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	BreachPulse, LLC
Contact Name	Gonzalez, Rebecca
Contact Title	Penetration Tester

Document History

Version	Date	Author(s)	Comments
001	27 November 2023	Gonzalez, Rebecca	1st Draft
002	4 December 2023	Gonzalez, Rebecca	Review
003	6 December 2023	Gonzalez, Rebecca	2nd Draft
004	7 December 2023	Gonzalez, Rebecca	Final Report

© 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.

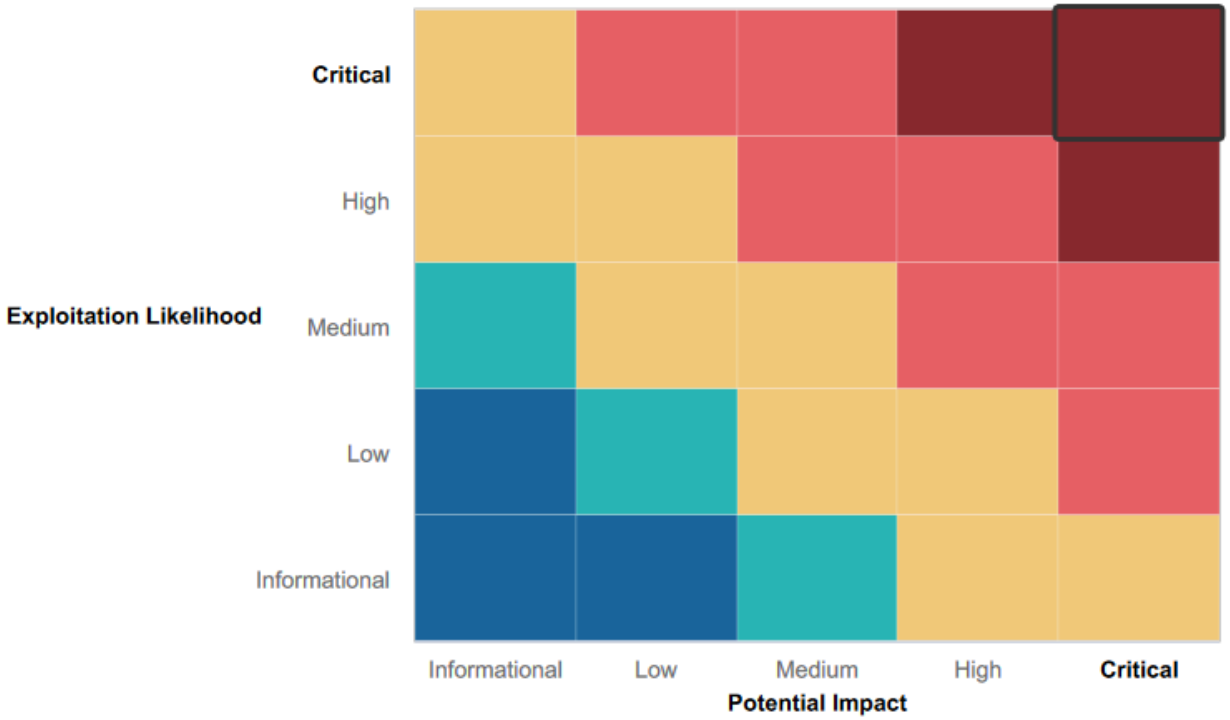
Executive Summary of Findings

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.

- Rekall did implement input validation in most input fields throughout its web app. In some instances, as with our initial attempts at command injection, we had to use more complex commands in an attempt to circumvent validation.
- A few exploits we attempted to run were not successful against the server.
- Rekall's greatest strength has been its proactivity about its security by testing its systems for improvement to improve its security posture.

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.

- The web app was vulnerable to a variety of injection attacks including but not limited to SQL, PHP, and XSS.
- HTML code on the web app contained sensitive data / credentials in plain-text.
- It was possible to gain unauthorized access to sensitive data like passwords and hashes and perform privilege escalation.
- Weak passwords and the ability to use usernames as passwords to easily gain access to hidden pages, remote access execution, and other credential-based tasks.
- Sensitive server and user data was publicly available with the use of OSINT tools (open source).
- We identified the use of open, unsecured ports on several systems which facilitated unauthorized access and privilege escalation.
- Input validation did not evaluate content and did allow extensions that could facilitate malicious scripts and data uploads.
- robots.txt file tags should be re-evaluated and labeled accordingly to ensure data safety.
- Systems across the network required the latest security updates and security patches to prevent some of the exploits we launched against them.
- Security policies such as password and authentication policies should be updated and enforced.
- Hidden pages in the web app contained sensitive data and required more secure forms of storage and encryption or should not have been included on the server for access.

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

Executive Summary

The BreachPulse pentesting team both acknowledges and commends Rekall Corporation's efforts in maintaining basic security protections for most vulnerabilities and weaknesses analyzed within the designated scope of our assessment. We encourage Rekall Corporation to raise and uphold security standards to ensure confidentiality, integrity, and accessibility of its data and operations across its network and systems.

Based upon the analysis and results of our testing, we strongly recommend an increased defense-in-depth approach to Rekall's security. We have included our recommendations in this report to address a variety of vulnerabilities encountered, several which were critical in nature.

In addition, we recommend updating policies, procedures, and systems to prevent future security incidents and strengthen Rekall's security posture. Taking heed to these recommendations also prevent resulting penalties and fines where these matters are of concern.

Our assessment began with a thorough analysis of Rekall's Web Application. We encountered critical vulnerabilities including sensitive data exposure involving credentials, input validation that did not evaluate content, and the ability to access additional resources and sensitive data through a variety of code injection methods inserted in input fields. Also noted was the presence of sensitive data hidden in public facing web pages and in plain-text.

Using a variety of techniques we were able to exploit the web app vulnerabilities even further. The BreachPulse team retrieved and implanted files to and from the server, accessed older versions of web pages, obtained unsecure credentials and other sensitive data. This allowed us to leverage and increase our attack surface. It was all facilitated by the lack of system updates, patches, and outdated technologies.

With these findings, we were able to access other systems and escalate our privileges throughout the network. The team obtained and used insecure passwords to gain access to remote shells and escalate access to root-level in most of these systems – a critical vulnerability allowing bypassing of security measures and total control of a vulnerable system. Please review this detailed report of our findings and security recommendations for each exposed vulnerability.

The BreachPulse team thanks you for this opportunity to assist you and commends you for being proactive concerning the matter of your security posture.We hope that you find these recommendations useful in achieving your security goals and wish you the best in your endeavors.

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

Summary Vulnerability Overview

Vulnerability	Severity
XSS Reflected	Critical
XSS Stored	Critical
Sensitive Data Exposure	High
Local File Inclusion (LFI)	Critical
SQL Injection	Critical
Sensitive Data Exposure / Credentials	Critical
Command Injection	Critical
Brute Force Attack	Critical
PHP Injection	High
Insecure Passwords	Critical
Session Management	Critical
Directory Traversal	Critical
robots.txt file (tags/sensitive data exposure)	Low
Open-Source Exposed Data	Medium
Nmap Scan Results	Low
Nessus scan results - 97610	Critical
CVE-2017-12617 - Apache Tomcat RCE Vulnerability	Critical
CVE-2014-7169-Shellshock	High
CVE-2019-6340 - Drupal	High
CVE-2019-14287 - Security Bypass	High
Open, unsecured ports	Critical

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

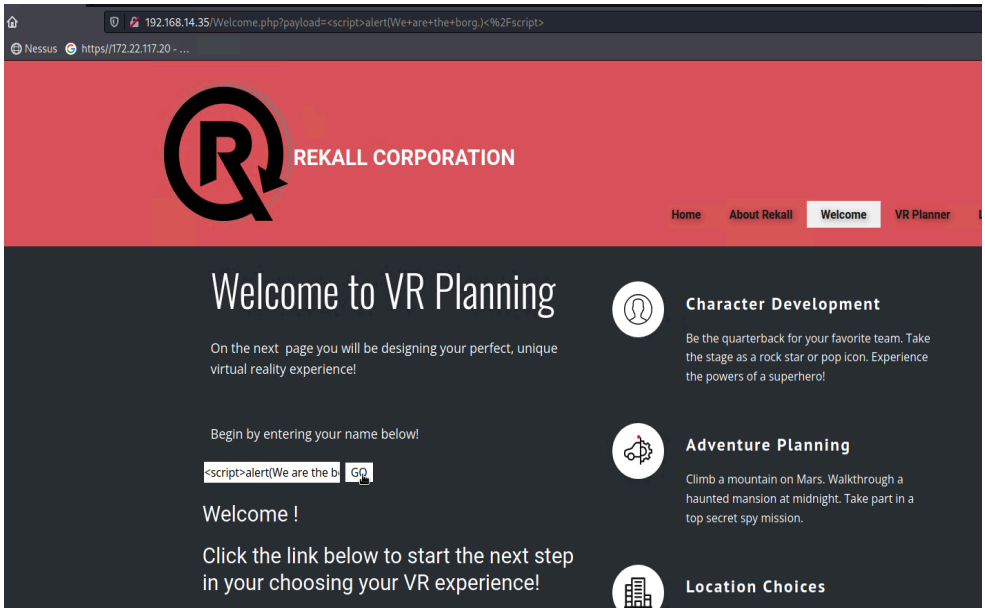
Scan Type	Total
Hosts	192.168.13.1 192.168.13.10 192.168.13.11 192.168.13.12 192.168.13.13 192.168.13.14 172.22.117.10 172.22.117.20 34.102.136.180 (Web App)
Ports	21, 22, 80, 8080, 5901, 6001, 10000, 10001

Exploitation Risk	Total

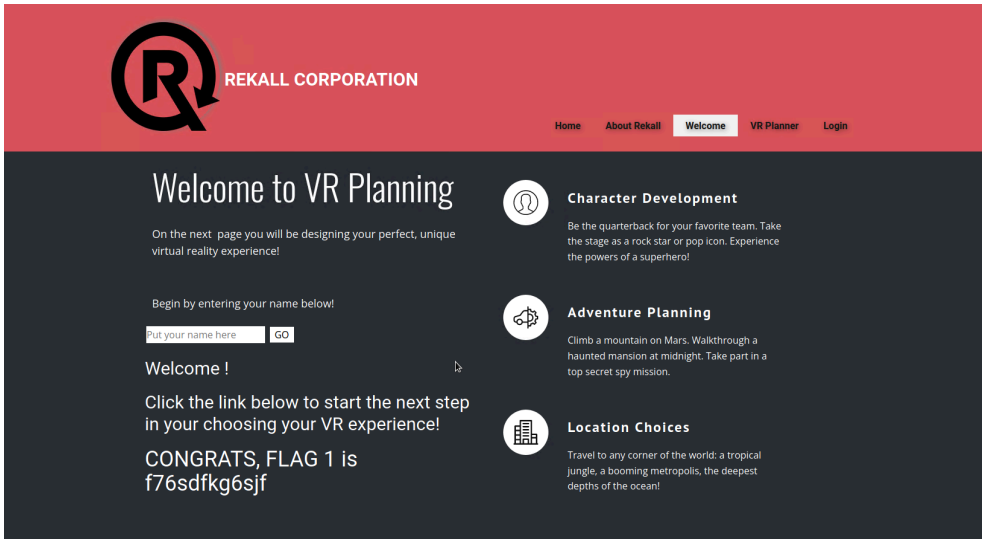
© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

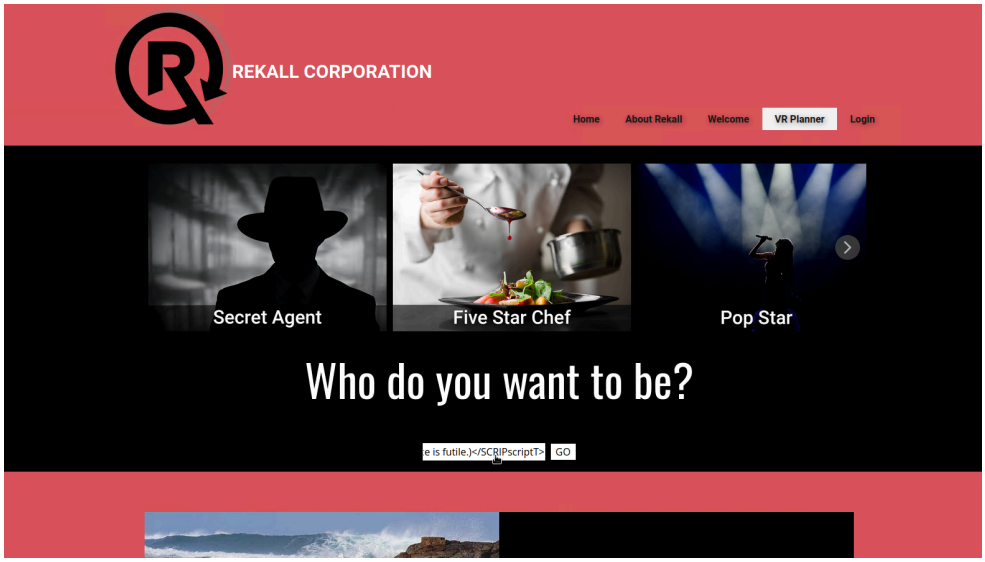
Critical	13
High	5
Medium	1
Low	2

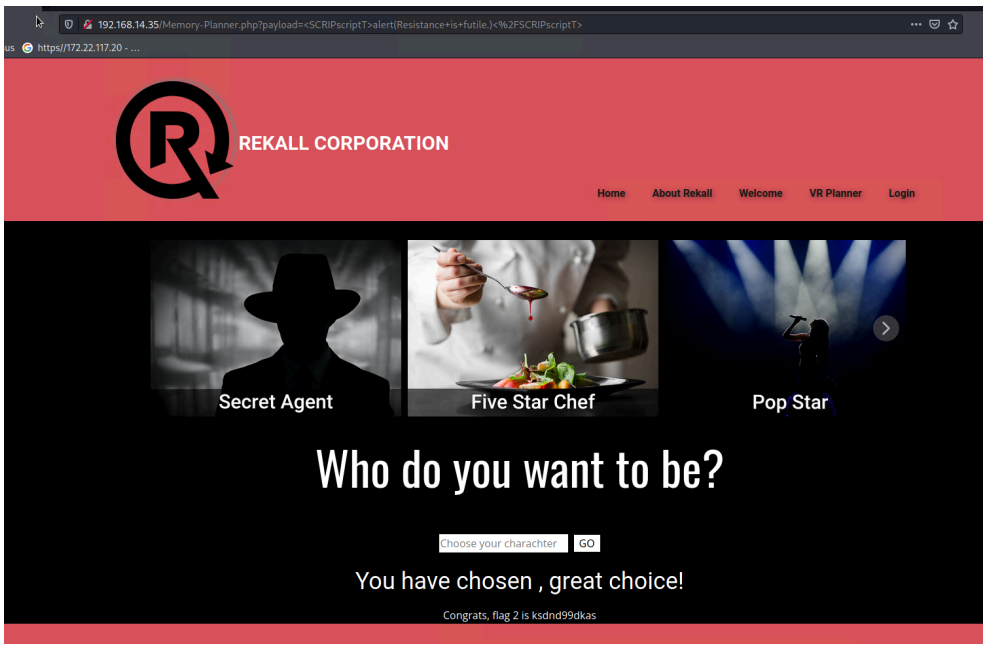
Vulnerability Findings

Vulnerability 1	Findings
Title	XSS Reflected
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Critical
Description	XSS reflected is done by Injecting malicious code into an HTTP response. The payload is not persistent - it does not reside on the web app. It is initiated when a trusting browser visits the exploited site and the malicious code or script is echoed in the HTML response.
Images	

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



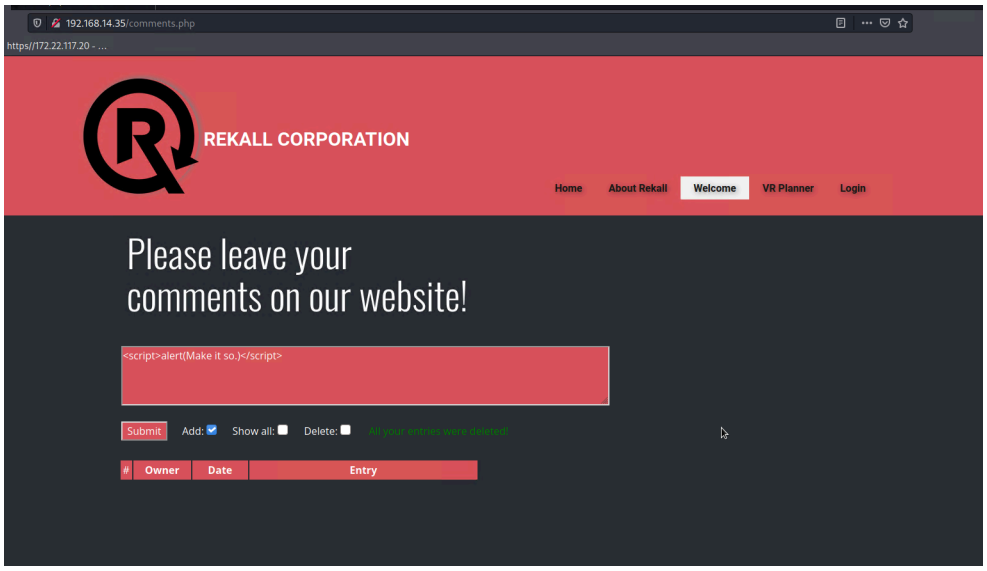




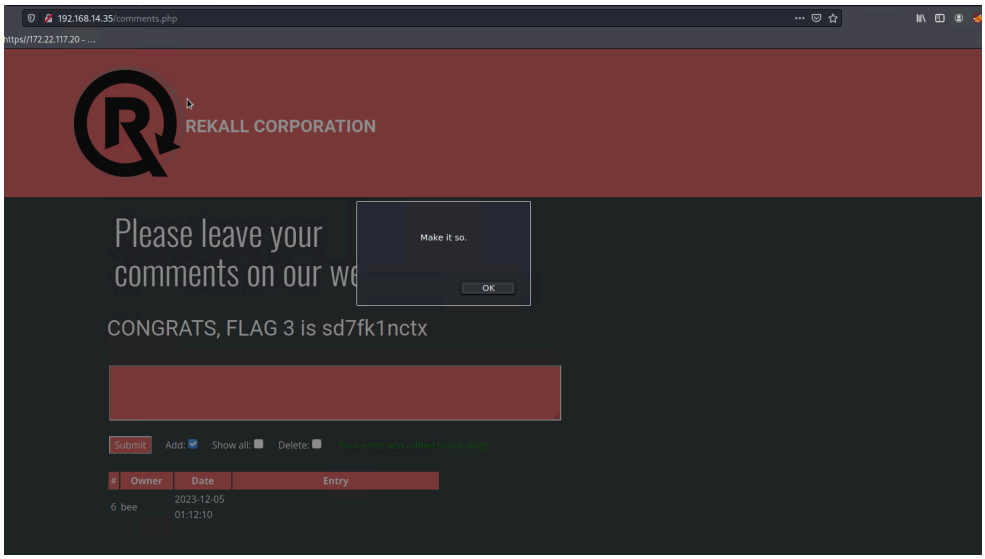
Affected Hosts	

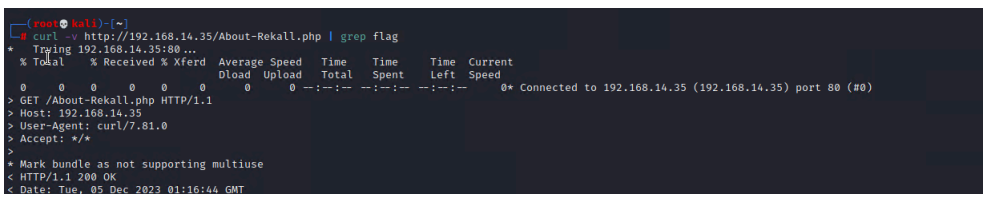
© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

Remediation	• Framework security protections • HTML sanitization, use safe sinks, and output encoding • Implement security controls such as cookie attributes and content security policy as an additional layer of defense

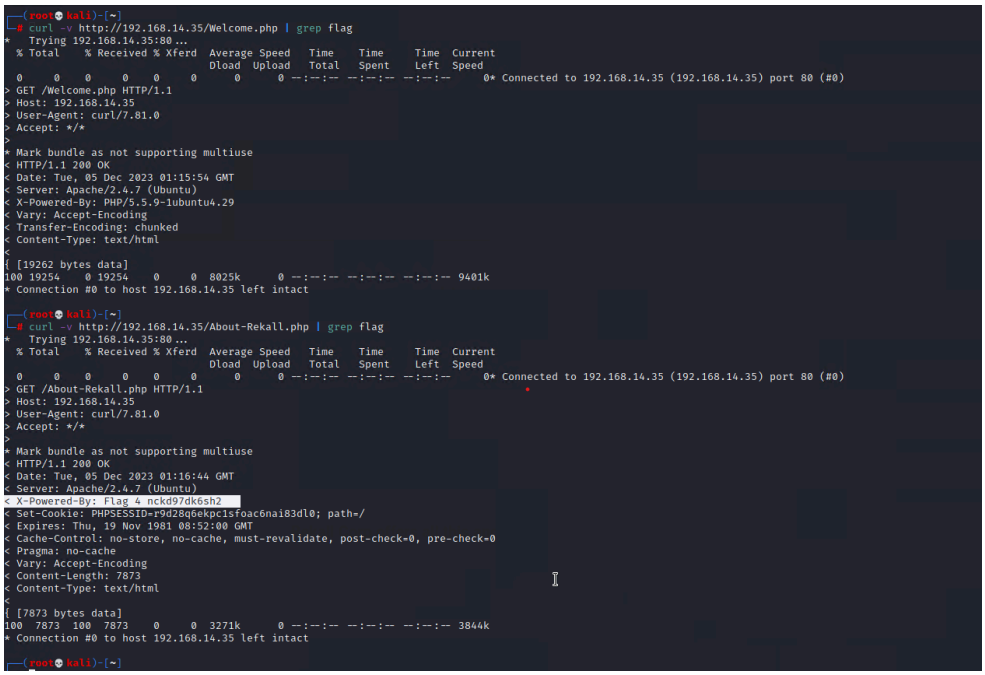
Vulnerability 2	**Findings**
Title	XSS Stored
Type (Web app / Linux OS / WIndows OS)	Web App • Welcome.php
Risk Rating	Critical
Description	Unlike XSS reflected, a stored XSS attack is persistent. We used code in the input field to successfully launch a payload. We used the word “SCRIPT” separated and surrounding the start and end script tags as follows: <SCRIPscriptT>alert(Make it so..)</SCRIPscriptT>
Images	 The payload proved successful.

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

	
Affected Hosts	34.102.136.180
Remediation	• Implementing modern web security frameworks, output encoding, and HTML sanitization should be considered the first line of defense. • Also recommended are cookie attributes, content security policies, and WAFs to mitigate attacks. • Input validation

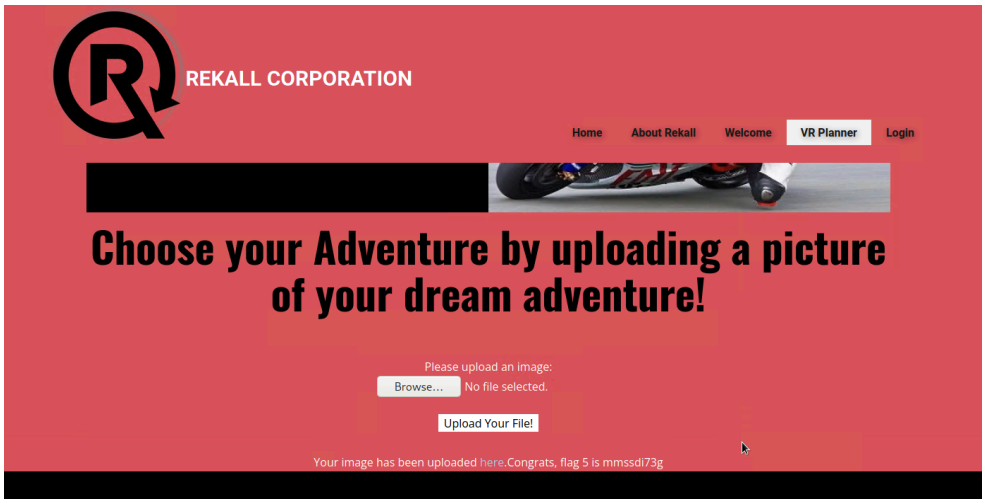
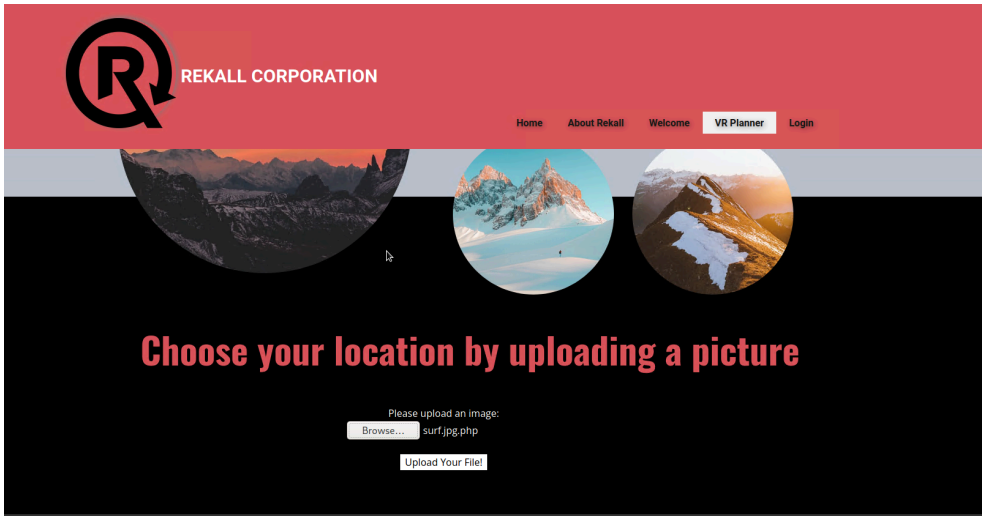
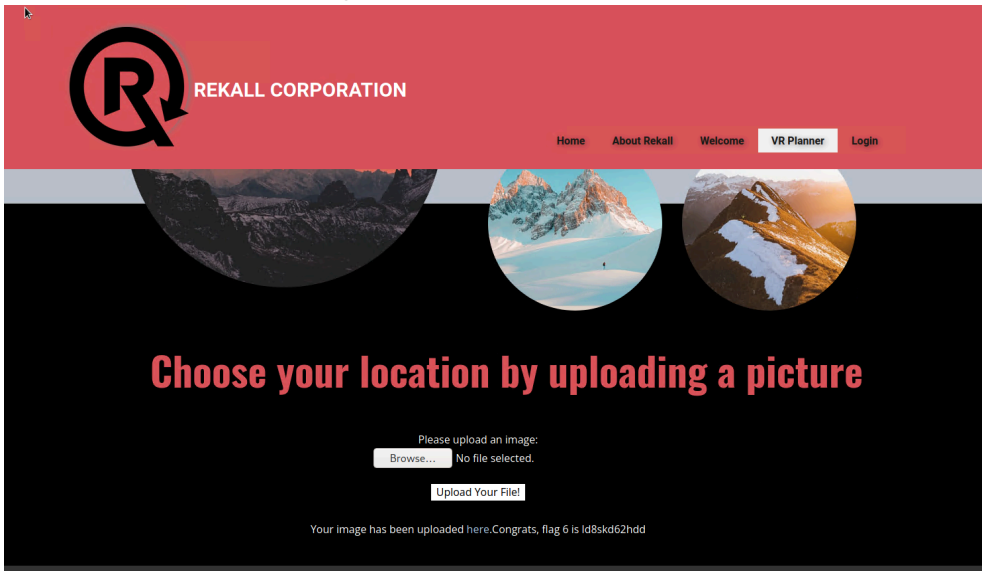
Vulnerability 3	**Findings**
Title	Sensitive Data Exposure
Type (Web app / Linux OS / WIndows OS)	Web App • Welcome.php • About-Rekall.php Windows OS
Risk Rating	Critical
Description	Sensitive data is data or information that should not be accessible to unauthorized parties. A violation of the CIA triad that may lead to heavy fines and penalties. We checked the headers of the web app by analyzing the Welcome.php and About-Rekall.php web pages. We used the curl command to expose sensitive data from those headers.
Images	

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

	
Affected Hosts	
Remediation	• Sensitive data (in motion or at rest) should be protected, and encrypted with strong encryption algorithms. • At rest, it should be stored securely, • Sensitive data should not be stored, if it is not needed.

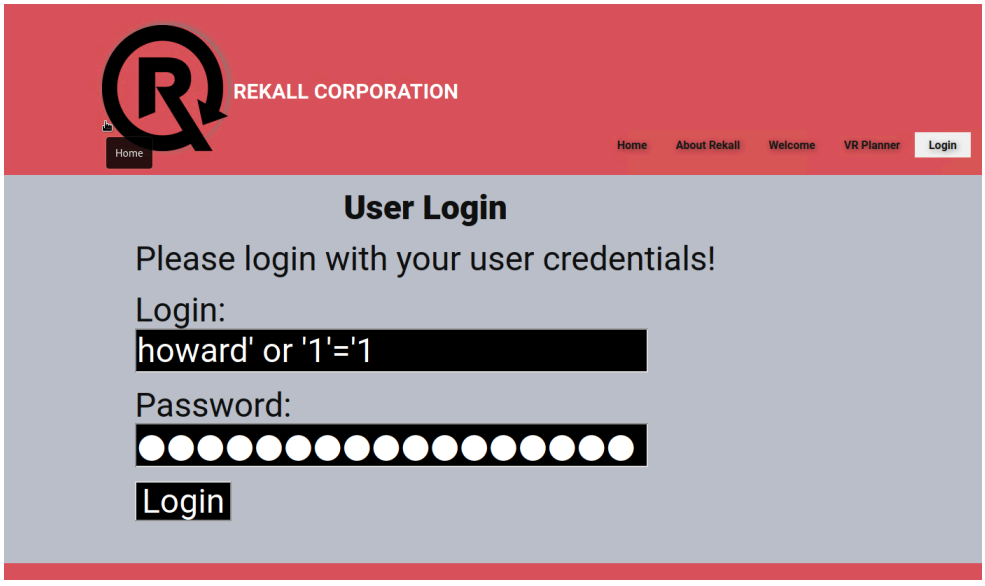
Vulnerability 4	Findings
Title	Local File Inclusion (LFI)
Type (Web app / Linux OS / WIndows OS)	Web App • Memory-Planner.php (2st field) • Memory-Planner.php (3rd field)
Risk Rating	Critical
Description	Next, we conducted an LFI exploit by uploading a file with a .php extension to access a flag and test the app. We created a file that contained the following payload: <?php phpinfo(): ?> We named the file, file.php and uploaded it to the web app where it was accepted without error messages or warnings.

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

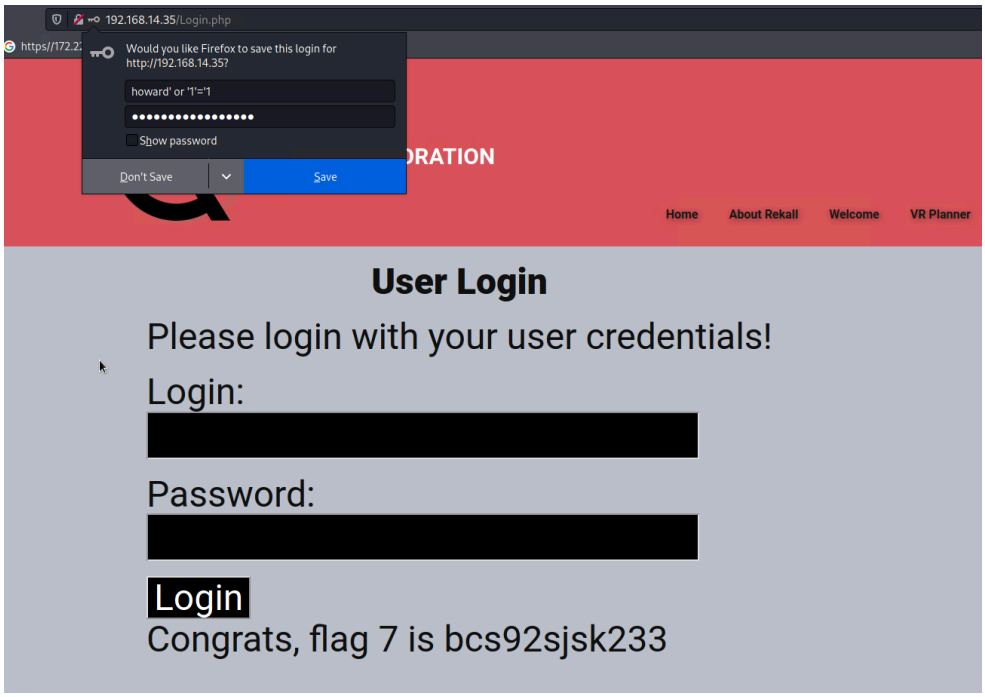
Images	 We performed a more advanced form of LFI in the 3rd field of this page. This time, we named the payload surf.jpg.php.  Input validation checks for .jpg extension. Although we appended the .php extension, we were still able to upload the file without incident and bypassed the filter as seen in this image: 

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

Affected Hosts	34.102.136.180
Remediation	• Avoid passing user-submitted input to any framework or API • Ensure input validation is in place before validating extensions • List and validate allowed extensions • Run files through antivirus to mitigate malicious data • Only allow authorized users to upload files

Vulnerability 5	**Findings**
Title	SQL Injection
Type (Web app / Linux OS / WIndows OS)	Web App • Login.php (1st field)
Risk Rating	Critical
Description	SQL injections involve manipulating SQL requests to perform nefarious commands and can be used to access sensitive data and establish persistence. We entered code in the 1st input field of the Login.php page to successfully perform an SQL injection.
Images	

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

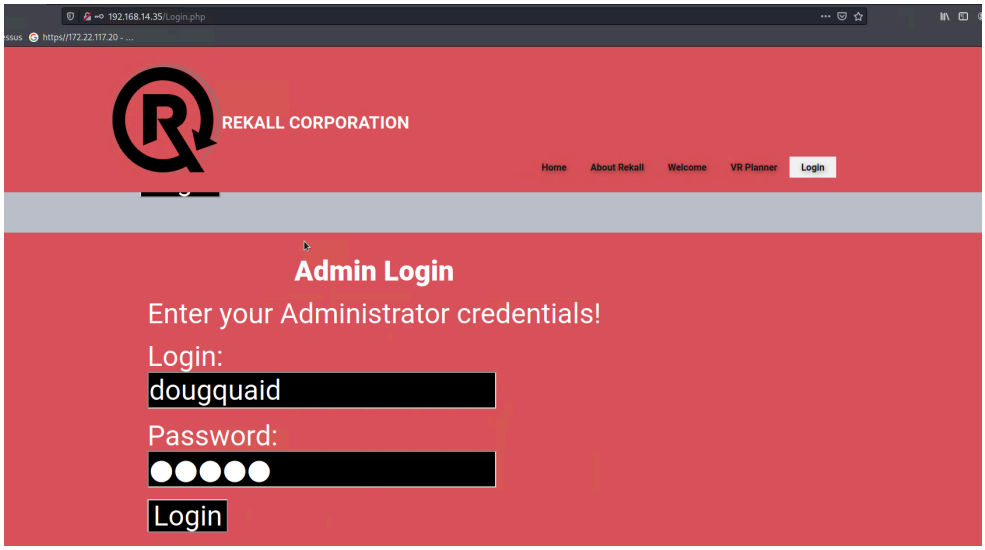
	
Affected Hosts	34.102.136.180
Remediation	• Use parameterized queries • Use properly constructed stored procedures • Allow-list input validation

Vulnerability 6	Findings
Title	Sensitive Data Exposure / Credentials
Type (Web app / Linux OS / WIndows OS)	Web App • Login.php
Risk Rating	Critical
Description	Administrator credentials were found in plain-text on a public-facing web page by viewing page source code.
Images	(see next page)

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

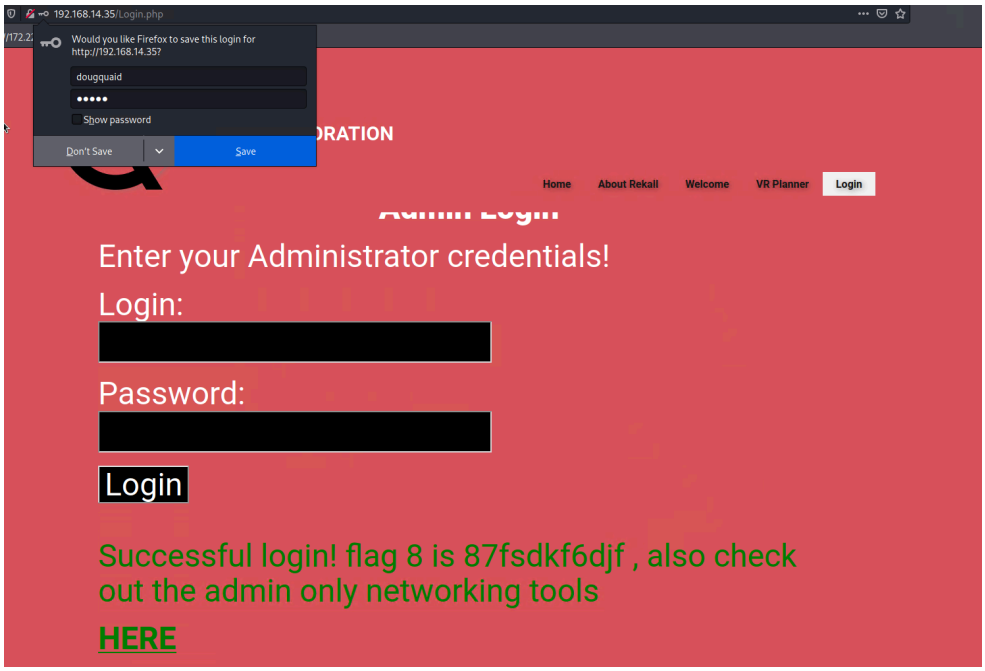
```
<!DOCTYPE html>
<html>


<div id="main">

    <p>Enter your Administrator credentials!</p>

<style>
input[type=text], input[type=password]{
  background-color: black;
  color: white;
}
button[type=submit]{
  background-color: black;
  color: white;
}
</style>

    <form action="/Login.php" method="POST">

        <p><label for="login">Login:</label><font color="#DB545A">dougquaid</font><br />
        <input type="text" id="login" name="login" size="20" /></p>

        <p><label for="password">Password:</label><font color="#DB545A">kuato</font><br />
        <input type="password" id="password" name="password" size="20" /></p>

        <button type="submit" name="form" value="submit" background-color="black">Login</button>

    </form>

    </br >
    <font color="red">Invalid credentials!</font>
</div>


</body>

</html>
```

We were able to use these highlighted administrative credentials to login into the web app.



Doing so, allowed us to access the admin networking tools and provided a link to access them.

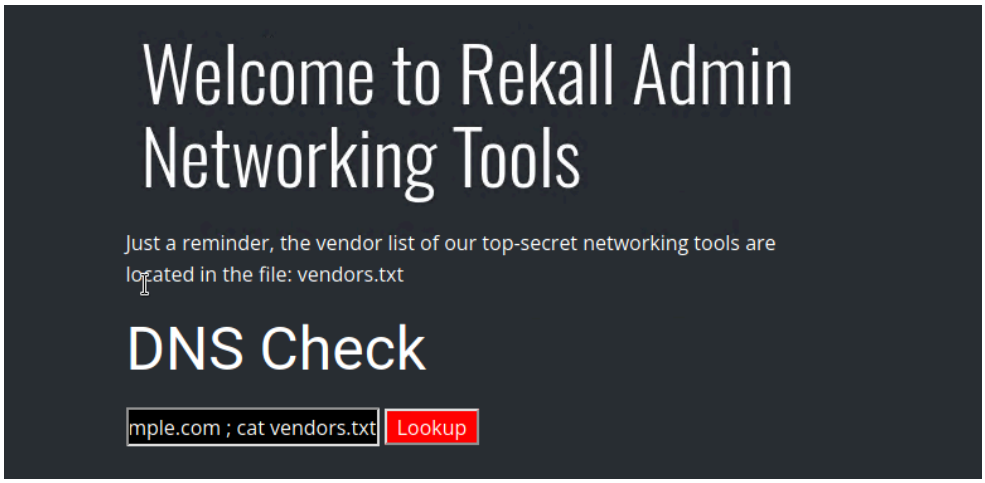
© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

	
Affected Hosts	34.102.136.180
Remediation	• Sensitive data should not be hidden in public-facing web pages or HTML code. • Credentials should be securely stored and encrypted, not plain-text views.

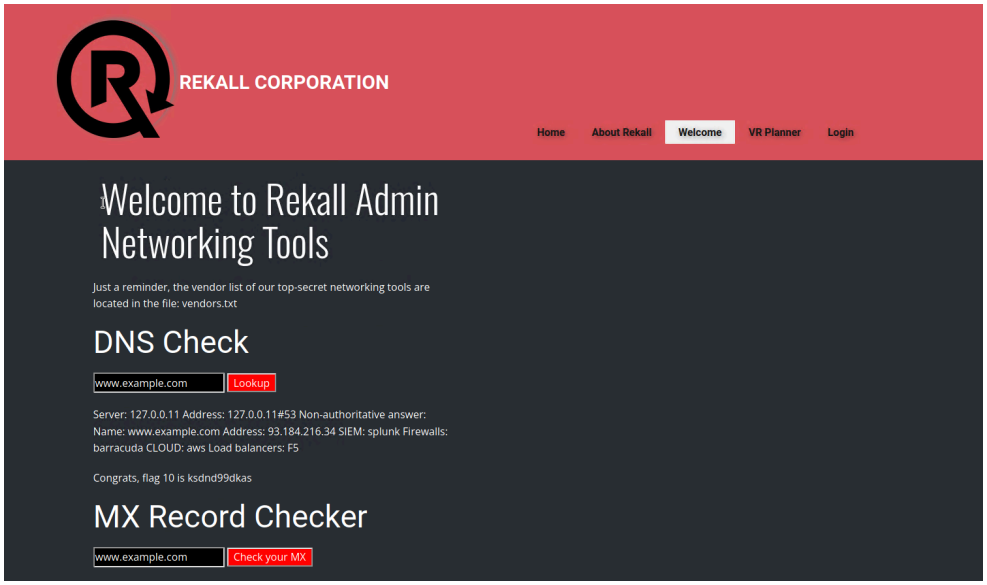
Vulnerability 7	Findings
Title	Command Injection
Type (Web app / Linux OS / WIndows OS)	Web App • networking.php
Risk Rating	Critical
Description	Landing on the networking.php web page we find a message indicating that there is a file containing top-secret networking information named: vendors.txt We proceeded to append `; cat vendors.txt` to the url www.example.com in the DNS checker field with hopes of executing a payload and accessing the secret data.

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

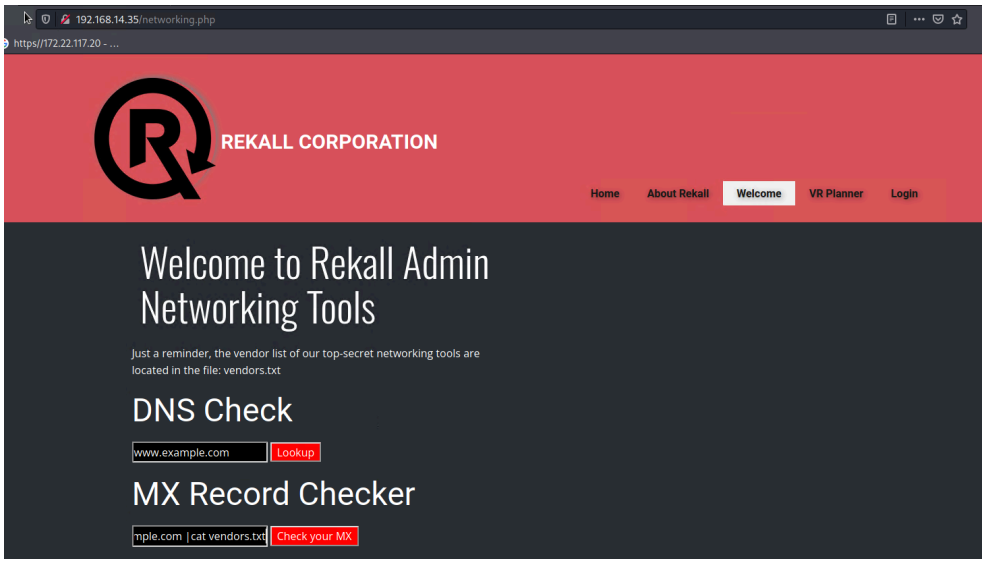
Images



Under the DNS Check input field, server information and the admin networking tools vendor list were revealed.



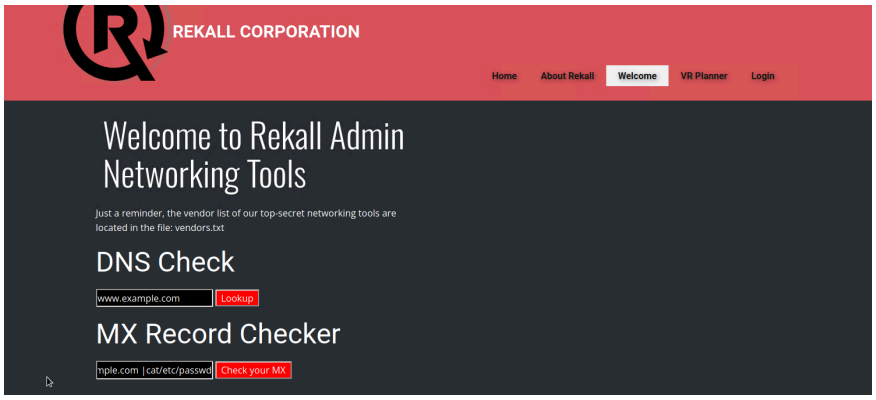
LIkely due to input validation, we were unable to do the same with the MX Record Checker field so we altered the command to: www.welcome.com | cat vendors.txt as shown:



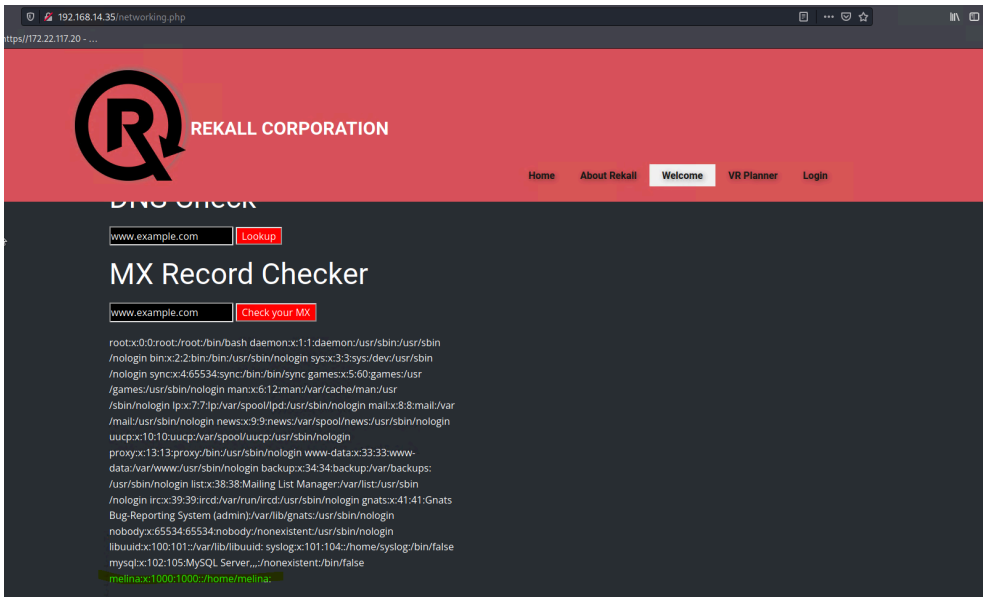
This isolated the vendors list for the admin networking tools but also confirmed

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

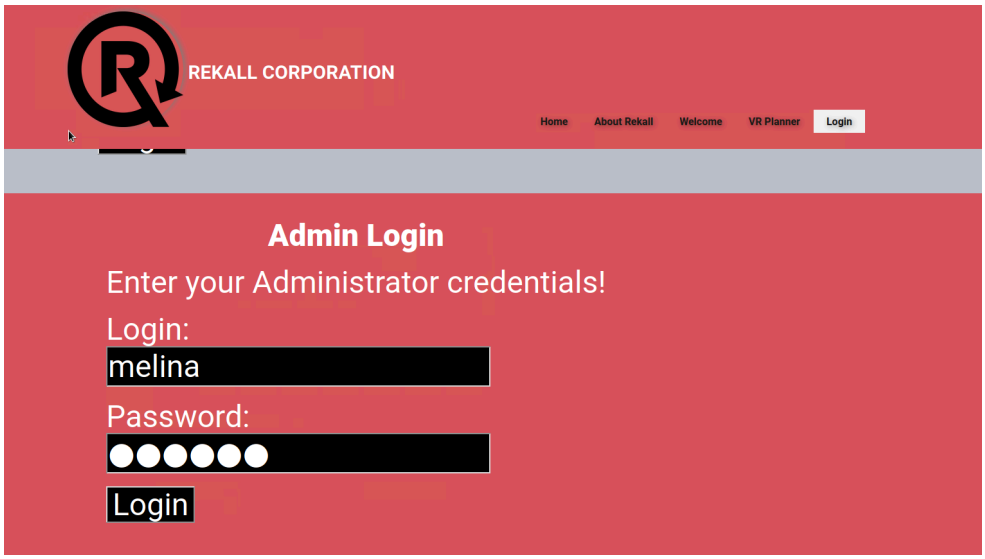
	that the page was prone to command injection vulnerabilities. This knowledge would allow us to continue to access sensitive data and increase our attack surface on the web app.
Affected Hosts	34.102.136.180
Remediation	• Parameterization • Input validation should include an allow-list of commands for validation. • Arguments used for command should also have a positive or allow-list where arguments are clearly defined. The same should apply to regular expressions. • Keeping systems updated and applying security patches for related and known vulnerabilities.

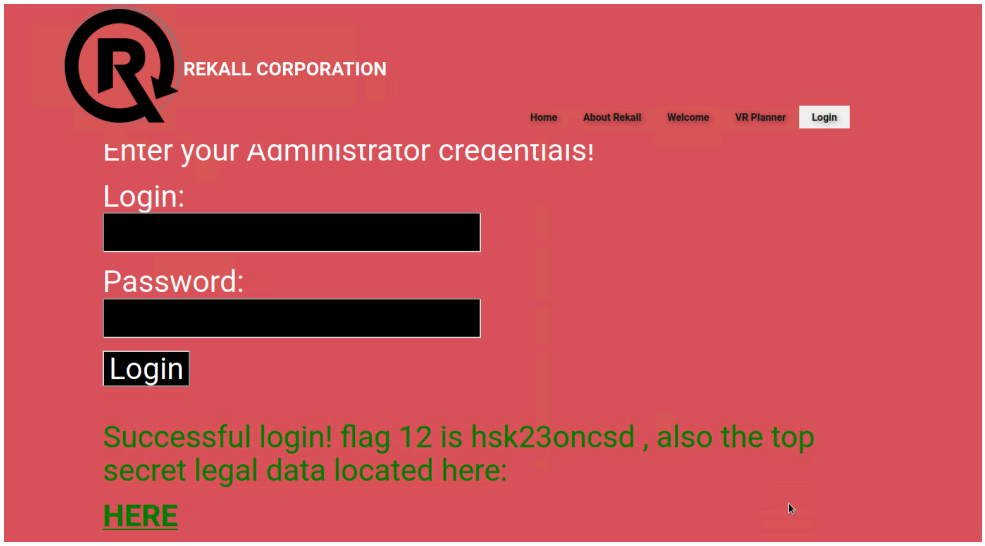
Vulnerability 8	**Findings**
Title	Brute Force Attack
Type (Web app / Linux OS / WIndows OS)	Web App • Welcome.php (2nd field)
Risk Rating	Critical
Description	Aware that we could use commands to access data and launch vulnerabilities, the BreachPulse team tested for brute force attacks. As with command injection, we used commands to navigate to a path where we knew we could find useful credentials: /etc/passwd. We succeeded by entering the following in the MX Record Checker field: www.example.com |cat/etc/passwd
Images	 A block of text containing usernames and passwords appeared under the input field. Among the usernames we found one with an UID of 1000 (highlighted in green below): melina.

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



With a UID of 1000, we entered “melina” as the username as well as the password.

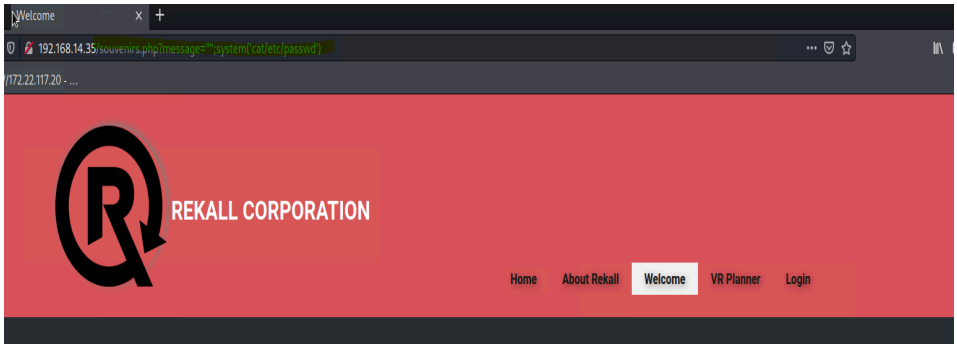




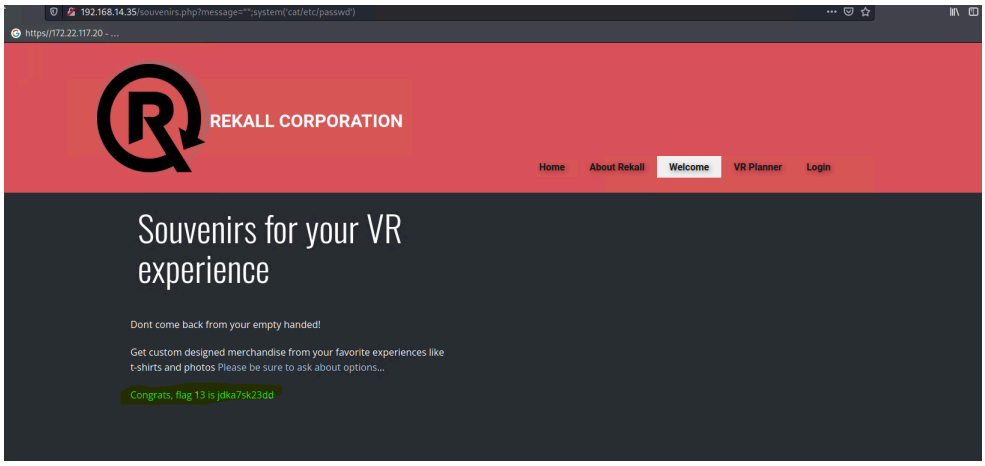
Not only was our brute force attack a success but we were able to obtain a

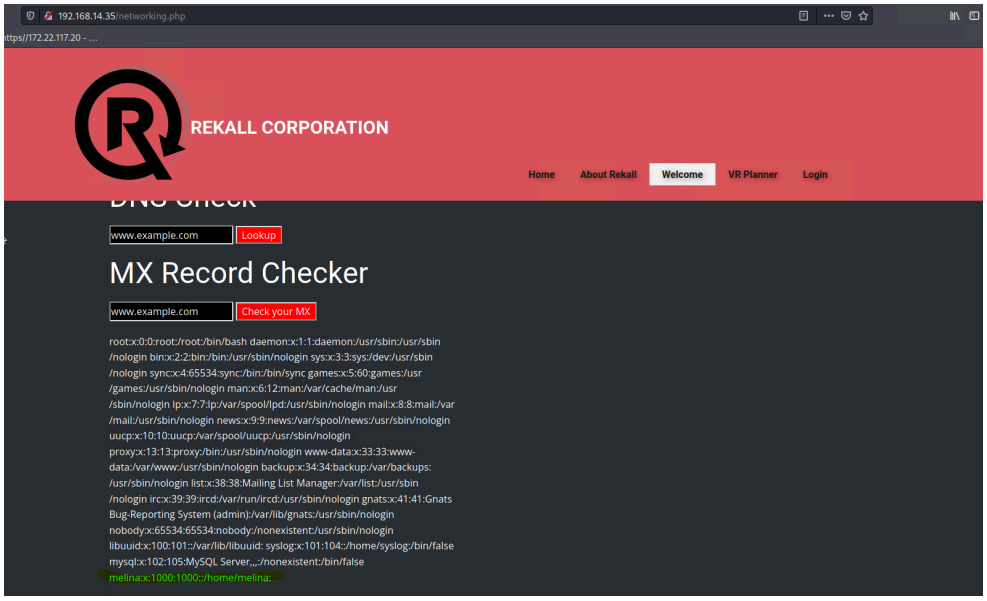
© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

	message with a link that was directing us to “top secret legal data”. We clicked the link and were provided with a the following: admin_legal_data.php
Affected Hosts	34.102.136.180
Remediation	• Use strong passwords and enforce and update password policy to meet best practices criteria • Limit login attempts • Monitor IP addresses • Use WAFs

Vulnerability 9	**Findings**
Title	PHP Injection
Type (Web app / Linux OS / WIndows OS)	Web App • souvenirs.php
Risk Rating	Critical
Description	As we continued in our search for sensitive data vulnerabilities we found a hidden web page named: souvenirs.php listed in our robots.txt file. BreachPulse used this information to run a payload and exploit the page by appending the following to the web page url: http://192.168.13.35/souvenirs.php?message””; system(‘cat /etc/passwd’)
Images	 Executing the payload revealed “Souvenirs” as seen in the next image:

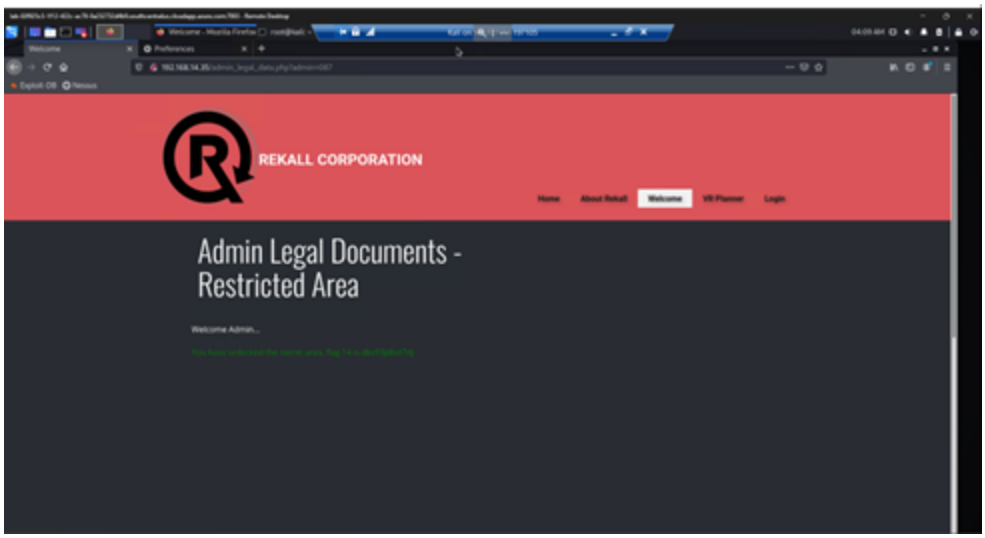
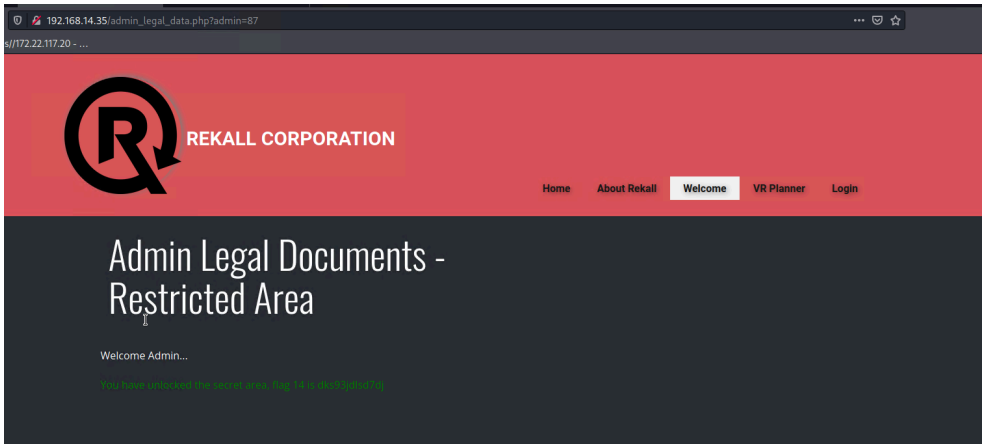
© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

	
Affected Hosts	34.102.136.180
Remediation	• Refrain from using direct shell execution functions. • Use built-in functions rather than OS commands.

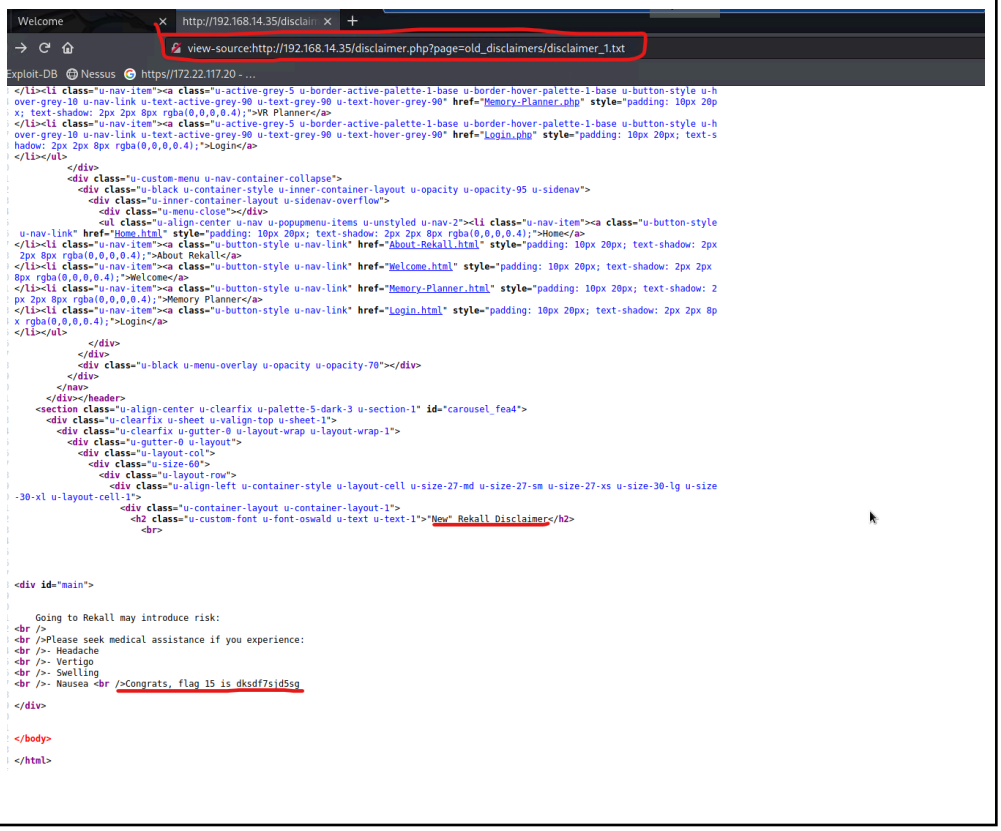
Vulnerability 10	**Findings**
Title	Insecure Passwords
Type (Web app / Linux OS / Wlndows OS)	Web App
Risk Rating	Critical
Description	Username, melina, was used as both username and password to log into web app after username was accessed via an injection attack using command: | cat /etc/passwd.Using username as password allowed a successful login attempt.
Images	
Affected Hosts	

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

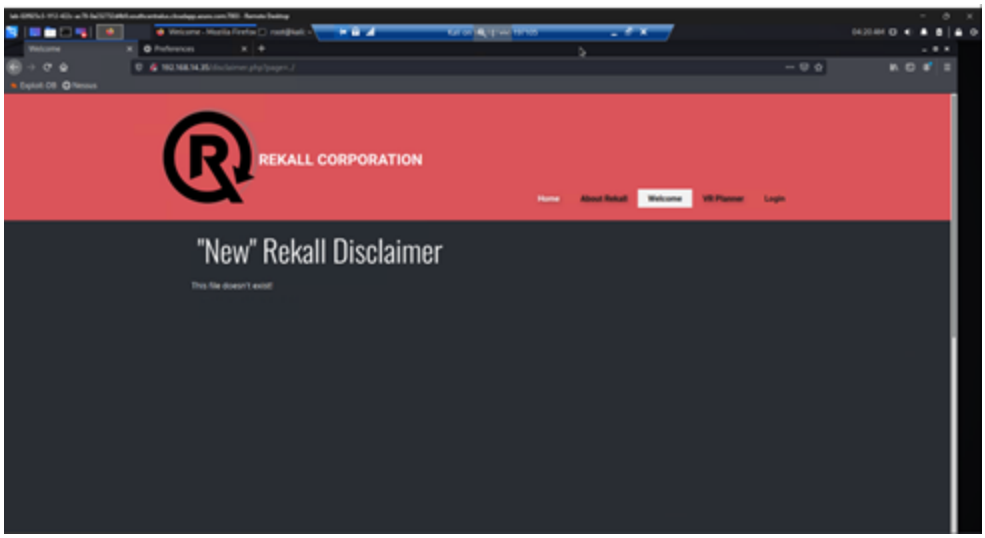
Remediation	Update and enforce a strong password policy

Vulnerability 11	Findings
Title	Session Management
Type (Web app / Linux OS / WIndows OS)	Web App • admin_legal_data.php
Risk Rating	
Description	Using the BurpSuite tool the team hijacked the session to access a restricted area of the web site. We used the tool to identify the Session ID.
Images	 We appended the session ID which was 87 in this manner 192.168.14.35/admin_legal_data.php?admin=87 and accessed the Restricted Area. 
Affected Hosts	
Remediation	• Use secure cookies

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

Vulnerability 12	Findings
Title	Directory Traversal
Type (Web app / Linux OS / WIndows OS)	Web App ● Disclaimer.php
Risk Rating	
Description	A hint within the source code of the disclaimer.php page indicates that there is a new disclaimer. We returned to the networking.php web page and using the input field entered the 'ls' command which revealed a "old_disclaimers" directory with file disclaimer_1.txt. We append this to the URL as seen in the image:
Images	

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



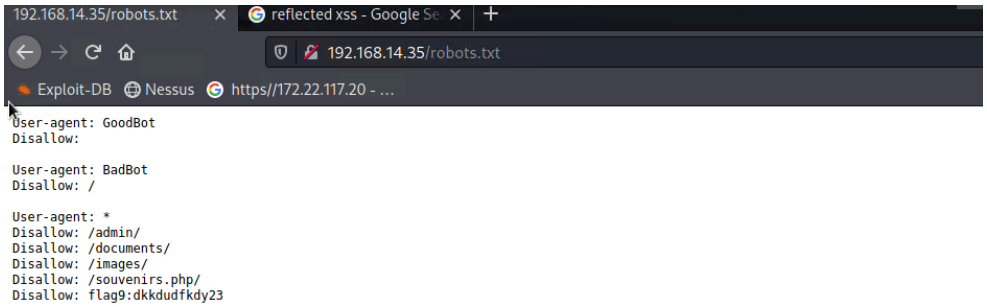
We manipulated the URL once more to access sensitive files. Here are the contents::

```
    Going to Rekall may introduce risk:
<br />
<br />Please seek medical assistance if you experience:
<br />- Headache
<br />- Vertigo
<br />- Swelling
<br />- Nausea <br />Congrats, flag 15 is dksdf7sjd5sg

</div>
```

Affected Hosts	:
Remediation	Work without user input when using file system calls. Input validation. Use policies to restrict where files can be obtained or saved to.

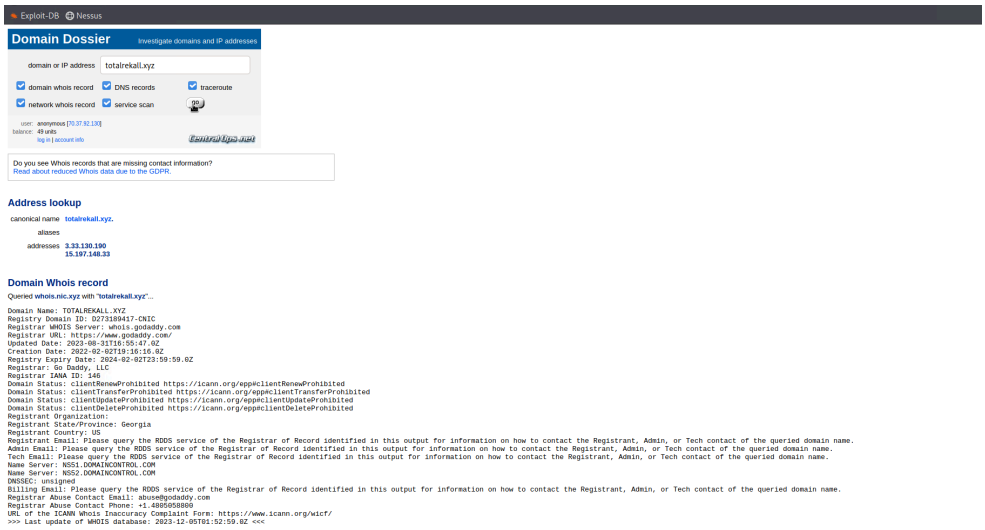
Vulnerability 13	Findings
Title	robots.txt file (tags/sensitive data exposure)
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Low
Description	robots.txt was easily accessible by appending its name to the web ip address as follows: 192.168.14.35/robots.txt. We were able to see directories and web pages that could potentially contain sensitive data in this manner but also noted the robots.txt file meta-tags. These tags have all been set to “disallow”. Of interest was the page /souvenirs.php
Images	

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

	
Affected Hosts	
Remediation	• There are other tags but one must understand the robots.txt and its contents to use these properly and prevent sensitive data exposure or caching. For example, The “disallow” tag tells search engines not to crawl a page. “no index” can be used to tell search engines not to index the page. • Sensitive data should not be stored in public-facing web pages or hidden in plain-text. • Anything containing credentials, sensitive documents, or web pages that were not meant to be accessed should be stored securely.

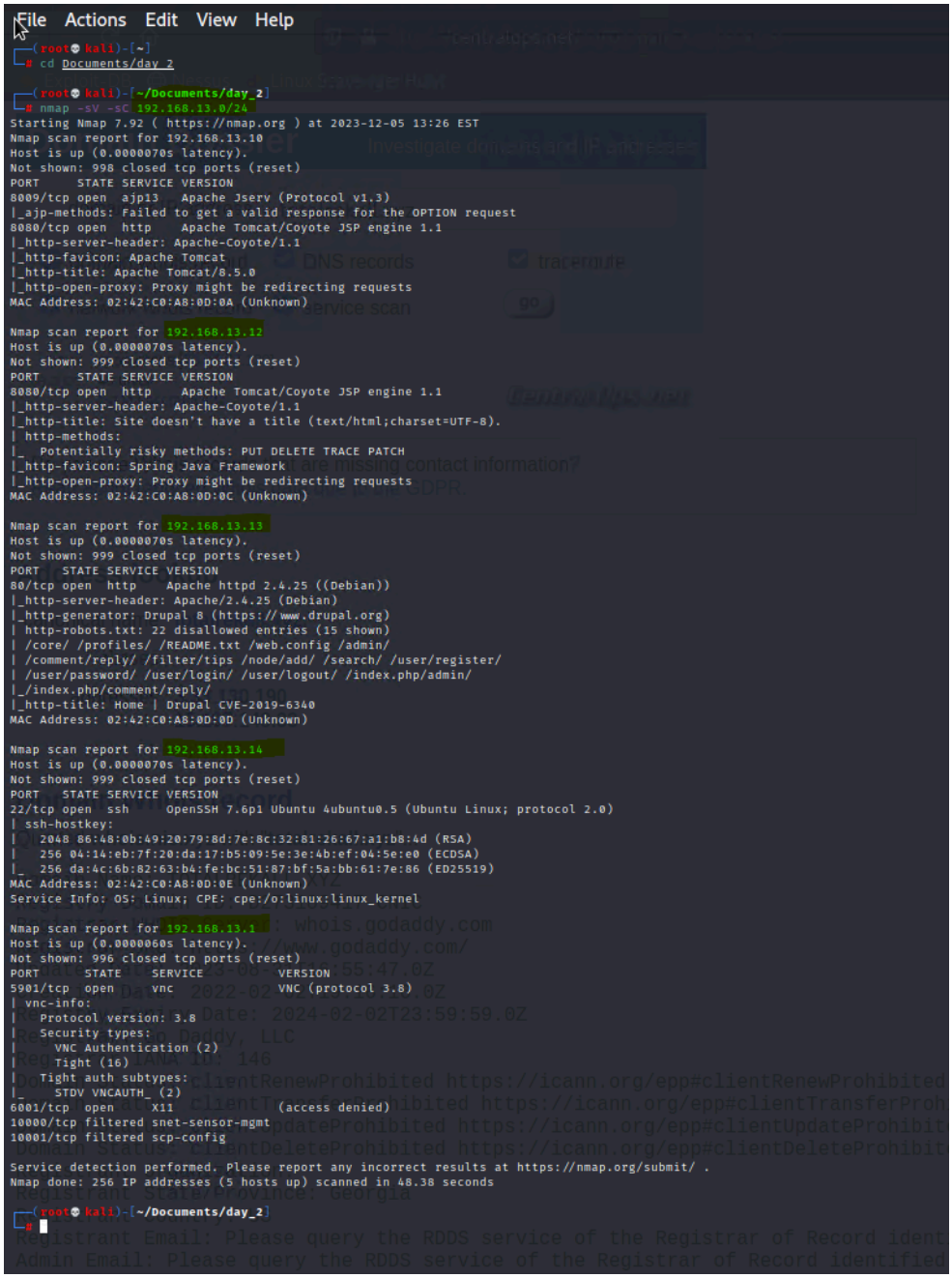
Vulnerability 14	Findings
Title	Open-Source Exposed Data
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Medium
Description	The team used the DomainDossier tool from ttps://centralops.net/co/DomainDossier.aspx to perform a WhoIs query for rekall.xyz. Code for Flag1 was obtained.

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

Images	 Along with Flag1, we can find the username for SSH login under Registrant Name: Queried whois.godaddy.com with "totalrekall.xyz"... Domain Name: totalrekall.xyz Registry Domain ID: D273189417-CNIC Registrar WHOIS Server: whois.godaddy.com Registrar URL: https://www.godaddy.com Updated Date: 2023-02-03T14:04:18Z Creation Date: 2022-02-02T19:16:16Z Registrar Registration Expiration Date: 2024-02-02T23:59:59Z Registrar: GoDaddy.com, LLC Registrar IANA ID: 146 Registrar Abuse Contact Email: abuse@godaddy.com Registrar Abuse Contact Phone: +1.4806242505 Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited Registry Registrant ID: CR534509109 Registrant Name: sshUser alice Registrant Organization: Registrant Street: h8s692hskasd Flag1 Registrant City: Atlanta Registrant State/Province: Georgia Registrant Postal Code: 30309 Registrant Country: US Registrant Phone: +1.7702229999 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: jlow@2u.com Registry Admin ID: CR534509111 Admin Name: sshUser alice Admin Organization: Admin Street: h8s692hskasd Flag1 Admin City: Atlanta Admin State/Province: Georgia Admin Postal Code: 30309 Admin Country: US Admin Phone: +1.7702229999 Admin Phone Ext: Admin Fax: Admin Fax Ext: Admin Email: jlow@2u.com Registry Tech ID: CR534509110 Tech Name: sshUser alice Tech Organization: Tech Street: h8s692hskasd Flag1 Tech City: Atlanta Tech State/Province: Georgia Tech Postal Code: 30309 Tech Country: US
Affected Hosts	
Remediation	Maintain and update publicly-accessible records Protect sensitive data by properly securing and encrypting it

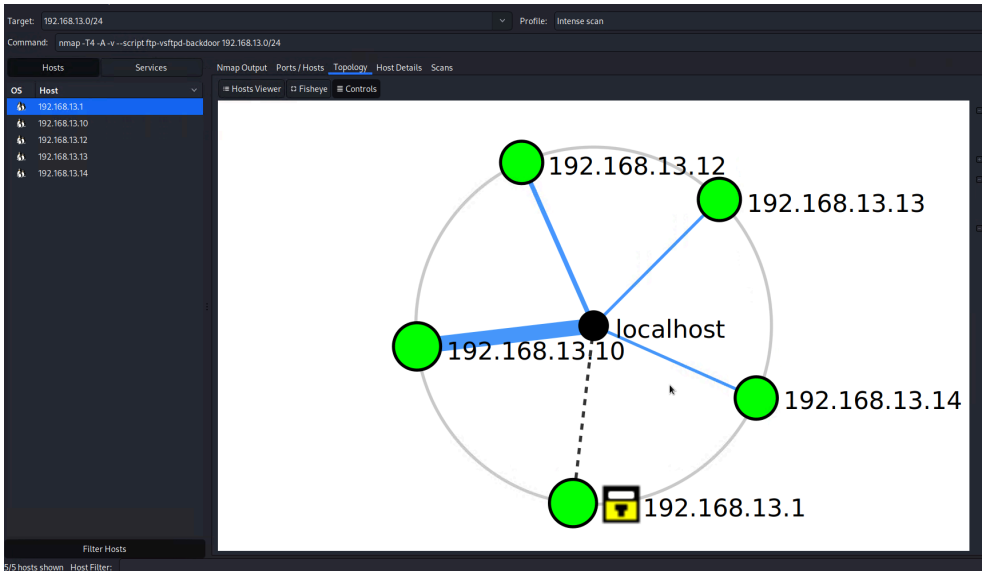
Vulnerability 15	Findings
Title	Nmap Scan Results
Type (Web app / Linux OS / WIndows OS)	Web App / Linux OS / Windows OS
Risk Rating	Low

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

Description	We used Nmap, an open-source network scanning tool to run an aggressive scan. The scan results provided the following information about the network and ports: ● There were 5 hosts discovered on the network ● The host ending in .13 was running Drupal ● The following ports were open: 21, 22, 80, 8080, 5901, 6001, 10000, 10001
Images	

```
File  Actions  Edit  View  Help
┌──(root㉿kali)-[~]
└─# cd Documents/day_2

┌──(root㉿kali)-[~/Documents/day_2]
└─# nmap -sV -sC 192.168.13.0/24
Starting Nmap 7.92 ( https://nmap.org ) at 2023-12-05 13:26 EST
Nmap scan report for 192.168.13.10
Host is up (0.0000070s latency).
Not shown: 998 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
8009/tcp open  ajp13   Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTION request
8080/tcp open  http    Apache Tomcat/Coyote JSP engine 1.1
|_http-server-header: Apache-Coyote/1.1
|_http-favicon: Apache Tomcat
|_http-title: Apache Tomcat/8.5.0
|_http-open-proxy: Proxy might be redirecting requests
MAC Address: 02:42:C0:A8:0D:0A (Unknown)

Nmap scan report for 192.168.13.12
Host is up (0.0000070s latency).
Not shown: 999 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
8080/tcp open  http    Apache Tomcat/Coyote JSP engine 1.1
|_http-server-header: Apache-Coyote/1.1
|_http-title: Site doesn't have a title (text/html;charset=UTF-8).
| http-methods:
|_  Potentially risky methods: PUT DELETE TRACE PATCH
|_http-favicon: Spring Java Framework
|_http-open-proxy: Proxy might be redirecting requests
MAC Address: 02:42:C0:A8:0D:0C (Unknown)

Nmap scan report for 192.168.13.13
Host is up (0.0000070s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.25 ((Debian))
|_http-server-header: Apache/2.4.25 (Debian)
|_http-generator: Drupal 8 (https://www.drupal.org)
| http-robots.txt: 22 disallowed entries (15 shown)
| /core/ /profiles/ /README.txt /web.config /admin/
| /comment/reply/ /filter/tips /node/add/ /search/ /user/register/
| /user/password/ /user/login/ /user/logout/ /index.php/admin/
|_/index.php/comment/reply/
|_http-title: Home | Drupal CVE-2019-6340
MAC Address: 02:42:C0:A8:0D:0D (Unknown)

Nmap scan report for 192.168.13.14
Host is up (0.0000070s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 86:48:0b:49:20:79:8d:7e:8c:32:81:26:67:a1:b8:4d (RSA)
|   256 04:14:eb:7f:20:da:17:b5:09:5e:3e:4b:ef:04:5e:e0 (ECDSA)
|_  256 da:4c:6b:82:63:b4:fe:bc:51:87:bf:5a:bb:61:7e:86 (ED25519)
MAC Address: 02:42:C0:A8:0D:0E (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 192.168.13.1
Host is up (0.0000060s latency).
Not shown: 996 closed tcp ports (reset)
PORT     STATE    SERVICE       VERSION
5901/tcp open     vnc           VNC (protocol 3.8)
| vnc-info:
|   Protocol version: 3.8
|   Security types:
|     VNC Authentication (2)
|     Tight (16)
|   Tight auth subtypes:
|_    STDV VNCAUTH_ (2)
6001/tcp open     X11           (access denied)
10000/tcp filtered snet-sensor-mgmt
10001/tcp filtered scp-config

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (5 hosts up) scanned in 48.38 seconds

┌──(root㉿kali)-[~/Documents/day_2]
└─#
```

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

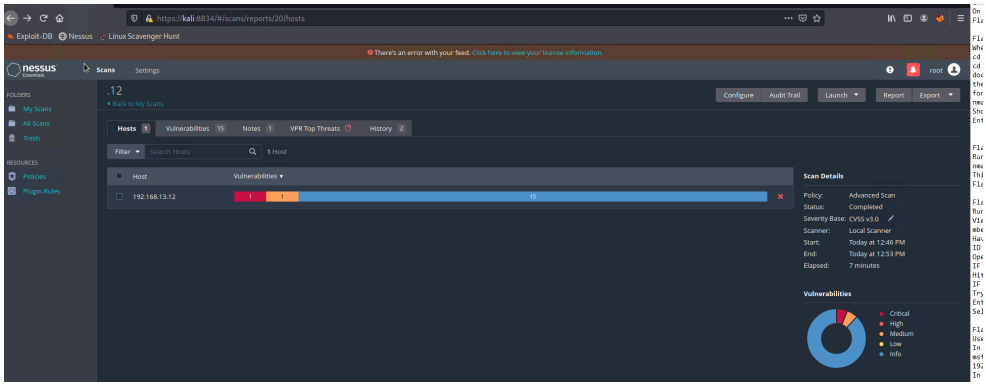
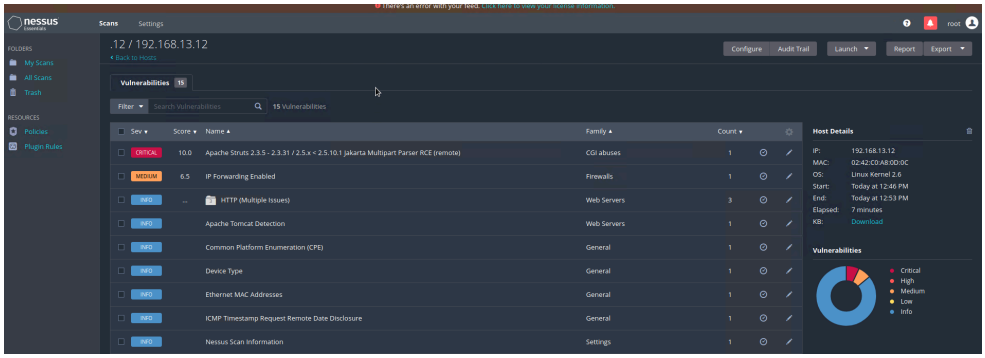
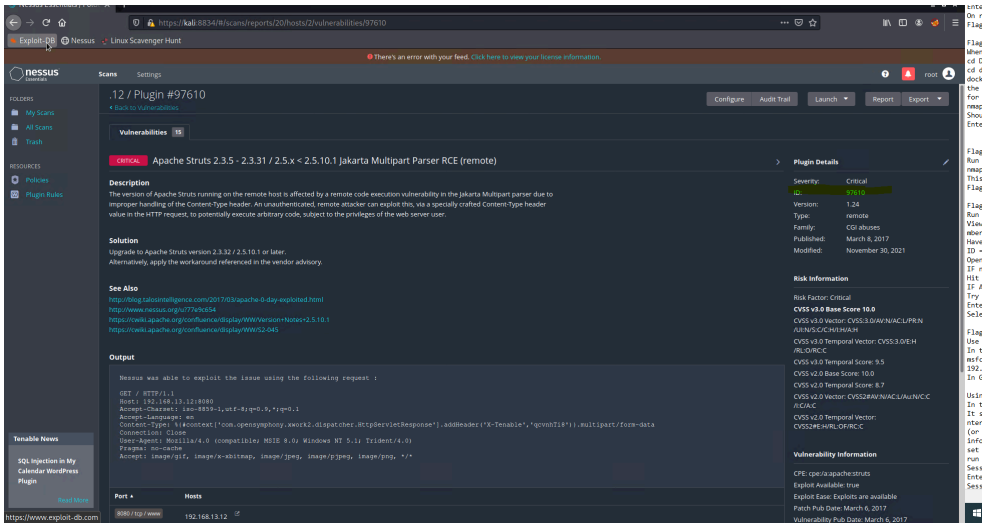


This host is running Drupal:

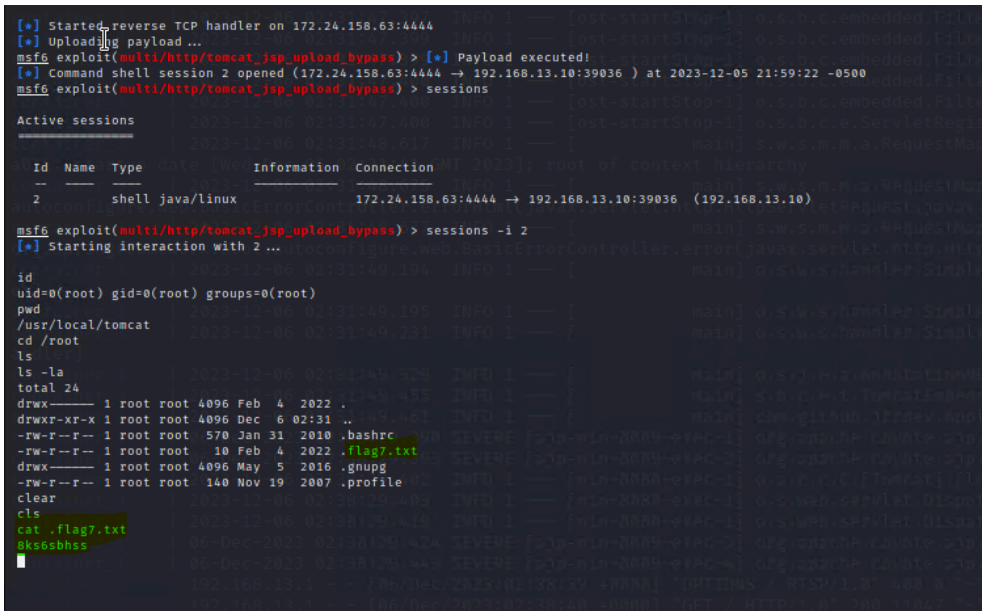
```
┌──(root㉿kali)-[~/Documents/day_2]
└─# nmap -A 192.168.13.0/24
Starting Nmap 7.92 ( https://nmap.org ) at 2023-12-05 13:46 EST
Nmap scan report for 192.168.13.10
Host is up (0.000082s latency).
Not shown: 998 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
8009/tcp open  ajp13   Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTION request
8080/tcp open  http    Apache Tomcat/Coyote JSP engine 1.1
|_http-server-header: Apache-Coyote/1.1
|_http-title: Apache Tomcat/8.5.0
|_http-favicon: Apache Tomcat
MAC Address: 02:42:C0:A8:0D:0A (Unknown)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.6
Network Distance: 1 hop

TRACEROUTE
HOP RTT     ADDRESS
1   0.08 ms 192.168.13.10

Nmap scan report for 192.168.13.12
Host is up (0.000023s latency).
Not shown: 999 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
8080/tcp open  http    Apache Tomcat/Coyote JSP engine 1.1
|_http-server-header: Apache-Coyote/1.1
| http-methods:
|_  Potentially risky methods: PUT DELETE TRACE PATCH
|_http-title: Site doesn't have a title (text/html;charset=UTF-8).
|_http-favicon: Spring Java Framework
MAC Address: 02:42:C0:A8:0D:0C (Unknown)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.6
Network Distance: 1 hop

TRACEROUTE
HOP RTT     ADDRESS
1   0.02 ms 192.168.13.12

Nmap scan report for 192.168.13.13
Host is up (0.000015s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.25 ((Debian))
|_http-server-header: Apache/2.4.25 (Debian)
|_http-generator: Drupal 8 (https://www.drupal.org)
|_http-title: Home | Drupal CVE-2019-6340
| http-robots.txt: 22 disallowed entries (15 shown)
| /core/ /profiles/ /README.txt /web.config /admin/
| /comment/reply/ /filter/tips /node/add/ /search/ /user/register/
| /user/password/ /user/login/ /user/logout/ /index.php/admin/
|_/index.php/comment/reply/
MAC Address: 02:42:C0:A8:0D:0D (Unknown)
Device type: general purpose
```

Affected Hosts	192.168.13.1 192.168.13.10 192.168.13.12 192.168.13.13 192.168.13.14
Remediation	Properly configured a firewall and custom rules. Use secure ports Test and update firewall and its configuration.

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

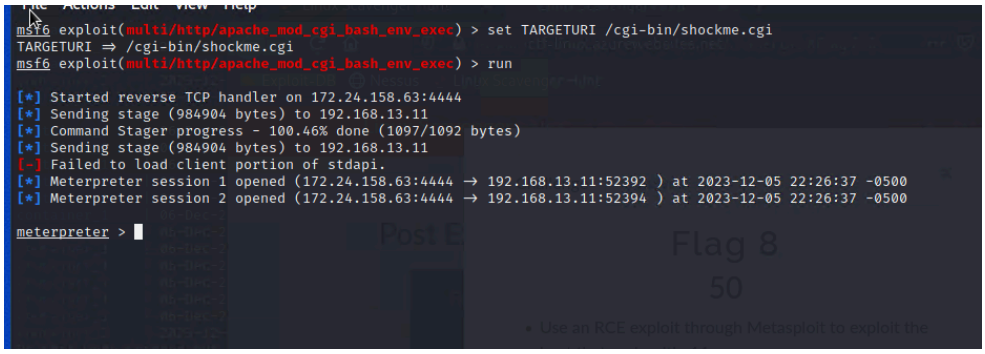
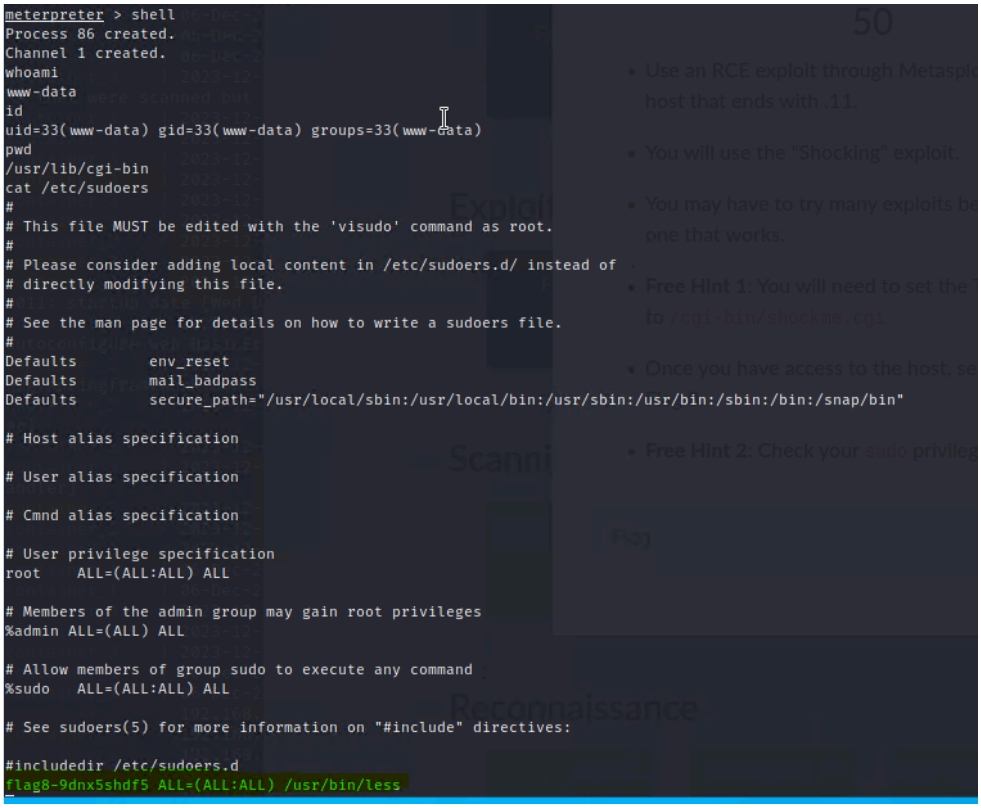
Vulnerability 16	Findings
Title	Nessus Scan Results - CVE-2017-12617 - Apache Tomcat RCE
Type (Web app / Linux OS / WIndows OS)	Linux OS • 192.168.13.12
Risk Rating	Critical
Description	We performed a Nessus scan for 192.168.13.12 and found a single, critical vulnerability for Apache Tomcat Remote Code Execution Vulnerability (CVE-2017-12617). Vulnerability ID = 97610.
Images	 It is also known as “Apache Struts”   • Using MSFconsole we were able to successfully deploy the

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

	exploit:exploit/multi/http/tompcat_jsp_upload_bypass  We used the Meterpreter shell to access .flag7.txt which contained the code for Flag7.
Affected Hosts	192.168.13.12
Remediation	• Update system and apply the latest security patches.

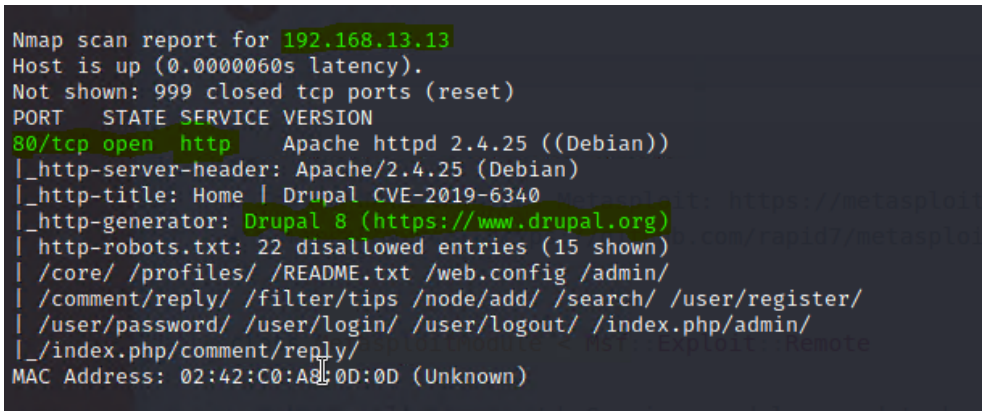
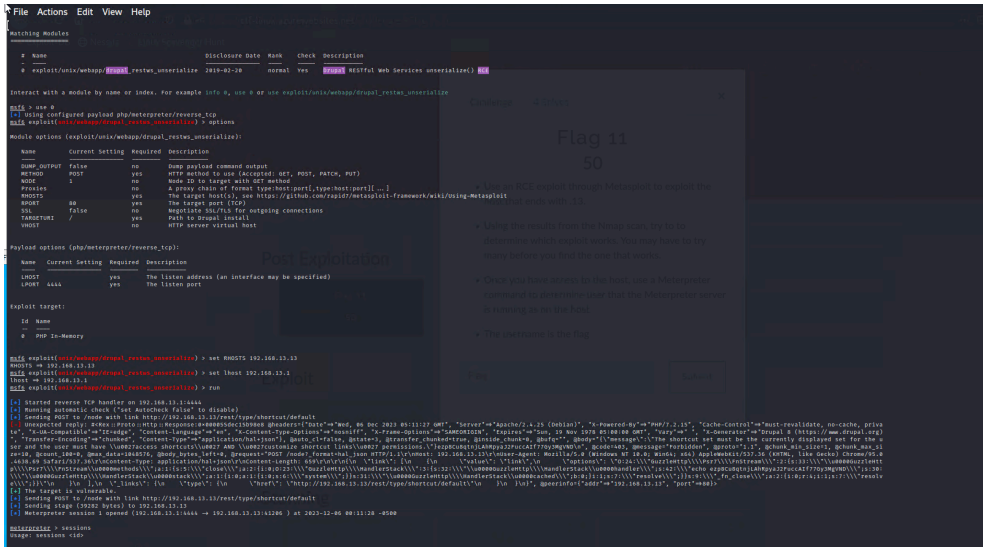
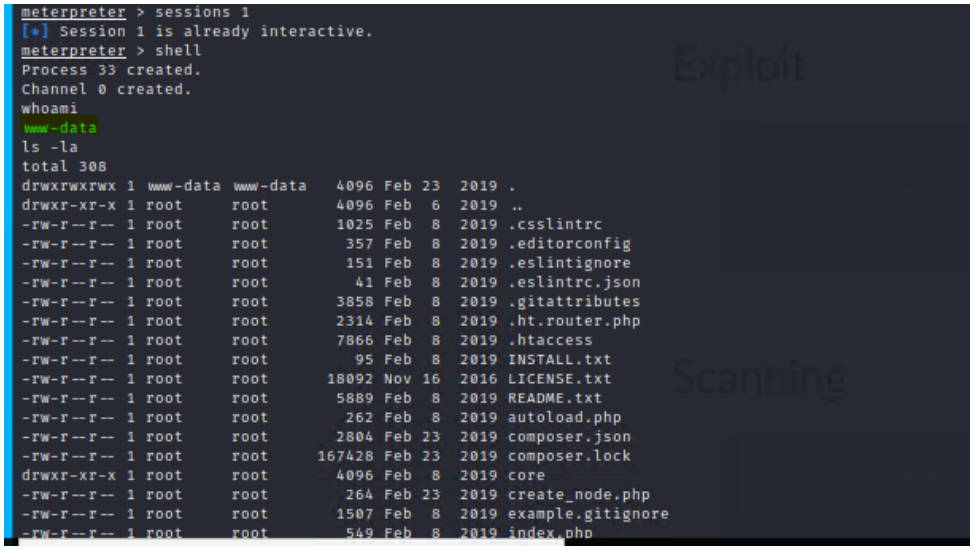
Vulnerability 17	Findings
Title	CVE-2014-7169 - Shellshock
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	High
Description	We ran MSFconsole and sought exploits containing the term “shellshock” and selected the following as the exploit to launch: exploit/multi/http/apache_mod_cgi_bash_env_exec Then, we set the target URI as /cgi-bin/shockme.cgi (the vulnerable web page) and the remote host as 192.168.13.11. We ran the exploit, accessed a Meterpreter shell, and obtained the sudoers file using command: cat /etc/sudoers.

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

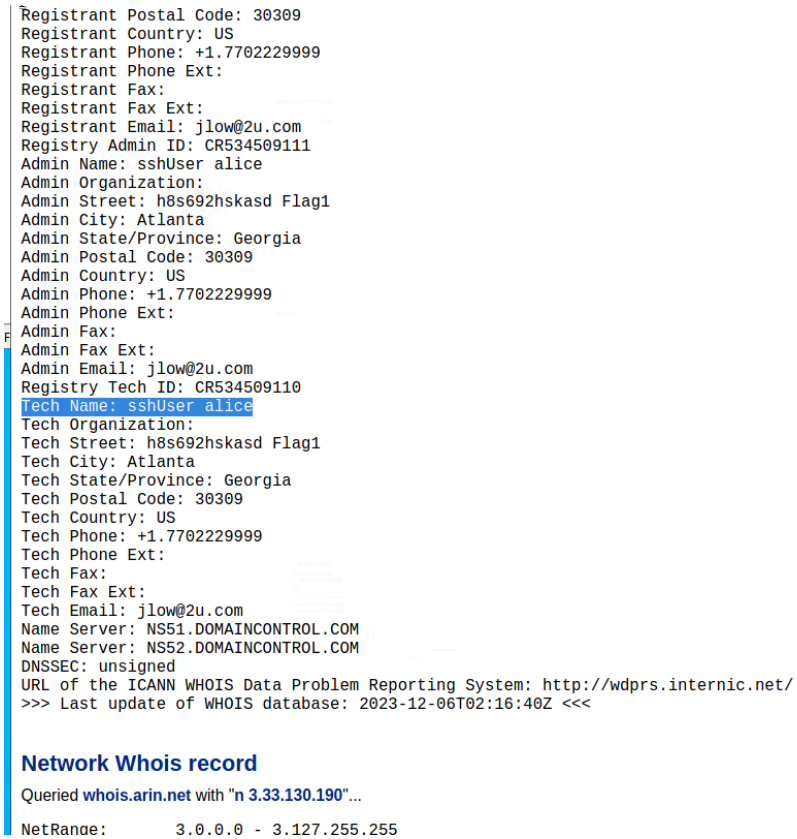
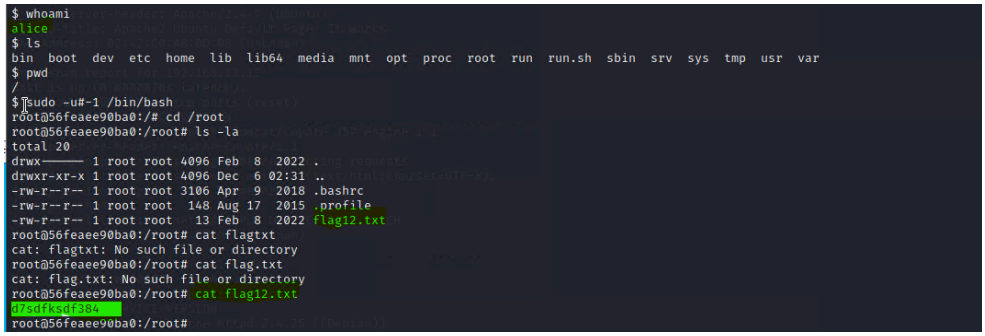
Images	 cat /etc/sudoers 
Affected Hosts	192.168.13.11
Remediation	Apply updates per vendor instructions.

Vulnerability 18	Findings
Title	CVE-2019-6340 - Drupal
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	In a previous Nmap scan we learned that 192.168.13.13 was running Drupal 8. We used MSFconsole to deploy another exploit:

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

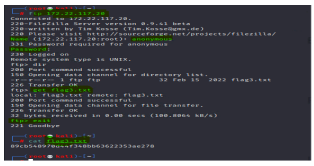
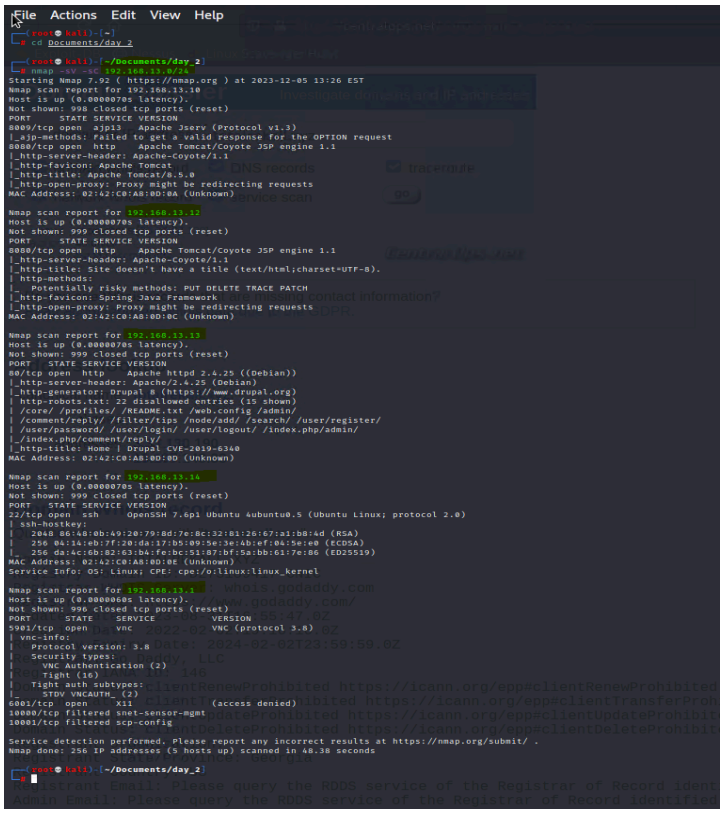
	https://nvd.nist.gov/vuln/detail/CVE-2019-6340 or as seen in the image: unix/webapp/drupal_restws_unserialize
Images	  Again, we accessed the Meterpreter shell and discovered the root user as www-data. 
Affected Hosts	192.168.13.13
Remediation	• This system can be updated to the latest version and patched to address the security vulnerability.

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

Vulnerability 19	Findings
Title	CVE-1019-14287 - Security Bypass
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	We ran a security bypass. Using sensitive data contained in the WhoIs record from our previous search, we were able to obtain an SSH username for login using open port 22. Details for exploit/vulnerability can be found here: https://nvd.nist.gov/vuln/detail/CVE-2019-14287
Images	 We gained access using ssh alice@192.168.13.14. As with the open port 21 vulnerability, we gained access to the system by using the username as login name and password. With this information we were able to conduct a privilege escalation exploit. 

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

Affected Hosts	192.168.13.14
Remediation	Properly secure, store, and encrypt sensitive data. Do not leave sensitive data (especially credentials) in public facing apps and plain-text. Update password policy. Secure ports and update firewall custom rules Apply system patches and update security.

Vulnerability 20	Findings
Title	Open, Unsecured Ports
Type (Web app / Linux OS / WIndows OS)	Windows OS / Linux OS
Risk Rating	Critical
Description	Nmap scan revealed that 172.22.117.20 (Windows OS) had an open port 21 (ftp) that allowed anonymous access. The Linux OS had open port 22 (ssh) which we used to login into with the exposed ssh alice credential.
Images	 

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

	192.168.13.14 has port 22 (ssh) open.
Affected Hosts	172.22.117.20 192.168.13.14
Remediation	● Use secure ports and protocols. ● Set secure username and passwords and follow recommended best practices for authentication and firewall rules.

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