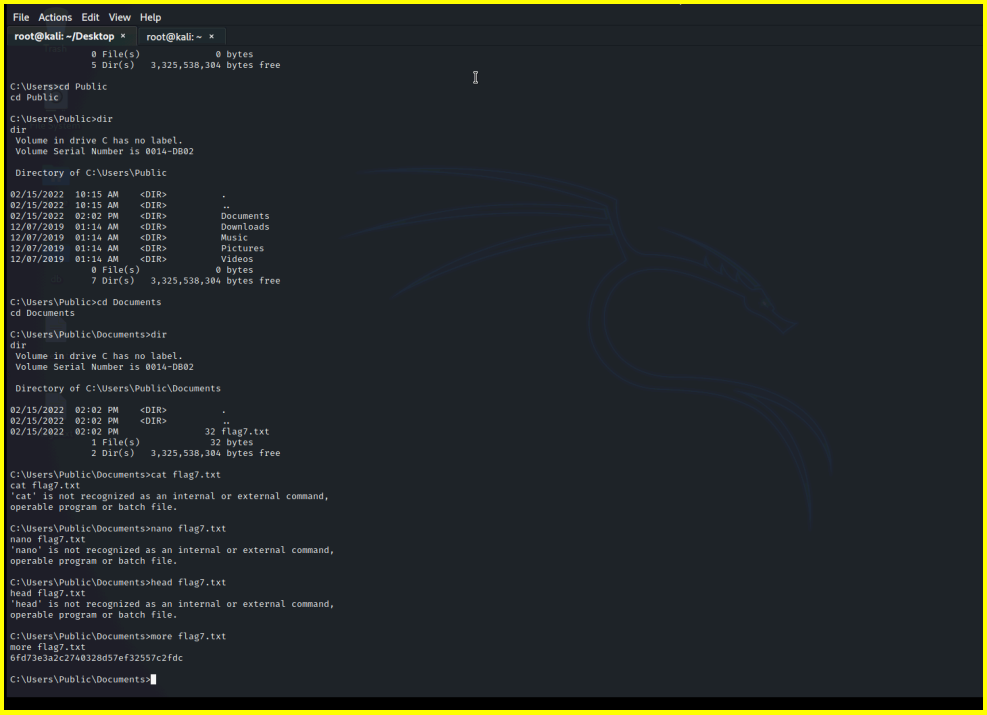
Vulnerability 33	Findings
Title	SLmail exploit on Windows 10
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	High
Description	I ran another MSFconsole with the exploit for SLmail then by loading Kiwi and using the command lsa_dump_sam to give me the user flag6 then after using created a txt file with the hash I used john and format to crack the hash password which resulted in Computer!

© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

Images	 
Affected Hosts	172.22.117.20
Remediation	Audit the accounts of all users making sure they have strong passwords while at the same time checking for any unusual login attempts.

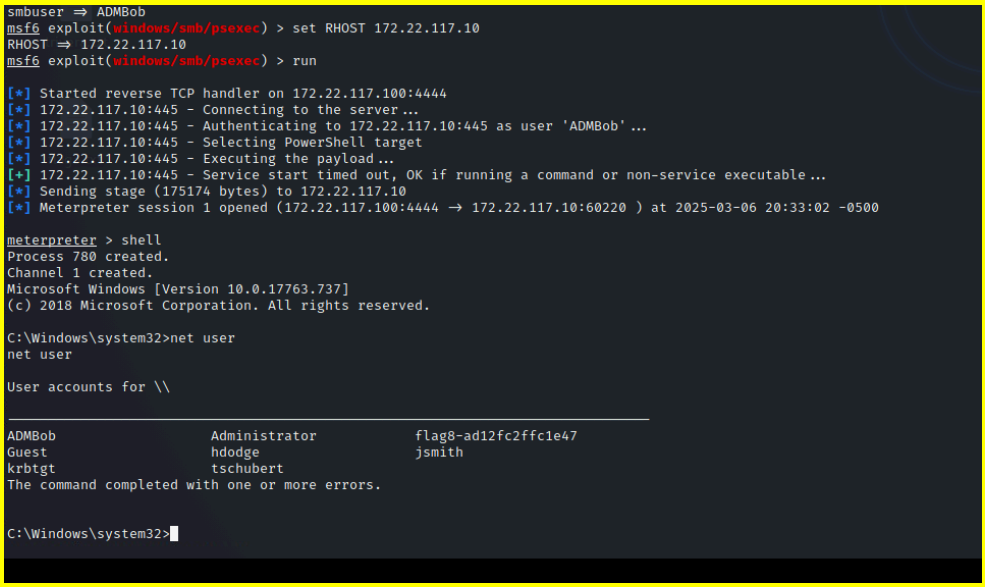
Vulnerability 34	Findings
Title	File Enumeration
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Low

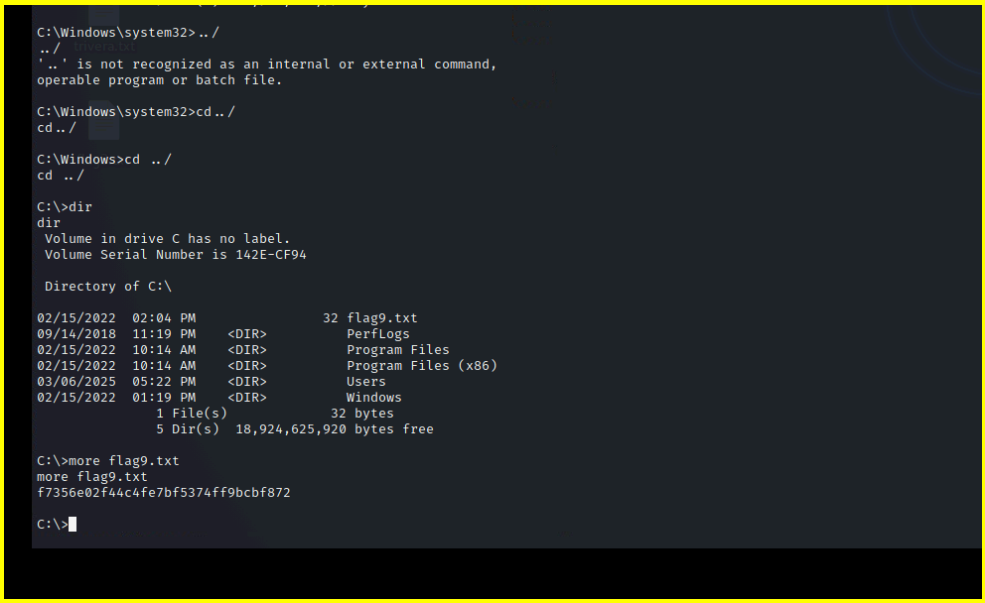
© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

Description	In the Metepreter shell I used search commands to help discover flag7.txt which was in the Users/Public/Documents folder
Images	
Affected Hosts	172.22.117.20
Remediation	Audit user privileges

Vulnerability 35	Findings
Title	Win 10 to Server2019 Exploit
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Critical
Description	I used Kiwi again on the Win 10 to reveal to me that ADMBob had their credentials cached. After solving the hashed password which was Changeme! I used these credentials with the psexec module in metasploit which returned to me a shell containing the Flag 8 code

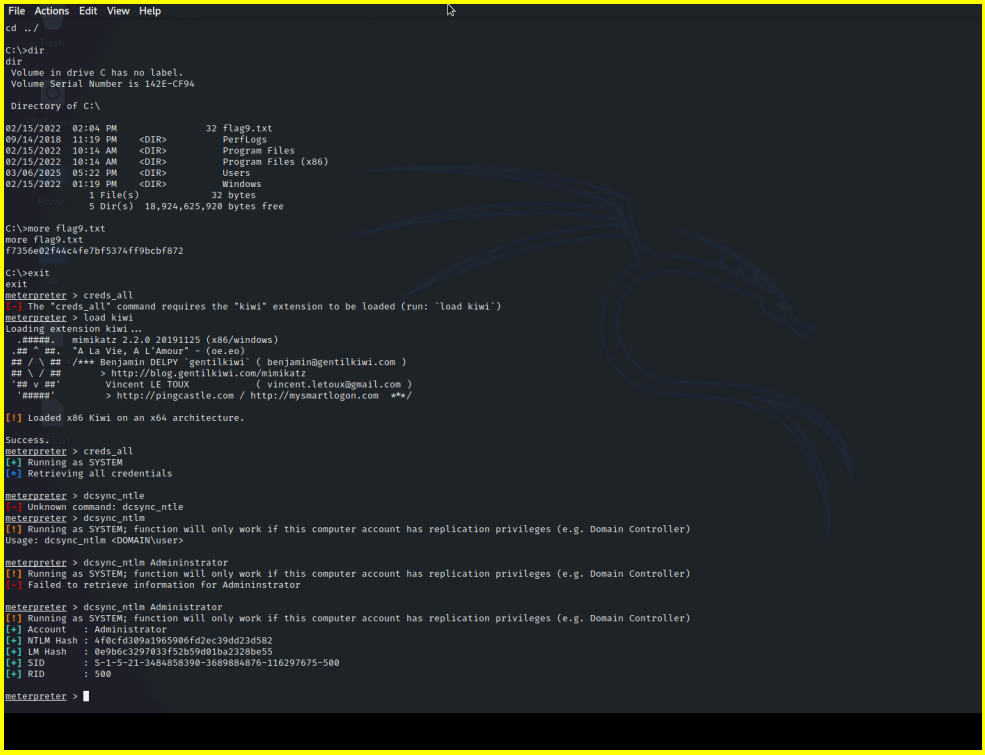
© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

Images	
Affected Hosts	172.22.117.20
Remediation	Again audit user privileges to make sure not everyone has access to root and on top, audit the network to prevent lateral movement being possible to a certain extent.

Vulnerability 36	Findings
Title	Escalating Access
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Critical
Description	In the same exploit I moved to root and listed Directories and then using the command more on flag9.txt to uncover the code.
Images	

© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

Affected Hosts	172.22.117.20
Remediation	Audit user privileges to make sure not everyone has access to root and on top making sure all systems and firewalls are able to detect escalation attempts and if not making sure to implement them asap.

Vulnerability 37	**Findings**
Title	Compromising Admin
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	High
Description	loaded Kiwi and by using dcync_ntlm on Administrators I was able to NTLM hashed password which was the code needed for Flag 10
Images	
Affected Hosts	172.22.117.20
Remediation	Audit users and systems this may involve updating all passwords to all users to make sure none of them have been compromised and/or updating systems to patch the vulnerability that gives any comprised user/system the chance to move throughout the system.

Add any additional vulnerabilities below.

© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

README!

During my time with this project I had multiple sources of help. Many of which came from my peers who were able to get the information and provide the steps on how they completed the task. On top of figuring things out when my groups would get stuck on a flag I would turn to AI to assist with pointing us in the right direction. which in some cases made me go a different path compared to others. I also used AI to help with naming the Title sections for the Windows OS as I simply forgot and did not know how to title each vulnerability. Finally with the help of peers and AI again it allowed me to develop the proper wording for the summaries from Strengths to Weaknesses and as well with the executive summaries to fully complete this Penetration Test Report.

© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.