Main Website Vulnerability Test

Team 10.2

Website: https://internshala.com/

- **CWE - 319: Cleartext Transmission of Sensitive Information**
- **OWASP Category: A06:2021 - Security Misconfiguration**

Description:

Port 80 is commonly used for unencrypted HTTP communication. When data is transmitted over HTTP, it is susceptible to interception and eavesdropping, as the information is sent in plain text. This can lead to a variety of security issues:
- **Man-in-the-Middle Attacks**: Without encryption, attackers can intercept and read sensitive data such as login credentials, personal information, and session tokens.
- **Data Tampering**: Attackers can modify the data being transmitted, potentially leading to unauthorized access, injection attacks, or other forms of data manipulation.
- **Session Hijacking**: Session IDs can be captured, allowing attackers to impersonate authenticated users.

Business Impact:

- **Data Exposure**: Sensitive information can be easily intercepted, potentially leading to data breaches.

- **Reputation Damage**: Customers may lose trust in the website's security, affecting the reputation of the organization.

Mitigation:

- **Implement HTTPS**: All communication should be redirected from port 80 to port 443 to ensure encryption.
- **HSTS (HTTP Strict Transport Security):** Implementing HSTS headers enforces the use of secure connections and helps prevent downgrade attack.

- **CWE - 319: Cleartext Transmission of Sensitive Information**(if not configured properly)

- **CWE - 295: Improper Certificate Validation** (if SSL/TLS implementation is flawed)

- **OWASP Category: A06:2021 - Security Misconfiguration**

-

Description:

Port 443 is used for secure, encrypted HTTPS communication. However, even with encryption, there can be vulnerabilities if not configured correctly:
- **Weak Cipher Suites**: Outdated or weak encryption algorithms can leave the communication vulnerable to attacks.
- **Improper Certificate Validation**: If the SSL/TLS implementation doesn't properly validate certificates, it can expose users to man-in-the-middle attacks.
- **Misconfigurations**: Incorrect configurations of SSL/TLS settings can lead to security holes.

Business Impact:

- **Data Exposure**: Misconfigurations can result in the unintentional exposure of sensitive information.
- **Man-in-the-Middle Attacks**: If SSL/TLS is not implemented correctly, attackers can intercept and manipulate the communication.

Mitigation:

- **SSL/TLS Best Practices**: Ensure that SSL/TLS configurations are up-to-date and follow best practices to maintain a high level of security.
- **Certificate Management:** Regularly update SSL certificates to prevent expiration or misuse.
- **Security Audits and Testing:** Perform regular security audits and penetration testing to identify and address potential vulnerabilities.

- **CWE - 284: Improper Access Control**

- **OWASP Category: A01:2021 – Broken Access Control**

Description:

If the SSH protocol is left open without adequate security measures, it can be vulnerable to various exploits and attacks. Some of the potential vulnerabilities include:

-Brute force attacks: Attackers may attempt to guess the SSH username and password combination through successive login attempts.
-SSH key compromise: If SSH keys are not protected securely, they may be stolen or leaked, allowing attackers to gain unauthorized access to systems using those keys
-Denial of Service (DoS) attacks: Attackers can flood the SSH server with excessive connections or malformed packets to overwhelm its resources, making it inaccessible to legitimate users.
-Password-based attacks: Weak or easily guessable passwords can be exploited, allowing unauthorized access to the system.

Business Impact:

Security risks: Opening port SSH can expose the system to potential security threats if not properly secured. Attackers may attempt to compromise the SSH service, exploit vulnerabilities, or use brute force attacks to gain unauthorized access to the system.

Compliance concerns: Depending on the industry and regulatory requirements, open SSH ports may violate security standards. Organizations need to ensure they comply with relevant regulations and protect sensitive data

- **CWE - 200: Exposure of Sensitive Information to an Unauthorized Actor**
- **OWASP Category: A01:2021 – Broken Access Control**

Description:

Opening port 8083 on a system may expose it to certain vulnerabilities, depending on the specific services running on that port. Here are some potential vulnerabilities associated with an open port 8083:

-**Misconfigured or vulnerable service**: If there is a service running on port 8083, it could have misconfigurations or security vulnerabilities. Attackers could potentially exploit these vulnerabilities to gain unauthorized access, execute arbitrary code, or manipulate sensitive data.

-Information disclosure: Depending on the service listening on port 8083, there may be a risk of unintentional information disclosure. If the service is not properly secured, sensitive data could be exposed, leading to privacy breaches or unauthorized access to confidential information.

-Brute-force attacks: If port 8083 is open, it might be the default port for a service that requires authentication. Attackers could launch brute-force attacks attempting to guess usernames and passwords to gain access to the system.

Business Impact:

Increased network vulnerability: Open ports can be potential entry points for hackers and unauthorized access to a network. If port 8083 has security vulnerabilities, it can lead to data breaches or unauthorized activities within the business network.

Increased risk of malware or viruses: If port 8083 is left open, it can expose the network to various malware or virus attacks that specifically target open ports. This can result in compromised systems, data loss, or disruptions to business operations.

Compliance and regulatory concerns: Depending on the industry or nature of the business, there might be specific regulations or compliance requirements that dictate which ports should be closed or restricted. Having an open port 8083 without proper justifications can lead to non-compliance and potential legal consequences.