# ■ Risk Summary Report

**Vulnerability Scan Report Summary for Top Management**

As a cybersecurity analyst, I have analyzed the vulnerability scan report and identified key risks that requir

**Main Risk Areas:**

1. **Remote Access Vulnerabilities**: The scan revealed multiple vulnerabilities related to remote access,
2. **Web Application Vulnerabilities**: PHP 5.3.x < 5.3.29 Multiple Vulnerabilities (12 instances) and Apacl
3. **Unpatched Systems**: The scan identified hosts with outdated software versions, including Apache 2.

**Most Vulnerable Systems or Services:**

1. Host **192.168.11.131**, which has been affected by 210 vulnerabilities, making it a high-risk host that I
2. Nessus SNMP Scanner and Service Detection services, with 27 and 6 instances respectively, are also c
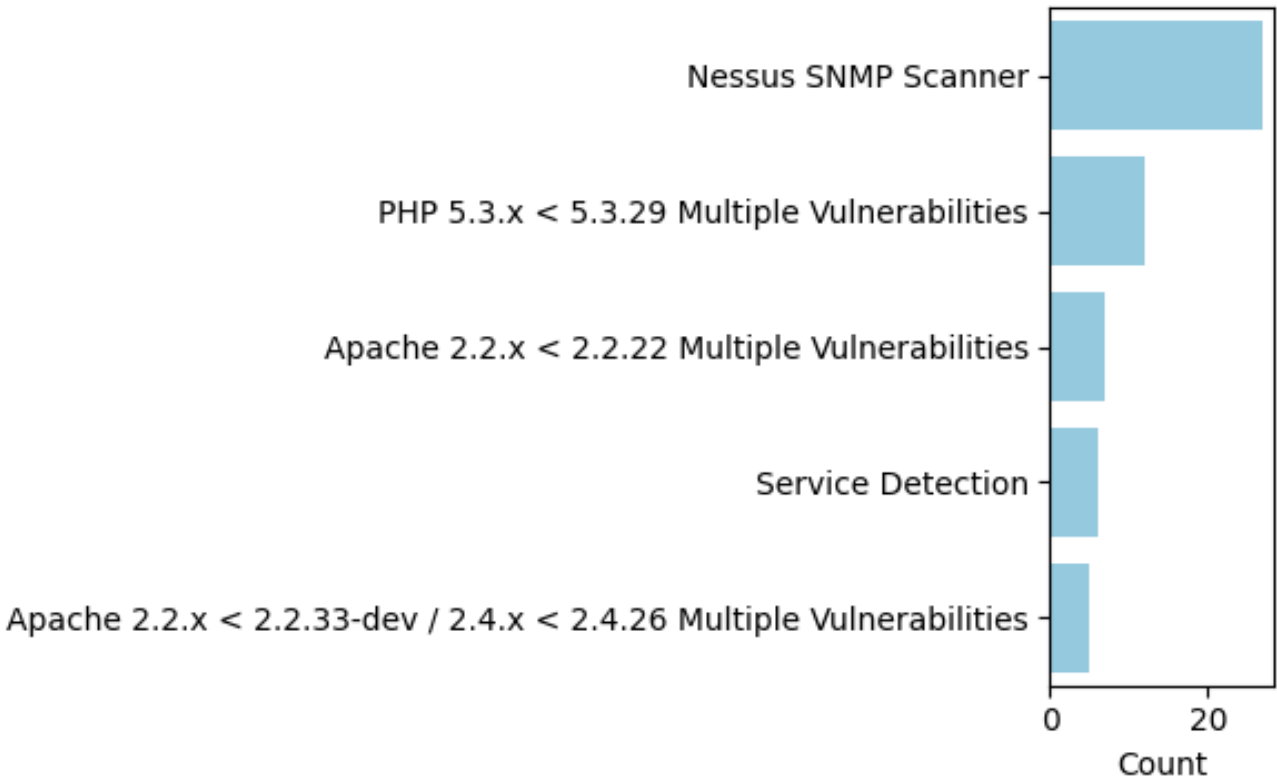
**Recommended Actions:**

1. **Immediate Patching**: Prioritize patching of all identified vulnerable systems and services to prevent e
2. **Secure Remote Access**: Implement secure remote access protocols and restrict access to only nece
3. **Web Application Security**: Conduct thorough security assessments of web applications using PHP ar
4. **Host Segmentation**: Segment high-risk hosts, such as **192.168.11.131**, from the rest of the netwo
5. **Continuous Monitoring**: Schedule regular vulnerability scans and monitoring to ensure timely detectio

I recommend that top management review these findings and provide guidance on prioritizing and allocatir

Risk Severity Levels
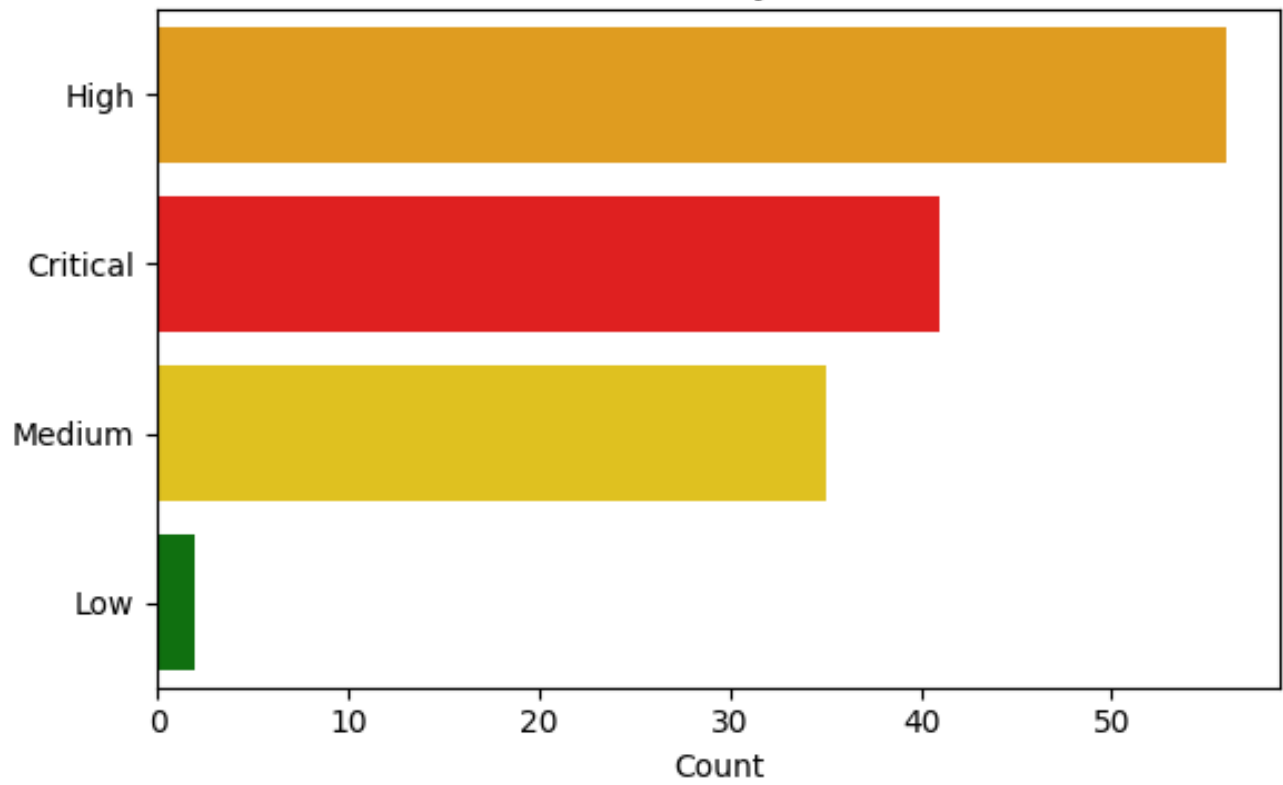
Top Vulnerabilities (Pl...

# Most Affected Hosts

192.168.11.131

Count