



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

Confidentiality Statement	2
Contact Information	4
Document History	4
Introduction	5
Assessment Objective	5
Penetration Testing Methodology	6
Reconnaissance	6
Identification of Vulnerabilities and Services	6
Vulnerability Exploitation	6
Reporting	6
Scope	7
Executive Summary of Findings	8
Grading Methodology	8
Summary of Strengths	9
Summary of Weaknesses	9
Executive Summary Narrative	10
Summary Vulnerability Overview	13
Vulnerability Findings	14

Contact Information

Company Name	Cover Your Ash LLC
Contact Name	John Ash
Contact Title	CEO-Owner

Document History

Version	Date	Author(s)	Comments
001	10/14/2022	John Ash	Pentest covered the following days. 10/3/2022-10/8/2022

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.

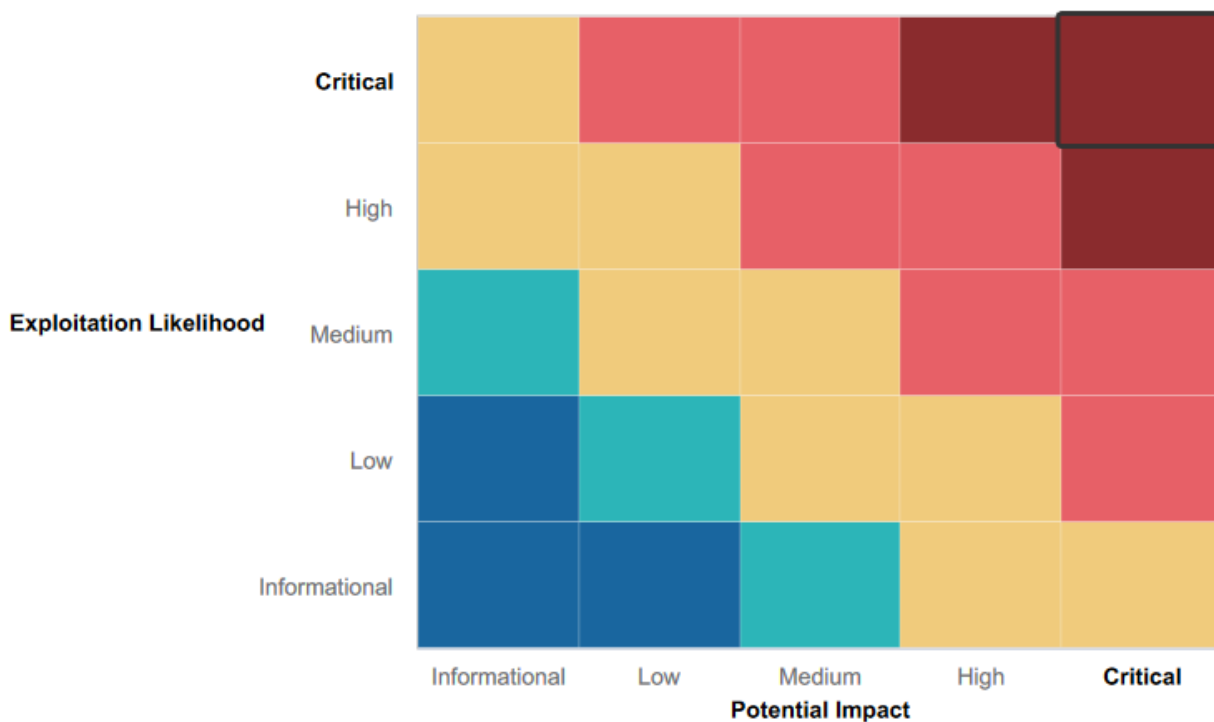
Executive Summary of Findings

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.

- Basic Networking for business operations
- File Directories were consistent and managed
- Multiple failed directory traversal 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.

- Common open ports and unpatched applications running for exploitation
- Weak password credentials
- No security measures for common password attacks
- Weak input validation on web application
- very susceptible to cross site scripting
-
-

Executive Summary

Our plan first consisted of our planning and reconnaissance phase. We conducted an NMAP scan and found IP information and open ports for every machine that was connected to the internet on your network. Here we found seven IP addresses, their open ports and services. With this critical information we were able to move to the next phase.

With the information gathered during our reconnaissance phase we are able to use that information to exploit Rekall's network and gain access. We found admin credentials, were able to browse the servers files and ultimately gain root access to the servers.

Summary Vulnerability Overview

Vulnerability	Severity
Cross Site Scripting	High
Cross Site Scripting around input validation	High
SQL injection into username / password database	Critical
Local File Inclusion	High
PHP injection	Critical
Sensitive Data Exposure (through Burp Suite)	High
Cross Site Request Forgery	High
DNS WHO.IS Look up	Low
RCE Exploit into 192.168.13.10	High
RCE exploit into 192.168.13.11	High
RCE exploit into 192.168.13.12	High
Drupal Exploit into 192.168.13.13	High
FTP Enumeration	High
HTTP Enumeration of 172.22.117.0/24 subnet	High
Escalating Access into WinDC machine	Critical
SLmail Metasploit Exploit	Critical
Nmap -Pn Scans on 192.168.13.0/24	Low
OSNIT gitlab reconnaissance for totalrekall	Low
Credential Dumping of Admin credentials on winDC machine	Critical
User Enumeration on Win10 machine	Critical
Nmap -Pn scan on 172.22.117.0/24	Low

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

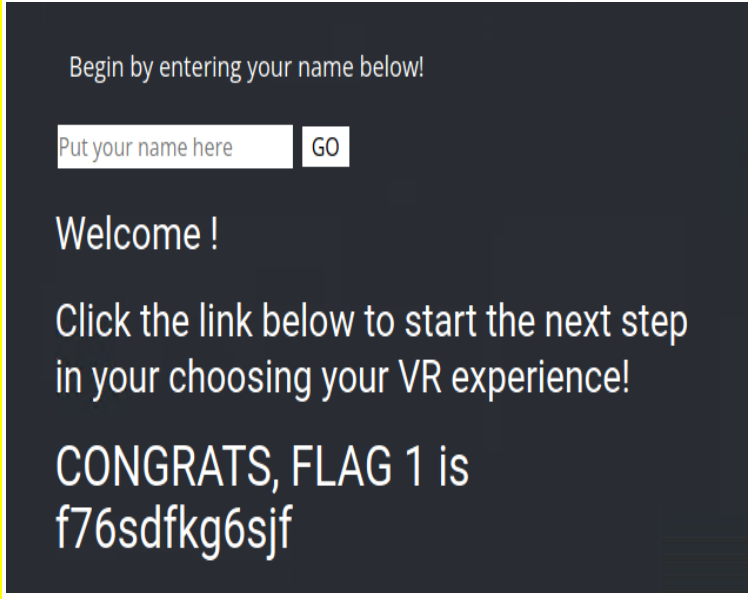
Scan Type	Total
Hosts	Linux (5)
	- 192.168.13.10
	- 192.168.13.11
	- 192.168.13.12
	- 192.168.13.13
	- 192.168.13.14
	Windows (2)
	- 172.22.117.10
	- 172.22.117.20
Ports	Linux
	- 22/tcp (ssh)
	- 80/tcp (http)

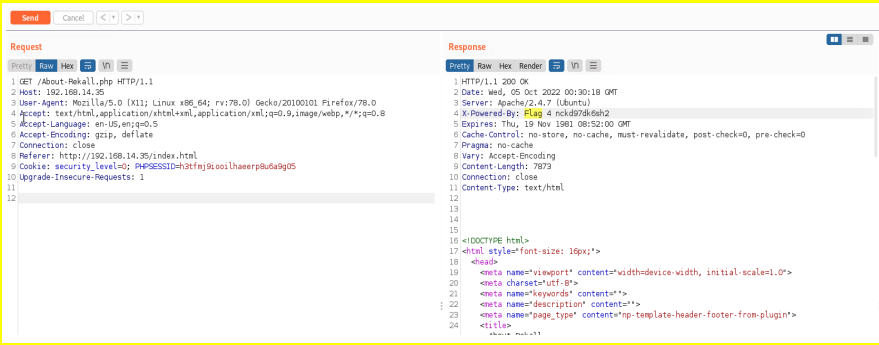
	<ul style="list-style-type: none"> - 8009/tcp (ajp13) - 8080/tcp (http-proxy) <p>Windows</p> <ul style="list-style-type: none"> - 53/tcp (domain) - 88/tcp (Kerberos-sec) - 135/tcp (msrpc) - 139/tcp (netbios-ssn) - 389/tcp (ldap) - 445/tcp (microsoft-ds) - 464/tcp (kpasswd5) - 593/tcp (http-rpc-epmap) - 636/tcp (ldapssl) - 3268/tcp (globalcatldap) - 3269/tcp(globalcatldapssl)
--	--

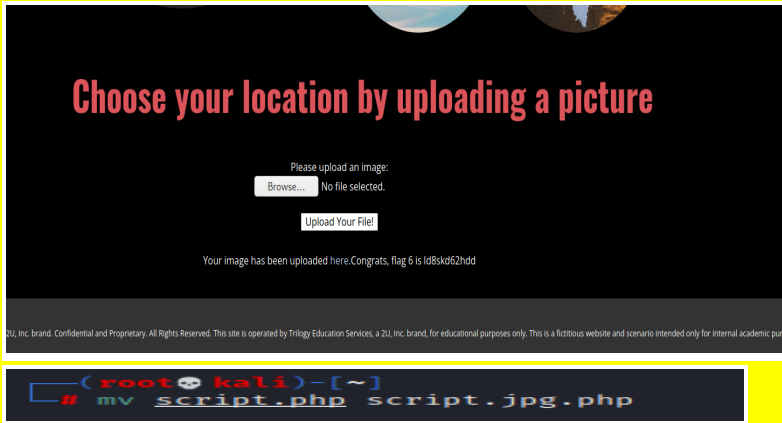
Exploitation Risk	Total
Critical	6
High	11
Medium	0
Low	4

Vulnerability Findings

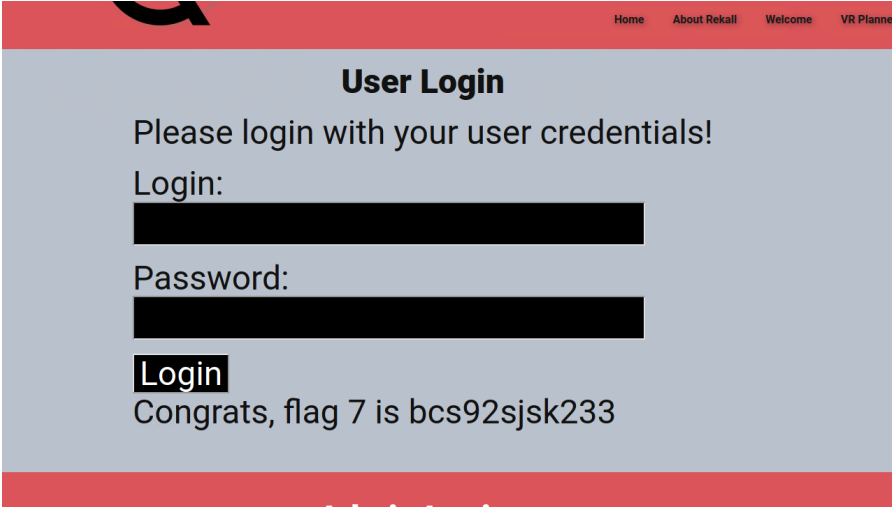
Vulnerability 1	Findings
Title	Cross Site Scripting
Type (Web app / Linux OS / Windows OS)	Web Application
Risk Rating	High
Description	We were able to type HTML code into an input field in order to execute the code onto the website itself.

Images	
Affected Hosts	Totalrekall.xyz (web application itself)
Remediation	For front end / client side we can use input validation and sanitize the input fields to not allow any type of script type language to be used.

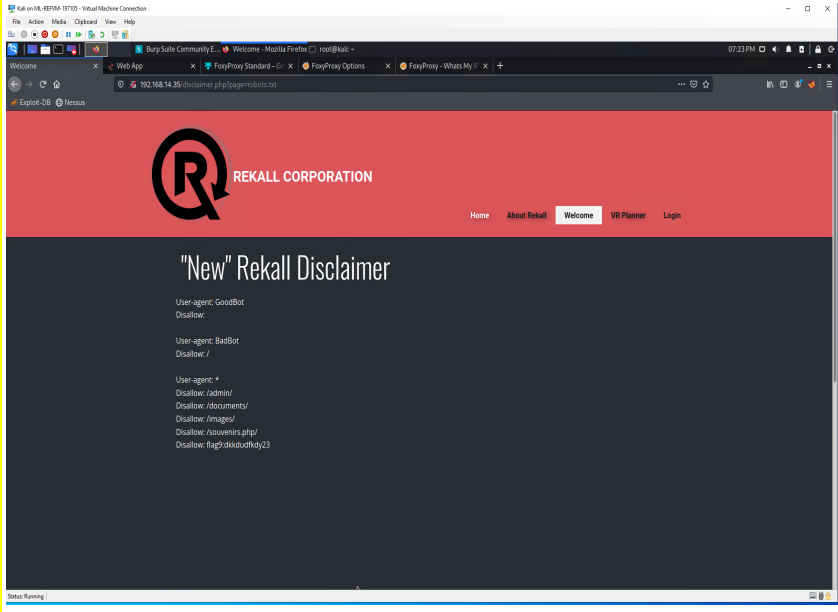
Vulnerability 2	Findings
Title	Sensitive Data Exposure
Type (Web app / Linux OS / Windows OS)	Web Application
Risk Rating	High
Description	Through tools like foxy proxy and burpsuite we were able to intercept an HTTP request to see sensitive data that pertained to the type of server (X-Powered By), which would give attackers insight to what ty of exploits to run against the server
Images	
Affected Hosts	totalrekall.xyz
Remediation	This can be disabled or manipulated by the server in the server settings.

Vulnerability 3	Findings
Title	PHP injection
Type (Web app / Linux OS / Windows OS)	web application
Risk Rating	Critical
Description	Through a photo upload input we were able to upload a malicious payload disguised as a .jpg file
Images	
Affected Hosts	totalrekall.xyz
Remediation	We could use a PHP security linter, or utilize a SAST tool to identify code injection issues, as well as hardening input validation methods and input sanitization methods.

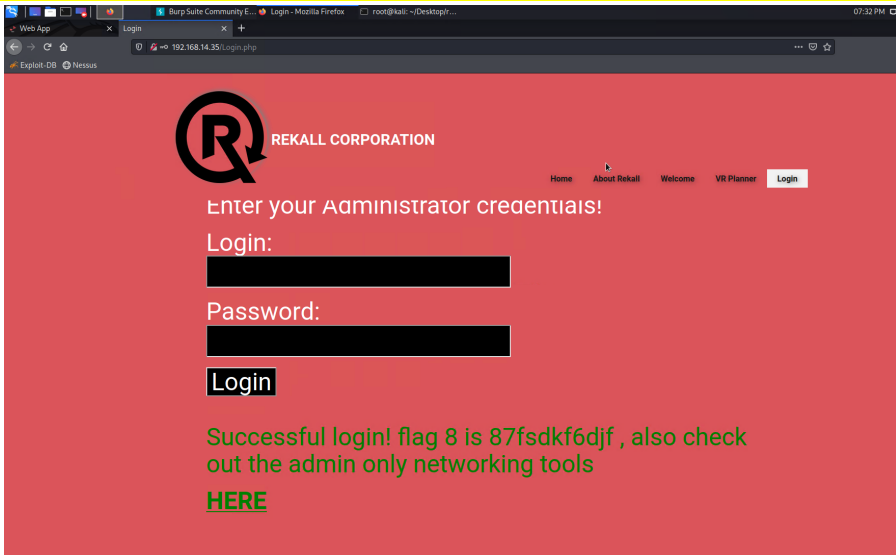
Vulnerability 4	Findings
Title	SQL injection
Type (Web app / Linux OS / Windows OS)	Web Application
Risk Rating	Critical
Description	By using SQL injections we were able to log into the web applications database by using a command code of dog' OR '1'='1 for both username and password. We could take it steps further and actually delete entire databases worth of information.

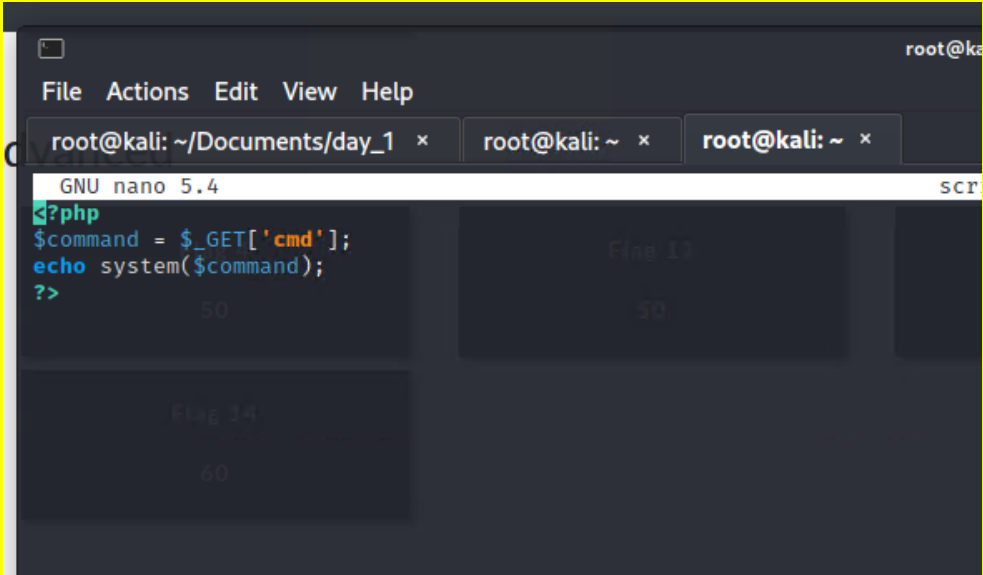
<p>Images</p>	
<p>Affected Hosts</p>	<p>totalrekall.xyz</p>
<p>Remediation</p>	<p>On the client side/ front end side we should be using input validation to stop these attacks and for the backend / server side we can use stored procedures to protect the databases</p>

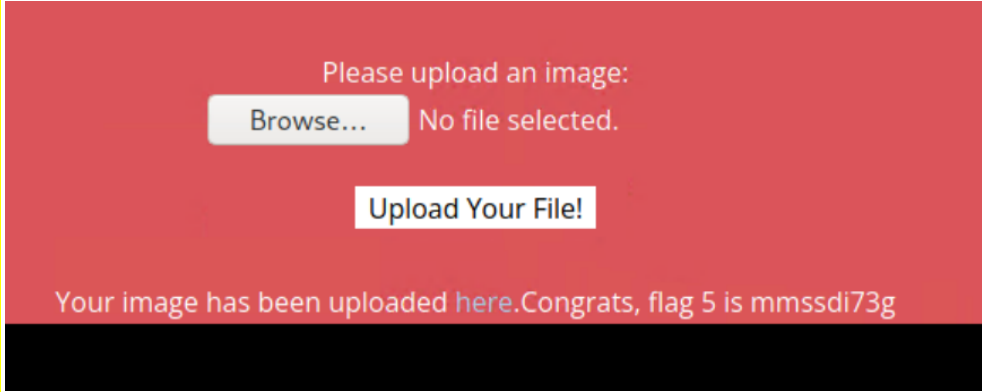
Vulnerability 5	Findings
<p>Title</p>	<p>Sensitive Data Exposure</p>
<p>Type (Web app / Linux OS / Windows OS)</p>	<p>Web Application</p>
<p>Risk Rating</p>	<p>Critical</p>
<p>Description</p>	<p>By altering the URL we were able to uncover sensitive data to totalrekall as an organization. putting '?page=robots.txt' is how we altered the URL to gain this access</p>

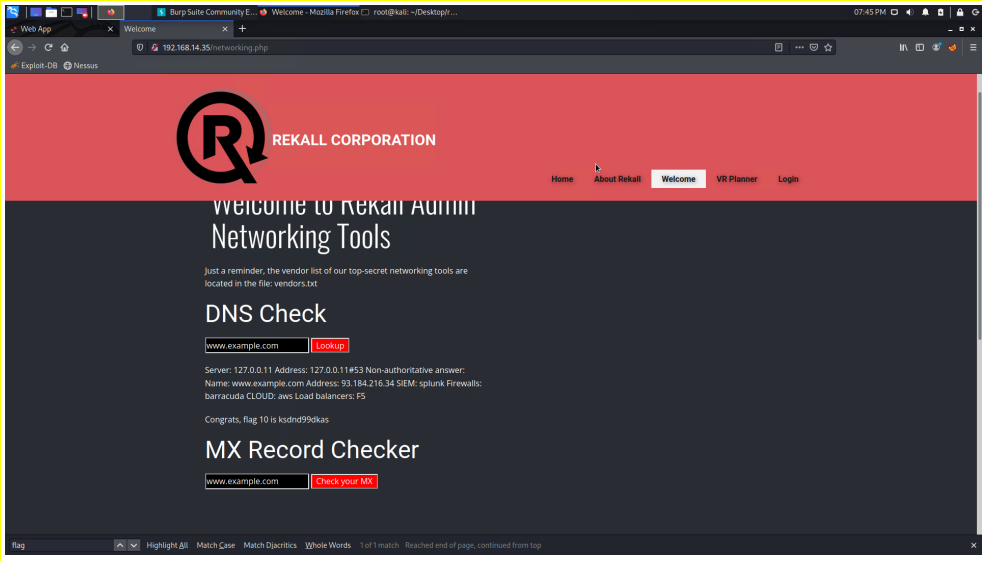
<p>Images</p>	
<p>Affected Hosts</p>	<p>totalrekall.xyz</p>
<p>Remediation</p>	<p>Once more input validation would help us remediate this, as well as server side validation so that only certain file types can be uploaded.</p>

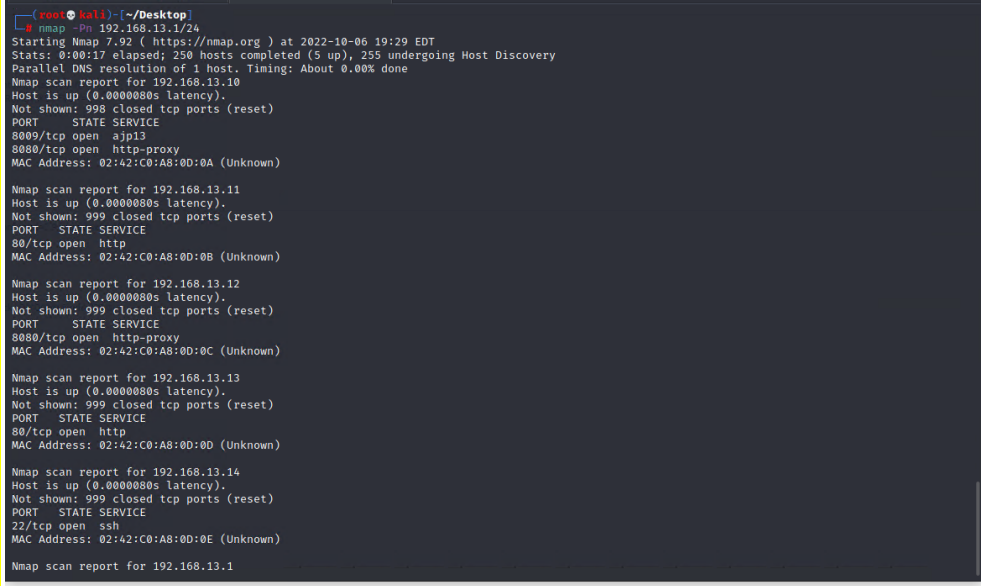
Vulnerability 6	Findings
<p>Title</p>	<p>Brute Force Attack</p>
<p>Type (Web app / Linux OS / Windows OS)</p>	<p>Web Application</p>
<p>Risk Rating</p>	<p>Critical</p>
<p>Description</p>	<p>Through a brute force password attack we were able to log into the Admin account for the web application. With the admin account we have escalated privileges immediately which would damage the website and reputation of company</p>

Images	
Affected Hosts	totalrekall.xyz
Remediation	Using complex username and password combinations would be a good start, as well as adding MFA (multi-factored authentication) and enabling a lockout policy for failed login attempts.

Vulnerability 7	Findings
Title	Local File Injection
Type (Web app / Linux OS / Windows OS)	Web Application
Risk Rating	High
Description	By creating a code injection we were able to upload a malicious payload and camouflage it as a file upload to the site.
Images	

	
Affected Hosts	totalrekall.xyz
Remediation	Input validation as well as server side validation would really help remediate this as well as setting security controls that only certain file types can be uploaded to the site.

Vulnerability 8	Findings
Title	Command Injection
Type (Web app / Linux OS / Windows OS)	Web Application
Risk Rating	Critical
Description	By running a command into an input field we were able to inject a malicious code onto the site and have it run what we wanted.
Images	
Affected Hosts	totalrekall.xyz
Remediation	A running theme on the web application side is input validation, as well as sanitizing the input fields to not allow certain characters to even be allowed to be typed/input.

Vulnerability 9	Findings
Title	Nmap scan of subnet
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	Low
Description	by running a nmap -Pn 192.168.13.1/24 scan of the network we were able to see how many hosts were up and what ports were open to which host.
Images	 <pre> (root@kali) [~/Desktop] # nmap -Pn 192.168.13.1/24 Starting Nmap 7.92 (https://nmap.org) at 2022-10-06 19:29 EDT Stats: 0:00:17 elapsed; 250 hosts completed (5 up), 255 undergoing Host Discovery Parallel DNS resolution of 1 host. Timing: About 0.00% done Nmap scan report for 192.168.13.10 Host is up (0.0000000s latency). Not shown: 998 closed tcp ports (reset) PORT STATE SERVICE 8009/tcp open ajp13 8080/tcp open http-proxy MAC Address: 02:42:C0:A8:0D:0A (Unknown) Nmap scan report for 192.168.13.11 Host is up (0.0000000s latency). Not shown: 999 closed tcp ports (reset) PORT STATE SERVICE 80/tcp open http MAC Address: 02:42:C0:A8:0D:0B (Unknown) Nmap scan report for 192.168.13.12 Host is up (0.0000000s latency). Not shown: 999 closed tcp ports (reset) PORT STATE SERVICE 8080/tcp open http-proxy MAC Address: 02:42:C0:A8:0D:0C (Unknown) Nmap scan report for 192.168.13.13 Host is up (0.0000000s latency). Not shown: 999 closed tcp ports (reset) PORT STATE SERVICE 80/tcp open http MAC Address: 02:42:C0:A8:0D:0D (Unknown) Nmap scan report for 192.168.13.14 Host is up (0.0000000s latency). Not shown: 999 closed tcp ports (reset) PORT STATE SERVICE 22/tcp open ssh MAC Address: 02:42:C0:A8:0D:0E (Unknown) Nmap scan report for 192.168.13.1 </pre>
Affected Hosts	Entire subnet of 192.168.13.1/24
Remediation	A well configured firewall can effectively block or slow down many avenues of NMAP scans.

Vulnerability 10	Findings
Title	OSNIT WHO.IS / Domain Dossier
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	Low
Description	By doing Reconnaissance and using opened sourced information on the totalrekall website we were able to find certain pieces of information that would help us throughout the Pentesting project.

Images	<p>Queried whois.godaddy.com with "totalrekall.xyz"...</p> <p>Domain Name: totalrekall.xyz Registry Domain ID: D273189417-CNIC Registrar WHOIS Server: whois.godaddy.com Registrar URL: https://www.godaddy.com Updated Date: 2022-02-02T19:16:19Z Creation Date: 2022-02-02T19:16:16Z Registrar Registration Expiration Date: 2023-02-02T23:59:59Z Registrar: GoDaddy.com, LLC Registrar IANA ID: 146 Registrar Abuse Contact Email: abuse@godaddy.com Registrar Abuse Contact Phone: +1.4806242505 Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited Registry Registrant ID: CR534509109 Registrant Name: sshUser alice Registrant Organization: Registrant Street: h8s692hskasd Flag1 Registrant City: Atlanta Registrant State/Province: Georgia</p>
Affected Hosts	totalrekall.xyz / linux OS
Remediation	Scrubbing the information provided to give minimized data to the public will make it harder for attackers to find a way in through reconnaissance

Vulnerability 11	Findings
Title	RCE exploit into host of 192.168.13.12
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	Critical
Description	was able to use an RCE exploit found on metasploit to patch into the root of 192.168.13.12 and browse through files and make changes if needed.

<p>Images</p>	 <p>The top screenshot shows a terminal session where a user has gained a shell on a Linux system (192.168.13.12). The user is listing files in the root directory, and the output shows a list of directories and files, including 'bin', 'cve-2017-538', 'dev', 'etc', 'home', 'lib', 'media', 'mnt', 'opt', 'proc', 'root', 'run', 'sbin', 'srv', 'sys', 'tmp', 'usr', 'var', and '~'. The user then runs 'ls' and 'cat flaginThisfile.7z', which outputs '7z++'fV%*!***flag 10 is wjasdufsdkg'. The bottom screenshot shows the Metasploit framework interface with the 'options' and 'payload' sections expanded. The 'options' section shows settings for a reverse_tcp payload, including 'Proxies', 'RHOSTS', 'RPORT', 'SSL', 'TARGETURI', and 'VHOST'. The 'payload' section shows settings for a reverse_tcp payload, including 'LHOST', 'LPORT', and 'Exploit target'.</p>
<p>Affected Hosts</p>	<p>Linux OS / 192.168.13.12</p>
<p>Remediation</p>	<p>running regular vulnerability scans or even credentialed scans would help make sure that all software is up to date and patched correctly to help protect exploits like this from working.</p>

Vulnerability 12	Findings
<p>Title</p>	<p>Drupal Exploit into 192.168.13.13</p>
<p>Type (Web app / Linux OS / Windows OS)</p>	<p>Linux OS</p>

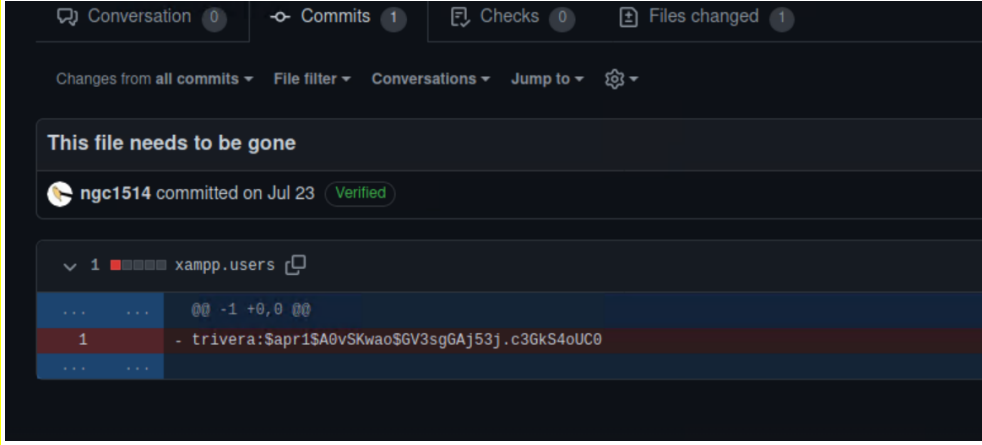
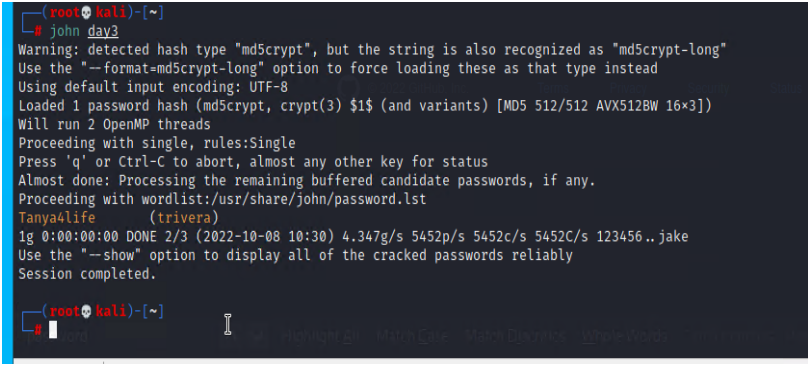
Risk Rating	Critical
Description	By searching which host was using Drupal we were able to use metasploit to find an exploit that attacks the Drupal part of the host and patch into the 192.168.13.13 host
Images	<p>Nmap scan report for 192.168.13.13 Host is up (0.000018s latency). Not shown: 999 closed tcp ports (reset) PORT STATE SERVICE VERSION 80/tcp open http Apache httpd 2.4.25 _http-server-header: Apache/2.4.25 (Debian) _http-robots.txt: 22 disallowed entries (15 shown) _/core/ /profiles/ /README.txt /web.config /admin/ _/comment/reply/ /filter/tips /node/add/ /search/ /user/register/ _/user/password/ /user/login/ /user/logout/ /index.php/admin/ _/index.php/comment/reply/ _http-generator: Drupal 8 (https://www.drupal.org) _http-title: Home Drupal CVE-2019-6340 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 Service Info: Host: 192.168.13.13</p> <p>TRACEROUTE HOP RTT ADDRESS 1 0.02 ms 192.168.13.13</p>
Affected Hosts	Linux OS / 192.168.13.13
Remediation	Run vulnerability scans to make sure software is up to date and patched as well as closing any unnecessary ports and services to harden the host.

Vulnerability 13

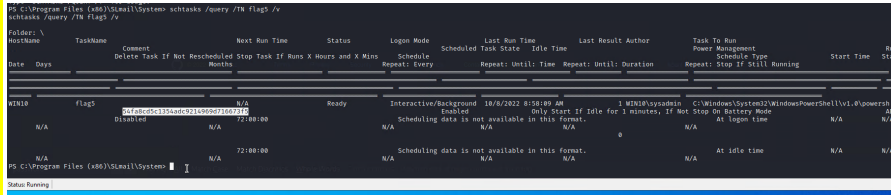
Findings

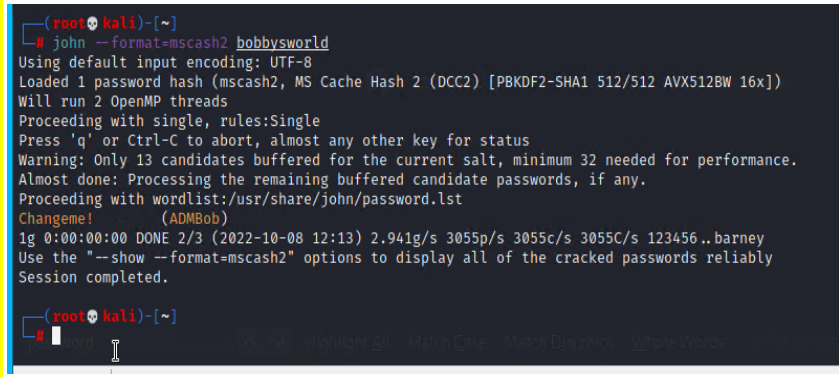
Title	Nmap -Pn scan on 172.22.117.0/24
Type (Web app / Linux OS / Windows OS)	Window OS
Risk Rating	Low
Description	Ran a Nmap scan on the entire subnet of 172.22.117.0/24 to see the hosts and open ports along side the hosts to try and gain access/exploit the open ports
Images	 <pre> (root@kali)-[~] # nmap -Pn 172.22.117.0/24 Starting Nmap 7.92 (https://nmap.org) at 2022-10-08 10:32 EDT Nmap scan report for WinDC01 (172.22.117.10) Host is up (0.00077s latency). Not shown: 989 closed tcp ports (reset) PORT STATE SERVICE 53/tcp open domain 88/tcp open kerberos-sec 135/tcp open msrpc 139/tcp open netbios-ssn 389/tcp open ldap 445/tcp open microsoft-ds 464/tcp open kpasswd5 593/tcp open http-rpc-epmap 636/tcp open ldapssl 3268/tcp open globalcatLDAP 3269/tcp open globalcatLDAPssl MAC Address: 00:15:5D:02:04:13 (Microsoft) Nmap scan report for Windows10 (172.22.117.20) Host is up (0.0011s latency). </pre>
Affected Hosts	Windows OS / 172.22.117.0/24 subnet
Remediation	Close any unnecessary open ports and services as well as configured a hardened firewall.

Vulnerability 14	Findings
Title	OSNIT on Github / Cracking User password
Type (Web app / Linux OS / Windows OS)	LinuxOS
Risk Rating	Medium
Description	By using OSNIT and looking onto TotalRekalls Github Repository we were able to find credentials of an employee at totalrekall, then by using a password cracking tool called John the Ripper we were able to crack that password and gain access to the system.


<p>Images</p>	 
<p>Affected Hosts</p>	<p>Windows OS / 172.22.117.0/24 subnet</p>
<p>Remediation</p>	<p>Would make sure all open sourced information is researched and scrubbed clean, would set up a threat hunting exercise by the IT team every month / quarter to make sure nothing on the open web can harm the company or its reputation</p>

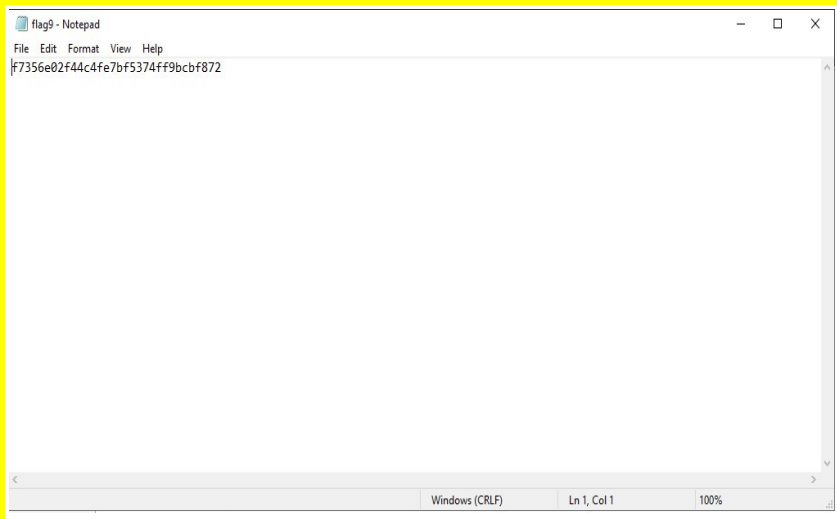
Vulnerability 15	Findings
<p>Title</p>	<p>SLmail exploit through metasploit</p>
<p>Type (Web app / Linux OS / Windows OS)</p>	<p>Windows OS</p>
<p>Risk Rating</p>	<p>Critical</p>
<p>Description</p>	<p>By finding an exploit using metasploit we were able to gain root access to one of the windows hosts and browse the entire file library and search through scheduled tasks, while in there we could have made our own tasks or made a backdoor account for persistence in the system.</p>

Images	
Affected Hosts	windows OS / 172.22.117.10
Remediation	Running regular vulnerability scans on every host machine or device in the network to make sure all software and applications are up to date with the latest security patches.

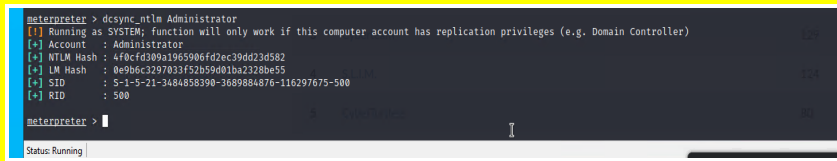
Vulnerability 16	Findings
Title	Cracking Admins Password
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	Critical
Description	By gaining access to different hosts and using lateral movement around the windows systems, we were able to find credentials of a admin level user which would give us immediate privilege escalation once the password is cracked.
Images	
Affected Hosts	Windows OS / 172.22.117.10
Remediation	By using salt (random bits added to the hash) and using complex passwords on top of that would make it even tougher for a password cracker to crack the credentials.

Vulnerability 17	Findings
Title	

Type (Web app / Linux OS / Windows OS)	User enumeration onto the WindDC machine
Risk Rating	Critical
Description	By using the cracked password of the Admin Bob we were able to gain access to the Domain Controller machine on the windows network. This gave us SYSTEM privileges which allows us to do almost anything to the entire network
Images	
Affected Hosts	Windows OS / 172.22.117.0/24 Network
Remediation	For the Domain Controller machine use MFA with TOTP as well as make sure that any one with access to this machine has complex salted passwords so attackers can not easily crack them to gain access to the system.

Vulnerability 18	Findings
Title	Enumerating the WinDC machine
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	Critical
Description	While exploring the WinDC machine we were able to browse through any file we wanted since having SYSTEM level privileges, this is how we were able to find more credentials to the network.
Images	
Affected Hosts	windows OS / 172.22.117.0/24 Network
Remediation	Once into the WinDC machine there cant be much done so the remediation has to come before gaining access to the WinDC system by hardening the

	authentication process as well as making sure any one with credentials to access this machine is following proper password protocols.
--	---

Vulnerability 19	Findings
Title	Compromising the ADMIN of WindDC machine by Credential Dumping
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	Critical
Description	While in the WinDC machine we were able to run a dsync_ntlm command to dump the credentials of the Admin of the WinDC machine, which is the admin of the entire system/network with these credentials we have total control over the entire windows server network.
Images	 <pre> meterpreter > dsync_ntlm Administrator [*] Running as SYSTEM; function will only work if this computer account has replication privileges (e.g. Domain Controller) [*] Account : Administrator [*] NTLM Hash : 4f0cfd309a1965906fd2ec39d423d582 [*] LM Hash : 0e9b6c3297033f52b59d01ba2328be55 [*] SID : S-1-5-21-3484858390-3689884876-116297675-500 [*] RID : 500 meterpreter > </pre>
Affected Hosts	Windows os / 172.22.117.0/24 network
Remediation	Just like any other password, especially the admin to the DC machine, we must make sure it is very complex and salted to make it as hard as possible for attackers to crack the password if they do gain access to the DC machine.

Add any additional vulnerabilities below.