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	Natasha pentestingcorp
Contact Name	Natasha Harris
Contact Title	pentesters

Document History

Version	Date	Author(s)	Comments
001	06/31/2023	Natasha H.	

© 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.

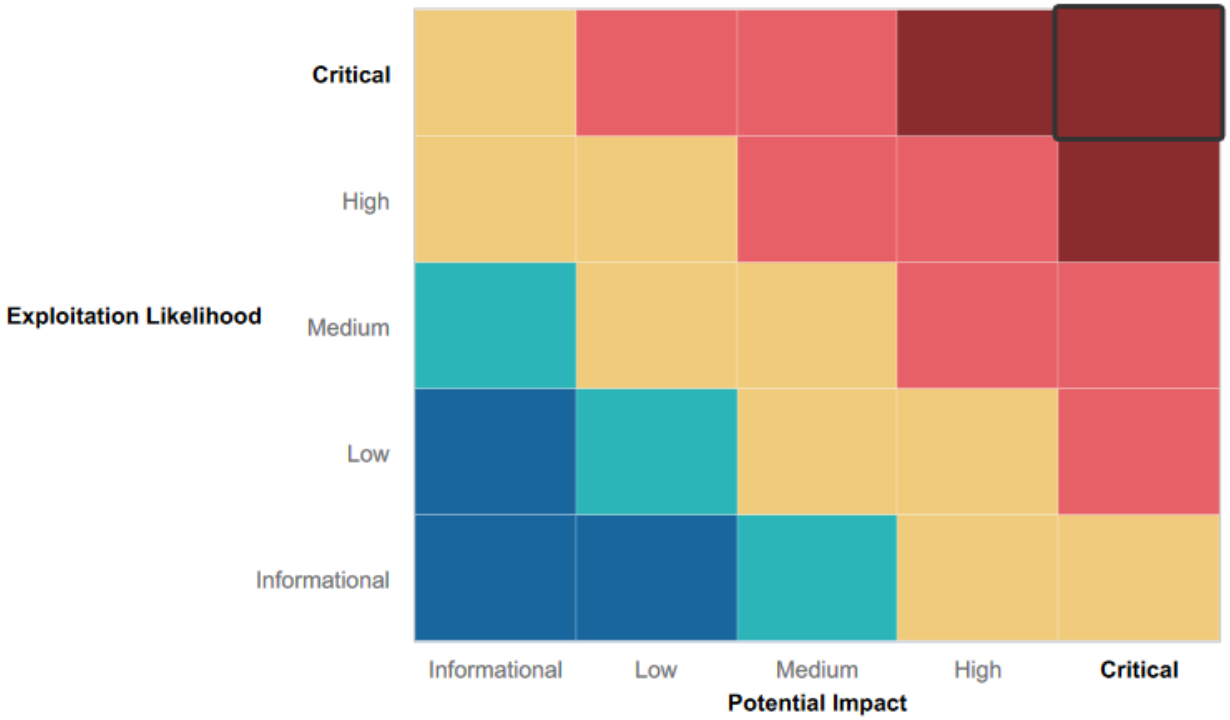
Executive Summary of Findings

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.

- The website looks pretty
- Some system services required user authentication

Summary of Weaknesses

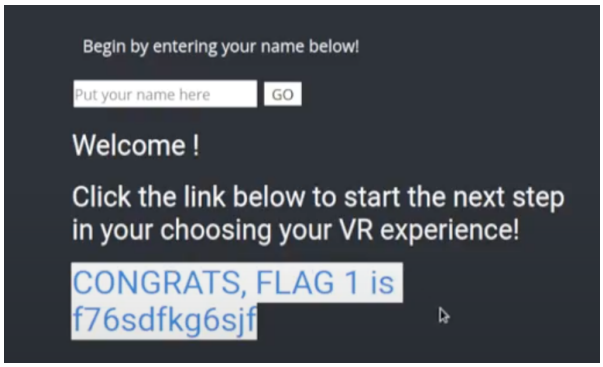
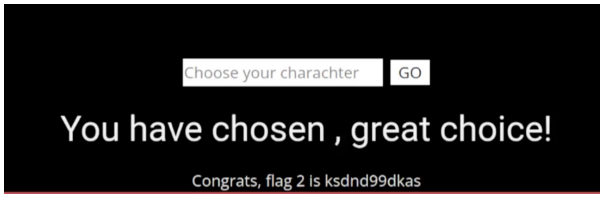
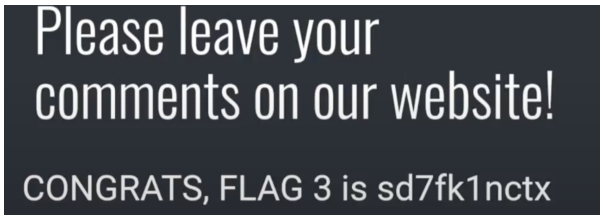
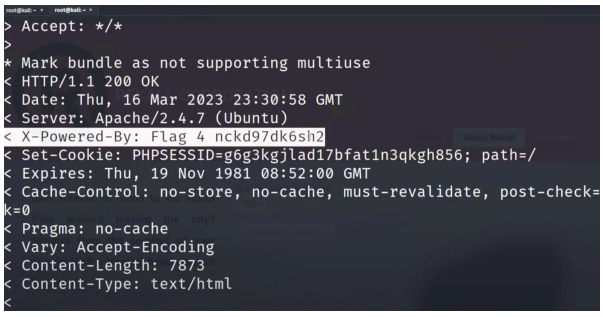
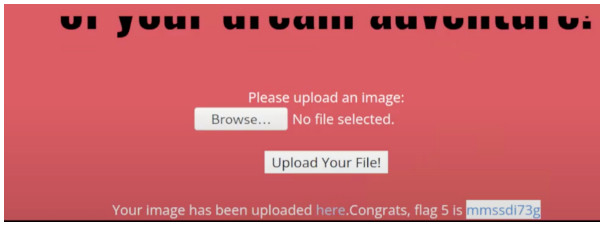
We successfully found several critical vulnerabilities that should be immediately addressed in order to prevent an adversary from compromising the network. These findings are not specific to a software version but are more general and systemic vulnerabilities.

- XSS Reflected
- XSS Stored
- Sensitive Data Exposure
- Local File Inclusion
- Advanced Local File Inclusion
- SQL Injection
- Sensitive Data Exposure
- Command Injection
- Advanced Command Injection
- Weak User Credentials
- PHP Injection
- Session Management
- Directory Traversal

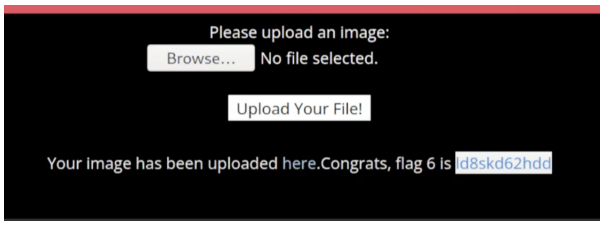
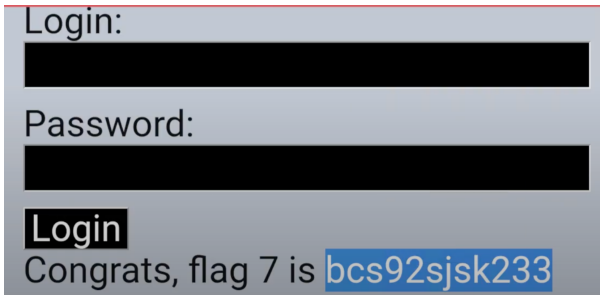
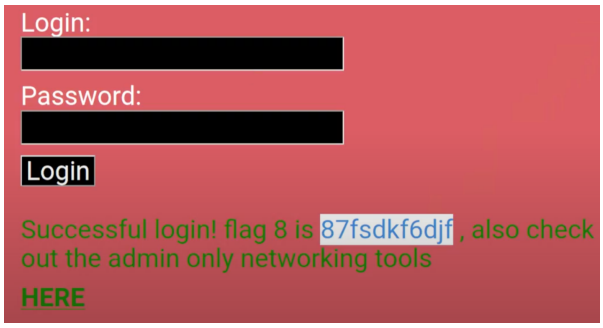
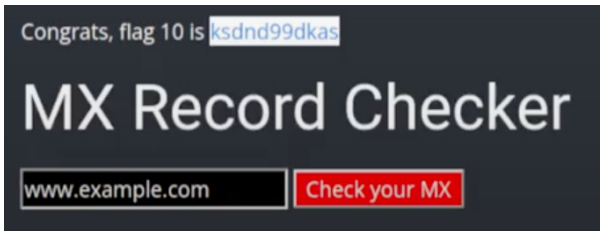
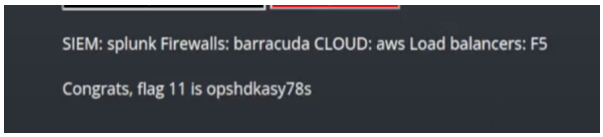
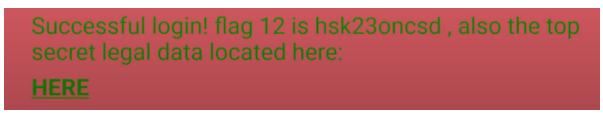
© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

Executive Summary

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

Day 1	Images
Flag 1 Vulnerability: XSS Reflected	
Flag 2 Vulnerability: Advanced XSS Reflected	
Flag 3 Vulnerability: XSS Stored	
Flag 4 Vulnerability: Sensitive Data Exposure	
Flag 5 Vulnerability: Local File Inclusion	

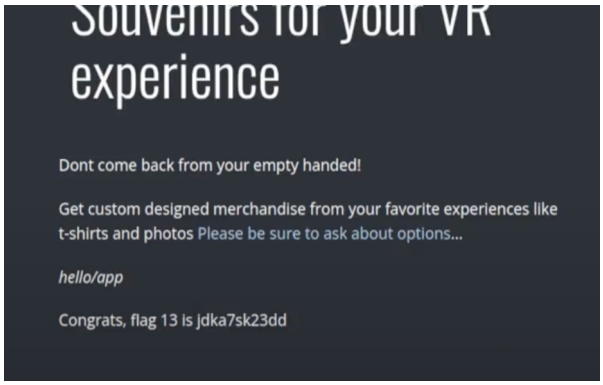
© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

Flag 6 Vulnerability: Local File Inclusion	
Flag 7 Vulnerability: SQL Injection	
Flag 8 Vulnerability: Sensitive Data Exposure	
Flag 9 Vulnerability: Sensitive Data Exposure	
Flag 10 Vulnerability: Command Injection / Session Management vulnerability	
Flag 11 Vulnerability: Command Injection	
Flag 12 Vulnerability: Weak User Credentials	

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

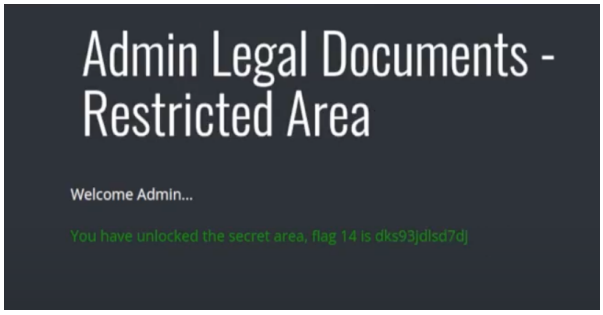
Flag 13

Vulnerability: PHP Injection



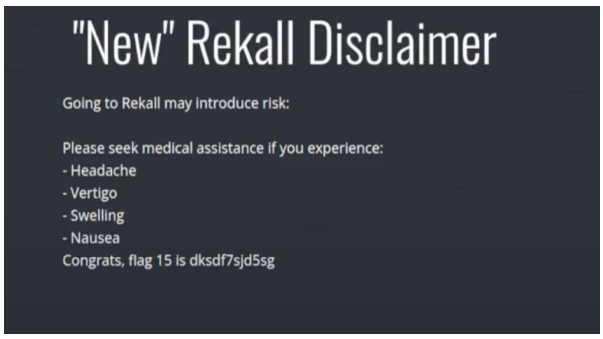
Flag 14

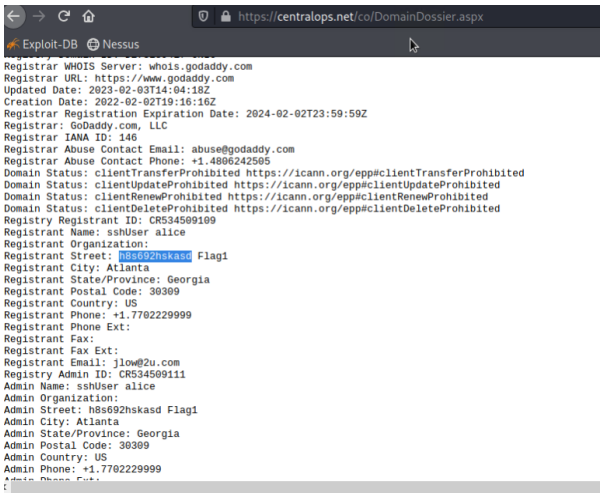
Vulnerability: Session Management



Flag 15

Vulnerability: Directory Traversal

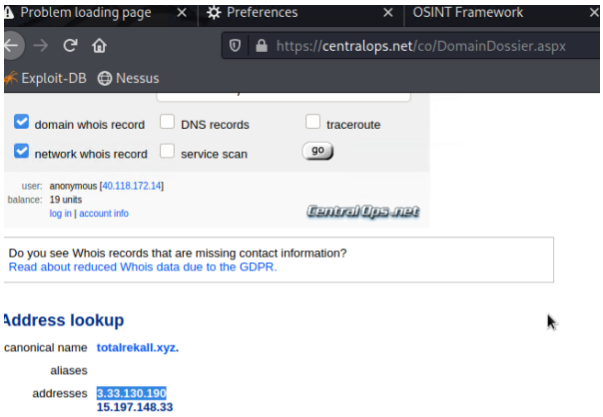


Day 2	Images
Flag 1 Vulnerability: Open Sourced Data	

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

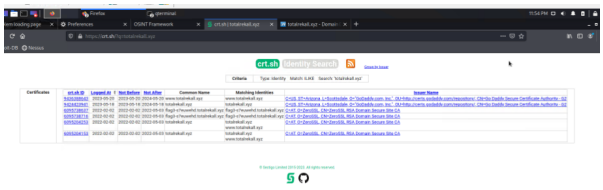
Flag 2

Vulnerability: Open sourced data



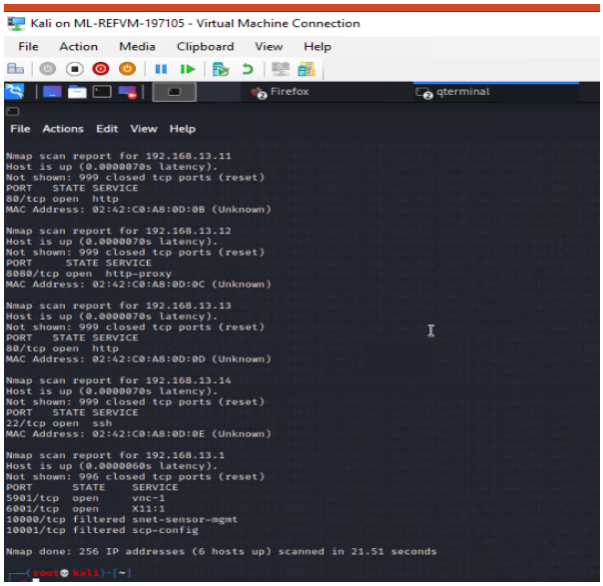
Flag 3

Vulnerability: Open sourced data



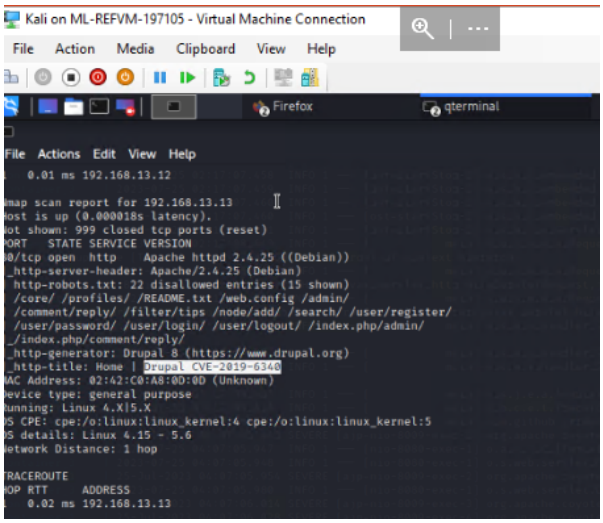
Flag 4

Vulnerability: Total hosts within local network



Flag 5

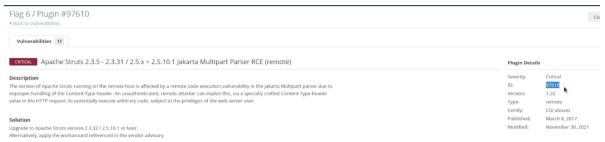
Vulnerability: Drupal, Returned Scan Results



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

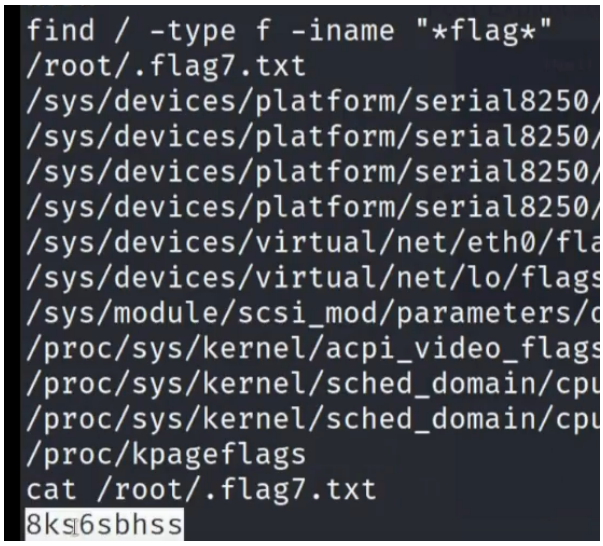
Flag 6

Vulnerability: Apache Struts



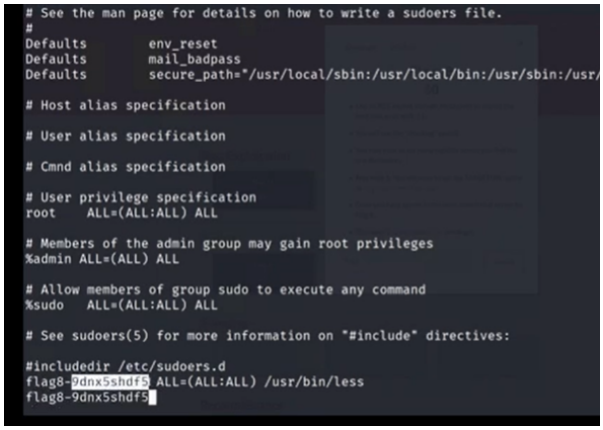
Flag 7

Vulnerability: Apache Tomcat Remote Code Execution

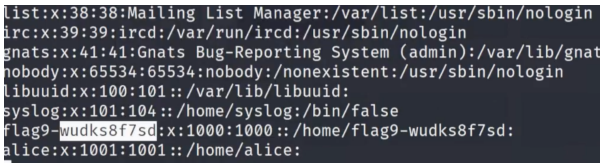


Flag 8

Vulnerability: Shellshock

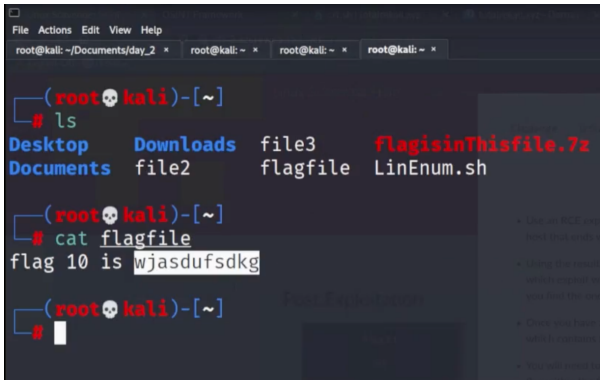


Flag 9

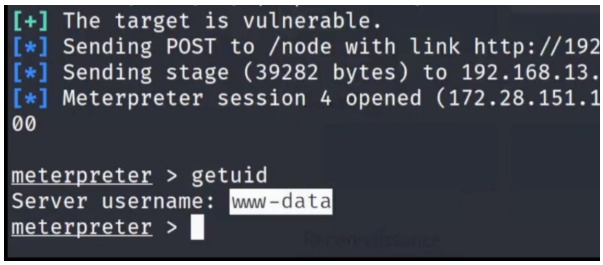
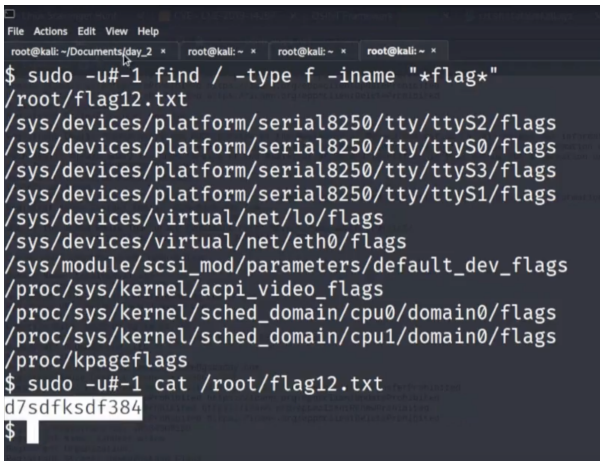


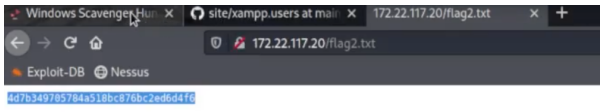
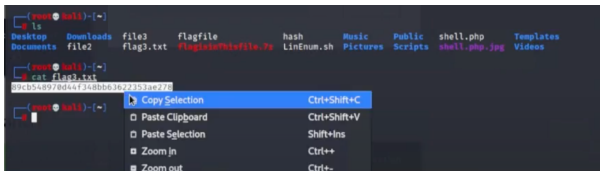
Flag 10

Vulnerability: Struts exploitation

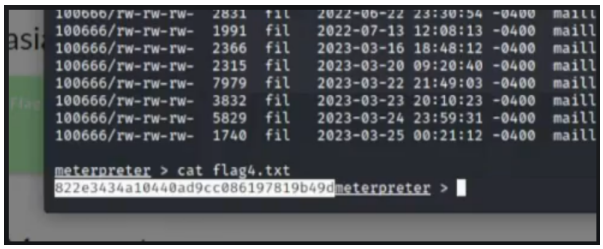
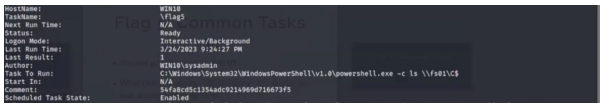
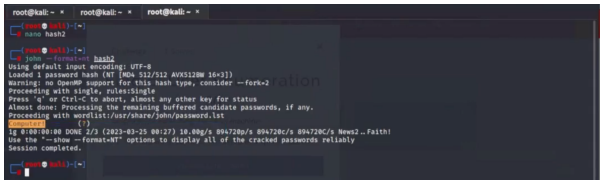
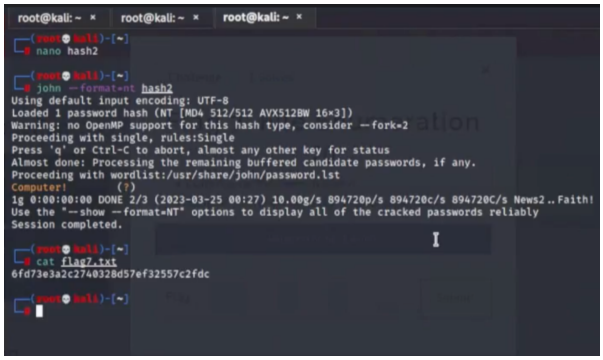
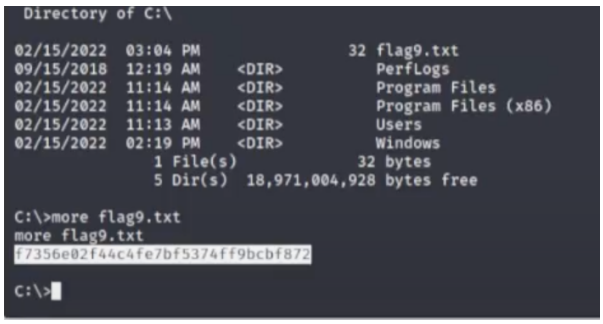


© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

Flag 11	
Flag 12	

Days 3	Images
Flag 1 Vulnerability: Open Source Exposed Information	
Flag 2	
Flag 3	

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

Flag 4	
Flag 5	
Flag 6	
Flag 7	
Flag 8	
Flag 9	
Flag 10	

Summary Vulnerability Overview

Vulnerability	Severity

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

XSS Reflected	low
XSS Stored	Medium
Sensitive Data Exposure	Medium
Local File Inclusion	Critical
Advanced Local File Inclusion	Critical
SQL Injection	Critical
Sensitive Data Exposure	High
Command Injection	Critical
Advanced Command Injection	Critical
Weak User Credentials	Medium
PHP Injection	High
Session Management	Critical
Directory Traversal	Medium

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

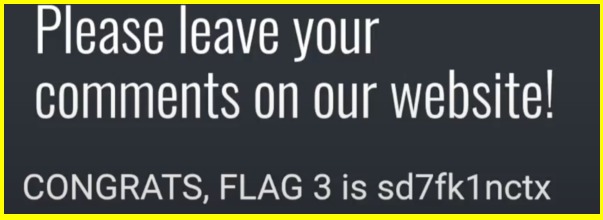
Scan Type	Total
Hosts	172.22.117.0/24
Ports	80, 22, 5901, 6001, 10000, 10001

Exploitation Risk	Total
Critical	6
High	2
Medium	4
Low	1

Vulnerability Findings

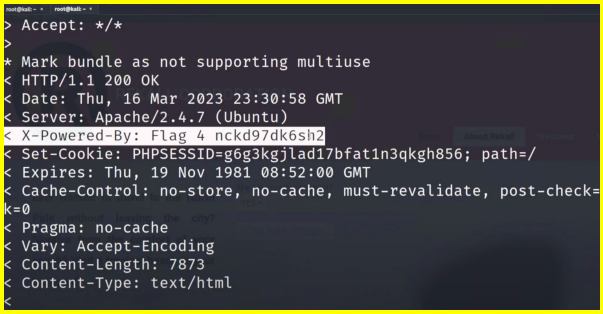
© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

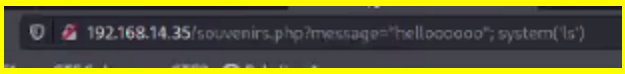
Vulnerability 1	Findings
Title	XSS Reflected
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	Low
Description	The website has a lack of input validation allowing for users to push across html scripting tags to cause the page to return information about their session or to display a notification to users.
Images	
Affected Hosts	192.168.14.35
Remediation	Implement input validation on all user input boxes

Vulnerability 2	Findings
Title	XSS Stored
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Medium
Description	Users can inject html scripting tags into the page to modify how the page reacts to other users, This can allow for malicious users to force others to be redirected to other pages.
Images	
Affected Hosts	totalrekall.com

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

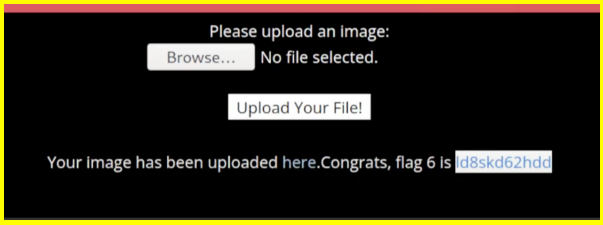
Remediation	Store all user submitted data into a database to be called on and remove directly appending them to the page so they will not be executed on load for the client. Implement input validation to watch for any html script tags as they are not found natively in english.

Vulnerability 3	Findings
Title	Sensitive Data Exposure
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	Medium
Description	Due to a misconfiguration on the machine standard request cause for the machine to return information about the services it is running.
Images	
Affected Hosts	192.168.13.14
Remediation	

Vulnerability 4	Findings
Title	Local File Inclusion
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	Critical
Description	A user can upload a malicious shell script to the website that calls on the server to execute commands pushed across the url
Images	
Affected Hosts	192.168.14.35
Remediation	Implement input validation on all user submitted files, Upload all user

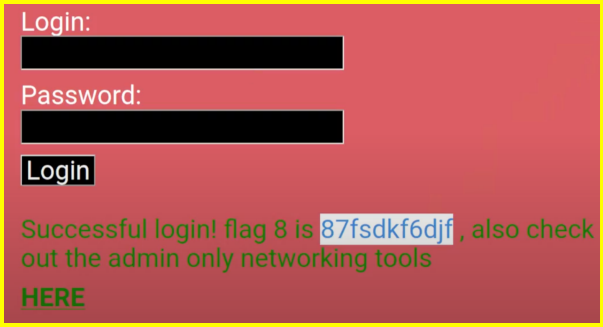
© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

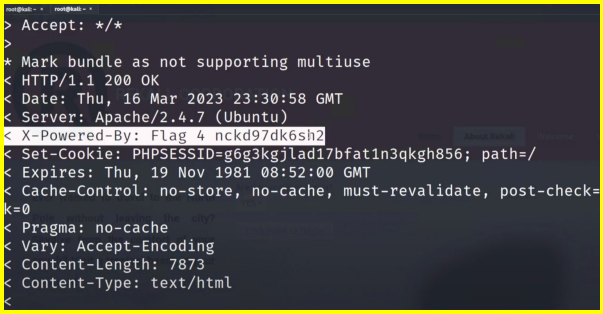
	submitted content to a database to be called on to review direct server execution potential.

Vulnerability 5	Findings
Title	Advanced Local File Inclusion
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	Critical
Description	Even though the server now limits the type of file that a user can upload, A user can still upload a shell file under a different type. Since the server still executes the file it will still allow for remote code execution
Images	
Affected Hosts	192.168.13.14
Remediation	Upload all user submitted files into a backend database that can be called and displayed without directly executing the file being loaded

Vulnerability 6	Findings
Title	SQL Injection
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	Critical
Description	A user can submit the payload ok' '1'='1' –, to cause the sql database to return true validating the user to log in even though they did not provide a valid password

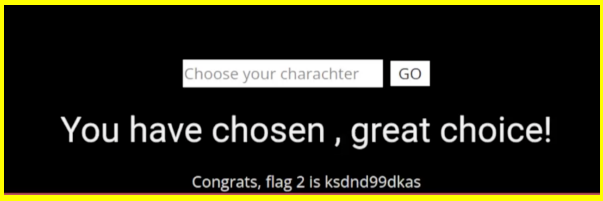
© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

Images	
Affected Hosts	192.168.13.14
Remediation	Implement input validation on all logins to catch for sql syntax, Normalize the server input to look for valid logins and drop anything defined outside normal password syntax

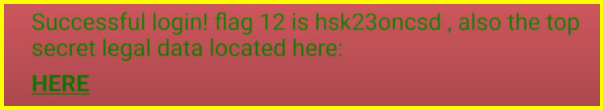
Vulnerability 7	Findings
Title	Sensitive Data Exposure
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	High
Description	When a user submits a request for the welcome page the server is mis configured and sends the user excess information, including the direct service running the server.
Images	
Affected Hosts	192.168.13.14
Remediation	Reconfigure the server's settings when responding to a request at this page.

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

Vulnerability 8	Findings
Title	Command Injection
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	Critical
Description	Users are able to submit commands through the websites mx record checker
Images	
Affected Hosts	192.168.13.14
Remediation	Implement input validation on all user submitted information, Remove the ability to submit symbols into the web form as they are not found in the standard english language when speaking.

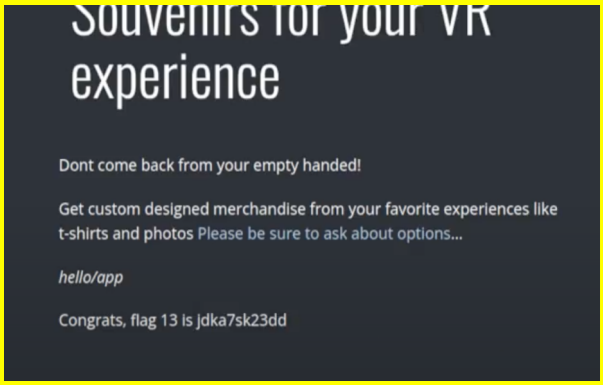
Vulnerability 9	Findings
Title	Advanced Command Injection
Type (Web app / Linux OS / WIndows OS)	web app
Risk Rating	critical
Description	In this input field the website has input validation to catch for ampersand characters but the website does not catch the pipe operator ||.
Images	
Affected Hosts	192.168.13.14
Remediation	Redefine the characters that are usable within the input box to strictly those found within standard english language.

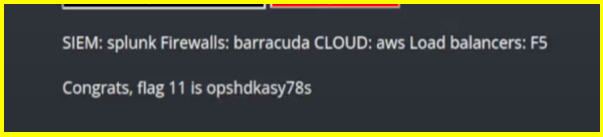
© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

Vulnerability 10	Findings
Title	Weak User Credentials
Type (Web app / Linux OS / WIndows OS)	web app
Risk Rating	Medium
Description	Due to a previous vulnerability allowing users to request the /etc/passwd file, we discover all users available within the environment, with this they are able to use a brute force attack to discover the user malina's password is malina.
Images	
Affected Hosts	192.168.13.14
Remediation	Change user credentials and fix the previous mentioned vulnerabilities to remove attackers ability to determine users found within the environment.

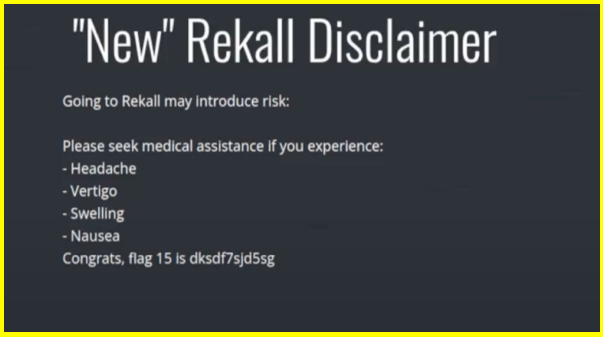
Vulnerability 11	Findings
Title	PHP Injection
Type (Web app / Linux OS / WIndows OS)	web app
Risk Rating	High
Description	An attacker is able to submit malicious php queries through the url when requesting a page from the server.

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

Images	
Affected Hosts	192.168.13.14
Remediation	Disable the ability for the server to execute arbitrary requests, specify the list of pages a user is able to access with user role management dependent on the submitted cookie associated with their user.

Vulnerability 12	**Findings**
Title	Session Management
Type (Web app / Linux OS / WIndows OS)	web app
Risk Rating	critical
Description	An individual is able to notice an ID declaration in the url bar for the admin page. Using a brute forcing tool they are able to increment through as many id's as they may need, to find the correct id for the administrator.
Images	 
Affected Hosts	192.168.13.14
Remediation	Implement session management through user cookies rather than the url bar. and randomize the users id through random number generation.

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

Vulnerability 13	Findings
Title	Directory Traversal
Type (Web app / Linux OS / WIndows OS)	web app
Risk Rating	medium
Description	A user is able to request different subpages within the website to be displayed through the URL bar. With the previous vulnerability of command injection the user can
Images	
Affected Hosts	192.168.13.14
Remediation	Disable the ability for the server to execute arbitrary requests, specify the list of pages a user is able to access with user role management dependent on the submitted cookie associated with their user.

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