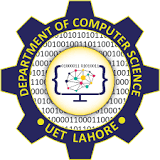
**LAB REPORTS**



**Session 2023-2027**

**Submitted by:**

Sumaira Hafeez 2023-CS-1

**Supervised by:**

Dr. Faiza

**Course:**

Information Security

**Department of Computer Science**

**University of Engineering and Technology,**

**Lahore Pakistan**

Contents

[**TASK 2 VULNERABLITIY RESEARCH** 3](#_Toc188786668)

[**1.** **Vulnerability:** 3](#_Toc188786669)

[**2.** **Vulnerability Analysis:** 3](#_Toc188786670)

[ **OpenSSH:** 3](#_Toc188786671)

[ **Apache Struts RCE:** 3](#_Toc188786672)

[**3.** **Common Vulnerabilities and Exposure IDs(CVE(ID)):** 3](#_Toc188786673)

[**4.** **Severity Score using CVSS:** 4](#_Toc188786674)

[**5.** **Mitigation Steps:** 4](#_Toc188786675)

[**6.** **CONCLUSION:** 4](#_Toc188786676)

# **TASK 2 VULNERABLITIY RESEARCH**

## **Vulnerability:**

This report presents an analysis of vulnerabilities identified in the software assets using Nmap vulnerability scanning.

## **Vulnerability Analysis:**

### **OpenSSH:**

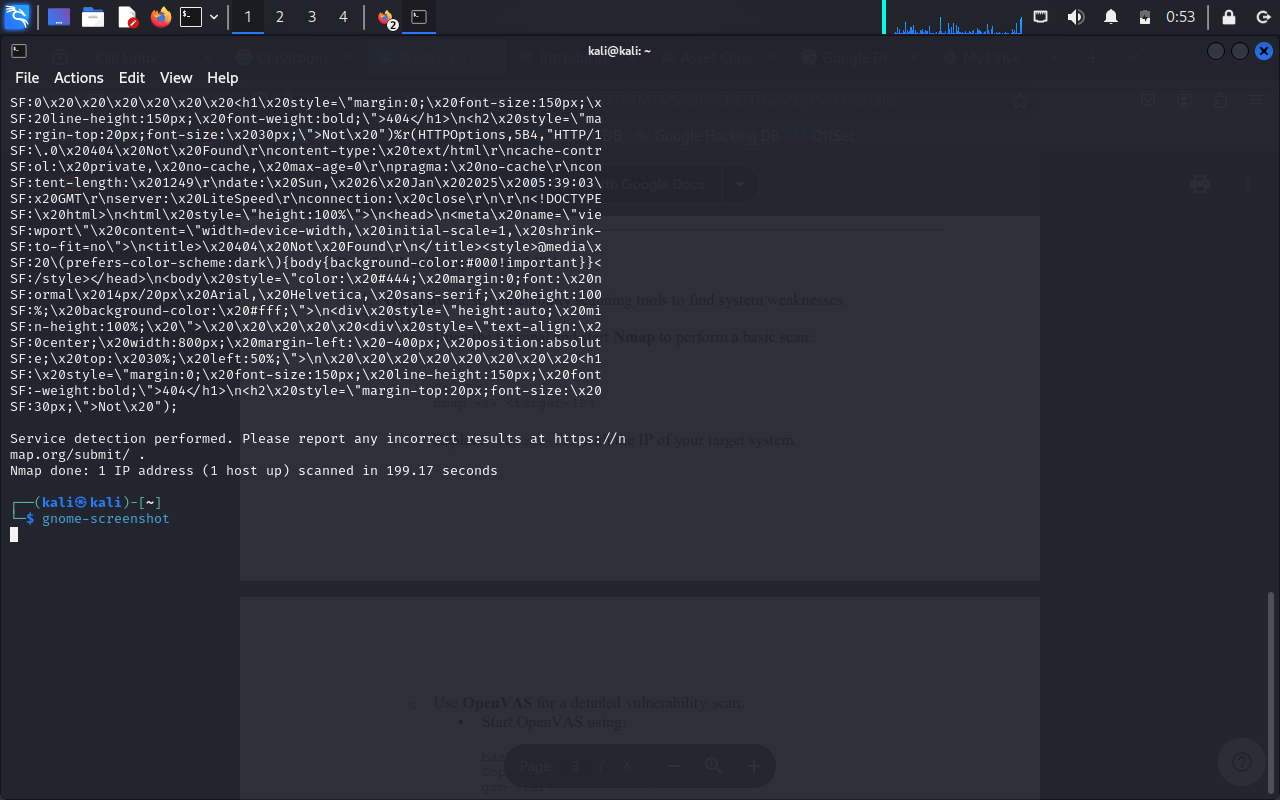
It means that this version is outdated and susceptible to privilege escalation attacks. Its CVE(ID) is **CVE-2021-41417**

### **Apache Struts RCE:**

Detected in the web application, allowing remote attackers to execute arbitrary code. Its CVE(ID) is **CVE-2021-41417**

* **Unencrypted Database communications:**

Lack of encryption can lead to interception of sensitive data.

****

## **Common Vulnerabilities and Exposure IDs(CVE(ID)):**

A **CVE ID (Common Vulnerabilities and Exposures Identifier)** is a unique identifier assigned to publicly known cybersecurity vulnerabilities. The CVE system is managed by MITRE Corporation and is widely used by security professionals to track and address software and hardware vulnerabilities.

OpenSSH: **CVE-2021-41417**

Apache struts RCE: **CVE-2021-41417**

Unencrypted Database communication: **CVE-2023-4537**

## **Severity Score using CVSS:**

The **CVSS (Common Vulnerability Scoring System)** is a standardized framework used to assess the severity of software vulnerabilities. The severity score is a numerical value between **0 and 10**, which indicates how critical a vulnerability is.

### **Mitigation Steps:**

**Upgrade OpenSSH:** Update to the latest stable version to patch security flaws.

**Patch Web Server:** Apply security updates to Apache Struts and related dependencies.

**Encrypt Database Traffic:** Use TLS encryption for all database connections.

# **CONCLUSION:**

The vulnerability research identified critical security risks in the software infrastructure. Immediate remediation actions are recommended to address high-risk vulnerabilities. Implementing long-term security best practices will further strengthen the system’s resilience against cyber threats.