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	Swish Corp
Contact Name	Jonathan Dunn
Contact Title	Pen Tester

Document History

Version	Date	Author(s)	Comments
001	07-02-2023	Jonathan Dunn	

© 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.

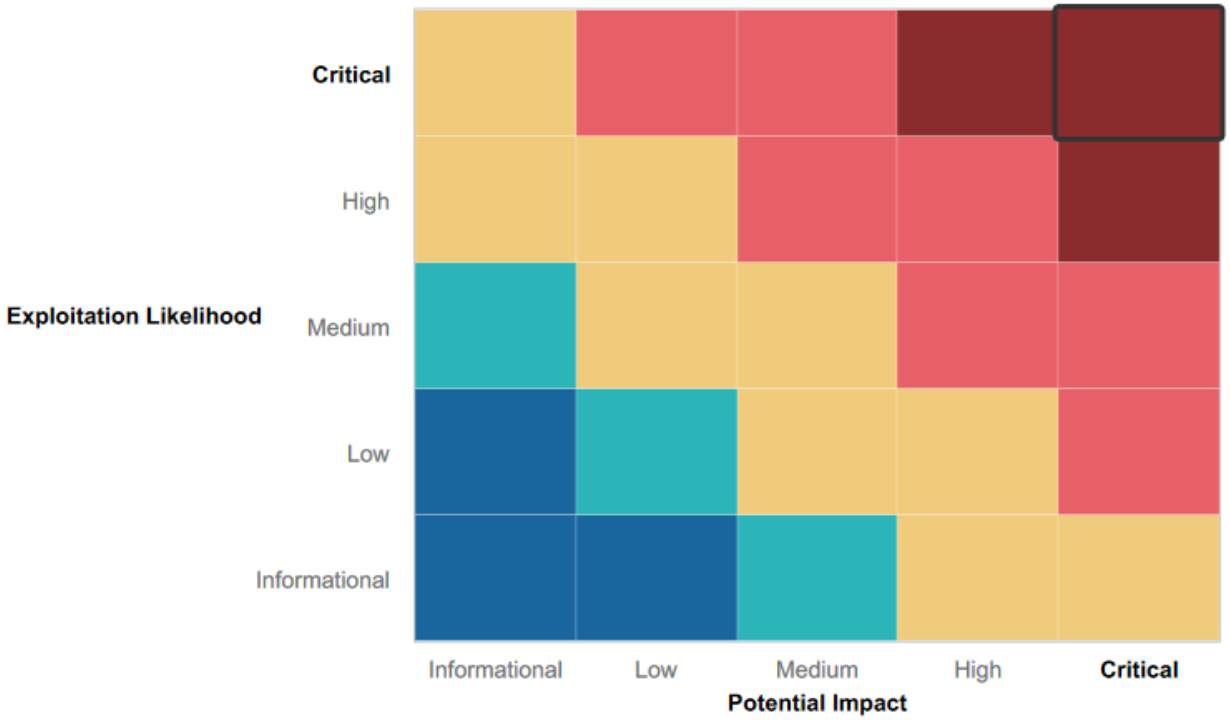
Executive Summary of Findings

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.

- Hackers cannot access the root or administration user's system because sudo privileges aren't available, and staff aren't opening phishing emails.
- Exploitation details
- To prevent unauthorized access, tools such as Nmap and Metasploit are used

Summary of Weaknesses

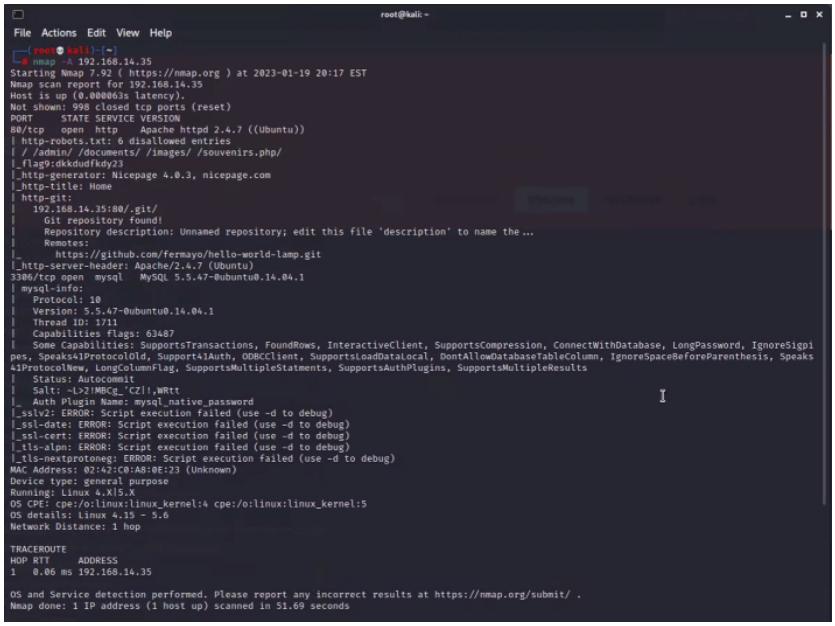
We successfully found several critical vulnerabilities that should be immediately addressed in order to prevent an adversary from compromising the network. These findings are not specific to a software version but are more general and systemic vulnerabilities.

- Block ports 22 and 80, and 135
- It is possible for attackers to access user accounts and compromise sensitive information
- There are multiple vulnerabilities in Apache's web server
- The physical address of Rekall is available to the public

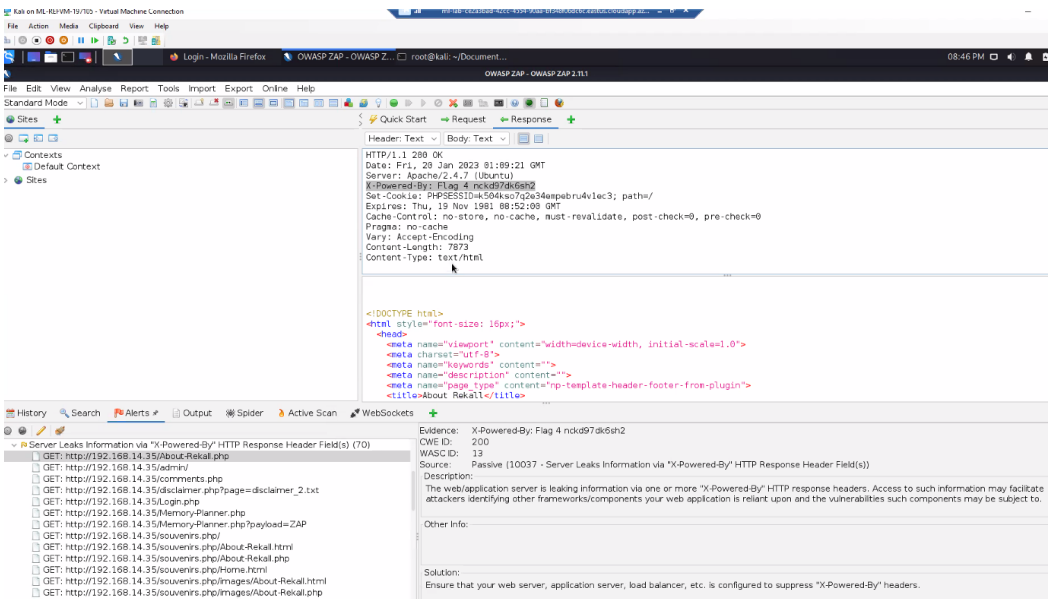
© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

Executive Summary

Found several vulnerabilities during penetration test, some of which could be easily exploited by malicious actors. One key finding from the test was that the company's firewall was vulnerable to being accessed simply from the internet. Additionally, a vulnerability in the company's email server could allow hackers to gain access to confidential information, and another vulnerability in the email server could allow attackers to spoof emails. Rekall Corp. recommends that their security be reviewed and their firewalls be updated as part of this process.

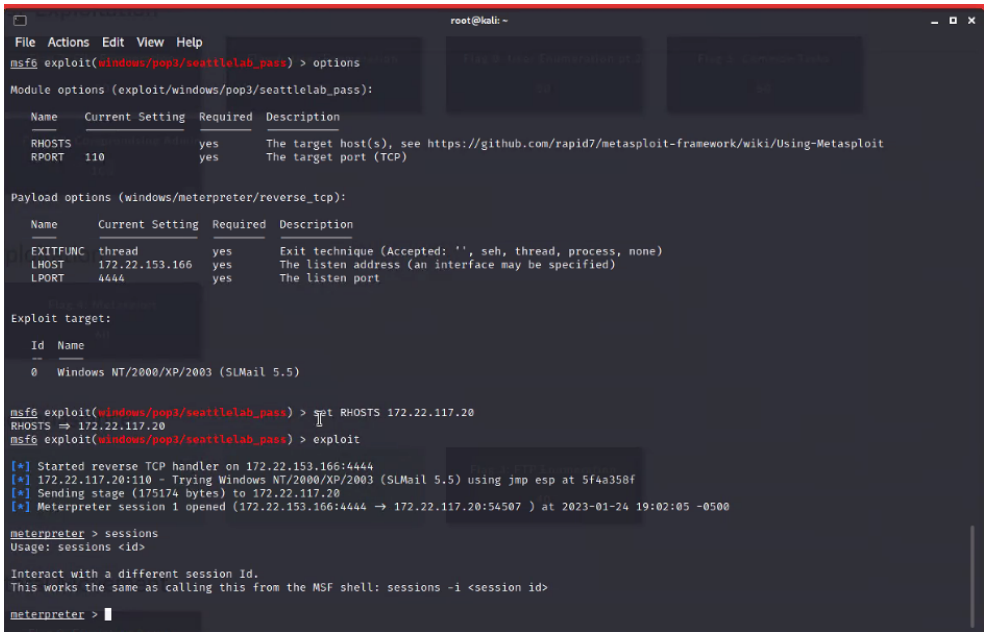


(Nmap scan 192.168.14.35)



(Leaked Server Info - OWASP Tool - About-Rekall.php)

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



Metasploit

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

Summary Vulnerability Overview

Vulnerability	Severity
The firewall helps enables access to the network through the internet.	High
The web server makes it possible for attackers to obtain private data.	Medium
A weakness in the email server that can allow spoofing of emails by an attacker.	Medium
FTP port 21 is open	High
Public Documents and Folder Storing Sensitive Data	High
The IP address is visible to Nmap scan	Critical
SQL Injection	Critical
Shellshock on Web Server (port 80)	Critical
Sensitive Data Exposure	Critical
Linux Privilege Escalation	Critical
User Credential Exposure	Critical
Open Source Exposed Data	High
Tomcat Remote Code Execution Vulnerability	High
Port SLMail Exploited Through Metasploit	Critical

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

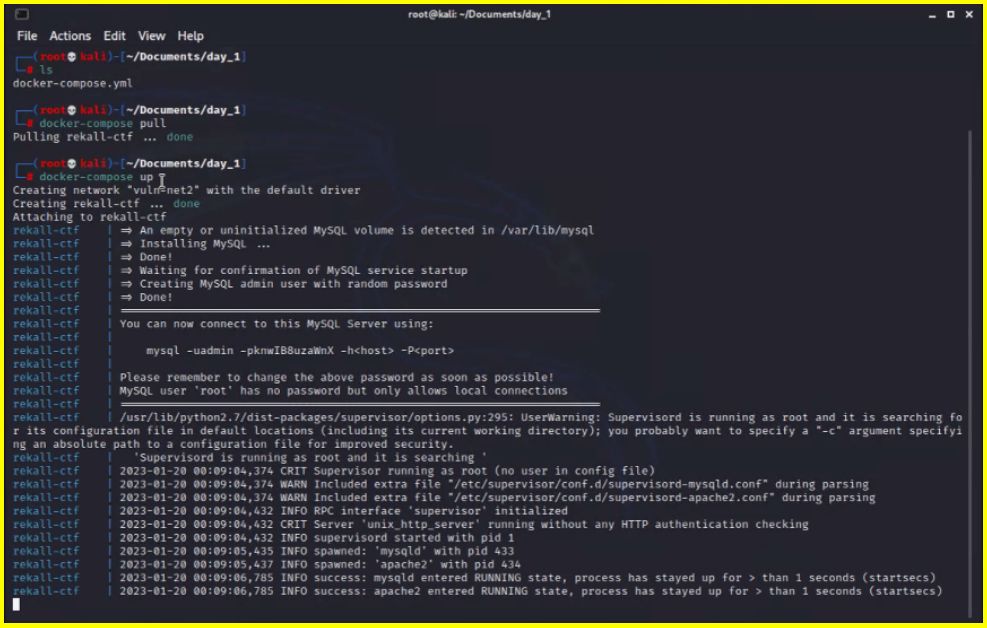
Scan Type	Total
Hosts	192.168.14.0/24 192.168.13.14 192.168.13.11 172.22.117.20 192.168.13.13
Ports	22, 80, 135

Exploitation Risk	Total
Critical	14
High	5

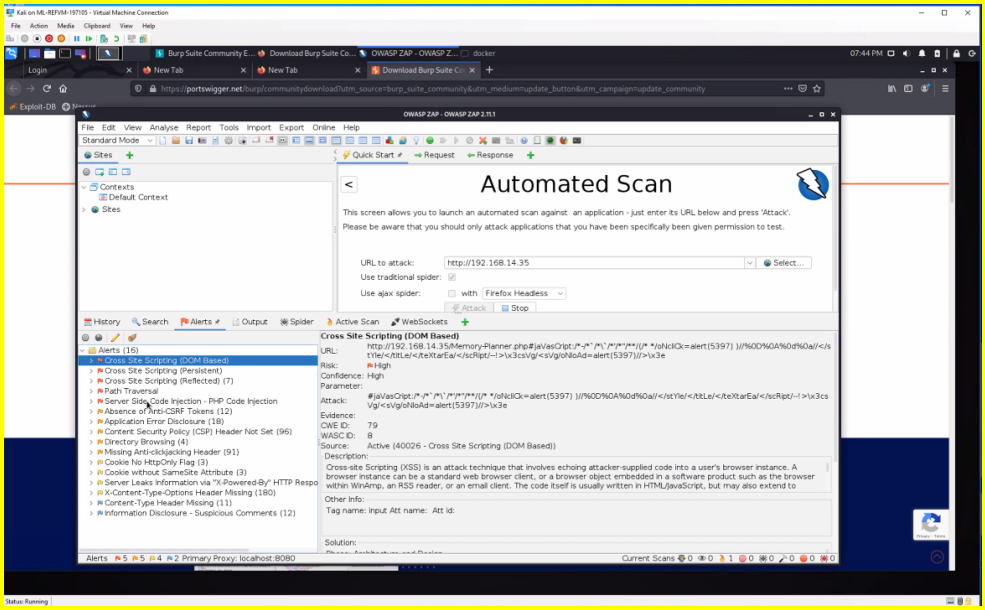
© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

Medium	3
Low	0

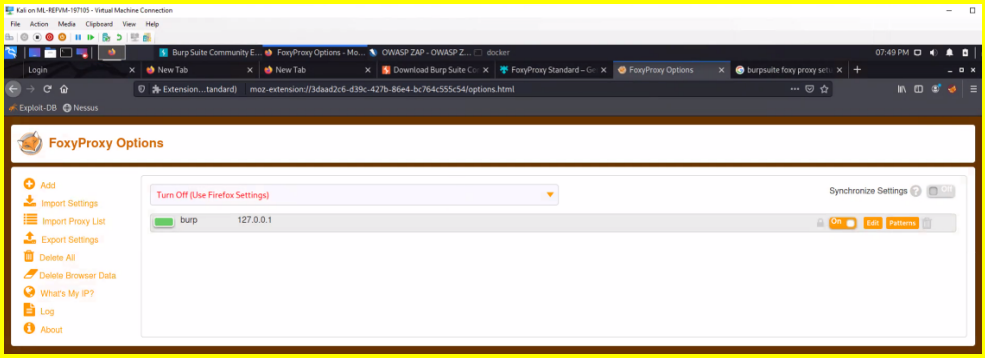
Vulnerability Findings

Vulnerability 1	Findings
Title	SQL Database Provide Credentials
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	High
Description	Database startup provided free credentials
Images	
Affected Hosts	192.168.14.35
Remediation	Update passwords and turn on encryption

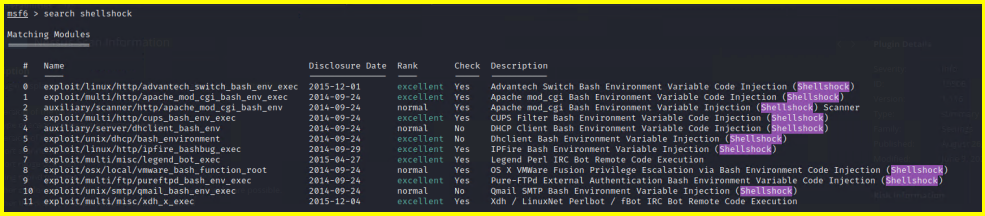
© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

Vulnerability 2	Findings
Title	OWASP ZAP
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	High
Description	Passive Active Scanning
Images	
Affected Hosts	192.168.14.35
Remediation	Develop a secure coding practises strategy.

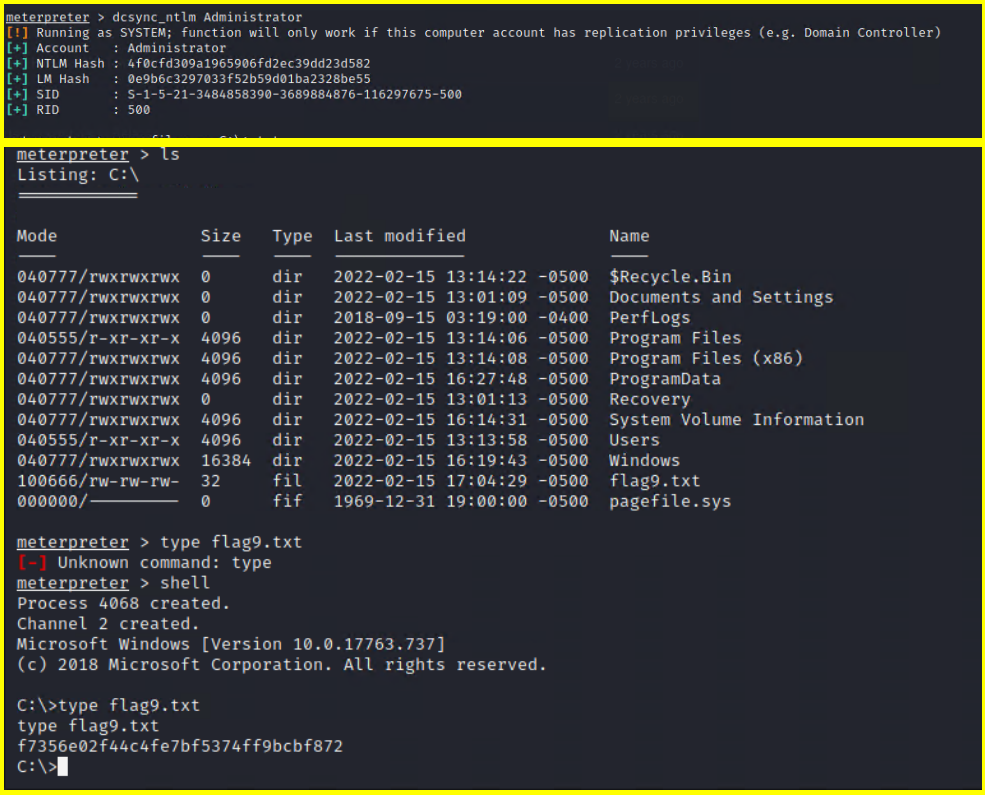
© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

Vulnerability 3	Findings
Title	Foxyproxy
Type (Web app / Linux OS / WIndows OS)	Linux os
Risk Rating	Medium
Description	Bypassing Internet Censorship
Images	
Affected Hosts	127.0.0.1
Remediation	Check the proxy servers. Take care with sensitive information.

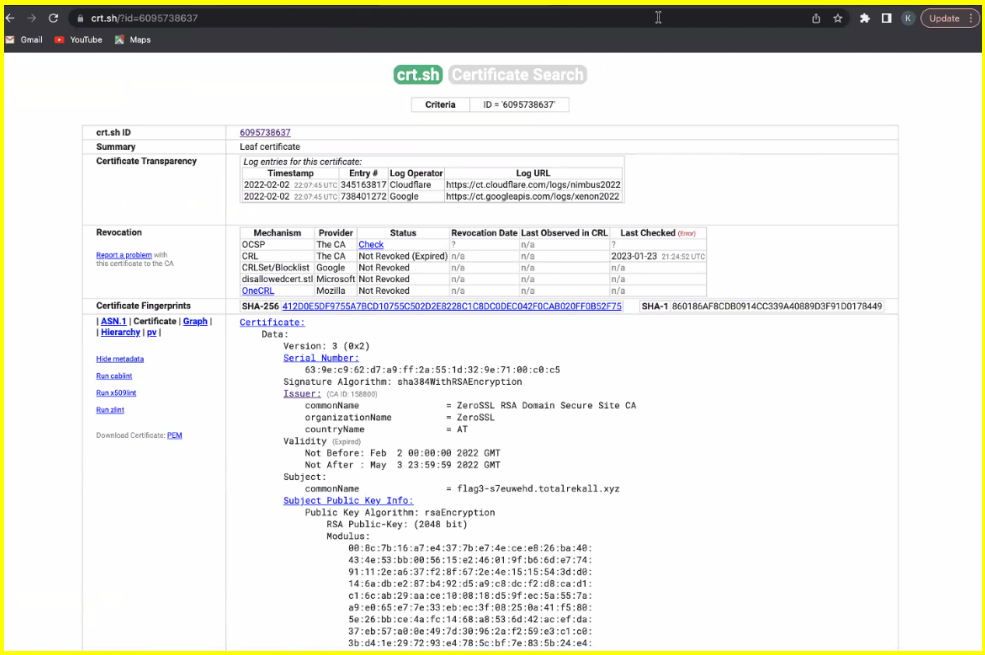
© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

Vulnerability 4	Findings
Title	Shellshock
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	Use sudoers and apache to grant root privileges
Images	
Affected Hosts	192.168.13.14
Remediation	impose restrictions on all sudo accounts

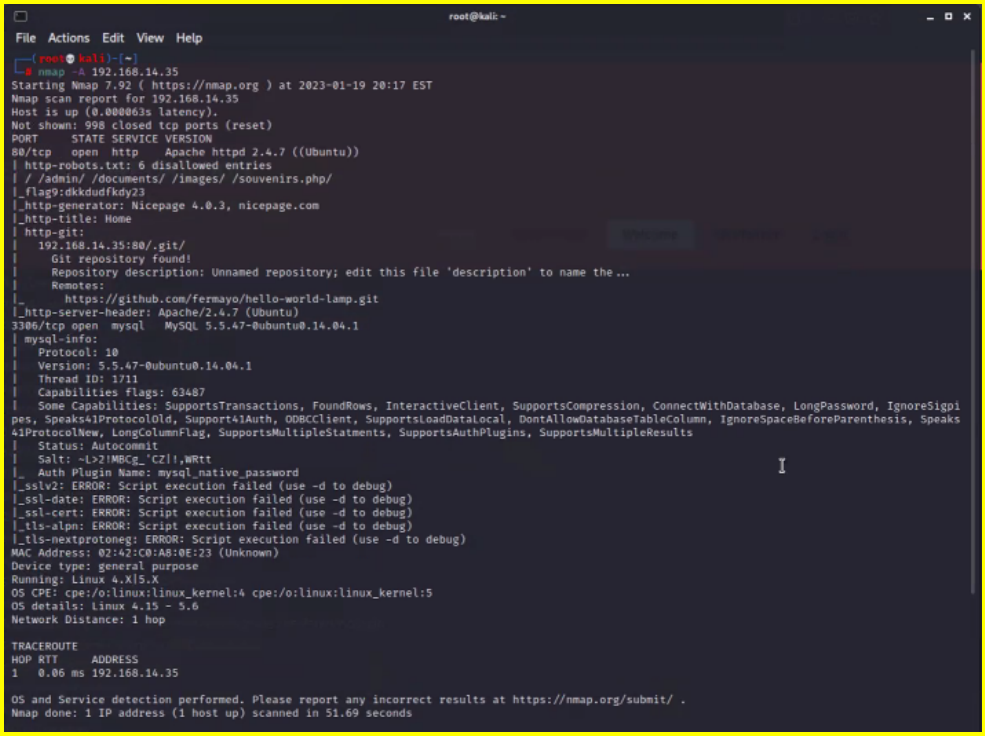
© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

Vulnerability 5	Findings
Title	Meterpreter
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	Payload Exploitation
Images	
Affected Hosts	192.168.13.12
Remediation	Use Updates

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

Vulnerability 6	Findings
Title	Certificate Search
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Medium
Description	Rekall Search on crt.sh
Images	
Affected Hosts	34.102.136.180
Remediation	Accessible information on the crt.sh website, thus preventing information from being exposed to the site would be necessary to address the issue.

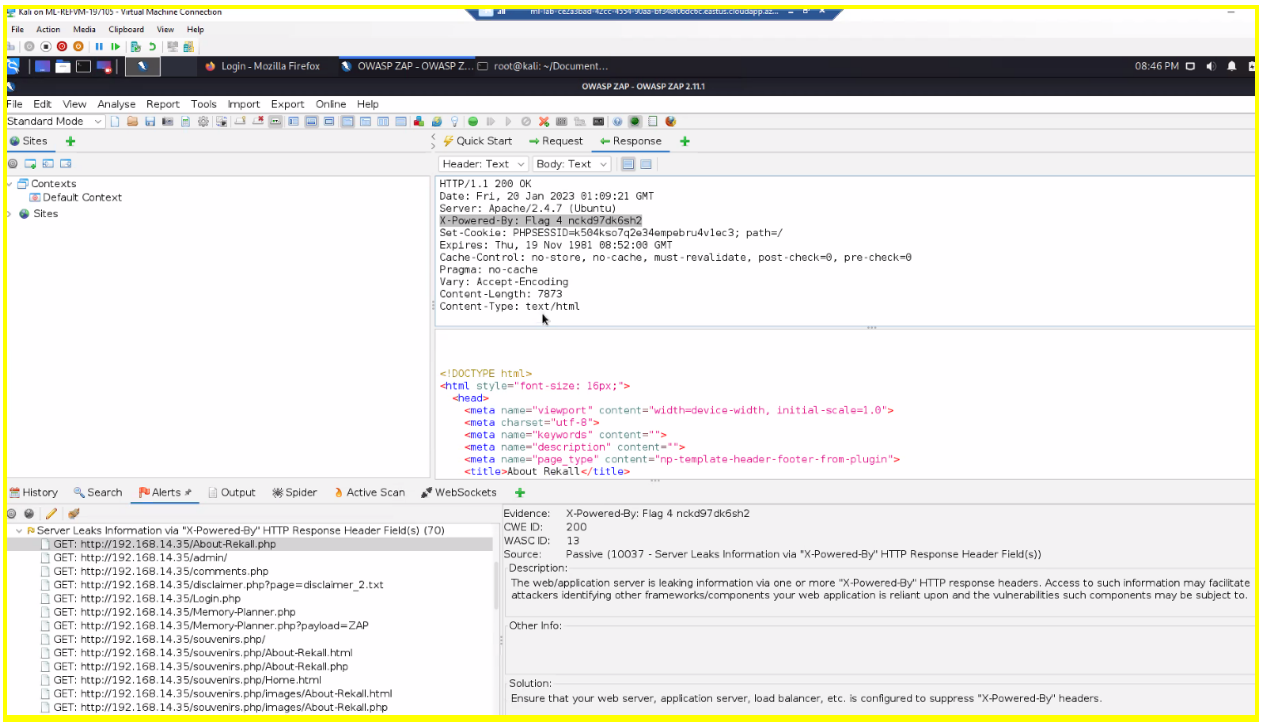
© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

Vulnerability 7	Findings
Title	Nmap Scan Results
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	Nmap scan 192.168.14.35
Images	
Affected Hosts	192.168.14.35
Remediation	For unauthorized users, IP blocking

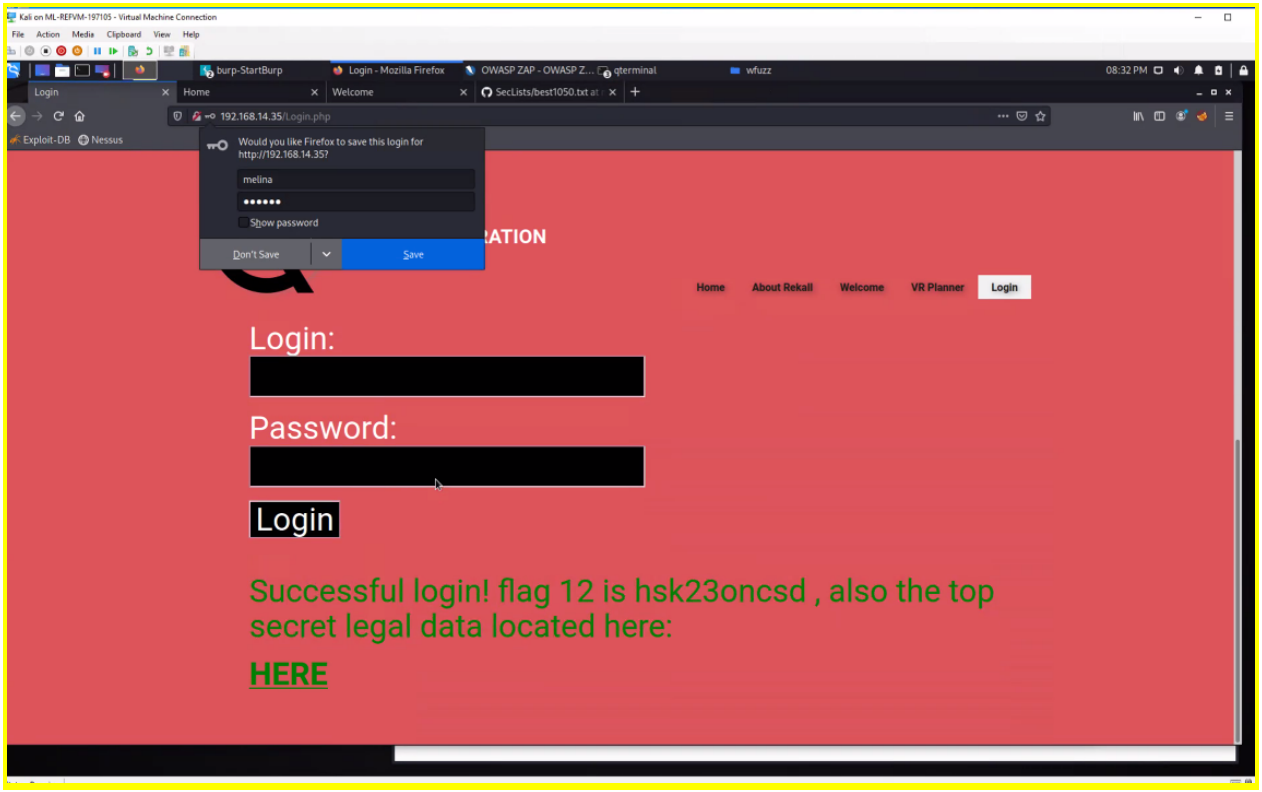
© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

We also discovered the following additional vulnerabilities in addition to the ones mentioned above;

- Leaked server information

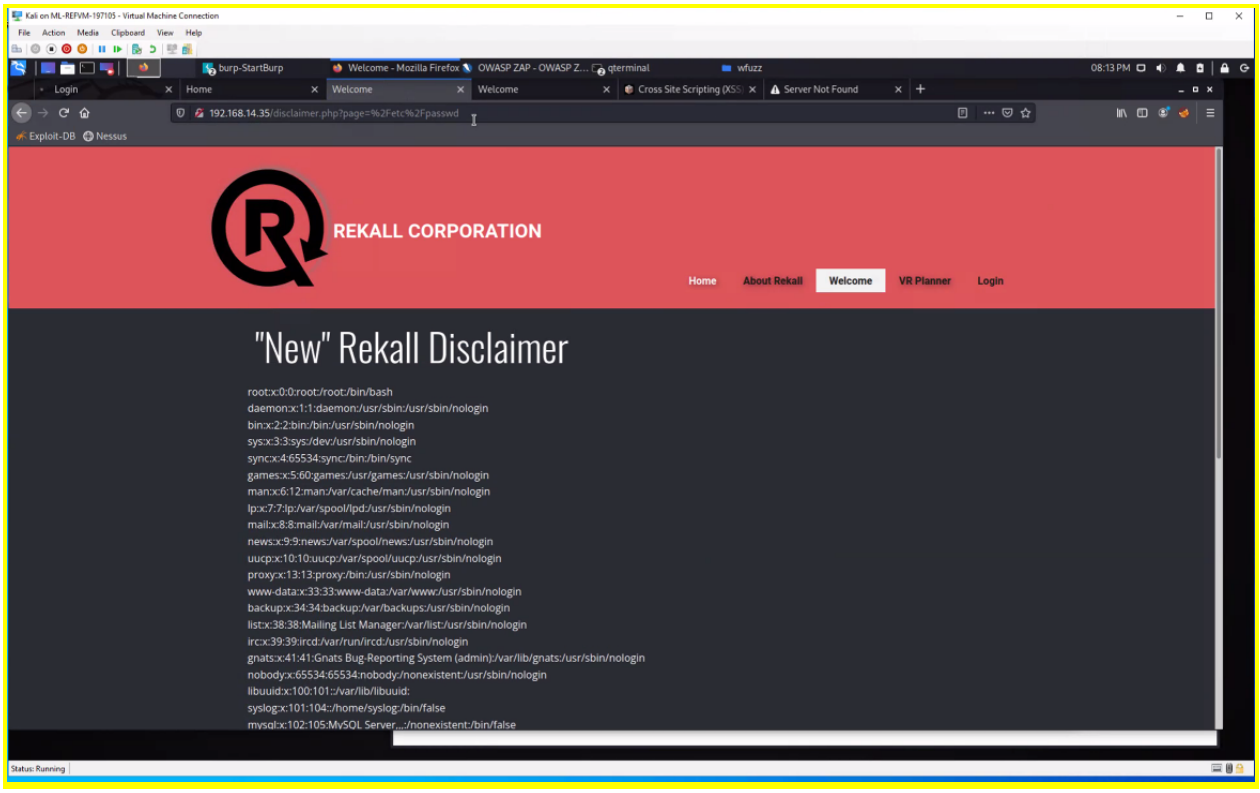


- Simple password cracking

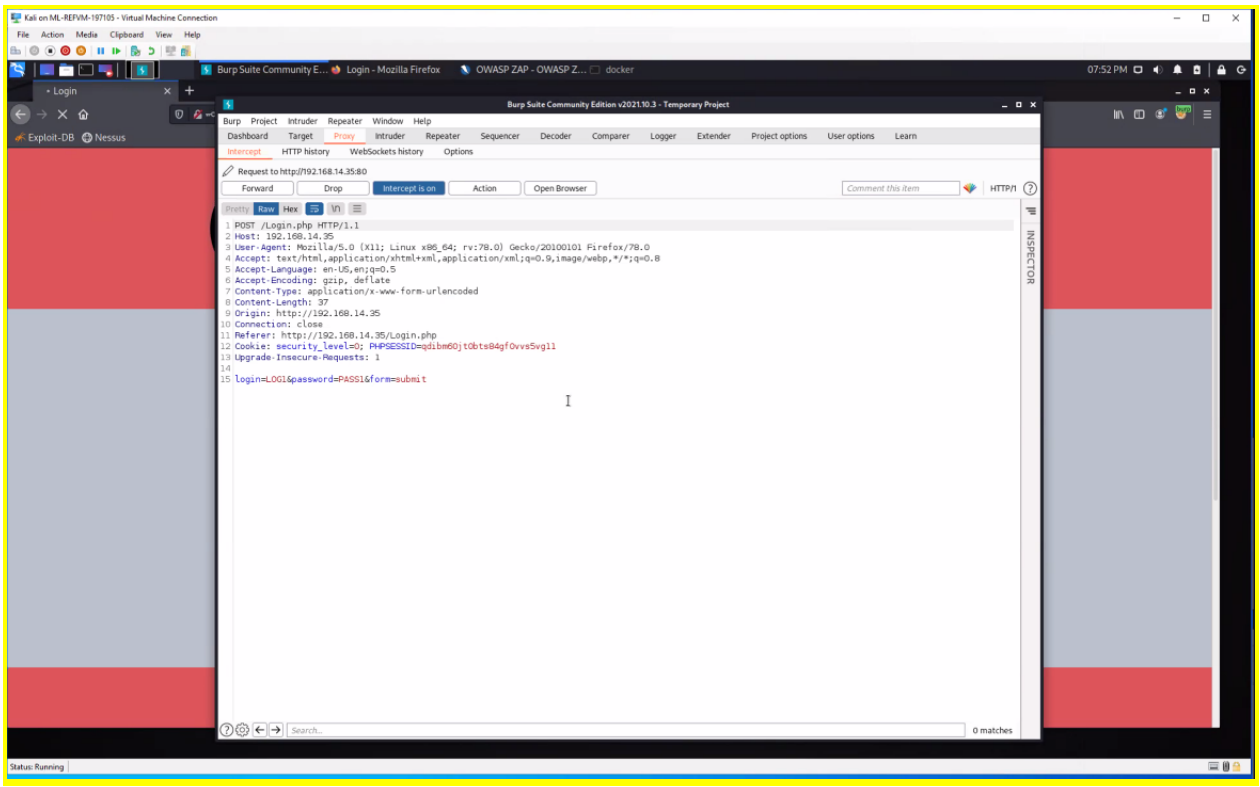


- Multiple usernames were retrieved

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

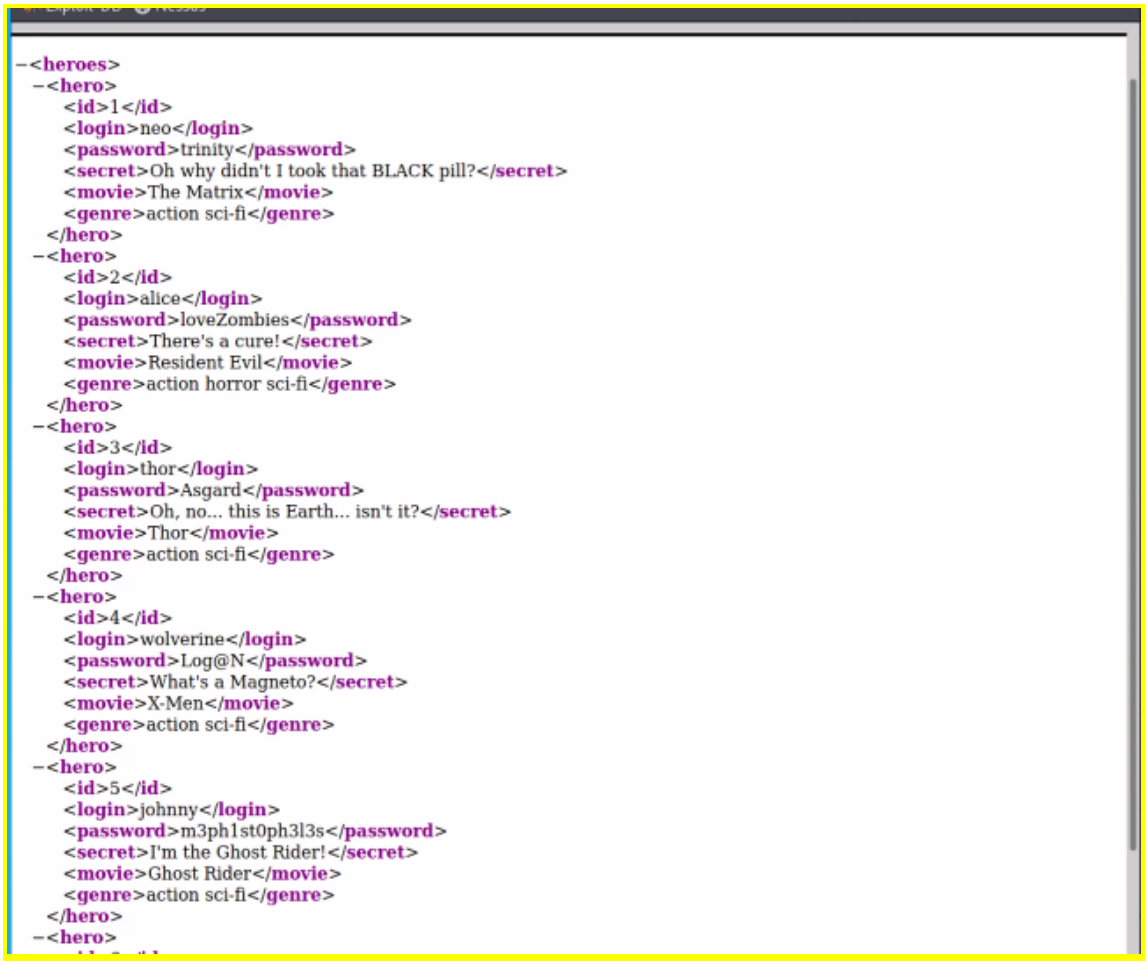


- There is no coded output.



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

- There is no coded output



```
-<heroes>
 -<hero>
    <id>1</id>
    <login>neo</login>
    <password>trinity</password>
    <secret>Oh why didn't I took that BLACK pill?</secret>
    <movie>The Matrix</movie>
    <genre>action sci-fi</genre>
  </hero>
 -<hero>
    <id>2</id>
    <login>alice</login>
    <password>loveZombies</password>
    <secret>There's a cure!</secret>
    <movie>Resident Evil</movie>
    <genre>action horror sci-fi</genre>
  </hero>
 -<hero>
    <id>3</id>
    <login>thor</login>
    <password>Asgard</password>
    <secret>Oh, no... this is Earth... isn't it?</secret>
    <movie>Thor</movie>
    <genre>action sci-fi</genre>
  </hero>
 -<hero>
    <id>4</id>
    <login>wolverine</login>
    <password>Log@N</password>
    <secret>What's a Magneto?</secret>
    <movie>X-Men</movie>
    <genre>action sci-fi</genre>
  </hero>
 -<hero>
    <id>5</id>
    <login>johnny</login>
    <password>m3ph1st0ph3l3s</password>
    <secret>I'm the Ghost Rider!</secret>
    <movie>Ghost Rider</movie>
    <genre>action sci-fi</genre>
  </hero>
 -<hero>
```

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