**Stage 2**

**Overview: -**

**Nessus Overview**

Nessus is a widely acclaimed and robust vulnerability assessment and management tool that plays a pivotal role in maintaining the security and integrity of computer networks. Developed by Tenable, Nessus has become an indispensable asset for organizations and security professionals seeking to proactively identify and address vulnerabilities in their IT environments.

At its core, Nessus is designed to detect and assess weaknesses within networks, applications, and infrastructure. It accomplishes this through a comprehensive and systematic scanning process, which entails examining hosts, servers, and devices for known and potential security issues. Nessus employs a combination of active and passive scanning techniques, making it versatile and adaptable to various network configurations.

One of the standout features of Nessus is its extensive vulnerability database. It maintains an expansive and up-to-date repository of known vulnerabilities, which it leverages during scans to compare and evaluate the configuration and security posture of the scanned systems. This database includes information on software flaws, misconfigurations, and potential threats, allowing users to stay ahead of emerging cyber threats.

Nessus offers a user-friendly and highly customizable interface, making it accessible to both novice and experienced security professionals. It provides flexibility in defining scan policies, enabling users to tailor their scans to specific needs, compliance requirements, or industry standards. The tool's scanning capabilities encompass a wide range of systems and services, including web applications, databases, cloud resources, and network devices.

In addition to its vulnerability detection capabilities, Nessus is equipped with advanced reporting features. It generates comprehensive reports that detail identified vulnerabilities, their severity, and recommended mitigation steps. These reports are essential for helping organizations prioritize and address vulnerabilities in a structured and systematic manner.

Nessus further supports integrations with various security information and event management (SIEM) solutions, as well as workflow and ticketing systems, streamlining the vulnerability remediation process. This integration capability ensures that detected vulnerabilities are efficiently communicated to the appropriate teams for mitigation and resolution.

Furthermore, Nessus is frequently used in compliance and audit scenarios, helping organizations adhere to industry-specific regulations and standards like PCI DSS, HIPAA, and NIST. Its ability to automate compliance checks simplifies the process of ensuring that systems and networks meet the required security benchmarks.

In summary, Nessus is a powerful, flexible, and indispensable tool for identifying and managing vulnerabilities in complex network environments. It aids organizations in maintaining a proactive approach to cybersecurity, allowing them to remediate vulnerabilities before they can be exploited by malicious actors. With its extensive vulnerability database, user-friendly interface, and reporting capabilities, Nessus remains a cornerstone of modern cybersecurity efforts, contributing significantly to the ongoing battle against cyber threats and ensuring the integrity and security of digital assets.

**Target website: -** [VIT Bhopal](https://vitbhopal.ac.in/)

**Target IP address: -** 14.99.16.249

**List of Vulnerability-**

|  |  |  |  |
| --- | --- | --- | --- |
| S.no | Vulnerabiliy name | Severity | Plugins |
| 1 | Apache Tomcat 9.0.0-M1 < 9.0.68 Request Smuggling Vulnerability | HIGH | 166906 - ` |
| 2 | - Apache Tomcat 9.0.0.M1 < 9.0.37 Multiple Vulnerabilities | HIGH | 138591 |
| 3 | - Apache Tomcat 9.x < 9.0.40 Information Disclosure | HIGH | 144050 |
| 4 | Apache Tomcat 7.0.x <= 7.0.108 / 8.5.x <= 8.5.65 / 9.0.x <= 9.0.45 / 10.0.x <= 10.0.5 vulnerability | MEDIUM | 151502 - |
| 5 | Apache Tomcat 8.5.x < 8.5.58 / 9.0.x < 9.0.38 HTTP/2 Request Mix-Up | MEDIUM | 141446 - |
| 6 | Apache Tomcat 9.0.0.M1 < 9.0.48 vulnerability | MEDIUM | 152182 - |
| 7 | - Apache Tomcat 9.0.0.M1 < 9.0.72 | MEDIUM | 173251 |
| 8 | Apache Tomcat 9.0.0.M1 < 9.0.80 | MEDIUM | 180194 - |
| 9 | - Apache Tomcat 9.0.0.M1 < 9.0.62 Spring4Shell (CVE-2022-22965) Mitigations | MEDIUM | 159464 |
| 10 | - Apache Tomcat 9.0.30 < 9.0.65 vulnerability | MEDIUM | 162498 |

**REPORT**

**Apache Tomcat 9.0.0-M1 < 9.0.68 Request Smuggling Vulnerability**

Severity: High1

Plugin: Nessus 1669061

Description: The version of Tomcat installed on the remote host is 9.0.0-M1 or later but prior to 9.0.68. It is, therefore, affected by a request smuggling vulnerability as referenced in the fixed\_in\_apache\_tomcat\_9.0.68\_security-9 advisory1.

Business Impact: This vulnerability could allow an attacker to poison the web cache, bypass web application firewall protection, and conduct XSS attacks2.

**Apache Tomcat 9.0.0.M1 < 9.0.37 Multiple Vulnerabilities**

Severity: High3

Plugin: Nessus 1385913

Description: The version of Tomcat installed on the remote host is prior to 9.0.37. It is, therefore, affected by multiple vulnerabilities as referenced in the fixed\_in\_apache\_tomcat\_9.0.37\_security-9 advisory3.

Business Impact: These vulnerabilities could allow an attacker to trigger an infinite loop, leading to a denial of service4.

**Apache Tomcat 9.x < 9.0.40 Information Disclosure**

Severity: High5

Plugin: Nessus 1440505

Description: The version of Tomcat installed on the remote host is 9.0.x prior to 9.0.40. It is, therefore, affected by an information disclosure vulnerability5.

Business Impact: This vulnerability could allow an attacker to access sensitive information, which under normal conditions, would be restricted6.

**Apache Tomcat 7.0.x <= 7.0.108 / 8.5.x <= 8.5.65 / 9.0.x <= 9.0.45 / 10.0.x <= 10.0.5 vulnerability**

Severity: Medium1

Plugin: Nessus 1515021

Description: The version of Tomcat installed on the remote host is 7.0.x <= 7.0.108 / 8.5.x <= 8.5.65 / 9.0.x <= 9.0.45 / 10.0.x <= 10.0.5. It is, therefore, affected by a vulnerability as referenced in the fixed\_in\_apache\_tomcat\_10.0.6\_security-10 advisory. Queries made by the JNDI Realm did not always correctly escape parameters1.

Business Impact: This vulnerability could allow an attacker to authenticate using variations of their user name and/or to bypass some of the protection provided by the LockOut Realm1.

**Apache Tomcat 8.5.x < 8.5.58 / 9.0.x < 9.0.38 HTTP/2 Request Mix-Up**

Severity: Medium2

Plugin: Nessus 1414462

Description: The version of Tomcat installed on the remote host is 8.5.x prior to 8.5.58 or 9.0.x prior to 9.0.38. It is, therefore, affected by a vulnerability. If an HTTP/2 client exceeds the agreed maximum number of concurrent streams for a connection (in violation of the HTTP/2 protocol), it is possible that a subsequent request made on that connection could contain HTTP headers - including HTTP/2 pseudo headers - from a previous request rather than the intended headers2.

Business Impact: This can lead to users seeing responses for unexpected resources2.

**Apache Tomcat 9.0.0.M1 < 9.0.48 vulnerability**

Severity: Medium

Plugin: Nessus 1521821

Description: The version of Tomcat installed on the remote host is prior to 9.0.48. It is, therefore, affected by a vulnerability as referenced in the fixed\_in\_apache\_tomcat\_9.0.48\_security-9 advisory. Apache Tomcat 10.0.0-M1 to 10.0.6, 9.0.0.M1 to 9.0.46 and 8.5.0 to 8.5.66 did not correctly parse the HTTP transfer-encoding request header in some circumstances leading to the possibility to request smuggling when used with a reverse proxy1.

**Apache Tomcat 9.0.0.M1 < 9.0.72**

Severity: Medium

Plugin: 173251

Description: The version of Tomcat installed on the remote host is prior to 9.0.72. It is, therefore, affected by a vulnerability as referenced in the fixed\_in\_apache\_tomcat\_9.0.72\_security-9 advisory1.

Business Impact: This vulnerability could result in the user agent transmitting the session cookie over an insecure channel1. The recommended solution is to upgrade to Apache Tomcat version 9.0.72 or later1.

**Apache Tomcat 9.0.0.M1 < 9.0.80**

Severity: Medium

Plugin: 180194

Description: The version of Tomcat installed on the remote host is prior to 9.0.80. It is, therefore, affected by a vulnerability as referenced in the fixed\_in\_apache\_tomcat\_9.0.80\_security-9 advisory2.

Business Impact: This vulnerability could result in URL Redirection to Untrusted Site (‘Open Redirect’)2. The recommended solution is to upgrade to Apache Tomcat version 9.0.80 or later2.

**Apache Tomcat 9.0.0.M1 < 9.0.62 Spring4Shell (CVE-2022-22965) Mitigations**

Severity: Low

Plugin: 159464

Description: The version of Apache Tomcat installed on the remote host is 9.x prior to 9.0.623.

Business Impact: This vulnerability could cause client connections to share an Http11Processor instance resulting in responses, or part responses, to be received by the wrong client3. The recommended solution is to upgrade to Apache Tomcat version 9.0.62 or later3.

**Apache Tomcat 9.0.30 < 9.0.65**

Severity: Medium

Plugin: 162498

Description: The version of Tomcat installed on the remote host is prior to 9.0.655.

Business Impact: This vulnerability could cause client connections to share an Http11Processor instance resulting in responses, or part responses, to be received by the wrong client5. The recommended solution is to upgrade to Apache Tomcat version 9.0.65 or later5.