Cybersecurity

Penetration Test Report

Rekall Corporation

Penetration Test Report

Spalding Tech

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	Spalding Tech
Contact Name	Tony Gash
Contact Title	Penetration Tester

Document History

Version	Date	Author(s)	Comments
001	05/24/2023	Tony Gash	

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.

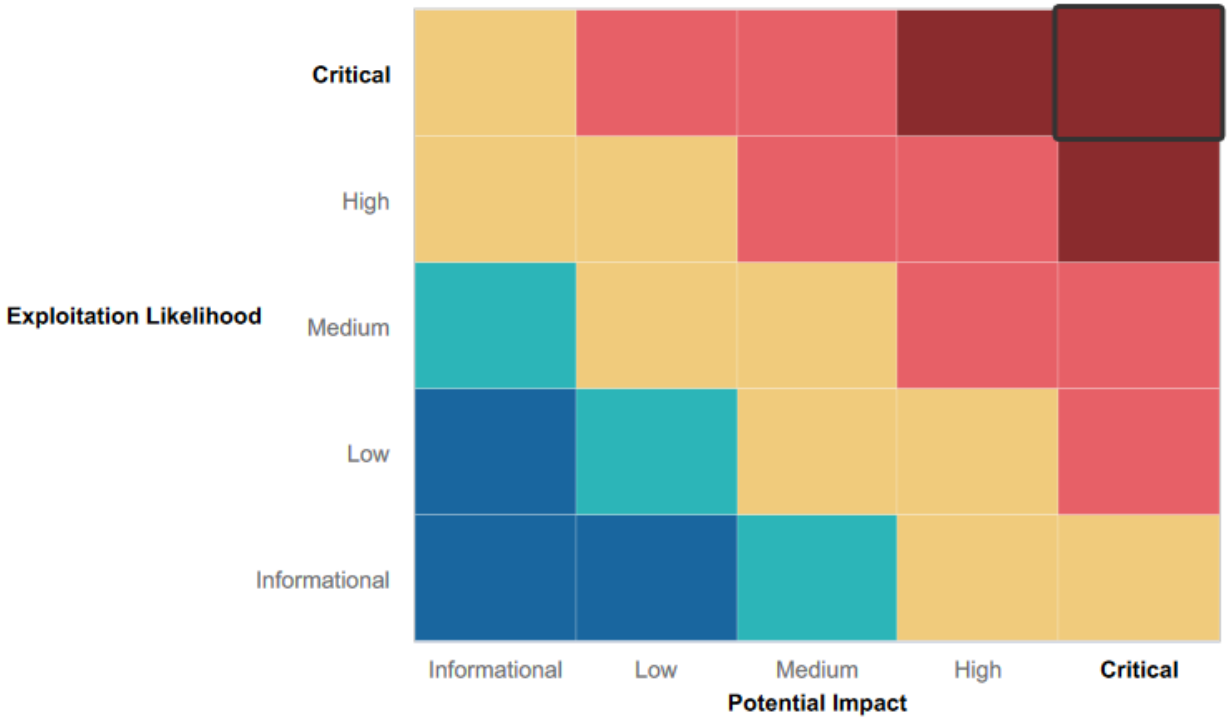
Executive Summary of Findings

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.

- Web App utilized various forms of input validation in an attempt to dissuade threat actors
- Web App filtered against some command injection

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.

- Weak Passwords
- Local File Inclusion on Web App
- Reflected XSS on Web App
- Stored XSS on Web App
- Sensitive Data Exposure
- Multiple Vulnerable Services
- Privilege Escalation Vulnerabilities
- Data Exfiltration through FTP
- Vulnerable POP3 Mail Server
- Excessive Open Ports
- Poor User Input Sanitization on Web App

Executive Summary

Spalding Tech performed a penetration test for Rekall to identify any potential exposure to threat actors. The vulnerabilities outlined below were discovered by simulating a malicious entity engaging in a targeted attack against Rekall. It was the goal of Spalding Tech to determine if a remote attacker could breach Rekall's defenses, and what the impact of such a breach might have on the company's private data.

The majority of the engagement focused on the identification and exploitation of various weaknesses discovered across several different hosts. The attacks were conducted from the perspective of a general user with no prior knowledge of the network or machines. This assessment was performed in accordance with the techniques and recommendations offered by the MITRE ATT&CK Framework.

During the test, Spalding Tech was able to identify numerous vulnerabilities that might expose Rekall to an attack. The current state of Rekall's security is in critical condition, with a wide range of concerning vulnerabilities found within the web application, Linux hosts, and Windows servers.

However with effective planning and swift action, it will be possible to reform the company's security posture and harden defenses against future threats. Spalding Tech has outlined potential remediation solutions for each vulnerability identified within the findings listed below. We hope these suggestions help to guide a secure future.

Summary Vulnerability Overview

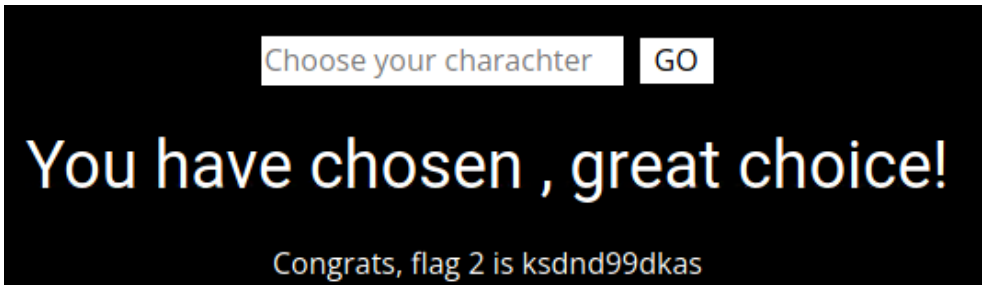
Vulnerability	Severity
Reflected XSS on `Welcome.php`	Critical
Reflected XSS on `Memory-Planner.php`	Critical
Stored XSS	Critical
Local File Inclusion	Critical
Apache Tomcat RCE (CVE-2017-12617)	Critical
ShellShock	Critical
Apache Struts RCE (CVE-2017-5638)	Critical
Drupal Core RCE (CVE-2019-6340)	Critical
Exposed Password Hash	Critical
Seattle Lab Mail POP3 Remote Buffer Overflow	Critical
Command Injection	Critical
Anonymous FTP	High
Sensitive Data Exposure on `Robots.txt`	Medium
Poor Access Control	Medium
Host Identification	Low

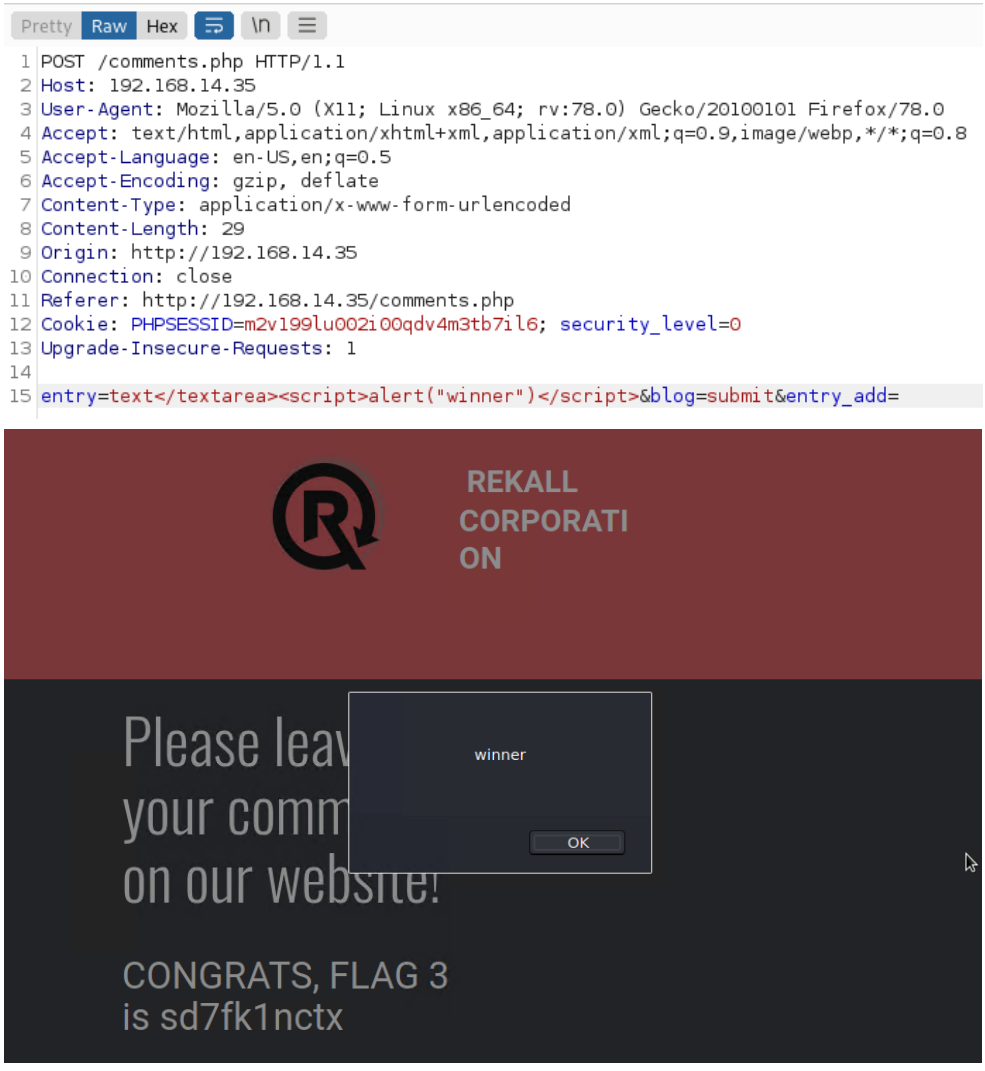
The following summary tables represent an overview of the assessment findings for this penetration test:

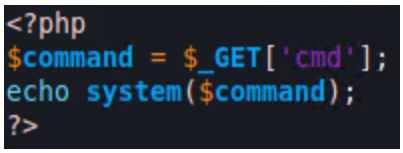
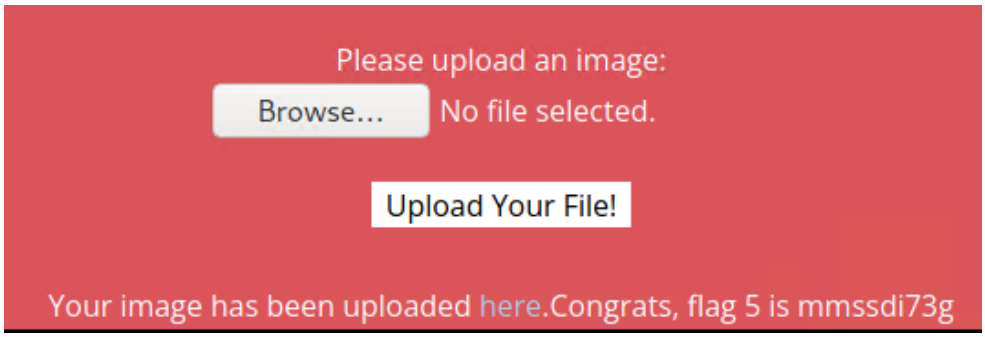
Scan Type	Total
Hosts	Web App: 192.168.14.35 Linux Servers: 192.168.13.10 192.168.13.11 192.168.13.12 192.168.13.13 192.168.13.14 Windows Servers: 172.22.117.20
Ports	21, 25, 80, 106, 110, 135, 139, 443, 445

Exploitation Risk	Total
Critical	11
High	1
Medium	2
Low	1

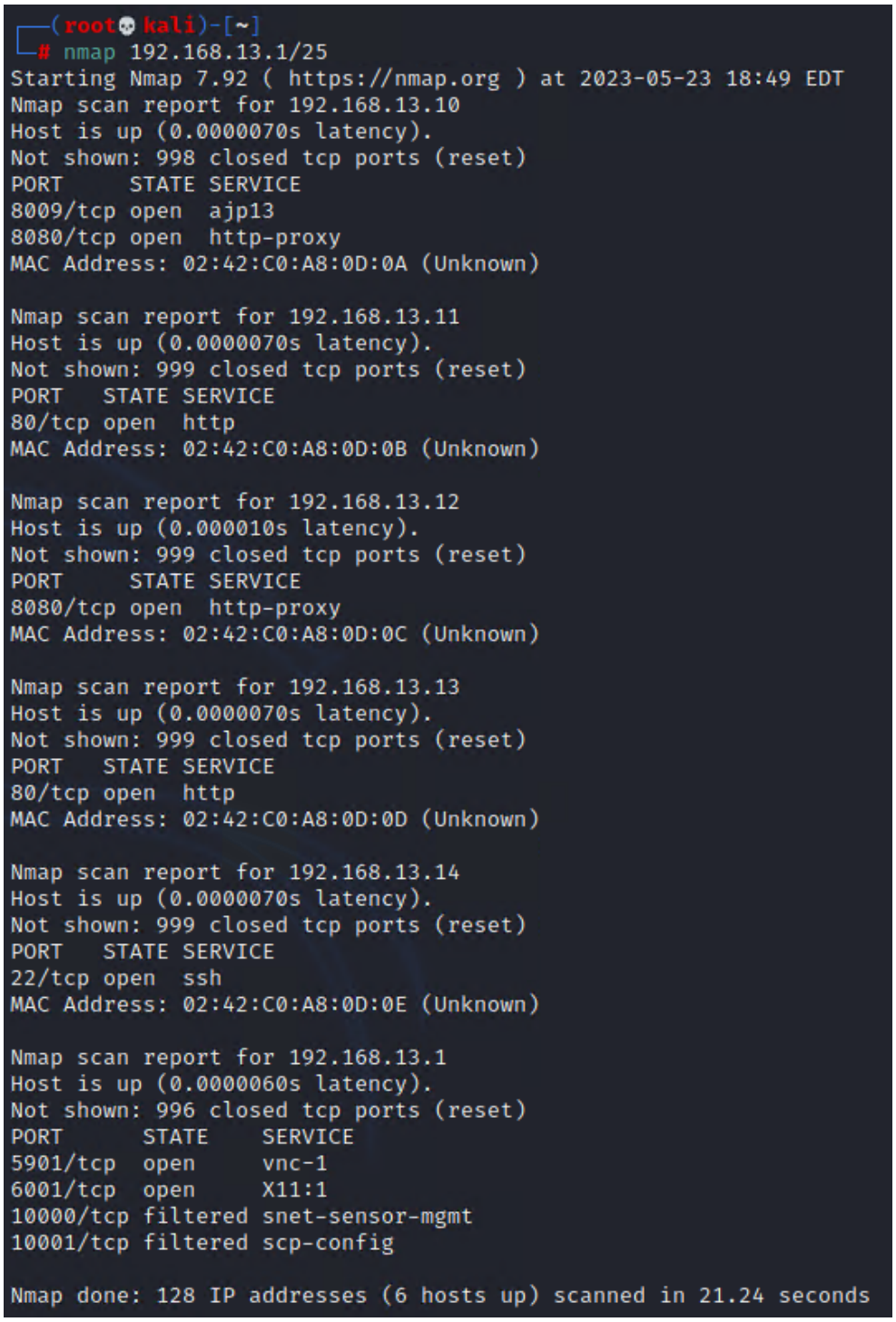
Vulnerability Findings

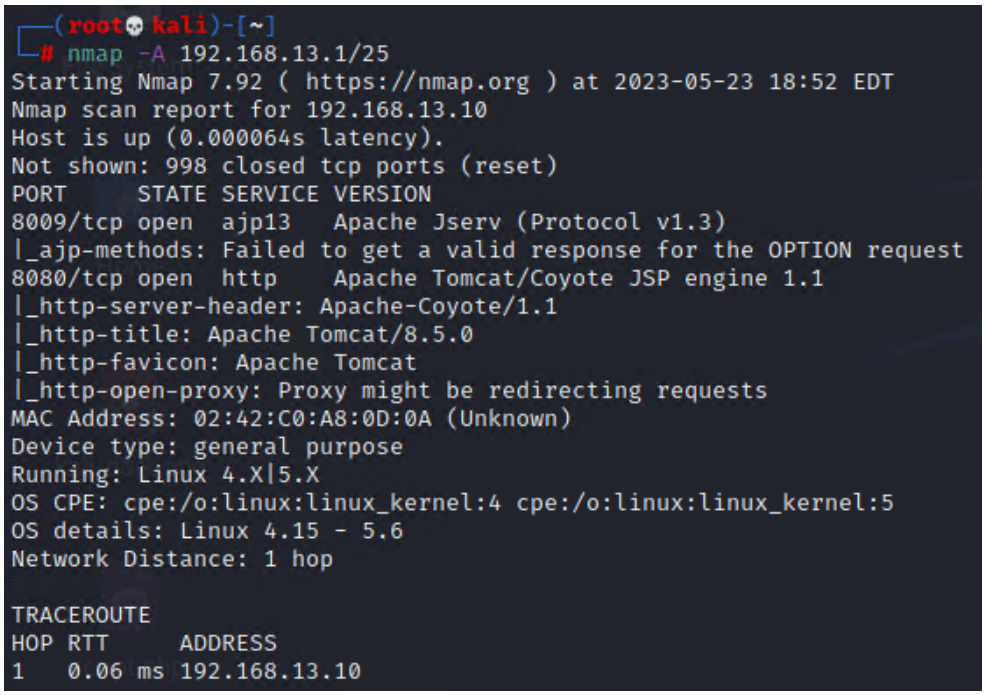
Vulnerability 1	Findings
Title	Reflected XSS on `Welcome-Planner.php`
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Critical
Description	Within the `Memory-Planner.php` page of the Rekall Website, the first user input field does perform some basic input validation by identifying and removing the word “script”, however it is not hard for a user to circumnavigate this barrier. Spalding Tech was able to make use of the following input to perform the attack: `<scrSCRIPTipt>alert("winner")</scrSCRIPTipt>`
Images	
Affected Hosts	192.168.14.35
Remediation	Stronger input validation. Rather than searching for specific words to remove, it would be easier to compare the input to the available options to choose from. Any input not directly matching a possible selection should throw an error to the user instructing them to only input a choice from the listed possibilities. Alternatively, this field could be made into a check box for the user to make a selection from. This eliminates any input needing to be validated.

Vulnerability 2	Findings
Title	Stored XSS
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	**Critical**
Description	Similar to the previous vulnerability, this exploit made use of weak input validation; this time on the `comments.php` page of the Rekall Website. For this attack, Spalding Tech examined the HTML responsible for the specific page in order to determine what sort of comment would break out of the `<textarea>` field and allow the insertion of a `<script>` field. For demonstration purposes, this comment has been left on the page, and any future visitor will be greeted with our pop-up declaring them a winner!
Images	
Affected Hosts	192.168.14.35
Remediation	Stronger input validation would remove any instances of a user attempting to insert HTML. Also, upgrading the site to make use of JavaScript could make it harder for a malicious actor to hunt down the necessary syntax to input.

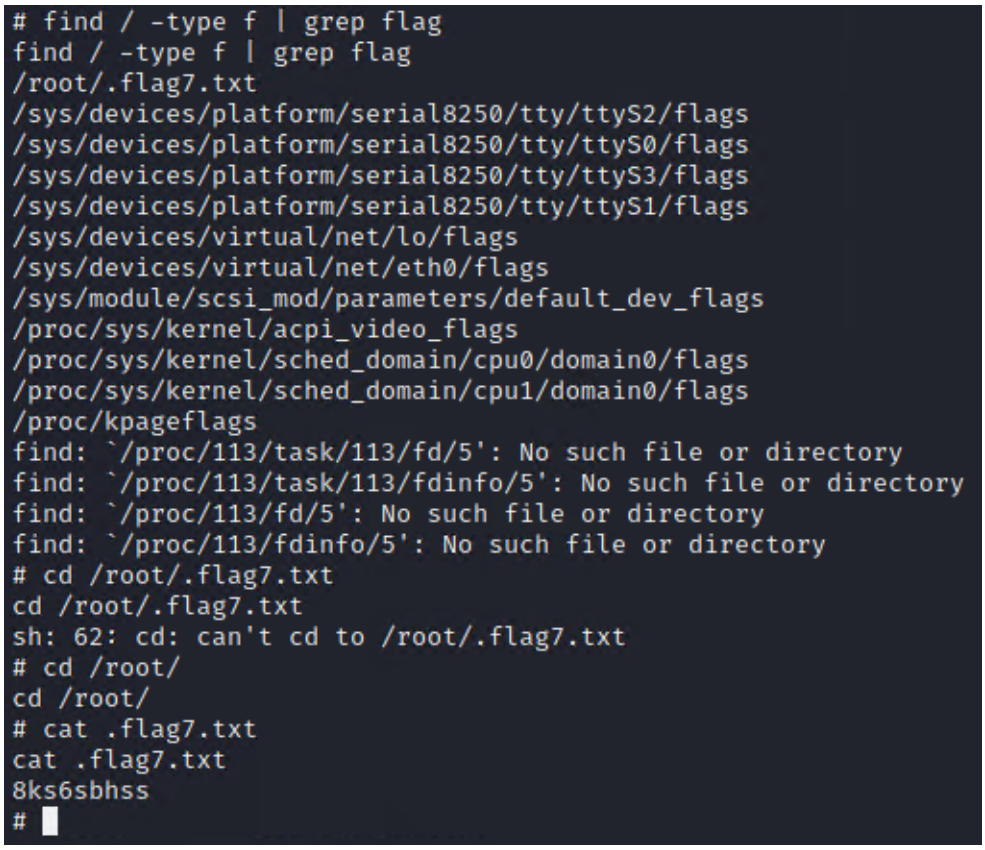
Vulnerability 3	Findings
Title	Local File Inclusion
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	**Critical**
Description	The `Memory-Planner.php` page of the Rekall Website allows users to upload an image to the site. Spalding Tech discovered there was no check on this input, and was able to successfully upload the below php script to the site. This vulnerability leaves the Rekall Website exposed to potential malicious actors wishing to upload malware which could affect the site and its users.
Images	 
Affected Hosts	192.168.14.35
Remediation	Limit acceptable file-types that can be uploaded to only image files and perform basic scans on files being uploaded to guarantee their safe and free of embedded scripts or malware.

Vulnerability 4	Findings
Title	Host Identification
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	**Low**
Description	By making use of the tool `nmap`, it is possible to scan the Rekall network to identify local hosts on the network. Spalding Tech was able to identify 5 hosts (the image below shows results that include Spalding Tech's source computer used to perform the scan) on the Rekall network. These hosts can then be further scanned and examined for vulnerabilities.

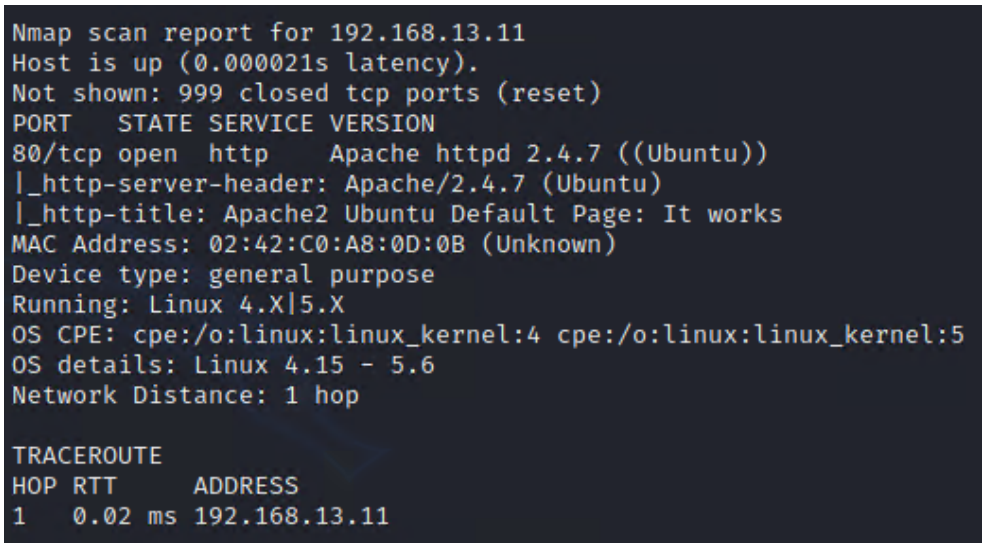
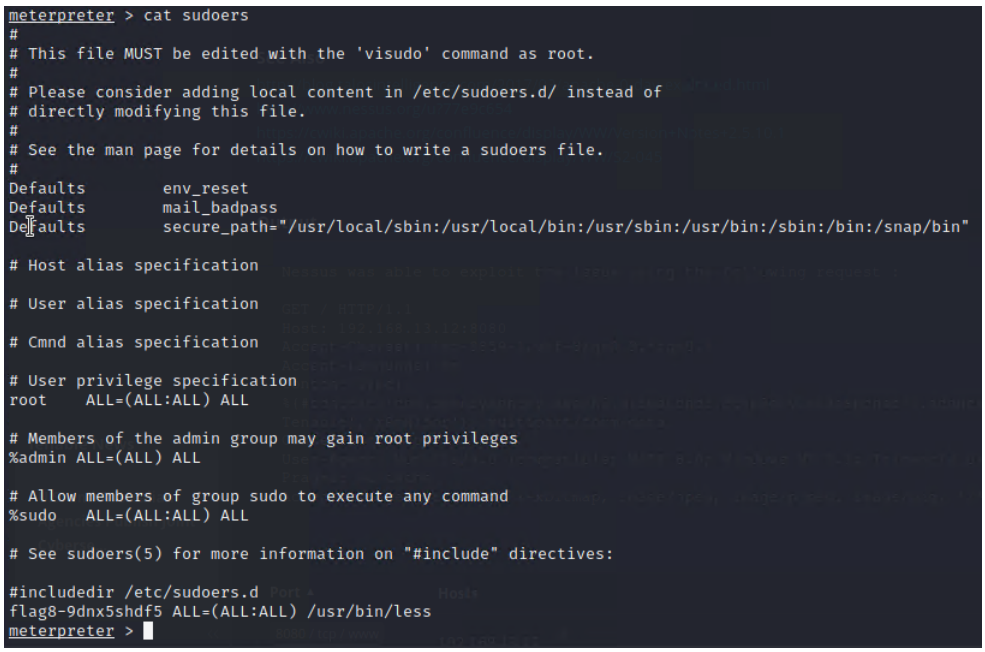
Images	
Affected Hosts	192.168.13.1 , 192.168.13.10 , 192.168.13.11 , 192.168.13.12 , 192.168.13.13 , 192.168.13.14
Remediation	Make use of more subnets, prevent devices from being accessed via the internet. The entire enterprise network could be hidden behind a firewall and jump-box. Additionally, a VPN may be used internally to create secure tunnels between hosts, preventing anyone outside the network from identifying these IP addresses.

Vulnerability 5	Findings
Title	Apache Tomcat RCE (CVE-2017-12617)
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	**Critical**
Description	When performing an aggressive scan against the Linux Host @ `192.168.13.10`, Spalding Tech was able to identify the version of the Apache service running on the server. After some research, a well-known vulnerability was identified as being associated with this particular version of Apache. Exploiting this vulnerability granted Spalding Tech access to this machine with `root` level privileges.
Images	

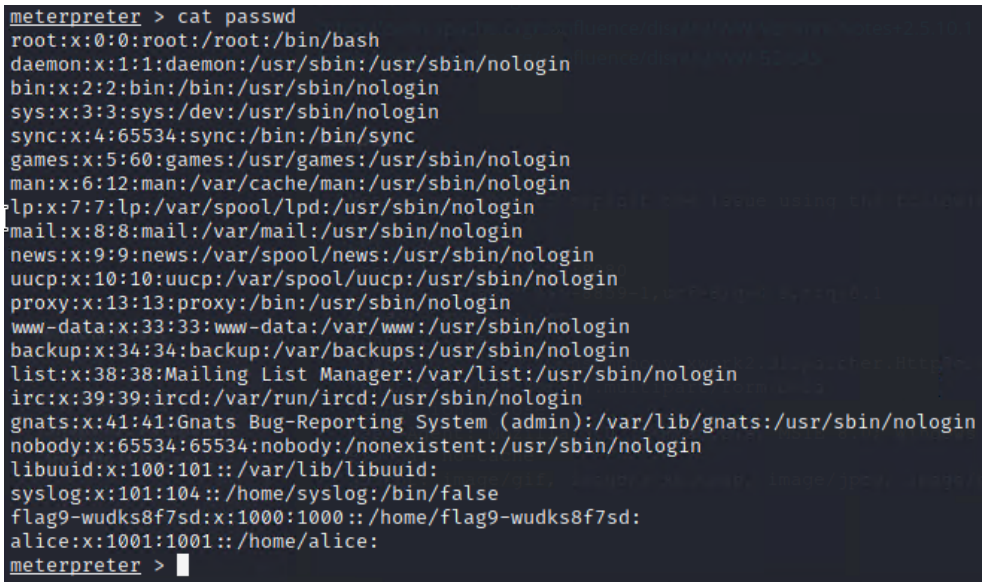
```
┌──(root💀kali)-[~]
└─# nmap -A 192.168.13.1/25
Starting Nmap 7.92 ( https://nmap.org ) at 2023-05-23 18:52 EDT
Nmap scan report for 192.168.13.10
Host is up (0.000064s latency).
Not shown: 998 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
8009/tcp open  ajp13   Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTION request
8080/tcp open  http    Apache Tomcat/Coyote JSP engine 1.1
|_http-server-header: Apache-Coyote/1.1
|_http-title: Apache Tomcat/8.5.0
|_http-favicon: Apache Tomcat
|_http-open-proxy: Proxy might be redirecting requests
MAC Address: 02:42:C0:A8:0D:0A (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

TRACEROUTE
HOP RTT     ADDRESS
1   0.06 ms 192.168.13.10
```

	
Affected Hosts	192.168.13.10
Remediation	Ensure that all services are updated and make use of firewalls to prevent unauthorized access to devices. Furthermore, stronger passwords and restricting access to white-listed IP addresses will add layers of security to the network.

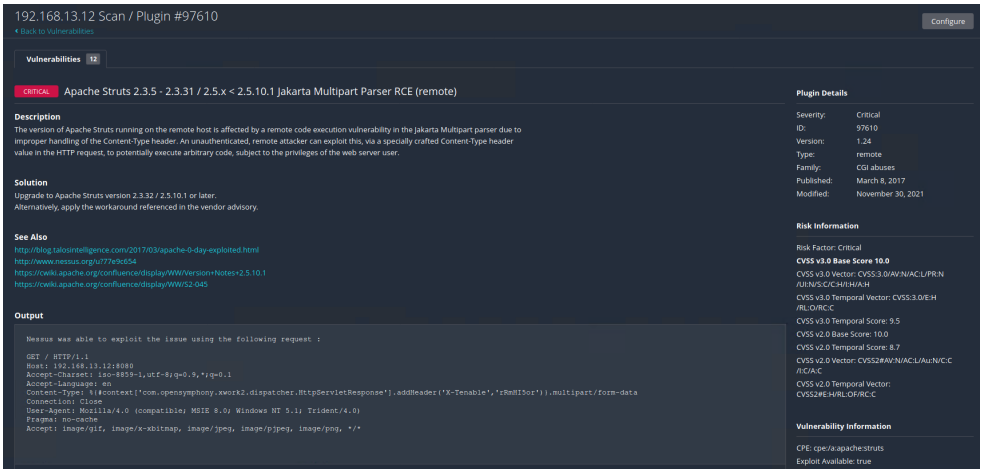
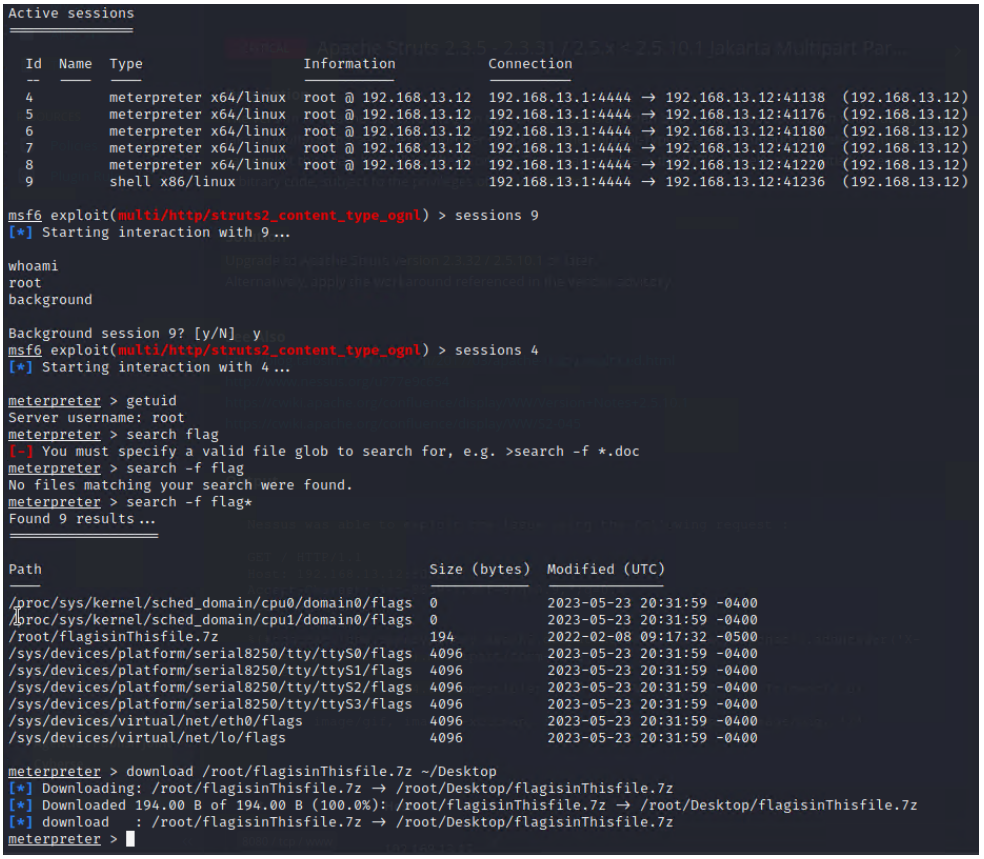
Vulnerability 6	Findings
Title	ShellShock
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	**Critical**
Description	Spalding Tech was able to gain access to the Linux Host @ `192.168.13.11` by making use of the ShellShock exploit. This exploit essentially grants Remote Execution via a vulnerability that exists within `BASH` due to a mishandling of trailing commands when importing function definitions stored within environment tables. Making use of the exploit gave Spalding Tech access to several sensitive areas of the host, including the `sudoers` file.

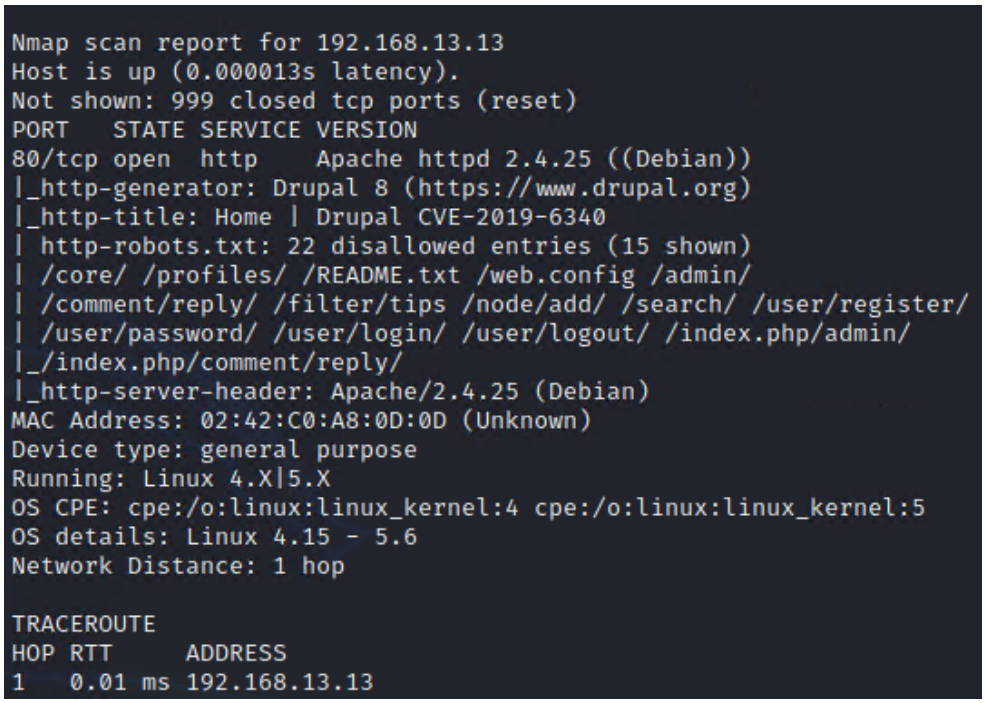
Images	 
Affected Hosts	192.168.13.11
Remediation	Any service or host utilizing `BASH` is at risk, as the vulnerability has existed since `BASH v1.03` was introduced in 1989. That said, it may be possible to make use of a different shell, such as `Fish` or `Zsh`. If maintaining the current configuration, it will be important to ensure `BASH` is updated with the latest available patches at all times.

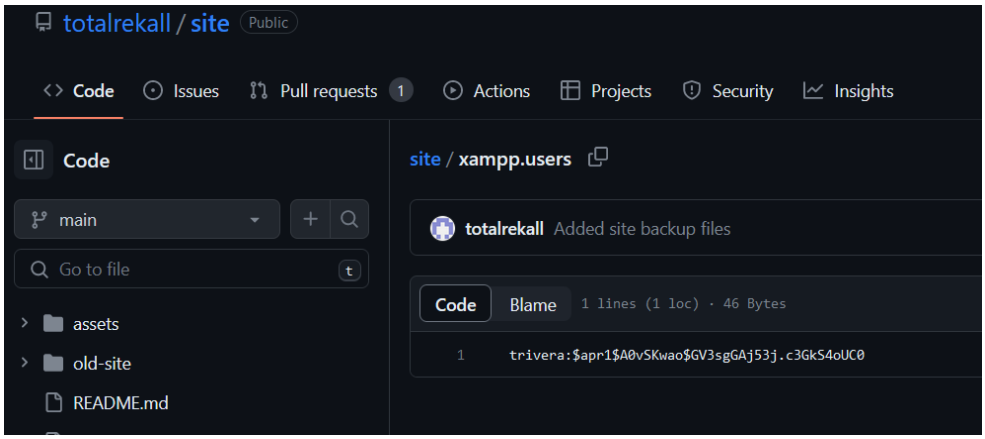
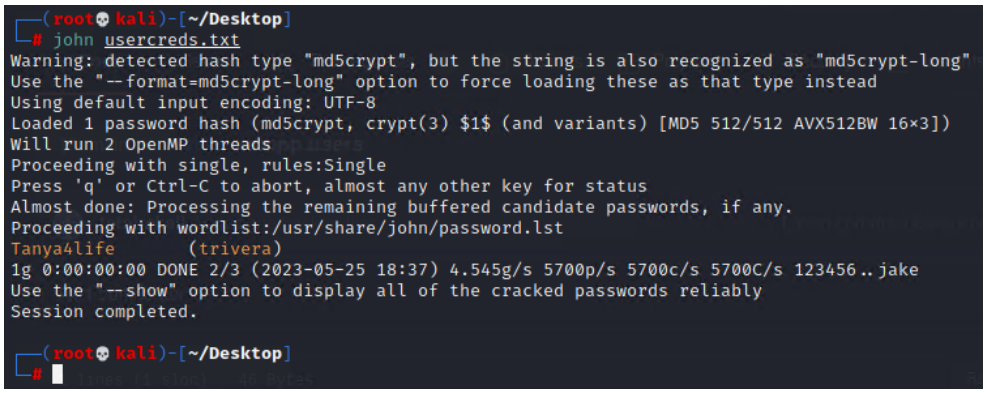
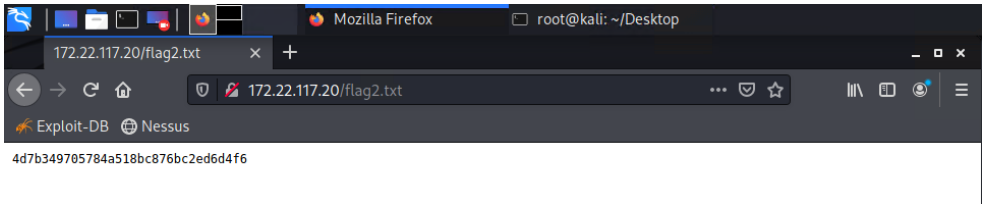
Vulnerability 7	Findings
Title	Poor Access Control
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	**Medium**

Description	While enumerating files on the Linux Host @ `192.168.13.11`, Spalding Tech was able to view the contents of the `/etc/passwd` file. While this file does not contain any actual passwords, it does contain a list of all users (and services) on the host. This list can be used for further attempts at credential stuffing, and presents a happy prize to any malicious actors.
Images	
Affected Hosts	192.168.13.11
Remediation	Check user permissions, and restrict access to sensitive files. This file in particular can be restricted to system administrators (or even simply the `root` account) as there is little reason to access the file when applying changes to user account configurations.

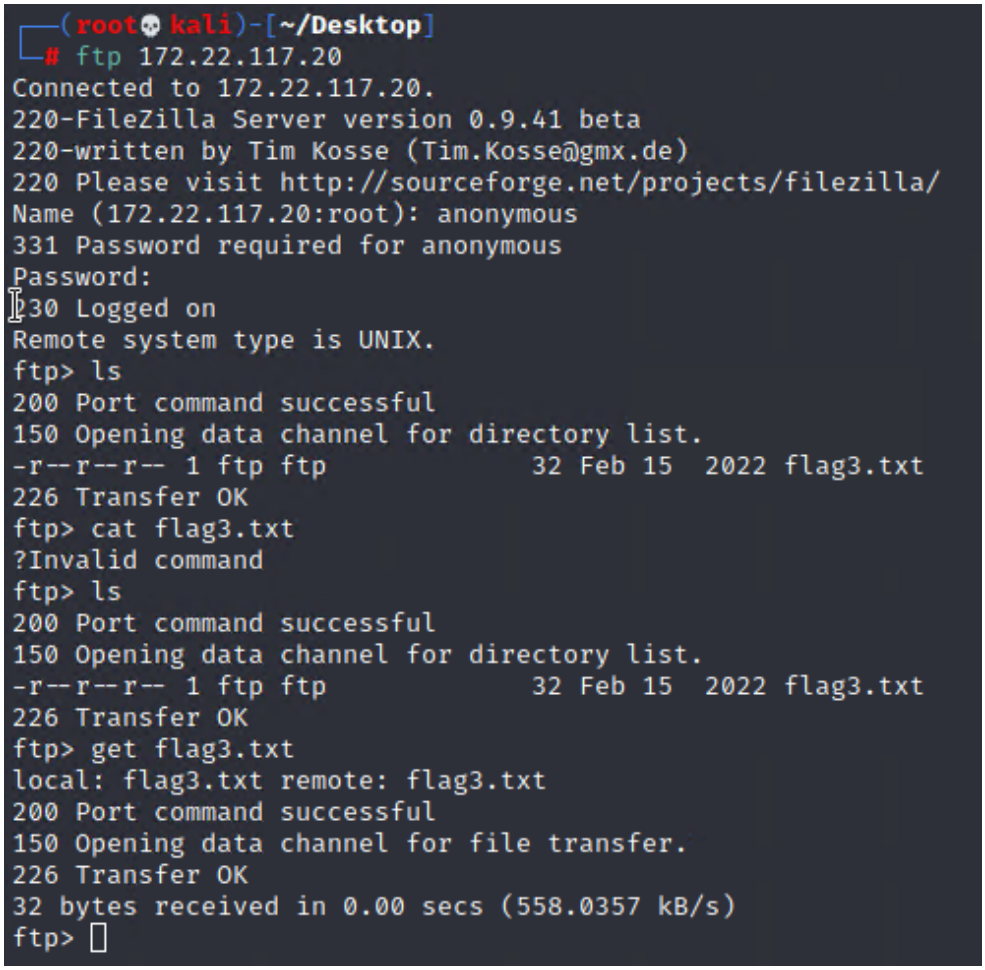
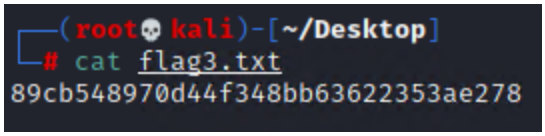
Vulnerability 8	Findings
Title	Apache Struts RCE (CVE-2017-5638)
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	**Critical**
Description	When Spalding Tech made use of `Nessus` to perform a vulnerability scan against the Linux Host @ `192.168.13.12`, a single critical vulnerability was identified. This host is running a version of `Apache Struts` which is vulnerable to potential remote execution due to incorrect exception handling within the service's Jakarta Multipart parser. Exploiting this vulnerability granted Spalding Tech access to the host and exfiltrate files.

Images	  
Affected Hosts	192.168.13.12
Remediation	The strongest mitigation would be to update the version of `Apache` running on this host, or switch to a different implementation of the Multipart parser. Additionally, there are a few workarounds that include implementing a Servlet filter to validate the `Content-Type` header and throw away any requests not matching `multipart/form-data`.

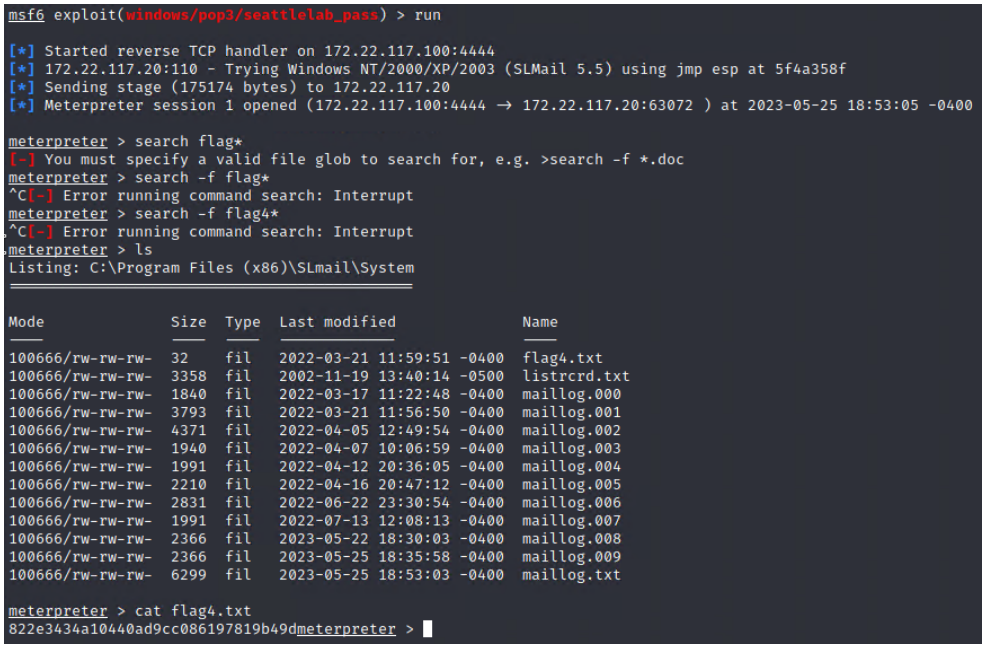
Vulnerability 9	Findings
Title	Drupal Core RCE (CVE-2019-6340)
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	**Critical**
Description	This vulnerability exists within the `Drupal 8 REST API`, and can be exploited by sending a `GET` request containing a serialized payload to execute in the server. By doing so, an attacker can run arbitrary commands on the web server. Spalding Tech was able to make use of this exploit to gain access to the Linux Host @ `192.168.13.13` as a low-level user and perform basic file enumeration.
Images	 
Affected Hosts	192.168.13.13
Remediation	

Vulnerability 10	Findings
Title	Exposed Password Hash
Type (Web app / Linux OS / WIndows OS)	Windows OS / GitHub
Risk Rating	**Critical**
Description	While performing OSINT, Spalding Tech was able to locate a GitHub repository containing a username and password hash. Once the hash had been cracked, Spalding Tech was able to use the credentials to gain access to the site hosted by the Windows Host @ `172.22.117.20` and perform HTTP enumeration.
Images	  
Affected Hosts	totalrekall github , 172.22.117.20
Remediation	Check all repositories and ensure there is no sensitive data that can be publicly viewed. Change current passwords, and enforce a strict policy for password complexity and rotation in the future.

Vulnerability 11	Findings

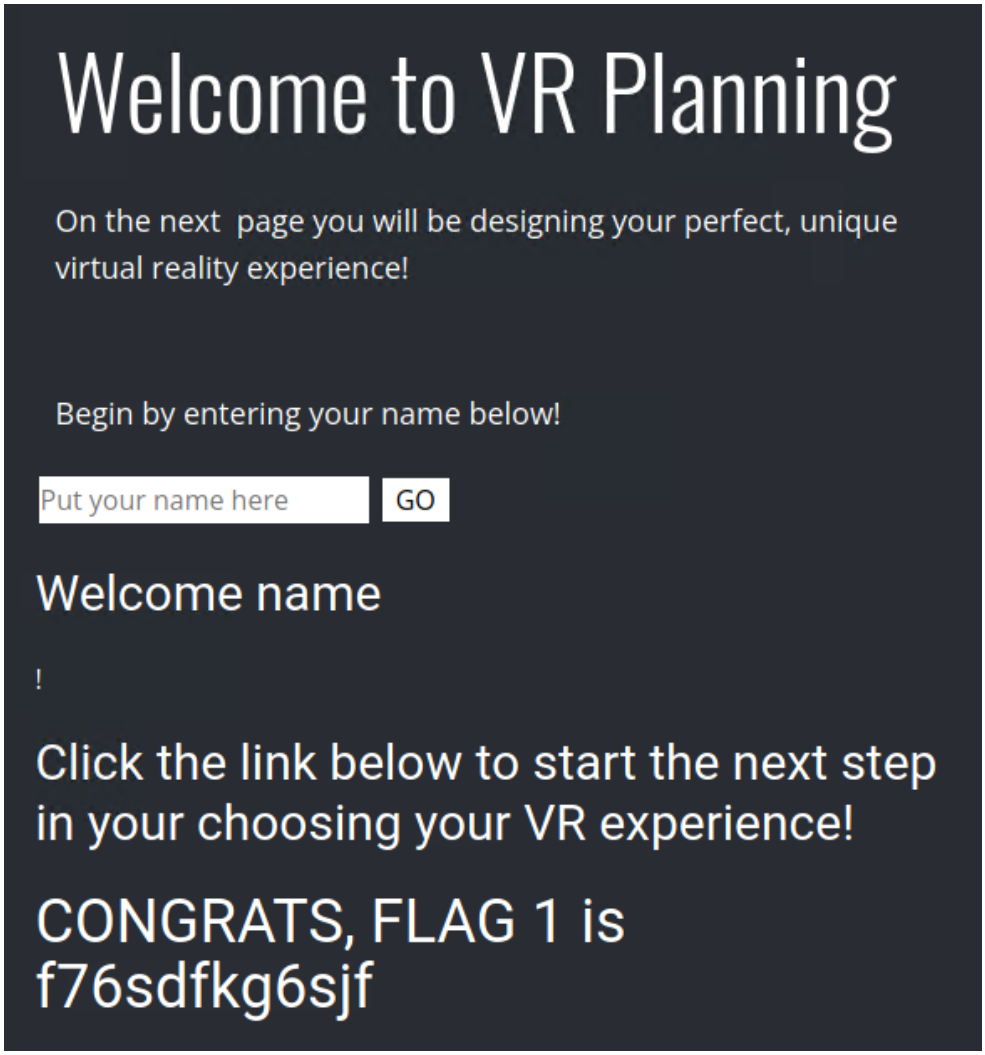
Title	Anonymous FTP
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	High
Description	Port 21 on the Windows Host @ `172.22.117.20` has been left open and is accepting anonymous `FTP` connections. This means any user can connect directly with the host and enumerate (or even exfiltrate) files. Spalding Tech was able to exploit this vulnerability to perform exactly those actions.
Images	 
Affected Hosts	172.22.117.20
Remediation	Unless absolutely necessary, close port 21 to all outside traffic. If this is not a viable solution, require a username and password to establish any `FTP` connections with the host.

Vulnerability 12	Findings

Title	Seattle Lab Mail POP3 Remote Buffer Overflow
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Critical
Description	A buffer overflow vulnerability exists within the `POP3` server of `SLMail 5.5` when sending a password of excessive length. It is possible to exploit this vulnerability to gain access to, and execute arbitrary commands on, a machine.
Images	
Affected Hosts	172.22.117.20
Remediation	Restrict access to Port 110 on this host, and consider updating or (better yet) replacing the `SLMail` service with a more secure option such as `IMAP`.

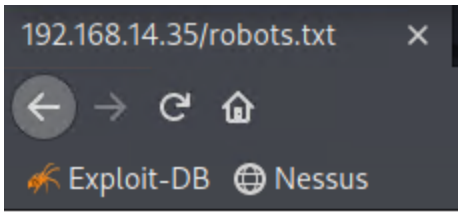
Vulnerability 13	Findings
Title	Reflected XSS on `Welcome.php`
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Critical
Description	This vulnerability is nearly identical to Vulnerability 1, however requires less effort from a malicious actor to exploit. Once again, it is possible for a user to input HTML code in a field; this time on the `Welcome.php` page. By using the following input, it is possible to break out of the written HTML and execute arbitrary script commands:

	name</h3><script>alert(“winner”)</script>
Images	

	
Affected Hosts	192.168.14.35
Remediation	Stronger input validation is needed here. Elsewhere on the site, there was enough validation to stop the exploitation used in this example, however still not enough to remove the overall vulnerability from the site entirely. Spalding Tech highly recommends sanitizing all user input before it is processed.

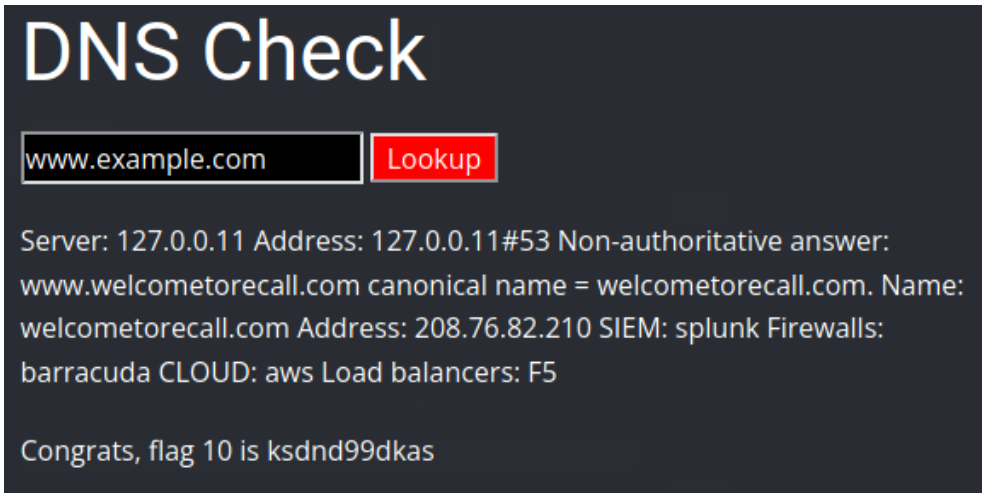
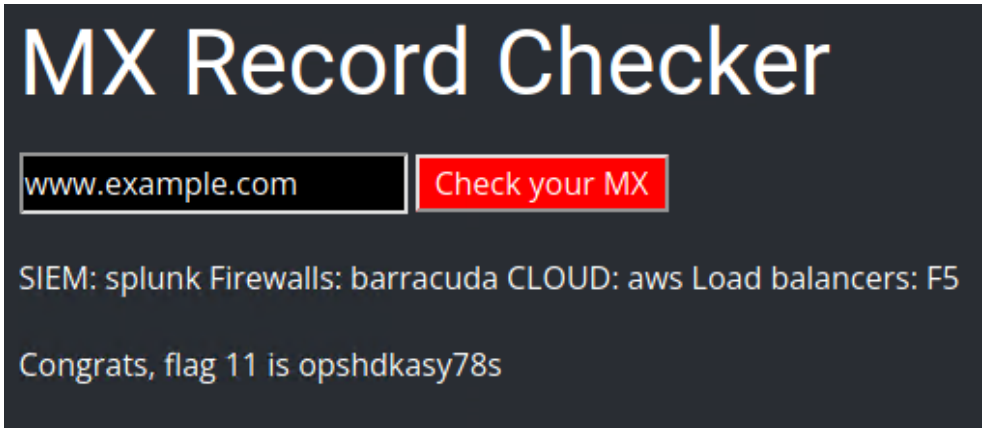
Vulnerability 14	Findings
Title	Sensitive Data Exposure on `Robots.txt`
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	**Medium**
Description	A website usually makes use of a `robots.txt` file to tell search engine crawlers which URLs can be accessed on the site. While these files are not inherently problematic, they can be used by malicious actors to identify private areas of a website. Rekall's website makes use of a `robots.txt` file that

	features hidden pages that can assist attackers in mapping out the site.

Images	
	`User-agent: GoodBot`
	`Disallow:`
	
	`User-agent: BadBot`
	`Disallow: /`
	
	`User-agent: *`
	`Disallow: /admin/`
	`Disallow: /documents/`
	`Disallow: /images/`
	`Disallow: /souvenirs.php/`
	`Disallow: flag9:dkkdudfkdy23`

Affected Hosts	192.168.14.35
Remediation	Remember attackers will find and make use of this file. Rather than making use of `Disallow`, use `Noindex`. This will tell search engines not to include the pages in search results, and further hide them from appearing.

Vulnerability 15	Findings
Title	Command Injection
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	**Critical**
Description	Making use of the record checking features on the `networking.php` page of Rekall's website, it is possible to execute arbitrary commands. A malicious actor could potentially exploit this vulnerability to fully compromise the web application and any data held within its database.

Images	 
Affected Hosts	192.168.14.35
Remediation	Make use of input validation to prevent such attacks. Sanitize user input so threat actors may not insert characters into the OS command. Furthermore, avoid system calls through user input, and create a white list of possible inputs to ensure no unintended input is accepted by the application.