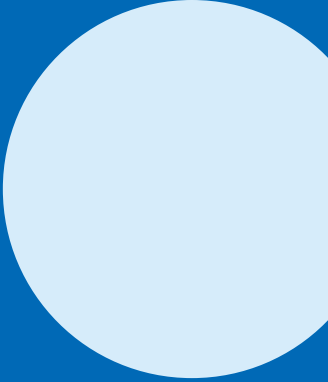




VULNERABILITY ASSESSMENT AND PENETRATION TESTING SERVICES

A Complete Guide for Businesses

Strengthen Your Cybersecurity. Identify Risks. Protect Your Business.

In today's digital environment, cybersecurity is essential for every business. Vulnerability Assessment and Penetration Testing (VAPT) helps organisations identify security weaknesses and take proactive steps to protect their digital infrastructure.

Presented by

Qdexi Technology

Professional IT and Cybersecurity Solutions for Modern Businesses

What Is Vulnerability Assessment and Penetration Testing?

Businesses depend on websites, applications, networks, cloud platforms, and digital systems to operate efficiently. However, security vulnerabilities in these environments can expose sensitive information to cyber threats.

Vulnerability Assessment and Penetration Testing Services help businesses evaluate their security posture and identify potential weaknesses before they become serious problems.

1. Vulnerability Assessment

A vulnerability assessment involves identifying, analysing, and prioritising potential security weaknesses in IT systems, applications, networks, and infrastructure.

2. Penetration Testing

Penetration testing is an authorised security exercise that simulates potential cyberattacks to determine whether identified vulnerabilities can be exploited.

Together, these processes provide businesses with a clearer understanding of their security risks and help security teams plan appropriate improvements.

Why Businesses Need VAPT Services

Cybersecurity risks can affect businesses of every size. Weak passwords, outdated software, misconfigured systems, and application vulnerabilities may create opportunities for unauthorised access.

- Identify weaknesses in IT infrastructure.
- Discover potential security gaps in web and mobile applications.
- Evaluate the effectiveness of existing security controls.
- Understand the possible impact of identified vulnerabilities.
- Prioritise security improvements based on risk.
- Support cybersecurity compliance and internal security policies.
- Reduce exposure to preventable security threats.

Proactive security testing helps organisations understand their risks before attackers can potentially exploit them.

What Does VAPT Include?

1. Network Vulnerability Assessment

Examines network devices, servers, and infrastructure for potential weaknesses, outdated configurations, and exposed services.

2. Web Application Security Testing

Reviews web applications for common security issues that may affect user data, authentication, access controls, and application functionality.

3. Mobile Application Testing

Assesses mobile applications for weaknesses involving data storage, communication, authentication, and application configurations.

4. Cloud Security Assessment

Examines cloud environments for potential configuration issues, access-control weaknesses, and security risks.

5. Internal and External Penetration Testing

Authorised testing can evaluate security from both external and internal perspectives, depending on the agreed scope.

6. API Security Testing

Assesses APIs for potential weaknesses involving authentication, authorisation, data exposure, and request handling.

How Does the VAPT Process Work?

Step 1: Planning and Scoping

Identify systems to be tested, define objectives, establish permissions, and agree on testing boundaries.

Step 2: Information Gathering

Collect relevant information about the target environment, architecture, technologies, and potential exposure.

Step 3: Vulnerability Identification

Use security tools and manual techniques to identify potential vulnerabilities within the agreed testing scope.

Step 4: Security Testing

Perform authorised penetration testing to assess whether selected vulnerabilities can be exploited under defined conditions.

Step 5: Risk Analysis

Review and prioritise findings according to severity, potential impact, and likelihood of exploitation.

Step 6: Reporting and Recommendations

Provide a detailed report covering vulnerabilities, supporting evidence, risk levels, and recommended remediation steps.

Step 7: Remediation and Retesting

After corrective actions, retesting can help verify whether identified vulnerabilities have been addressed.

Key Benefits of VAPT Services

Better Visibility into Security Risks

VAPT helps businesses understand where vulnerabilities may exist across their digital infrastructure.

Improved Security Planning

Detailed findings allow IT and security teams to prioritise improvements based on identified risks.

Protection of Sensitive Information

Identifying security weaknesses can help organisations strengthen controls designed to protect confidential business and customer data.

Stronger Application Security

Testing helps development and security teams identify potential weaknesses in applications and APIs.

Support for Compliance Requirements

VAPT reports may support internal audits, security assessments, and certain regulatory or contractual requirements. Specific obligations depend on the organisation and applicable standards.

Increased Security Awareness

Security testing helps businesses better understand their exposure to potential cyber threats and the importance of ongoing security management.

Security Weaknesses Businesses Should Watch For

Vulnerability	Potential Security Concern
Weak Authentication	Unauthorised access to accounts
Broken Access Controls	Users accessing restricted resources
Outdated Software	Exposure to known security weaknesses
Misconfigured Servers	Unnecessary exposure of systems or services
Insecure APIs	Unauthorised data access or manipulation
Sensitive Data Exposure	Improper protection of confidential information
Injection Vulnerabilities	Untrusted input affecting application behaviour
Security Misconfigurations	Weak or incorrectly implemented security controls

Not every vulnerability exists in every environment. A professional assessment helps determine which risks are relevant to a particular business.

Important: VAPT should always be conducted with proper authorisation and clearly defined testing boundaries.

How to Choose a VAPT Service Provider

Technical Expertise

Look for professionals with experience in network, application, cloud, and infrastructure security testing.

Defined Testing Scope

Ensure the provider clearly explains what systems, applications, and environments will be assessed.

Detailed Security Reports

Reports should explain vulnerabilities, potential impact, severity, evidence, and recommended remediation actions.

Secure Testing Practices

The provider should follow authorised testing procedures and take appropriate steps to minimise disruption to business operations.

Retesting Support

Post-remediation testing can help confirm whether previously identified vulnerabilities have been resolved.

Confidentiality and Data Protection

Businesses should understand how assessment data, credentials, reports, and sensitive information will be handled.

A clear scope, transparent communication, and actionable reporting are essential for a well-managed VAPT engagement.

Strengthen Your Business Security with Qdexi Technology

Qdexi Technology supports modern businesses with IT and cybersecurity solutions designed to address evolving technology and security requirements.

Our **Vulnerability Assessment and Penetration Testing Services** can help organisations identify potential security weaknesses, understand their risk exposure, and plan appropriate security improvements.

Our Cybersecurity Support Includes

- Vulnerability Assessment and Penetration Testing
- Network and Infrastructure Security
- Web Application Security Testing
- Cloud Security Support
- Security Monitoring and Incident Response
- Backup and Disaster Recovery Solutions
- IT Support and System Administration

Contact Qdexi Technology today to discuss your VAPT requirements.

Your digital infrastructure deserves a proactive security approach.

Vulnerability Assessment and Penetration Testing Services can help your business identify potential weaknesses, improve security visibility, and take informed steps toward stronger cybersecurity.

Whether you need application testing, network security assessment, cloud security evaluation, or a customised VAPT plan, Qdexi Technology can help you explore suitable cybersecurity solutions.

Get Started with Qdexi Technology

Call | WhatsApp us – 011-43053855

Web: www.qdexitechnology.com

Email Address: contact@qdexitechnology.com

Qdexi Technology

Your Technology Partner for Modern Business Security

Identify Vulnerabilities. Strengthen Security. Support Business Continuity.