



# asure**SECURE**<sup>TM</sup>

*Delivering Bespoke Penetration Testing and Vulnerability Assessment Services*

The TVS asureSECURE team are passionate about delivering bespoke penetration testing and vulnerability assessment services tailored to your unique requirements for the following major domains:

- Web Application Penetration Testing (internal and external)
- Mobile Application Penetration Testing

## Web Application Penetration Testing

A TVS Penetration Test simulates an attack on web applications. The TVS team will thoroughly search for exploitable vulnerabilities to determine the realistic threats to your data confidentiality, integrity, and availability. This testing mimics the actions of malicious attackers exploiting weaknesses in the applications, without actually causing the harm they would.

The TVS penetration tests satisfy the compliance requirements of ISO 27000, HIPAA, PCI:DSS and NIST.

## External Penetration Testing

External penetration testing is performed without prior knowledge of the internal structure/design/implementation of the system being tested. The objective is to discover vulnerabilities that could be exploited by external users without credentials or the appropriate rights to access a system.

## Our Approach

- Information gathering to map the application
- DNS analysis & DNS Brute-forcing
- Port scanning
- System fingerprinting to determine the technology in use
- Services probing
- Exploit research
- Manual vulnerability testing and verification of identified vulnerabilities
- Intrusion detection / prevention system testing
- Password service strength testing
- Remediation retest (optional)

## The Benefits of External Penetration Test

- Easy to identify architecture and design flaws in the application
- Improve business continuity
- Minimize Black Hat (malicious) attacks
- Protect clients, partners and third parties
- Protect public relationships and brand issues



## Internal Penetration Testing

Internal penetration testing is performed with knowledge of the internal structure/design/implementation of the system being tested. The major difference to external penetration testing is the tester doesn't need to spend time discovering the architecture of the system and therefore works from the point when an initial intrusion has occurred to discover if that can be escalated into breaches.

### Our Approach

- OWASP application security verification standard testing
- Internal application scanning
- System fingerprinting
- Services probing
- Exploit research
- Manual vulnerability testing and verification
- Manual configuration weakness testing and verification
- Application layer testing
- Users privileges escalation testing
- Password strength testing
- Database security controls testing
- Third-party / vendor security configuration testing

### Benefits of Internal Penetration Testing

- Improved Risk Management
- Minimize vulnerabilities to external and internal attacks
- Improve business continuity
- Minimize client-side attacks
- Protect clients, partners and third parties
- Comply with regulation or security standard certification (ISO 27001, PCI:DSS, NIST and HIPAA)
- Evaluate security investment
- Protect public relationships and brand issues

### Our Deliverables

#### Web Application Penetration Testing

- **Executive Summary:** Overview of the testing and to what extent the objectives were met, with a brief explanation of the threats facing the organization from a business perspective.
- **Testing Standards:** This section will identify any regulatory or policy security standards applied such as OWASP, NIST, SANS, PCI:DSS, DoD, HIPAA, COBIT.
- **Findings:** A detailed, technical explanation of the findings of the tests, with steps and proofs of the findings for each vulnerability.
- **Reference & Recommendations:** This section provides final recommendations and references the issues found in the security test.

## Mobile Application Penetration Testing

TVS asureSECURE provides comprehensive penetration testing services for mobile applications. We can help you evaluate the overall security posture of your Mobile Application and the associated services. Our mobile security services are compatible to across all platforms.

### Our Approach

- Identifying transport insecurities.
- Identifying insecure storage.
- Exposing security model weaknesses.
- Testing for runtime manipulation.
- Testing inter-process communication.
- Testing for injection, tap-jacking, weak trust boundaries, insecure services, and unprotected or misconfigured component vulnerabilities.
- Testing potential implementation insecurities within personally identifiable information, cryptography, data leaks, native code, and memory corruption.
- Application level security testing.

### Benefits of Mobile Penetration Testing

- Standards Based – Our penetration tests are based on Industry Security Standards and Best Practices such as OWASP
- Experience information security consultants - We are specialize in mobile application penetration testing
- State of the art Tools – We leverage state of the art commercial, open source & proprietary tools.
- Efficient & Cost Effective - We provide a one stops comprehensive mobile application penetration testing and leverage on a team of experience information security consultant to meet tight schedules and budgets.
- Safe approach - We adopt a safe approach to evaluate the security of your mobile applications to understand hacker mentality without disruption to your business operation.

### Our Deliverables

#### Mobile Application Penetration Testing

- **Executive Summary:** Overview of the testing and to what extent the objectives were met, with a brief explanation of the threats facing the organization from a business perspective.
- **Testing Standards:** This section will identify any regulatory or policy security standards applied such as OWASP, NIST, SANS, PCI:DSS, DoD, HIPAA, COBIT.
- **Findings:** A detailed, technical explanation of the findings of the tests, with steps and proofs of the findings for each vulnerability.
- **Reference & Recommendations:** This section provides final recommendations and references the issues found in the security test.

asure**SECURE**<sup>TM</sup>

[security@testandverification.com](mailto:security@testandverification.com)  
<http://asuresecure.testandverification.com/>