Summary Vulnerability Overview

Vulnerability	Severity
XSS reflected	High
XSS Stored	High
Sensitive data exposure in HTTP response headers	Critical
Local file inclusion	Critical
SQL injection	Critical
Sensitive data exposure in th HTML source code	Critical
Command injection	High
Brute force attack	Medium
PHP injection	High
Session management	Critical
Directory traversal	High
Open source exposed data	High
Apache Tomcat Remote Code Execution Vulnerability (CVE-2017-12617)	Critical
Shellshock	Critical
Struts - CVE-2017-5638	Critical
Drupal - CVE-2019-6340	Critical
FTP Anonymous READ	High
SL Mail Exploit	Critical
Credential Data Exposure	Critical
Weak user account passwords	High
Invalid Domain Certificates	Medium
CVE-2019-14287	Critical

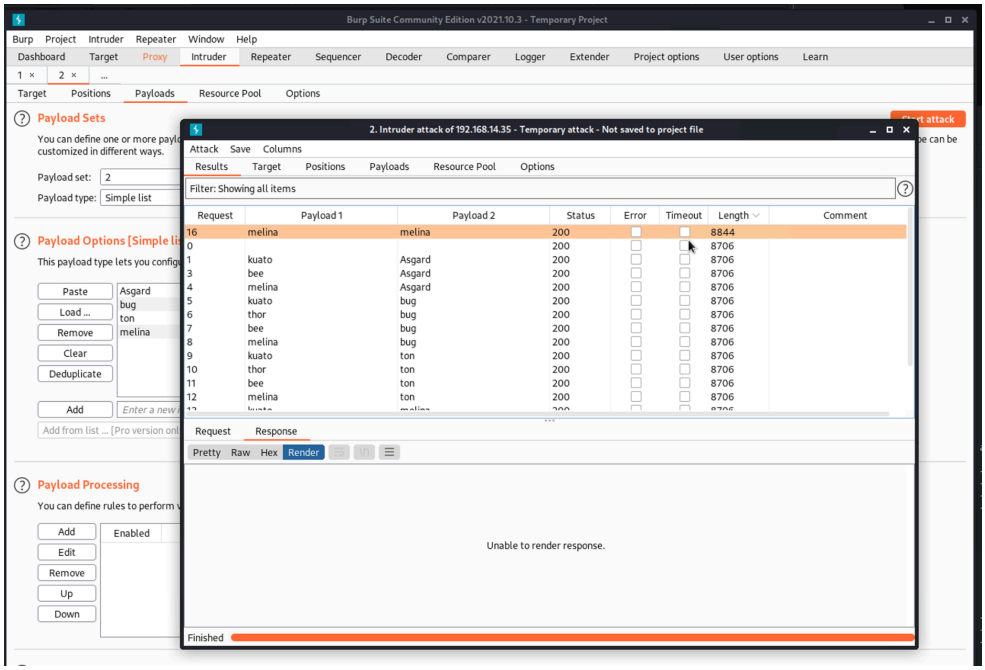
The following summary tables represent an overview of the assessment findings for this penetration test:

Scan Type	Total
Hosts	192.168.13.11, 192.168.13.12, 192.168.13.13, 192.168.13.14, 172.22.117.10, 172.22.117.20
Ports	21,25,79,80,106,110,225,6001,5901

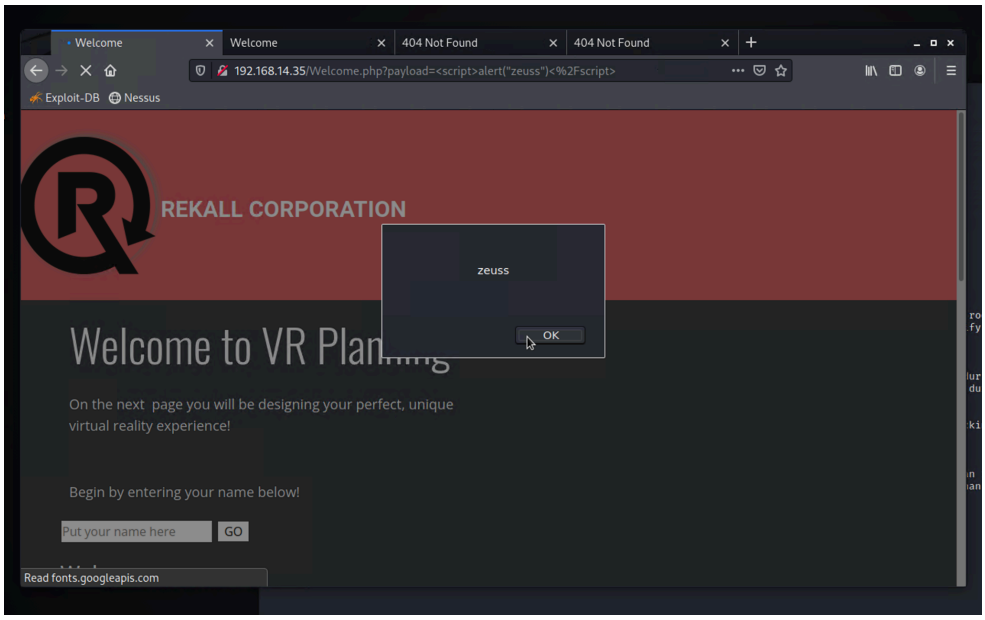
Exploitation Risk	Total
Critical	12
High	8
Medium	2

Low	0

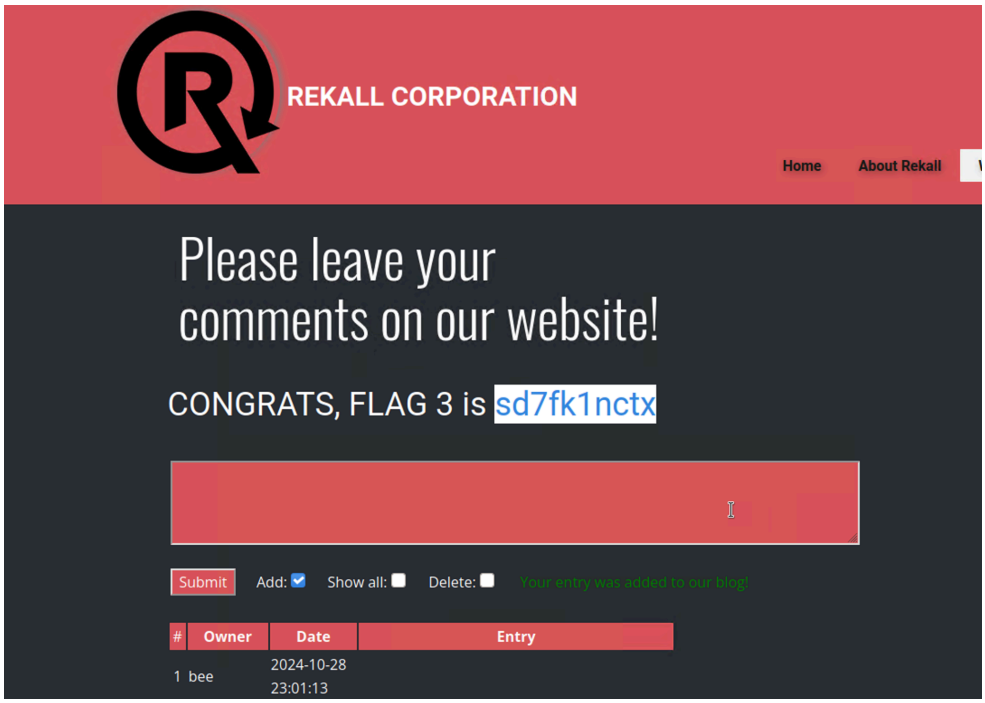
Vulnerability Findings

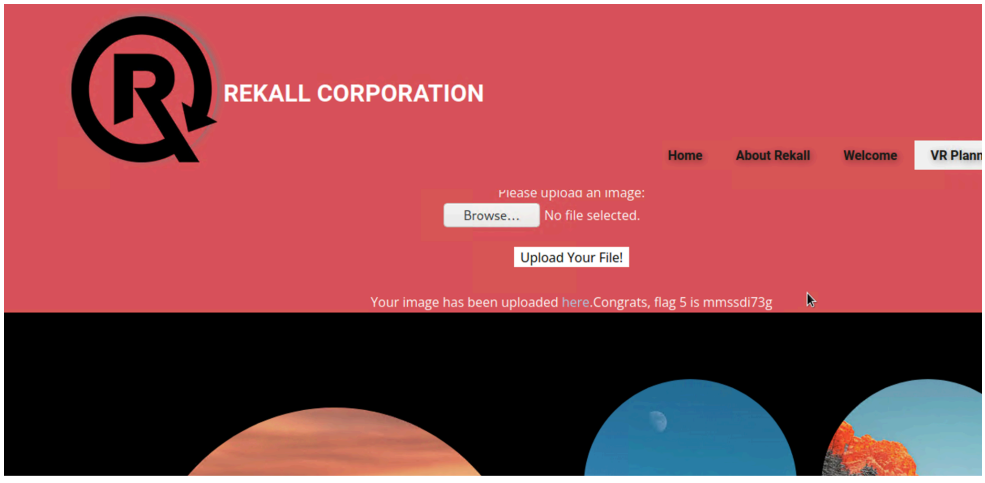
Vulnerability 1	Findings
Title	Brute force attack
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Medium
Description	Using brute force attacks to gain access to a user account
Images	
Affected Hosts	totalrekall.xyz
Remediation	Implement account lockout thresholds Require strong user passwords Implement multi factor authentication

Vulnerability 2	Findings
Title	XSS reflected

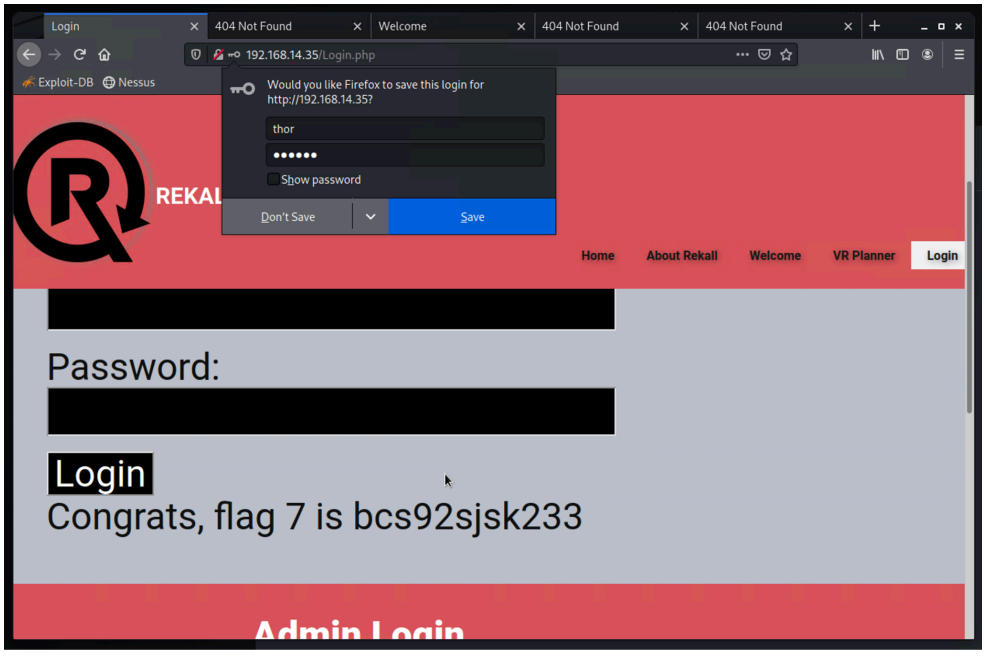
Type (Web app / Linux OS / WIndows OS)	Web Application
Risk Rating	High
Description	Injecting the webapp with user-input payload
Images	
Affected Hosts	totalrekall.xyz
Remediation	Implement better input validation to restrict any kind of scripting tags or entries

Vulnerability 3	Findings
Title	XSS Stored
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	High
Description	Having a user-iput script scored on the webserver

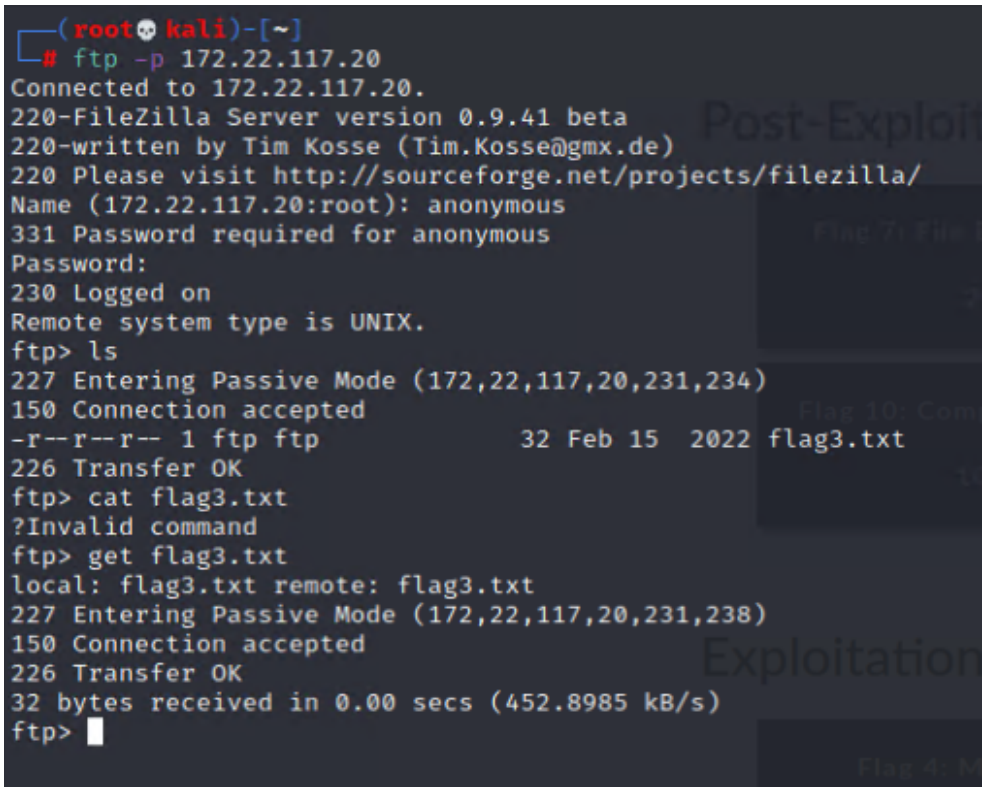
Images	
Affected Hosts	totalrekall.xyz
Remediation	Implement proper output encoding to prevent user-inserted content from being interpreted as HTML or Javascript code.

Vulnerability 4	Findings
Title	Local File inclusion
Type (Web app / Linux OS / WIndows OS)	webapp
Risk Rating	Critical
Description	uploading of php scripts to the backend of webapps to be able to run payloads
Images	

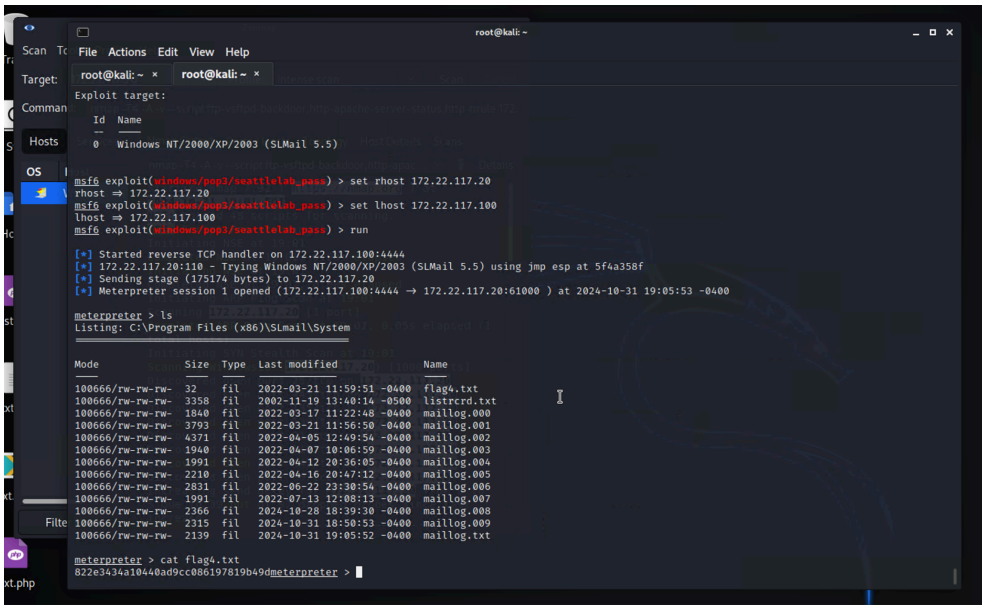
Affected Hosts	totalrekall.xyz
Remediation	File upload validation to ensure that only files with the extension of .jpg or image related extensions are allowed to be uploaded to the server.

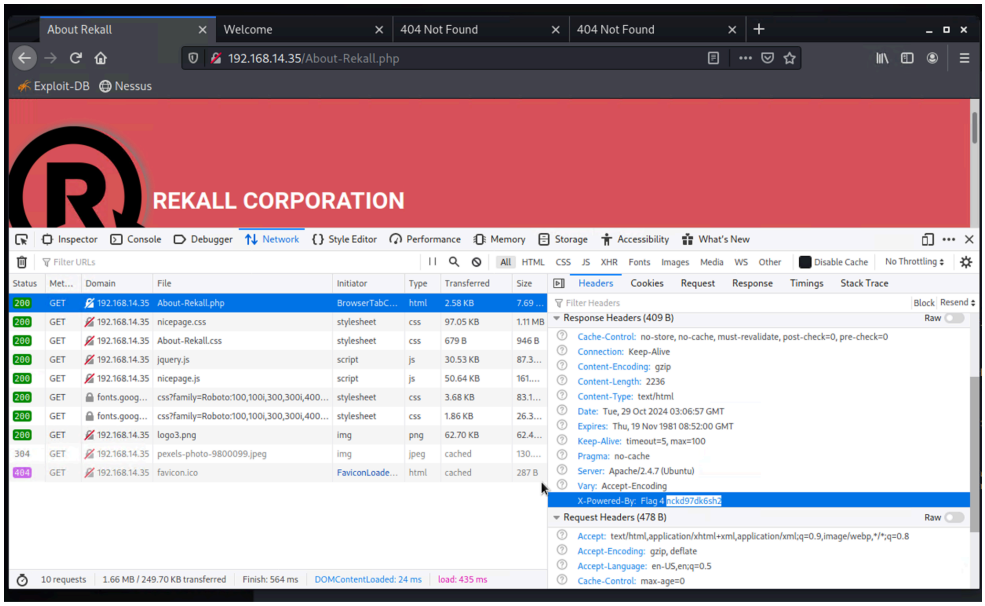
Vulnerability 5	**Findings**
Title	SQL injection
Type (Web app / Linux OS / WIndows OS)	web app
Risk Rating	critical
Description	using simple SQL true statements to make a webapp expose sensitive data
Images	
Affected Hosts	totalrekall.xyz
Remediation	Sanitizing and remediate codes before passing to the database.

Vulnerability 6	**Findings**
Title	FTP Anonymous READ
Type (Web app / Linux OS / WIndows OS)	Windows Os
Risk Rating	High
Description	Using the FTP vulnerability to access sensitive files

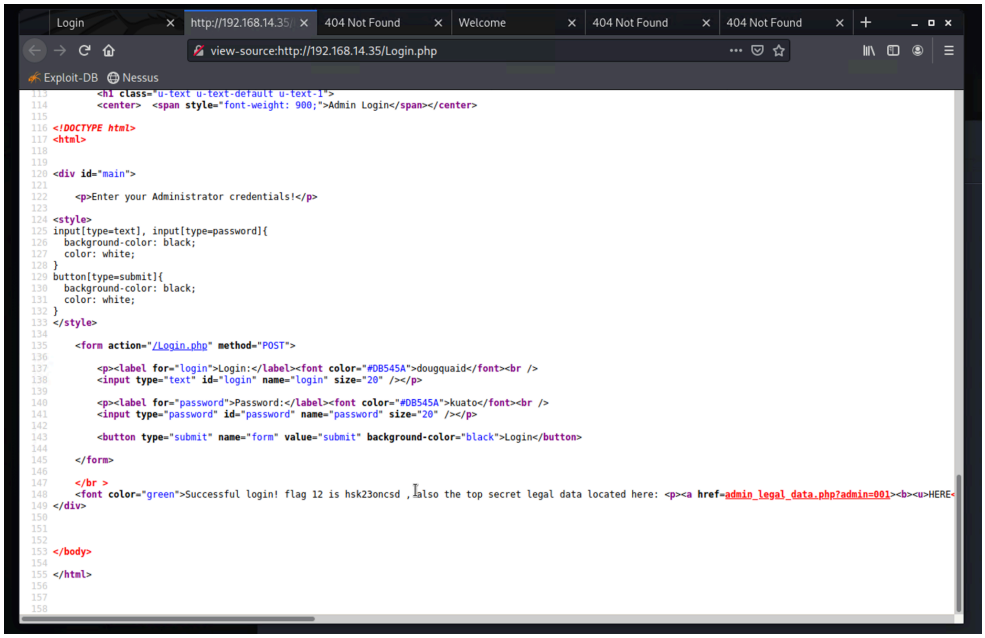
Images	
Affected Hosts	172.22.117.20
Remediation	Disable FTP for the host

Vulnerability 7	Findings
Title	SL Mail Exploit
Type (Web app / Linux OS / WIndows OS)	Windows Os
Risk Rating	Critical
Description	Using Pop3 exploits to open a session to the host

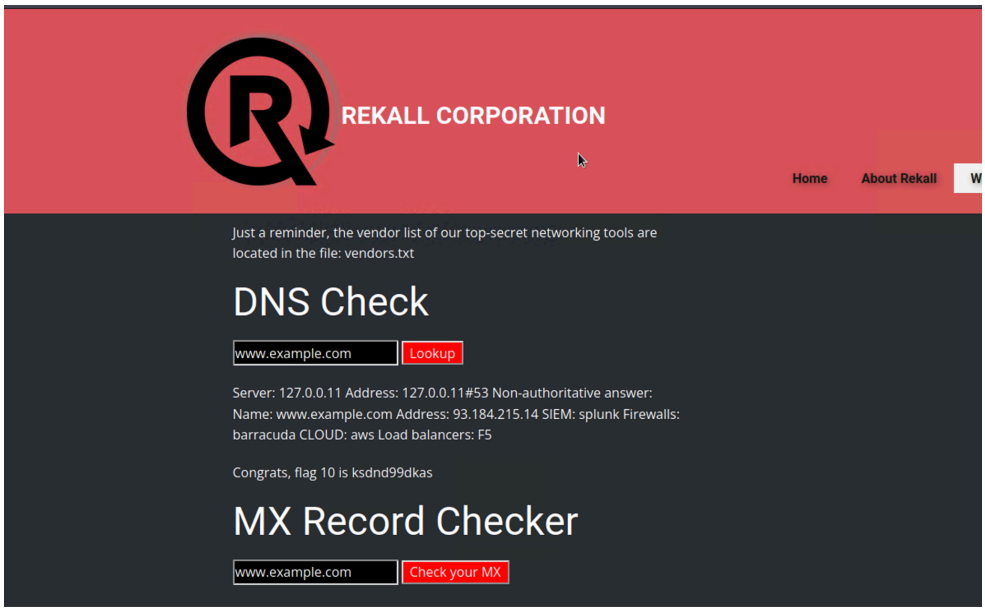
Images	
Affected Hosts	172.22.117.20
Remediation	Disable unnecessary SLMail services and update to a more stable and latest SLMail version for the server.

Vulnerability 8	Findings
Title	Sensitive Data exposure in HTTP response Headers
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Critical
Description	The HTTP response header contained the flag 4 for this exploit.
Images	

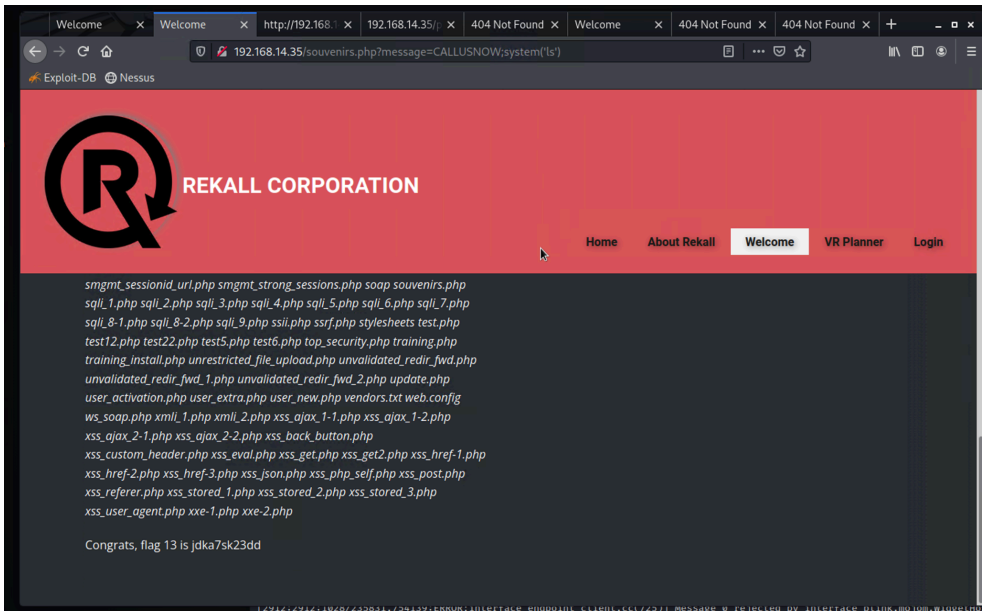
Affected Hosts	totalrekall.xyz
Remediation	mmediately edit the html codes to remove all sensitive data. Regularly inspect all html codes to verify no sensitive data is exposed

Vulnerability 9	**Findings**
Title	Sensitive Data exposure in HTML source code
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Critical
Description	The HTML source code of the login page of totalrekall contained the admin credentials for the web app
Images	
Affected Hosts	totalrekall.xyz
Remediation	Immediately edit the html codes to remove all sensitive data. Regularly inspect all html codes to verify no sensitive data is exposed

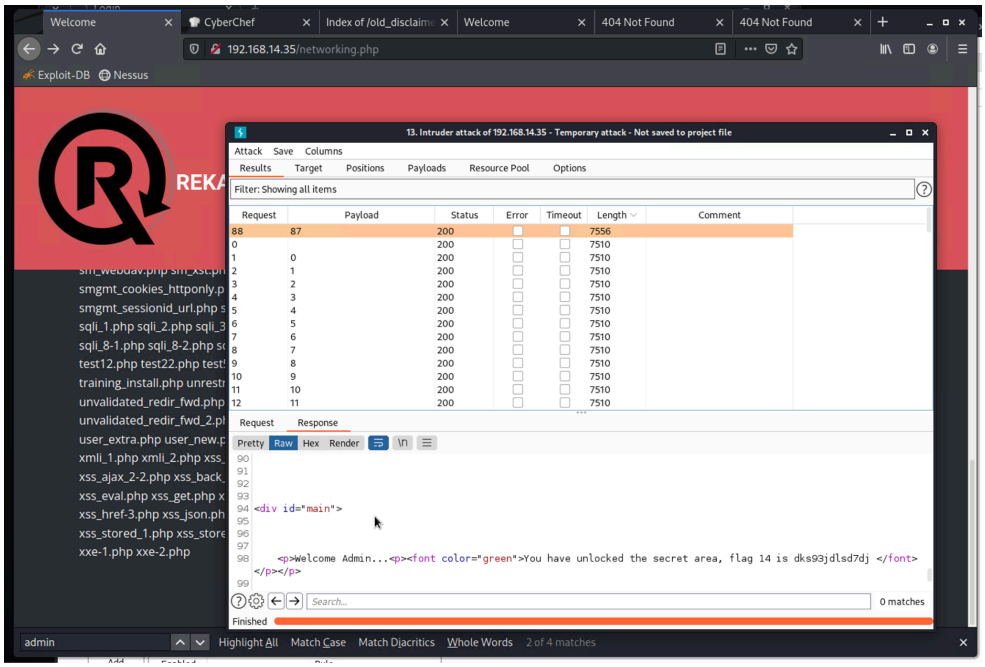
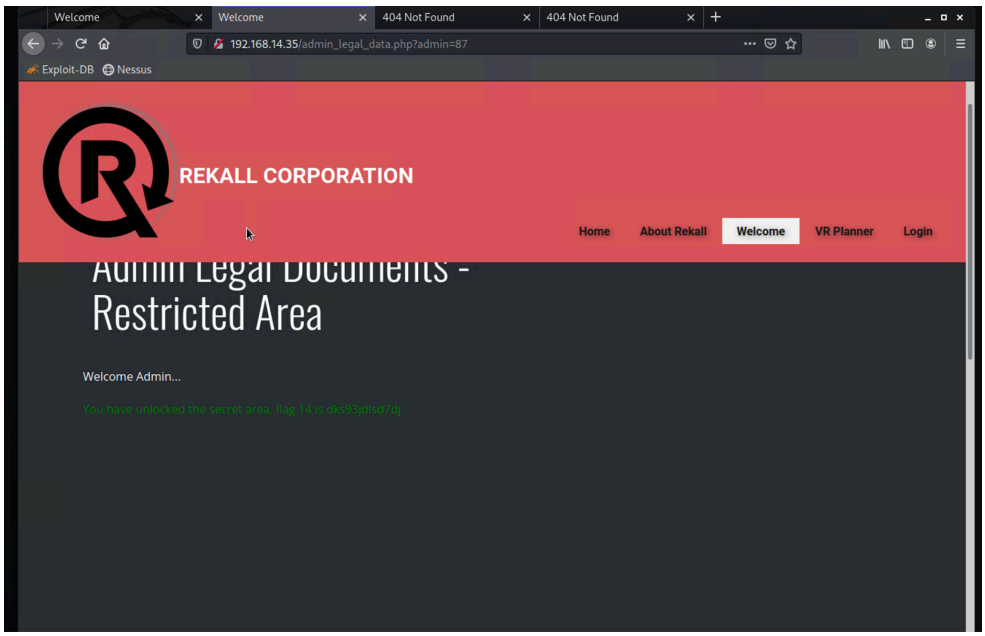
Vulnerability 10	**Findings**
Title	Command Injection
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	High

Description	The web app was vulnerable to command injection attacks. Was able to use this attack to access sensitive files on the backend of the web server.
Images	
Affected Hosts	totalrekall.xyz
Remediation	Validate and sanitize user input Conduct regular security testing

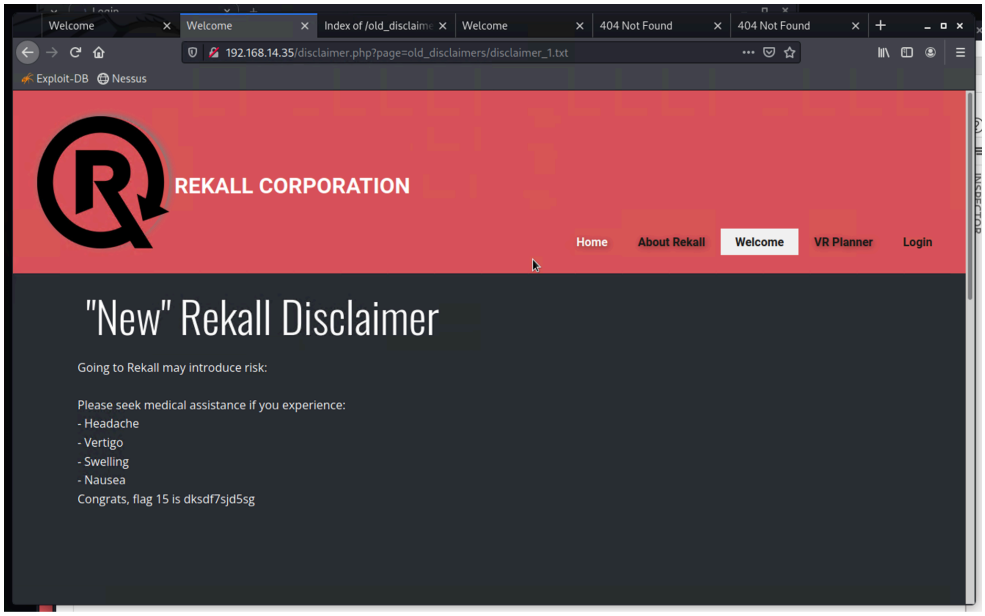
Vulnerability 11	Findings
Title	PHP Injection
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	High
Description	The souvenirs page of the web app was vulnerable to php injection attack. I was able to use this exploit to access files on the backend server

Images	
Affected Hosts	totalrekall.xyz
Remediation	Implement input validations Enforce better user input sanitization and handling

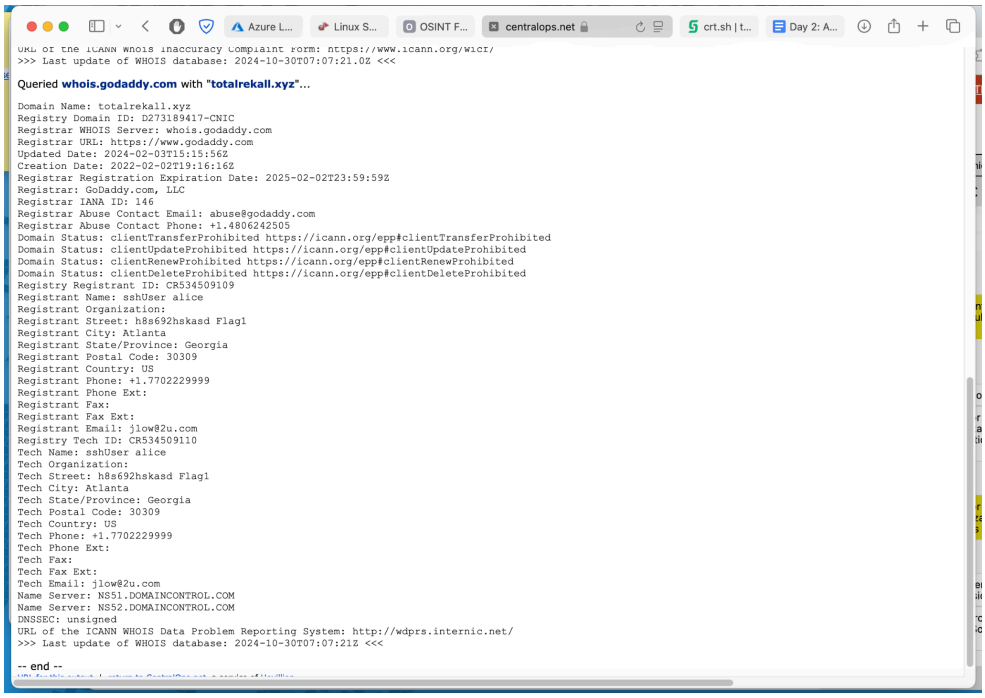
Vulnerability 12	Findings
Title	Session Management
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Critical
Description	Was able to use burp suite to brute force my session ID from 1-100. I was able to hijack an admin session when my ID got to 87.

Images	
Images	
Affected Hosts	totalrekall.xyz
Remediation	Avoid using predictable session IDs Implement manual session expiration Enforce and implement automatic session expiration and timeouts

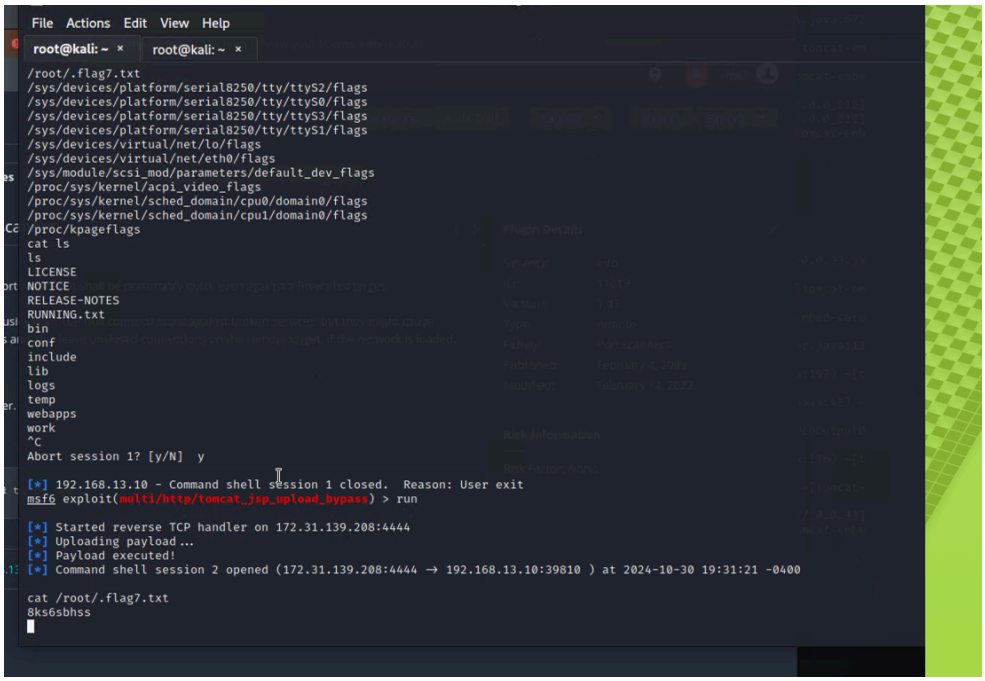
Vulnerability 13	Findings
Title	Directory Traversal
Type (Web app / Linux OS / WIndows OS)	Web App

Risk Rating	High
Description	I used directory traversal technique to view the older version of the disclaimer page in the server.
Images	
Affected Hosts	totalrekall.xyz
Remediation	Enforce input validation Limit application access to web servers files. Regularly test the server for vulnerabilities

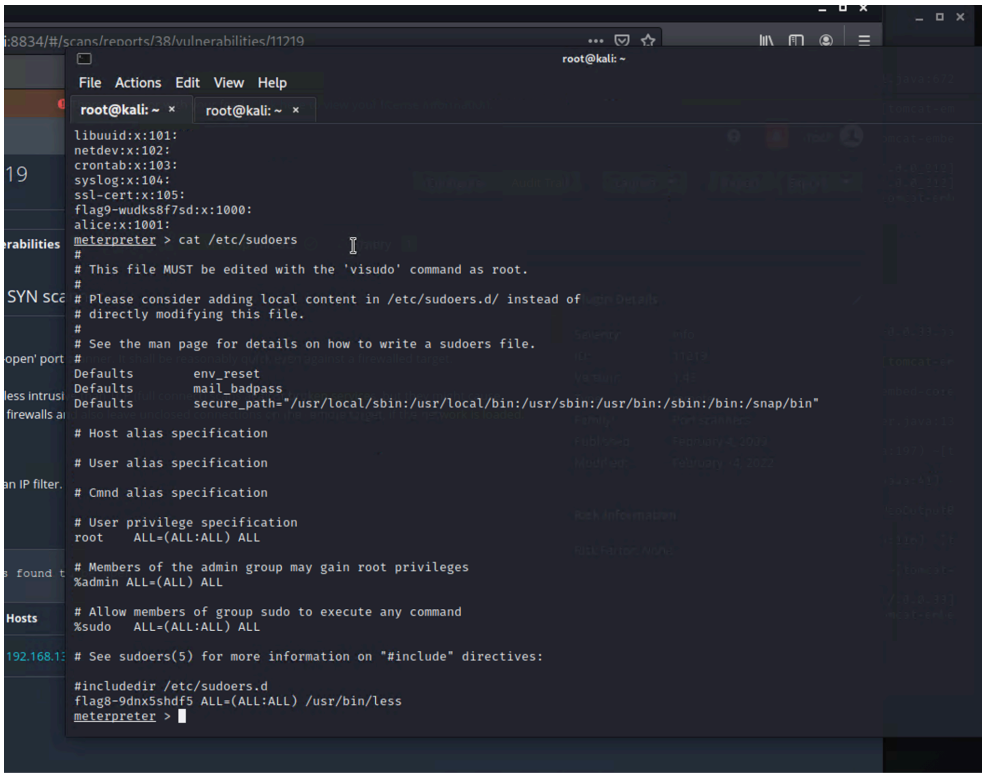
Vulnerability 14	Findings
Title	Open Source exposed data
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	High
Description	I did WHOIS lookup on totalrekall.xyz and found some sensitive data on their domain registration

Images	
Affected Hosts	totalrekall.xyz
Remediation	Update domain registration information to remove all sensitive data from the WHOIS registration. Update the user account password on the server .

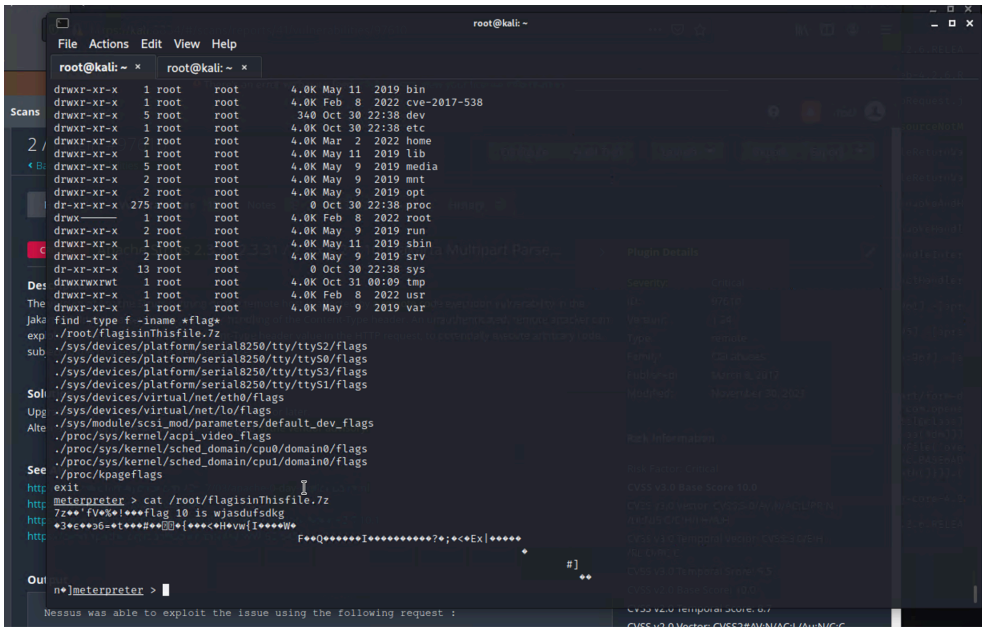
Vulnerability 15	Findings
Title	Apache Tomcat Remote Code Execution Vulnerability (CVE-2017-12617)
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	I was able to exploit the vulnerability of the host by using metasploit to create a session. the exploit on metasploit was (multi/http/tomcat_jsp_upload_bypass)

Images	
Affected Hosts	192.168.13.10
Remediation	Updating Tomcat to the latest version should fix this vulnerability

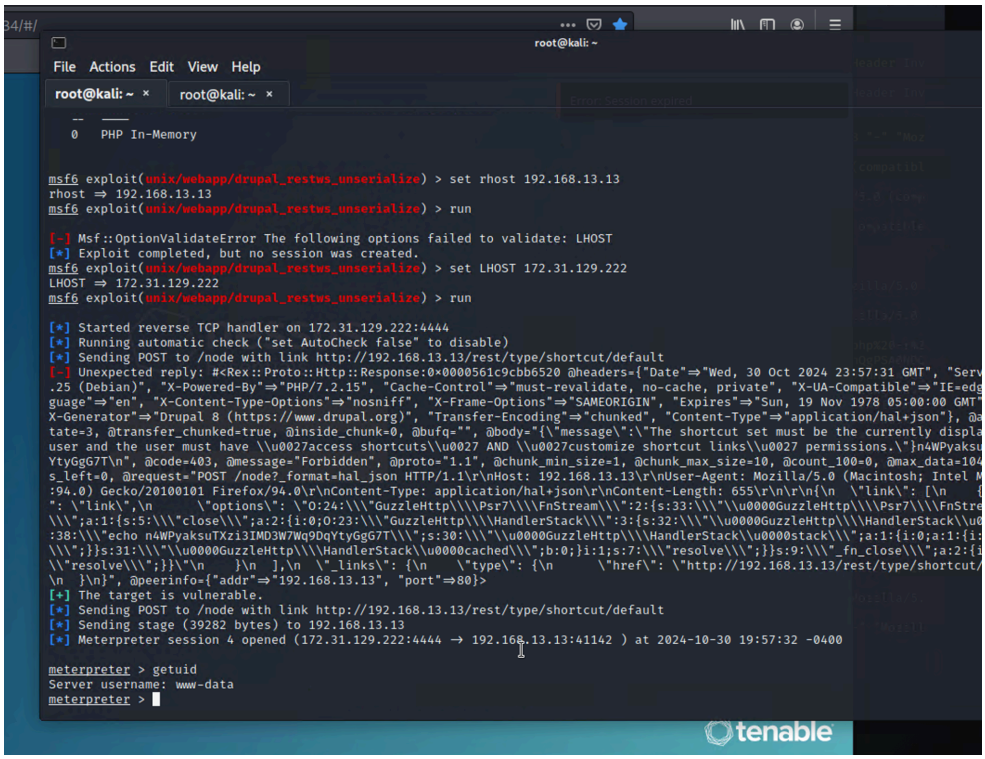
Vulnerability 15	Findings
Title	ShellShock
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	I looked for exploits that contained shellshock on metasploit and used it to create a meterpreter session to the host. The exploit that worked was `exploit/multi/http/apache_mod_cgi_bash_env_exec`

Images	
Affected Hosts	192.168.13.11
Remediation	Apply the latest security patches and updates provided by the Operating system vendor Update bash to the latest version on the server Limit access to bash shell in cases where it is not needed

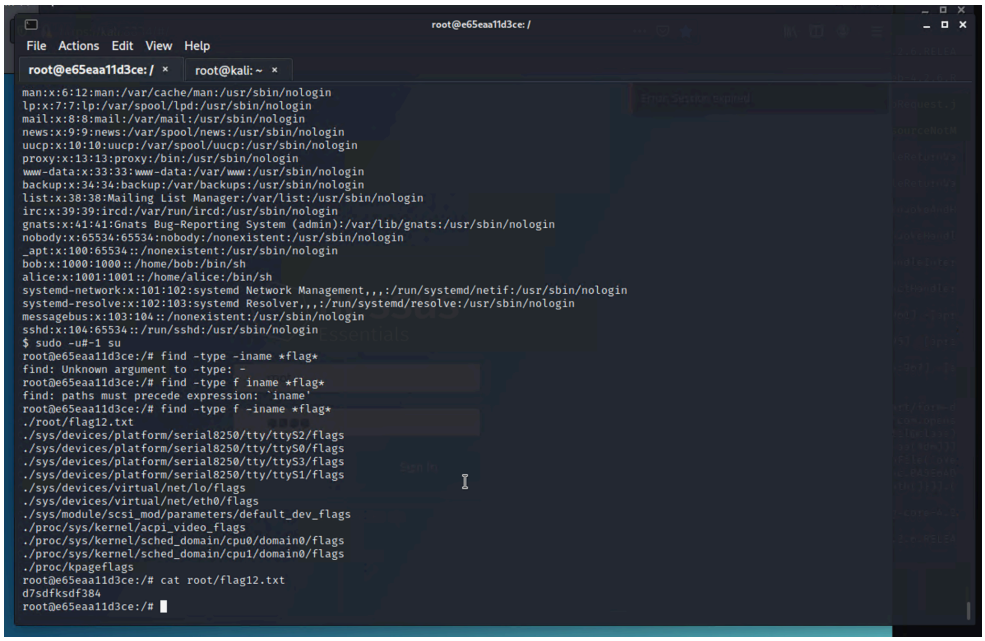
Vulnerability 17	Findings
Title	Struts - CVE-2017-5638
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	After discovering that the host was vulnerable to struts attacks through nessus, I searched for exploits that used struts on metasploit and used it to open a meterpreter session. The exploit used was multi/http/struts2_content_type_ognl

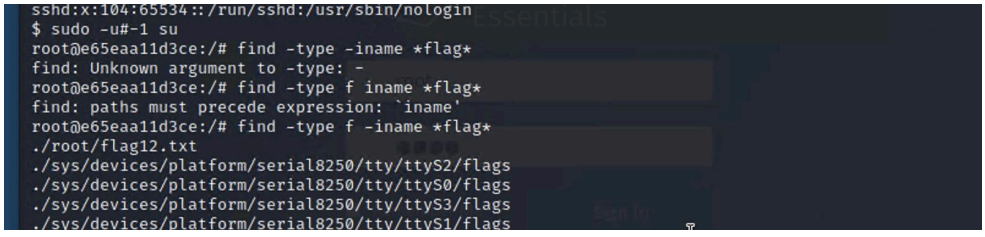
Images	
Affected Hosts	192.168.13.12
Remediation	Use a web application firewall and set it to only approve valid content types or ban OGNL expressions. Upgrade struts to a newer version

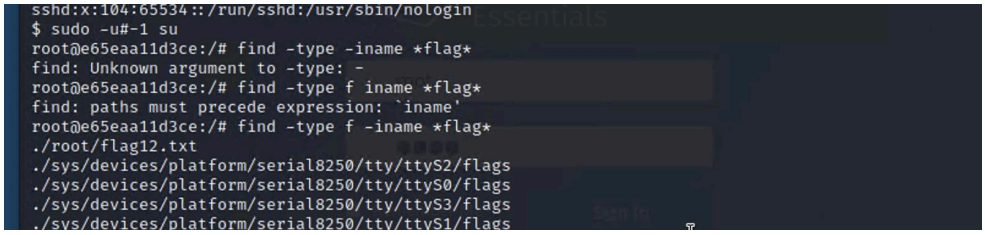
Vulnerability 18	Findings
Title	Drupal - CVE-2019-6340
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	The host has drupal running so I searched for drupal exploits on metasploit and used it to open a session.

Images	
Affected Hosts	192.168.13.13
Remediation	Update and upgrade Drupal to a newer released version

Vulnerability 19	Findings
Title	Weak user account password
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	When viewing the WHOIS lookup data, I discovered that the sshuser was alice. So I used password guessing techniques to connect to the host.

Images	
Affected Hosts	192.168.13.14
Remediation	Change user account passwords on the server and enforce strong password requirements. Use multi-factor authentication to ensure extra security.

Vulnerability 20	Findings
Title	CVE-2019-14287
Type (Web app / Linux OS / WIndows OS)	Linux
Risk Rating	Critical
Description	I used this vulnerability to run a sudo command as a non sudo user to escalate my privileges to root privileges.
Images	
Affected Hosts	192.168.13.14
Remediation	Immediately change sudo configurations to exclude root user id (#0) from being used to run commands. (`someuser ALL=(ALL, !#0) /usr/bin/somecommand`)

Vulnerability 21	Findings
Title	Invalid Domain certificates
Type (Web app / Linux OS / WIndows OS)	web app
Risk Rating	Medium
Description	I did a certificate search on crt.sh for totalrekall.xyz and found no valid certificates.
Images	
Affected Hosts	totalrekall.xyz
Remediation	Implement valid certificates to the domain to ensure secure communication between client and server.