Cybersecurity

Penetration Test Report

Rekall Corporation

Penetration Test Report

© 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	Rekall Corporation
Contact Name	Ben Agbonze
Contact Title	Penetration Tester

Document History

Version	Date	Author(s)	Comments
001			

© 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.

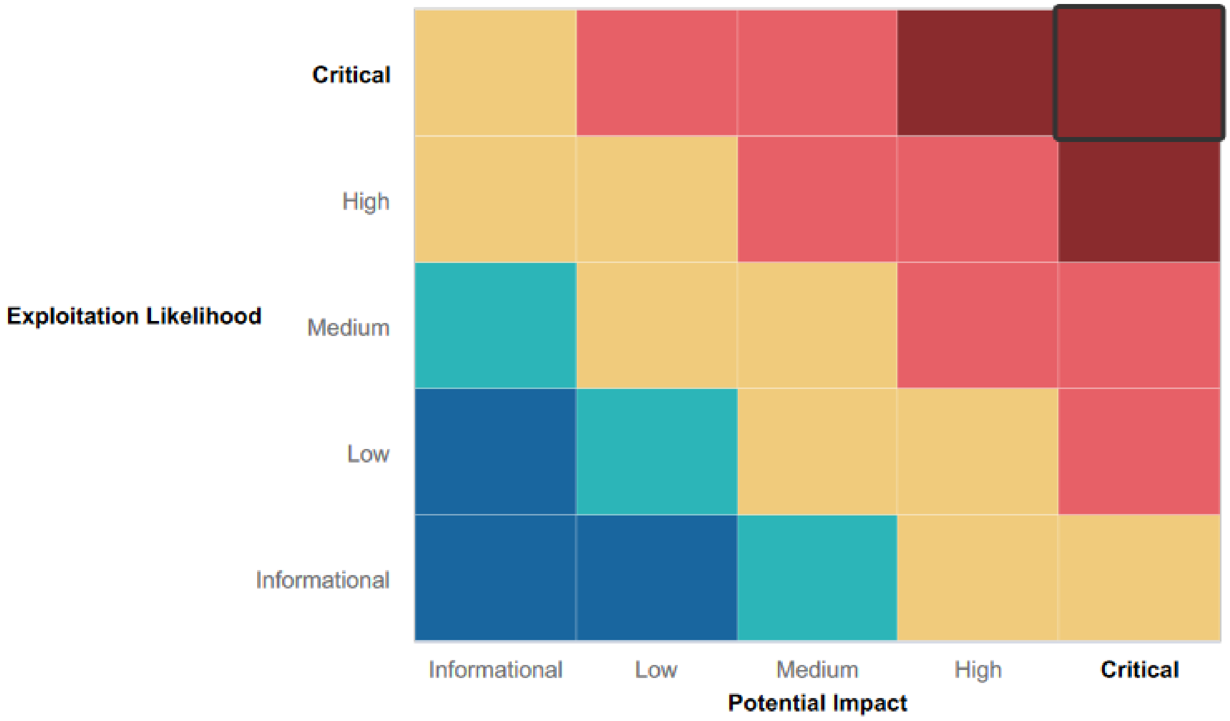
Executive Summary of Findings

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.

- Multi layer step required to attack PHP injection which was hidden in a webpage and requires one to change the URL
- Ping request denied
- No vulnerable open source data being exposed
- Tools like Metasploit/Hashcat/Nmap/nslookup are being utilized to prevent unauthorized access

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 is vulnerable to attack from hackers using either BURP or cURL request,
- Sensitive data are being left open to attacks by accessing the webpage
- Credentials such as usernames and passwords can be easily hacked from HTML
- Easily accessible IP addresses and open ports on the webpage

© 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.]

In the course of doing this penetration testing activity, I was able to find multiple vulnerabilities, including one that could have a great impact on Rekall. I was able to infiltrate Rekall webpage to find most of these vulnerabilities could harm the company revenue and reputation. Using Kall as my main tool, I first tested Rekall’s web application. I was able to see user credentials being exposed.. Using cURL -vhttp://192.168.14.35/About-Rekall.php, I was able to see these sensitive data. It also shows the port connection 80 being open. Using cURL -vhttp://192.168.14.35/robot.txt, I was able to get unrestricted access to view usernames and passwords. For PHP injection,it would take a multi-layer step. The information for the robot.txt would be the first step followed by changing the URL and the message in the URL. This was something I was unable to do and it took a long time to crack the first layer.

Open source data was exposed and viewable using OSINT, and searching crt.sh showed a stored certificate. I was able to see user login credentials. Within Linux, I did a nslookup on totalrekall.xyz which gave me the server and address of totalrekall.xyz. However, I was supposed to ping totalrekall.xyz to see the correct information.

Overall, I wasn’t able to find most of the vulnerabilities needed for this activity. Although there were a lot of them that could be exploited maliciously to cause massive damage. I was able to provide recommendations for mitigating each of these vulnerabilities to prevent harm and loss that could result in harming Rekall.

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

Summary Vulnerability Overview

Vulnerability	Severity
IP lookup is displaying credentials	**Critical**
Open Ports	**Critical**
Web Application is vulnerable to payload injection	**High**
Company’s server physical address is publicly available	**Medium**
Sensitive Data Exposure	**Critical**
Easy to access ping	**Low**
Open source exposed data	**Medium**
User Credentials Exposure	**Critical**
Certificate Search via crt.sh	**Medium**
Restrict access to unauthorized users	**High**

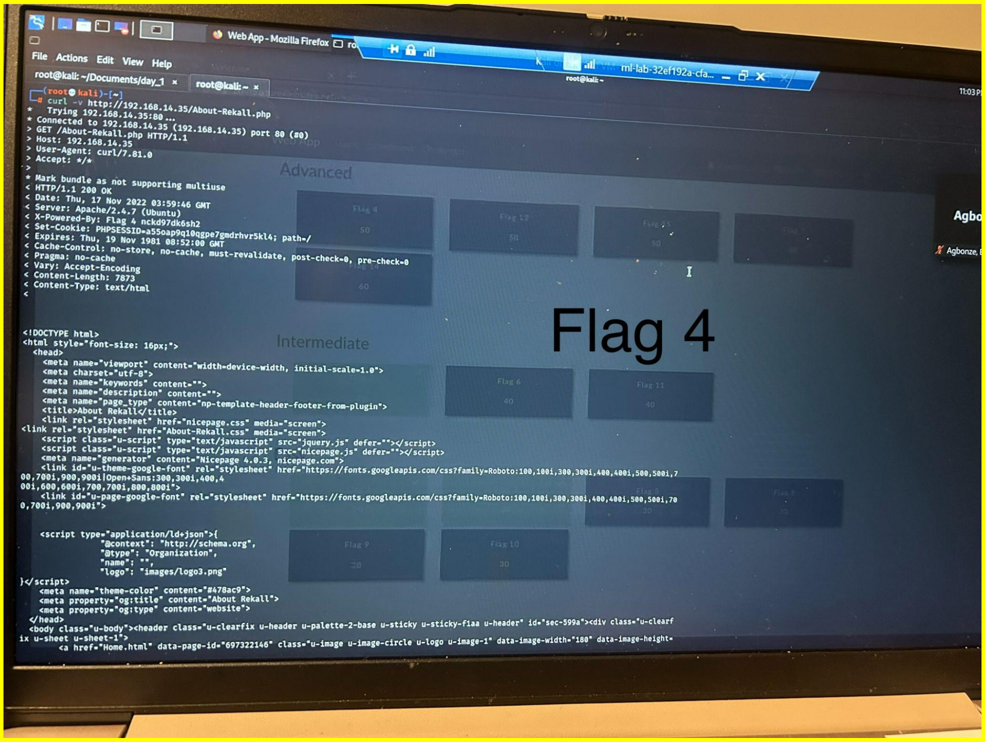
The following summary tables represent an overview of the assessment findings for this penetration test:

Scan Type	Total
Hosts	192.168.14.35 totalrekall.xyz 192.168.14.20 172.22.117.20
Ports	80 443 106 110

Exploitation Risk	Total
Critical	1
High	2

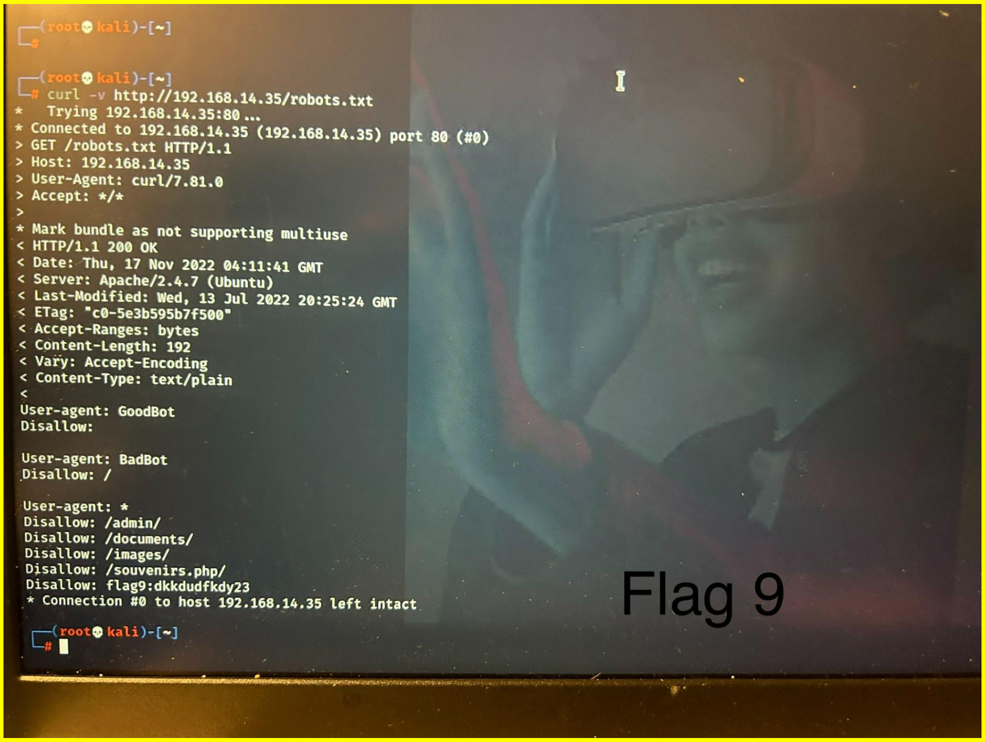
Medium	2
Low	1

Vulnerability Findings

Vulnerability 1	Findings
Title	User Credentials Exposure
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	Critical
Description	In the HTTP headers using either BURP or cURL, one can send a request using the ip address such as: curl -v http://192.168.14.35/About-Rekall.php to view sensitive data. It shows the port connection (80)
Images	 Web App - Mozilla Firefox File Actions Edit View Help root@kali: ~/Documents/day_1 root@kali: ~ Advanced Intermediate Flag 4
Affected Hosts	192.168.14.35
Remediation	block access to Rekall.php

```
┌──(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: Thu, 17 Nov 2022 03:59:46 GMT
< Server: Apache/2.4.7 (Ubuntu)
< X-Powered-By: Flag 4 nckd97dk6sh2
< Set-Cookie: PHPSESSID=a55oap9q10qgpe7gmdrhvr5kl4; 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
<


<!DOCTYPE html>
<html style="font-size: 16px;">
  <head>
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <meta charset="utf-8">
    <meta name="keywords" content="">
    <meta name="description" content="">
    <meta name="page_type" content="np-template-header-footer-from-plugin">
    <title>About Rekall</title>
    <link rel="stylesheet" href="nicepage.css" media="screen">
<link rel="stylesheet" href="About-Rekall.css" media="screen">
    <script class="u-script" type="text/javascript" src="jquery.js" defer=""></script>
    <script class="u-script" type="text/javascript" src="nicepage.js" defer=""></script>
    <meta name="generator" content="Nicepage 4.0.3, nicepage.com">
    <link id="u-theme-google-font" rel="stylesheet" href="https://fonts.googleapis.com/css?family=Roboto:100,100i,300,300i,400,400i,500,500i,7
00,700i,900,900i|Open+Sans:300,300i,400,4
00i,600,600i,700,700i,800,800i">
    <link id="u-page-google-font" rel="stylesheet" href="https://fonts.googleapis.com/css?family=Roboto:100,100i,300,300i,400,400i,500,500i,70
0,700i,900,900i">


    <script type="application/ld+json">{
                "@context": "http://schema.org",
                "@type": "Organization",
                "name": "",
                "logo": "images/logo3.png"
}</script>
    <meta name="theme-color" content="#478ac9">
    <meta property="og:title" content="About Rekall">
    <meta property="og:type" content="website">
  </head>
  <body class="u-body"><header class="u-clearfix u-header u-palette-2-base u-sticky u-sticky-f1aa u-header" id="sec-599a"><div class="u-clearf
ix u-sheet u-sheet-1">
        <a href="Home.html" data-page-id="697322146" class="u-image u-image-circle u-logo u-image-1" data-image-width="180" data-image-height=
```

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

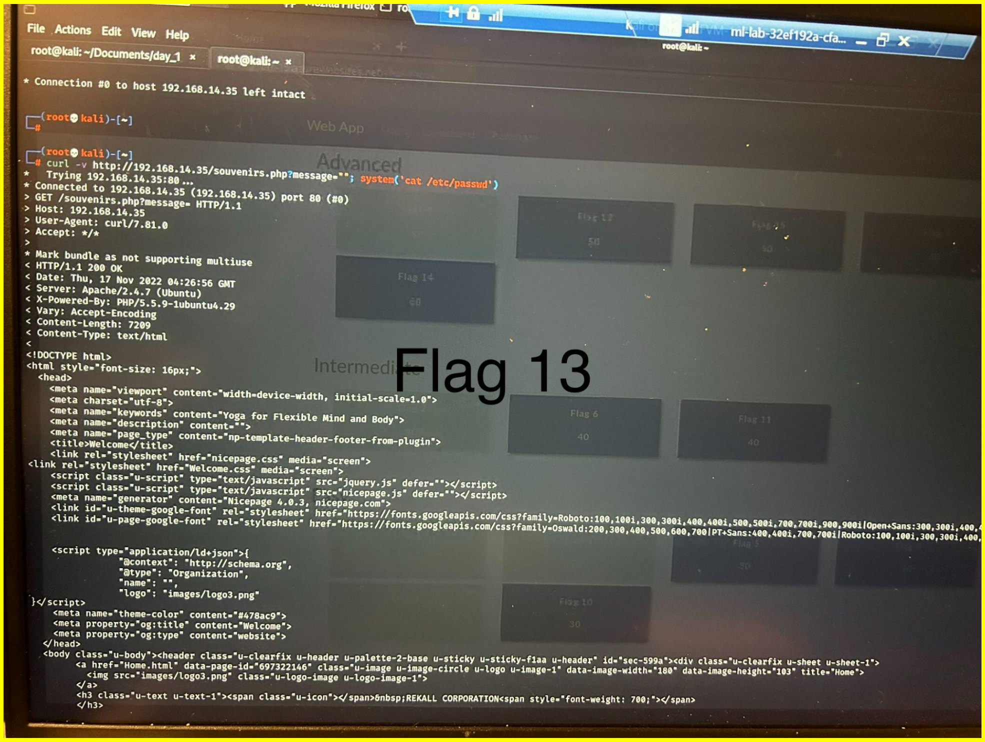
Vulnerability 2	Findings
Title	Sensitive Data Exposure
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	High
Description	Unrestricted access to robots.txt page
Images	
Affected Hosts	192.168.14.35
Remediation	Restrict access to robots.txt to authorized users

```
┌──(root💀kali)-[~]
└─#

┌──(root💀kali)-[~]
└─# curl -v http://192.168.14.35/robots.txt
*   Trying 192.168.14.35:80...
* Connected to 192.168.14.35 (192.168.14.35) port 80 (#0)
> GET /robots.txt 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: Thu, 17 Nov 2022 04:11:41 GMT
< Server: Apache/2.4.7 (Ubuntu)
< Last-Modified: Wed, 13 Jul 2022 20:25:24 GMT
< ETag: "c0-5e3b595b7f500"
< Accept-Ranges: bytes
< Content-Length: 192
< Vary: Accept-Encoding
< Content-Type: text/plain
<
User-agent: GoodBot
Disallow:

User-agent: BadBot
Disallow: /

User-agent: *
Disallow: /admin/
Disallow: /documents/
Disallow: /images/
Disallow: /souvenirs.php/
Disallow: flag9:dkkdudfkdy23
* Connection #0 to host 192.168.14.35 left intact

┌──(root💀kali)-[~]
└─# █
```

Flag 9

Vulnerability 3	Findings
Title	PHP injection
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	High
Description	After finding flag 9, the txt file would provide additional information on how to find this flag. The main part is changing the URL from http://192.168.13.35/souvenirs.php?message=""; system('cat /etc/passwd') OR http://192.168.13.35/souvenirs.php?message=%22%22;%20passthru(%27cat%20/etc/passwd%27)

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

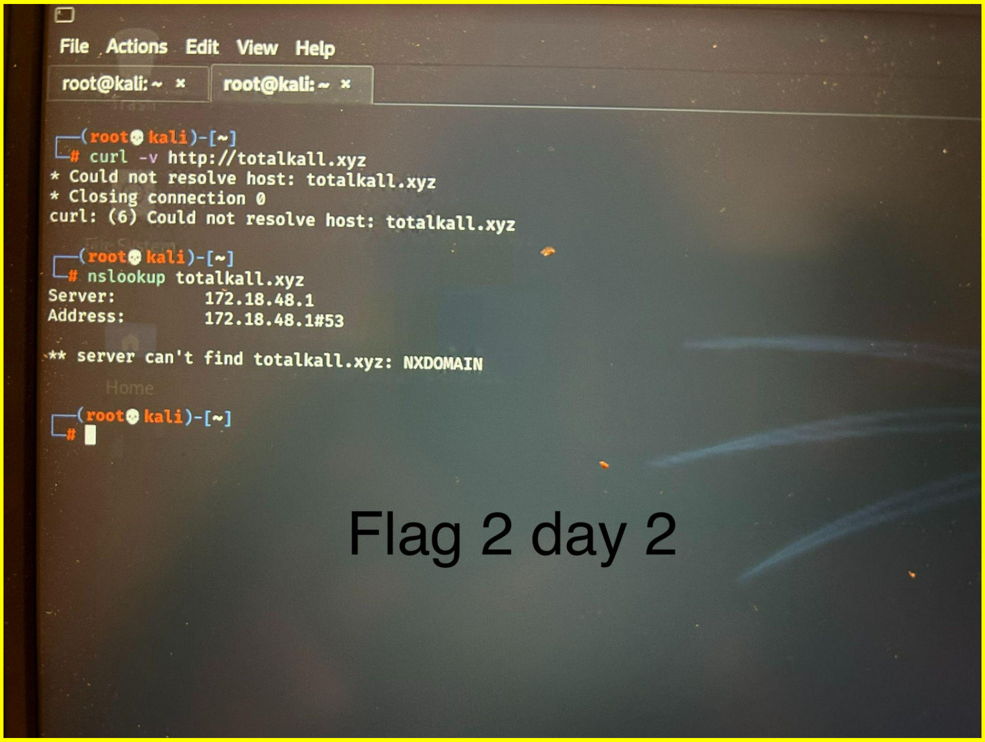
	I kept struggling with the URL and wasn't successful in finding this flag
Images	

```
File  Actions  Edit  View  Help
root@kali: ~/Documents/day_1  ×    root@kali: ~  ×
* Connection #0 to host 192.168.14.35 left intact

┌──(root💀kali)-[~]
└─#

┌──(root💀kali)-[~]
└─# curl -v http://192.168.14.35/souvenirs.php?message=""; system('cat /etc/passwd')
*   Trying 192.168.14.35:80...
* Connected to 192.168.14.35 (192.168.14.35) port 80 (#0)
> GET /souvenirs.php?message= 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: Thu, 17 Nov 2022 04:26:56 GMT
< Server: Apache/2.4.7 (Ubuntu)
< X-Powered-By: PHP/5.5.9-1ubuntu4.29
< Vary: Accept-Encoding
< Content-Length: 7209
< Content-Type: text/html
<
<!DOCTYPE html>
<html style="font-size: 16px;">
  <head>
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <meta charset="utf-8">
    <meta name="keywords" content="Yoga for Flexible Mind and Body">
    <meta name="description" content="">
    <meta name="page_type" content="np-template-header-footer-from-plugin">
    <title>Welcome</title>
    <link rel="stylesheet" href="nicepage.css" media="screen">
<link rel="stylesheet" href="Welcome.css" media="screen">
    <script class="u-script" type="text/javascript" src="jquery.js" defer=""></script>
    <script class="u-script" type="text/javascript" src="nicepage.js" defer=""></script>
    <meta name="generator" content="Nicepage 4.0.3, nicepage.com">
    <link id="u-theme-google-font" rel="stylesheet" href="https://fonts.googleapis.com/css?family=Roboto:100,100i,300,300i,400,400i,500,500i,700,700i,900,900i|Open+Sans:300,300i,400,4
    <link id="u-page-google-font" rel="stylesheet" href="https://fonts.googleapis.com/css?family=Oswald:200,300,400,500,600,700|PT+Sans:400,400i,700,700i|Roboto:100,100i,300,300i,400,

    <script type="application/ld+json">{
            "@context": "http://schema.org",
            "@type": "Organization",
            "name": "",
            "logo": "images/logo3.png"
}</script>
    <meta name="theme-color" content="#478ac9">
    <meta property="og:title" content="Welcome">
    <meta property="og:type" content="website">
  </head>
  <body class="u-body"><header class="u-clearfix u-header u-palette-2-base u-sticky u-sticky-f1aa u-header" id="sec-599a"><div class="u-clearfix u-sheet u-sheet-1">
        <a href="Home.html" data-page-id="697322146" class="u-image u-image-circle u-logo u-image-1" data-image-width="180" data-image-height="103" title="Home">
          <img src="images/logo3.png" class="u-logo-image u-logo-image-1">
        </a>
        <h3 class="u-text u-text-1"><span class="u-icon"></span>&nbsp;REKALL CORPORATION<span style="font-weight: 700;"></span>
        </h3>
```

Affected Hosts	192.168.14.35
Remediation	Block the payload to the URL or change the URL to be more complex so It can't be easy to hack

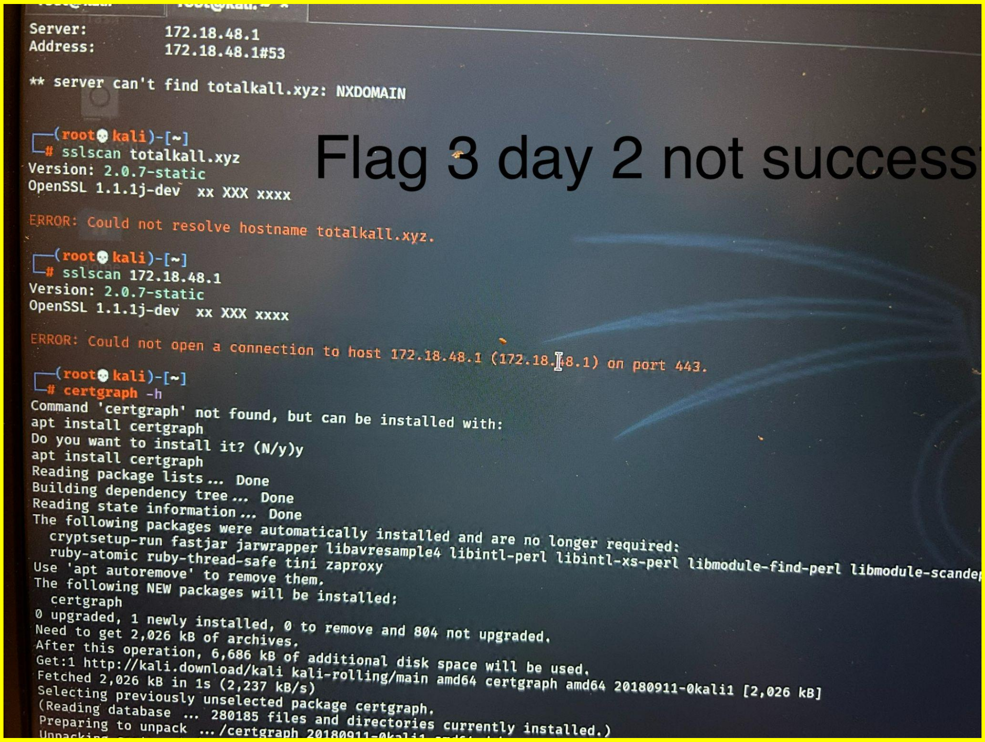
Vulnerability 4	**Findings**
Title	Ping
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Low
Description	Ping totalrekall.xyz would have capture this flag I did a nslookup on totalrekall.xyz which gave me the server and address of totalrekall.xyz

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

Images	 ┌──(root💀kali)-[~] └─# curl -v http://totalkall.xyz * Could not resolve host: totalkall.xyz * Closing connection 0 curl: (6) Could not resolve host: totalkall.xyz ┌──(root💀kali)-[~] └─# nslookup totalkall.xyz Server: 172.18.48.1 Address: 172.18.48.1#53 ** server can't find totalkall.xyz: NXDOMAIN ┌──(root💀kali)-[~] └─# Flag 2 day 2
Affected Hosts	totalrekall.xyz
Remediation	None; ping is not a security risk

Vulnerability 5	**Findings**
Title	Open source exposed data
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Medium
Description	The right way to do this: On crt.sh, search for totalrekall.xyz The way I did this: sslscan 172.18.48.1 and could not make a connection to port 443

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

Images	 Flag 3 day 2 not success
Affected Hosts	totalrekall.xyz
Remediation	Protect information from being exposed by the crt.sh site

```
Server:         172.18.48.1
Address:        172.18.48.1#53

** server can't find totalkall.xyz: NXDOMAIN

┌──(root💀kali)-[~]
└─# sslscan totalkall.xyz
Version: 2.0.7-static
OpenSSL 1.1.1j-dev  xx XXX xxxx

ERROR: Could not resolve hostname totalkall.xyz.

┌──(root💀kali)-[~]
└─# sslscan 172.18.48.1
Version: 2.0.7-static
OpenSSL 1.1.1j-dev  xx XXX xxxx

ERROR: Could not open a connection to host 172.18.48.1 (172.18.48.1) on port 443.

┌──(root💀kali)-[~]
└─# certgraph -h
Command 'certgraph' not found, but can be installed with:
apt install certgraph
Do you want to install it? (N/y)y
apt install certgraph
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  cryptsetup-run fastjar jarwrapper libavresample4 libintl-perl libintl-xs-perl libmodule-find-perl libmodule-scandep
  ruby-atomic ruby-thread-safe tini zaproxy
Use 'apt autoremove' to remove them.
The following NEW packages will be installed:
  certgraph
0 upgraded, 1 newly installed, 0 to remove and 804 not upgraded.
Need to get 2,026 kB of archives.
After this operation, 6,686 kB of additional disk space will be used.
Get:1 http://kali.download/kali kali-rolling/main amd64 certgraph amd64 20180911-0kali1 [2,026 kB]
Fetched 2,026 kB in 1s (2,237 kB/s)
Selecting previously unselected package certgraph.
(Reading database ... 280185 files and directories currently installed.)
Preparing to unpack .../certgraph 20180911-0kali1
```