Common OpenVAS Vulnerabilities and Remediation Guide

Critical Web Application Vulnerabilities

1. SQL Injection

Description: Allows attackers to manipulate database queries through unsanitized user input. **Impact:** Complete database compromise, data theft, unauthorized access. **Fix:**

- Implement parameterized queries/prepared statements
- Use input validation and sanitization
- Apply principle of least privilege for database accounts
- Enable SQL injection detection in WAF

2. Cross-Site Scripting (XSS)

Description: Malicious scripts injected into web applications execute in users' browsers. **Impact:** Session hijacking, credential theft, malicious redirects. **Fix:**

- Implement proper output encoding for all user data
- Use Content Security Policy (CSP) headers
- Validate and sanitize all user inputs
- Enable XSS protection in browsers

3. Directory Traversal

Description: Access files outside intended directory structure using path manipulation. **Impact:** Exposure of sensitive files, configuration data, source code. **Fix:**

- Validate file path parameters
- Use canonical path resolution
- Restrict file system permissions
- Implement proper access controls

4. File Upload Vulnerabilities

Description: Unrestricted file uploads allowing execution of malicious code. **Impact:** Complete server compromise, malware deployment. **Fix:**

- Implement file type validation
- Store uploads outside web root

- Scan files for malware
- Set non-executable permissions

Network and Service Vulnerabilities

5. Unencrypted Protocols

Description: Services using plaintext protocols (Telnet, FTP, HTTP, SNMP v1/v2). **Impact:** Credential interception, data eavesdropping. **Fix:**

- Migrate to encrypted alternatives (SSH, SFTP, HTTPS, SNMPv3)
- Disable legacy protocols
- Implement network segmentation
- Use VPN for remote access

6. Default Credentials

Description: Systems using manufacturer default usernames and passwords. **Impact:** Unauthorized administrative access. **Fix:**

- Change all default passwords immediately
- Implement strong password policies
- Use unique credentials per device
- Enable account lockout policies

7. Unnecessary Open Ports/Services

Description: Running services that are not required for system operation. **Impact:** Expanded attack surface, potential exploitation. **Fix:**

- Conduct service inventory and disable unused services
- Implement host-based firewalls
- Regular port scans and service audits
- Follow principle of least functionality

8. SMB/NetBIOS Vulnerabilities

Description: Weak SMB configurations, null sessions, anonymous access. **Impact:** Information disclosure, credential attacks, lateral movement. **Fix:**

- Disable SMBv1 protocol
- Configure proper authentication requirements

- Restrict anonymous access
- Implement SMB signing

SSL/TLS Configuration Issues

9. Weak SSL/TLS Configurations

Description: Use of deprecated protocols, weak ciphers, or improper certificate configurations. **Impact:** Man-in-the-middle attacks, data interception. **Fix:**

- Disable SSLv2, SSLv3, and weak TLS versions
- Use strong cipher suites only
- Implement proper certificate validation
- Enable HSTS headers

10. SSL Certificate Problems

Description: Expired, self-signed, or improperly configured certificates. **Impact:** Trust issues, potential MITM attacks. **Fix:**

- Use valid certificates from trusted CAs
- Implement certificate monitoring
- Configure proper certificate chains
- Set appropriate certificate lifespans

Operating System Vulnerabilities

11. Missing Security Patches

Description: Outdated systems lacking critical security updates. **Impact:** System compromise through known exploits. **Fix:**

- Implement automated patch management
- Establish regular patching schedules
- Test patches in staging environments
- Maintain patch inventory and tracking

12. Weak Authentication Mechanisms

Description: Poor password policies, no account lockouts, weak local accounts. **Impact:** Brute force attacks, unauthorized access. **Fix:**

- Enforce strong password complexity

- Implement account lockout policies
- Use multi-factor authentication
- Regular password policy audits

13. Privilege Escalation Vulnerabilities

Description: Local vulnerabilities allowing normal users to gain administrative rights. **Impact:** Complete system compromise from limited access. **Fix:**

- Apply security patches promptly
- Implement least privilege access
- Use application whitelisting
- Monitor for suspicious privilege changes

Information Disclosure Issues

14. Banner Grabbing/Version Disclosure

Description: Services revealing detailed version information in banners or headers. **Impact:** Assists attackers in identifying specific exploits. **Fix:**

- Customize service banners to remove version info
- Configure minimal HTTP headers
- Use security headers to hide server details
- Implement banner randomization where possible

15. Directory Listing Enabled

Description: Web servers configured to show directory contents when no index file exists. **Impact:** Information disclosure, potential sensitive file exposure. **Fix:**

- Disable directory browsing in web server configuration
- Ensure index files exist in all directories
- Implement proper access controls
- Use URL rewriting to hide directory structure

16. Backup and Temporary Files

Description: Accessible backup files, logs, or temporary files containing sensitive data. **Impact:** Information disclosure, credential exposure. **Fix:**

- Remove unnecessary backup files from web directories

- Implement proper file cleanup procedures
- Use appropriate file permissions
- Regular cleanup of temporary files

Network Security Vulnerabilities

17. DNS Zone Transfer

Description: Misconfigured DNS servers allowing unauthorized zone transfers. **Impact:** Network reconnaissance, infrastructure mapping. **Fix:**

- Restrict zone transfers to authorized servers only
- Use DNS security extensions (DNSSEC)
- Implement DNS filtering and monitoring
- Separate internal and external DNS

18. SNMP Community Strings

Description: Default or weak SNMP community strings allowing unauthorized access. **Impact:** Network device information disclosure, potential configuration changes. **Fix:**

- Change default community strings
- Use SNMPv3 with encryption
- Implement access control lists
- Disable SNMP if not required

Database Vulnerabilities

19. Database Misconfigurations

Description: Insecure database configurations, weak authentication, excessive privileges. **Impact:** Data breach, unauthorized data modification. **Fix:**

- Implement database hardening guidelines
- Use strong authentication mechanisms
- Apply principle of least privilege
- Enable database activity monitoring

20. Database Injection Flaws

Description: Various injection attacks beyond SQL injection (NoSQL, LDAP, etc.). **Impact:** Data compromise, unauthorized access, system compromise. **Fix:**

- Implement input validation for all database interactions
- Use parameterized queries for all database types
- Apply output encoding
- Regular security testing

Remediation Best Practices

Immediate Actions

1. **Prioritize Critical Vulnerabilities:** Address CVSS 9.0+ scores first
2. **Patch Management:** Implement automated patching for critical systems
3. **Access Control:** Review and restrict administrative access
4. **Network Segmentation:** Isolate critical systems from general network

Long-term Strategies

1. **Security Baseline:** Establish hardened system configurations
2. **Regular Scanning:** Schedule recurring vulnerability assessments
3. **Security Training:** Educate development and operations teams
4. **Incident Response:** Prepare procedures for vulnerability exploitation

Monitoring and Validation

1. **Remediation Verification:** Re-scan systems after fixes
2. **Continuous Monitoring:** Implement real-time security monitoring
3. **Metrics Tracking:** Monitor vulnerability remediation timelines
4. **Regular Audits:** Conduct periodic security assessments

The key to effective vulnerability management is establishing a systematic approach that combines automated scanning, prioritized remediation, and continuous monitoring to maintain a strong security posture against evolving threats.