Building Security Into Your Applications

asureSECURE™

Upskill your own staff to enable them to deliver secure software applications

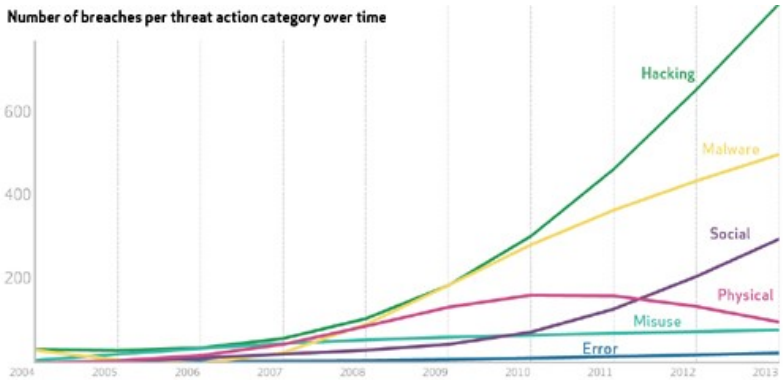
Malicious attacks that target the security vulnerabilities of business applications now represent a serious risk that conventional perimeter defences such as Firewalls, Intrusion Detection and Prevention Systems are unable to defend against. The latest breed of sophisticated attackers are now focused on exploiting web application security vulnerabilities and are investing in the tools and techniques for detecting and exploiting them. This means the security battle can be lost and your business put at risk if your development and test teams don't possess the latest skills required to effectively design, code and test applications that can defend themselves from attack.

The Security Concerns

Recent research highlights just some of the vulnerabilities;

- More software, more vulnerabilities. The respected Common Vulnerability and Exposures database lists over 68,000 recognized code vulnerabilities.(1)
- The MITRE Common Weakness Enumeration database exposes the 719 mistakes that applications developers can, and do make.(2)
- 96% of applications contain vulnerabilities with on average 14 per application.(3)
- Over half of organisations lack the knowledge needed to protect against today's sophisticated cyber-attacks, according to research by Symantec and Deloitte.

As a direct result of these vulnerabilities breaches are increasing in volume and impact, as shown by the Verizon graph below. Most security spending is still focused on network perimeter defences,(4) but the majority of breaches are now through applications as a result of security vulnerabilities not picked up during development or test. The majority of system testers have little or no working knowledge of application security and as reported by CISCO, the skills shortage is acute.



The TVS Solution

To help companies address these security concerns and protect against vulnerabilities TVS has designed a comprehensive suite of security; training, coaching, testing and project review packages that ensure your staff have the right skill-sets to be able to build effective security defences directly into you applications.

Notes:

1. https://cve.mitre.org/data/downloads/allitems.html
2. http://cwe.mitre.org/data/slices/2000.html
3. From OWASP
4. From Cenzic

Sample Penetration Report & Security White Papers

Download from our website now

TVS
Test and Verification Solutions

www.TESTANDVERIFICATION.com

e: info@testandverification.com

@testandverif

The TVS Solution

Our in-house security experts will help you to better understand what you can do internally to build security into your applications, how to test for vulnerabilities and what you should outsource to experts:

- Your developers can learn to build applications designed and coded with security in mind.
- Your testers can include security testing throughout the Security Development Life Cycle.
- You can make more cost efficient use of resources concentrating expert security consultancy spending on the most difficult tasks, once project teams know how to undertake non-expert security tasks.

The Advantages

- More secure applications that have been built with inherent security qualities from the start, instead of only patched up after vulnerabilities and breaches are discovered.
- Reduced costs
  - More in-house effort = less external consultancy spending
  - Fewer breaches = fewer recovery and reactive security costs.
- Better use of external security consultancy by transferring significant security skills into your project teams and reducing long-term dependency on external consultants.

The TVS Package

- Initial Training
  - Developer training – see details opposite.
  - Tester training - see detail opposite.
- A Review Package
  - Review or establish a security test framework for your security policies, standards and development practices, making recommendations for improvement as appropriate .
  - Establish a common threat and countermeasure taxonomy of terms.
  - Perform threat modelling for your applications.
- A Coaching Package
  - Add a coach into your projects to ensure that training is embedded into the development and testing processes.
  - Build processes into your projects to ensure that security considerations are embedded in your development practices.
  - Our coaching covers various aspects of application security testing such as: deriving risk-driven security test requirements through use and misuse cases; establishing security requirements and risk documentation; identifying gaps in security controls; performing and guiding SDLC-integrated tests to validate security requirements; perform offsite penetration testing; conduct periodic health-checks for maintenance and operations
- A Penetration Testing Package
  - TVS also offers specialist penetration testing services to complement your in-house capability developed through our training and coaching.

The Developer Security Training Package

An initial one-day training course on the Open Web Application Security Project (OWASP) Top-Ten security vulnerabilities. This will ensure developers understand the most critical generic security flaws and how to prevent them in design and coding. These are currently:

- Injection
- Broken Authentication and Session Management
- Cross-Site Scripting (XSS)
- Insecure Direct Object References
- Security Misconfiguration
- Sensitive Data Exposure
- Missing Function Level Access Control
- Cross-Site Request Forgery (CSRF)
- Using Known Vulnerable Components
- Un-validated Redirects and Forwards

The Coaching Package

- Conducting an application security threat modelling exercise to identify the potential security threats that need to be guarded against.
- Specifying prioritized controls (security requirements) to prevent threats from becoming exploitable.
- Validating security requirements.
- Understanding secure design practices and reviewing designs for security.
- Understanding and applying the Application Security Verification Standard (ASVS) for more effective application security configuration and testing. The ASVS is a 168 checkpoint system for targeted verification of the following areas:
  - Authentication
  - Session Management
  - Access Control
  - Malicious Input Control
  - Cryptography at Rest
  - Error Handling and Logging
  - Data Protection
  - Communications Security
  - HTTP Security
  - Malicious Control
  - Business Logic
  - Files & Resources
  - Mobile

The Tester Security Training Package

An initial one-day training course on the Open Web Application Security Project (OWASP) Top-Ten security vulnerabilities. This will ensure testers understand the most critical generic security flaws and how to test for them. These are currently:

- Injection
- Broken Authentication and Session Management
- Cross-Site Scripting (XSS)
- Insecure Direct Object References
- Security Misconfiguration
- Sensitive Data Exposure
- Missing Function Level Access Control
- Cross-Site Request Forgery (CSRF)
- Using Known Vulnerable Components
- Un-validated Redirects and Forwards

Penetration Testing Package

External Penetration Testing

External penetration testing consists of a review of vulnerabilities that could be exploited by external users without credentials or the appropriate rights to access a system.

Approach:

- Footprinting
- Public Information & Information Leakage
- DNS Analysis & DNS Brute-forcing
- Port Scanning
- System Fingerprinting
- Services Probing
- Exploit Research
- Manual Vulnerability Testing and Verification of Identified Vulnerabilities
- Intrusion Detection/Prevention System Testing
- Password Service Strength Testing
- Remediation Retest (optional)

Benefit of External Penetration Test:

- Easy to identify architecture and design flaws of application
- Increase Business Continuity
- Minimize Black Hat Attacks
- Protect Clients, Partners and Third Parties
- Protect Public Relationships and Brand Issues

Internal Penetration Testing

Internal penetration testing provides protection from internal threats and ensures that internal user privileges cannot be misused. The target is typically the same as external penetration testing, but the major differentiator is the "attacker" either has some sort of authorized access or is starting from a point within the internal network.

Insider attacks have the potential of being much more devastating than an external attack because insiders already have the knowledge of what's important within a network and where it's located, something that external attackers don't usually know from the start.

Approach:

- OWASP ASVS standard testing
- Internal Application Scanning
- Port 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

Benefit of Internal Penetration Test:

- Manage Risk Properly
- Minimize the External and Internal attacks
- Increase Business Continuity
- Minimize Client-side Attacks
- Protect Clients, Partners and Third Parties
- Comply With Regulation or Security Certification (27K,PCI:DSS,NIST and HIPPA)
- Evaluate Security Investment
- Protect Public Relationships And Brand Issues

Deliverables

- Upskilled development and test teams that are capable of building security into applications and providing assurance that it is built in
- A comprehensive document explaining what the OWASP Top-Ten application security vulnerabilities are, and how to test them.
- A concise report of the review of the security development lifecycle, policy and standards with recommendations.
- The ASVS assessment tool for measuring security strengths and weaknesses, plus identifying context-specific training needs.
- In addition, the test team will be guided in the production of a product threat model, security requirements (controls) and the development and execution of application security tests.

The asureSECURE Approach

asureSECURE helps companies develop the right mind-set to think like attackers trying to break application security and treating application security as part of the normal systems development and maintenance process rather than the costly alternative of reacting to a breach.

- Application Security
- Security by Design
- Security by Coding
- Security by Testing
- Coaching and Training
- Targeted Penetration Testing
- Application Sensors
- Code Scanning
- Manual Code Inspection
- Outsourced Testing

Assertive Testing

Assertive Testing is an important element of the asureSECURE offering and represents a paradigm shift in the organisational approach to security and uses proactive and preventative development techniques to avoid costly reactive and remedial responses to strategic security issues. Our Assertive Testing technique changes the paradigm which has until now established passive acceptance of poor security requirement specifications. Assertive Testers coached by TVS will object if presented with requirements that only capture what the customer wants to do, and contain little to prevent attackers from doing what they would like to do through misuse. The Assertive Tester makes statements such as: "In order to test this system for security I need you to explain how and where un-trusted data is validated". Using this approach enables security to be leveraged into projects by Assertive Testing which permanently changes the whole project team philosophy towards building secure applications.

Penetration Testing

asureSECURE offers cost-effective Penetration Testing that harmlessly mimics the investigations and attack vectors used by malicious hackers. We go beyond automated scanning and make intelligent use of tools combined with human expertise in our inspections.

Embedded Security Solutions

Semiconductor chip vendors and product manufacturers face ever increasing demands to adopt a stronger system wide security approach and require proven and reliable solutions that are capable of passing a variety of certifications. Through a strategic partnership with Embedded Security Solutions, a specialist embedded security consultancy, TVS is now able to help companies achieve first-pass silicon success and address the needs of emerging market such as the IoT (Internet of Things) by systematically tackling the complexities introduced by the increasing demand for both hardware and software to meet the latest security requirements.

About TVS

Test and Verification Solutions Ltd (TVS) provides services and products to organisations developing complex hardware and software products that need to be: fit for purpose, safe and secure.

TVS operates globally with offices in the UK, France, Germany, India, Singapore the USA and through a network of international partners.

Find out More

For more information on our asureSECURE service, including Security Coaching and Penetration Testing or to discuss you security requirements in more detail, please Contact Us.

asureSECURE™ http://asuresecure.testandverification.com/