E COM SECURITY®
SOLUTIONS

www.ecomsecurity.org

E Com Security Solutions

Application Security Portfolio

Learn how our applicaiton security portfolio can help you establish a secure foundation for better business outcomes.

Overview:

- Protect the confidentiality and integrity of your software
- Protect your IT resources and the business continuity of your operations
- Provide validation to meet your compliance requirements

Overview

Every enterprise's application landscape is now both business critical and rapidly expanding. Mobile and cloud computing are dramatically changing the way we do business. Today, the world runs on applications, and, as a result, every company is becoming a software company – regardless of its primary business. Organizations often lack the internal resources and expertise to keep up on an ever-changing security and regulatory landscape let alone test and assess their networks, applications and overall security programs. They need help elevating their security profile, reducing risk and achieving compliance with applicable laws and industry mandates. Our application penetration testing services deliver the independent expertise, experience and perspective you need to enhance your security posture, reduce your risk, facilitate compliance and improve your operational efficiency.

Roadmap to reduced risk

Application Security Assessments provide assurance that your mobile applications, web applications and APIs are secure. Leveraging our deep knowledge of the Tactics, Techniques and Procedures (TTP) threat actors use, our security consultants assess and test the state of your applications and provide actionable recommendations to enhance their security. A software "vulnerability" is an unintended flaw or weakness in the software that leads it to process critical data in an insecure way. By exploiting these "holes" in applications, cybercriminals can gain entry into an organization's systems and steal confidential data.

E Com Security Solutions Software Security Report revealed that about 70 percent of all applications had at least one vulnerability classified as one of the top 10 web vulnerability types which include commercial software, financial services software, software written by government agencies etc. all can be vulnerable Whether your custom applications have been developed in-house or commissioned through a third-party agency, time constraints and a lack of awareness around security best practice can often result in an application that puts the integrity and confidentiality of your corporate information and systems at risk of compromise. And enterprises are producing these applications faster than ever before, often using Agile development processes and then augmenting their internal development programs with third-party software and open source libraries and components. We provide a thorough security analysis of your custom application deployment and our penetration testing specialists will examine and assess all the key components of your application and supporting infrastructure.

Highlights

Continuous Assessment

Always-on risk assessment delivers:

- Alerts for newly discovered vulnerabilities
- Metrics to identify improvement in security measures over time
- Automatic detection and assessment of code changes to web applications

Zero False Positives

Verified, prioritized results eliminate false positives and streamlines the remediation process, including:

- Vulnerabilities are custom prioritized by risk – to target high priority issues
- Clear actions for fixing issues
- Eliminate triage of false positives & save valuable developer time & resources

Threat Research Center

Our security experts serve as an extension of your own website security team, providing:

- Direct access to a security engineer for remediation guidance
- Active management of your risk posture
- Proof of concepts for vulnerability exploits

Trending Analysis

Tacks real time and historical data to measure your risk exposure over time.

- At-a-glance view of exposure ratings and progress at closing vulnerabilities
- Customers range from start-ups to the Fortune 500
- Tens of thousands of simultaneous assessments
- Millions of vulnerabilities processed per week

E Com Security Solutions application security risk management practice delivers the independent expertise, experience and perspective you need to address your application security, risk and compliance concerns.

Application Security Portfolio

Application Security Assessments provide assurance that your web applications, mobile applications and API"s are secure. Our security consultants test the state of your applications and provide actionable recommendations to enhance your security posture. There are a variety of application security technologies available to help with this endeavor, but no one is a silver bullet. You need to gather the strengths of multiple analysis techniques along the entire application lifetime to drive down application risk. The end goal for any organization should be a mature, robust application security program that:

- Assesses every application, whether built in-house, purchased or compiled
- Enables developers to find and fix vulnerabilities while they are coding
- Takes advantage of automation and cloud-based services to more easily incorporate security into the development process and scale the program

Web Application Penetration Test

Our Application Penetration Testing and Security Assessment services can be employed to test your custom web applications as well as standard applications like antivirus, embedded applications, games, and other system applications. During application testing engagements, our consultants pursue the following goals:

- Explore weakness as a hacker & reveal security flaws resulting from implementation errors
- Assess application security versus attacks via multiple techniques
- Identify security design flaws and demonstrate the potential consequences
- Expose weaknesses stemming from application relationship to the the IT infrastructure
- Increase end-user confidence in the application's overall security

Web Services & Application Vulnerability Scanning

With Web vulnerability Assessment, we provide a non – invasive scanning that mimics real-world hacking techniques and attacks, and provides comprehensive dynamic analysis of complex web applications or solution based on Web Services technologies (e.g., SOAP or REST). Support modern technologies such as Mobile, Json, Rest, Soap, Html5 & Ajax. The Intelligent Scanning cover OWASP Top 10, SANS Top 25, OSSTMM, WASC.Given the complexity of Web services-based solutions, this service is highly customized and incorporates manual testing performed by professionals with vast experience in Web Services assessments.

Static / Source Code Security Assessment

Application Source Code review combines Static Analysis Security Testing (SAST) techniques with manual review and testing techniques of the target application, providing a deliverable with both tactical and strategic recommendations to improve the security posture of such target application. This level of testing validates the application layer security controls; the security effectiveness of software development and deployment standards by determining how resilient the web application is to determined attackers. This service includes:

- Pinpoint deficiencies in security controls
- Identify development errors that violate best-practices
- Identify development errors that lead to vulnerabilities
- Evaluate the third-party tools, applications, and libraries

Mobile App Security Assessment

Mobile application security solution combines automated code assessments with expert remediation services that enable IT teams to rapidly secure mobile applications in agile development environments — without slowing innovation. The goal is to:

- Provide risks in your mobile apps and helps you mitigate them through remediation guidance.
- Find risks in client-side / server-side code, third-party libraries, or underlying mobile platforms.
- Unique Behavioral analysis and privacy checks
- Supports all major smartphone platforms (including iOS, Android, Blackberry and Windows)

E Com Security solutions application security portfolio can help you meet information security best practices and your quarterly and annual compliance frameworks including PCI DSS, SOX, HIPAA, GLBA, FISMA, EI3PA.and ISO 27001/27002.

Unique Features

Business Logic Testing

Web Application Penetration testing subscribers receive special testing to find business logic vulnerabilities. This service entails:

- Creating a customized testing scheme developed and performed by security experts
- Mapping out your Web application, users, roles, and custom business workflow
- Identifying and validating account privileges across roles and between users
- Prioritizing vulnerabilities based on your business goals and intentions

Non Invasive Scanner Configuration and Continuous Tuning

Web Vulnerability scanning customization to ensure that scanner properly tests all forms and software languages, including Ajax/Web 2.0 requests and Rich Internet Applications, and to maximize scan coverage. This customization is designed to support a production-safe assessment-testing environment, including:

- Reviewing Web 2.0, rich Internet applications and Ajax requests
- Monitoring, tuning, and customizing scans to ensure thorough coverage

Accelerate Remediation

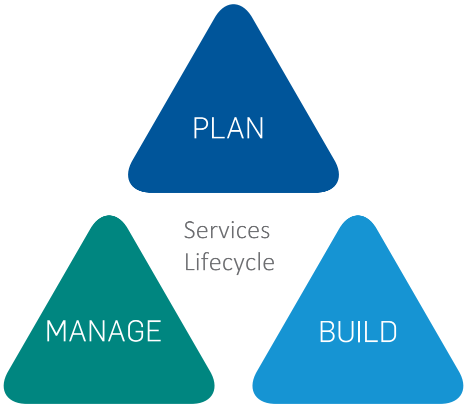
Application security soltutions delivers a proven, scalable, and affordable enterprise application security platform, accelerating the identification and remediation of Web application security vulnerabilities:

- Assess source code during development to uncover difficult-to-detect vulnerabilities in production, enabling remediation earlier in the development cycle.
- Full vulnerability verification by the TRC, which verifies the accuracy of all vulnerabilities, virtually eliminating false positives and dram atically simplifying remediation.

Production Safe

As a part of every subscription, members can alyze your Web application inputs, state-changing requests, and any sensitive functionality to customize testing for safety first, then for depth and coverage. Custom tuning of scans permits full coverage without performance impact, including:

- Eliminating any performance degradations—scanning payload is equivalent to a single user
- Assuring data integrity—using benign injections in place of live code



Get more out of your software—from planning to operation

E Com Security Solutions Professional Services support the lifecycle of software—from planning and implementation to ongoing operation of the system.

Security Consulting is available and ready when your organization would like to improve procedures and controls for current and future security challenges. Whether you need stronger internal controls to close security gaps and match best practices, or knowledge transfer for your people, we can quickly help you meet your information and network security needs.

Application Security testing framework

To ensure quality and consistency of results, the framework is designed to be comprehensive in nature to ensure all potential weaknesses in the application are properly assessed, but it is also flexible in testing methods and the specific tests that are performed to allow consultants to apply their expertise to the application being assessed. A summary of testing framework is shown below:

AUTHENTICATION	Directory permissions	INPUT DATA SANITIZATION
DESIGN FLAWS	HTTP Verb tampering	Script Injection
Authentication by pass Tests	Directory indexing	SQL Injection
Check for default accounts	Resource location	OS Command Injection
Transmission vulnerabilities	Path disclosure	LDAP Injection
Distribution	Source code disclosure	XSS Cross Site Scripting
Validation	Google hacking database	Injection flaws
Impersonation check	Path Traversal	Cross Site Request Forgery
Reflection checks	APPLICATION FUNCTIONALITY	Debug mode
IMPLEMENTATION FLAWS	Cache poisoning	Thread Safety
Open Login Mechanisms	Cross user defacement	Hidden Form Field Manipulation
Multistage Login Mechanisms	Object hijack	Cookie Security
Storage	CRPTOGRAPHIC EMPLOYMENT	Dangers of HTML Comments
MANAGEMENT FLAWS	Cryptanalysis	Malicious File inclusion
Credential management	Communication Security	Insecure Direct Object Reference
Privacy violation	Storage Security	Failure to restrict URL access
Key exchange	WEB SERVER	Insecure cryptographic usage
Login Management	SERVER CONFIGURATION	Insecure communications
ACCESS CONTROL	Environment related vulnerabilities	Command Injection
Privilege Management	Credential management	HTTP Response Splitting
Cross Site Request Forgery	Back-up Files and references	Arbitrary file creation
Secret Parameters	Web Server Components	Arbitrary file deletion
Forced Browsing	Common Paths	Code execution
Path Traversal	Application Admin Interfaces	Cookie manipulation
SESSION HANDLING MECHANISM	HTTP methods	CRLF Injection
SESSION TOKEN GENERATION	Proxying	Cross frame scripting
session prediction	SERVER SOFTWARE	Directory traversal
Session fixation	Virtual Hosting	File inclusion
SESSION TOKEN MAPPING	Canonicalization	File tampering
Session hijack	Path Traversal	Full path disclosure
Token mapping	APPLICATION ERROR HANDLING	URL Redirection
APPLICATION LOGIC	Uncaught Exception	Blind SQL / X Path Injection
Work flow patterns	Unchecked Error condition	BUSINESS LOGIC TEST COVERAGE
User privilege and bypass	Data in HTML	Identify logical threats
User access rights	Data Protection – SSL	Understand the functionality
Boundary value tests	Digital Certificate Validity and algorithms	Perform logical tests
INFORMATION EXPOSURE	Mis configuration	Check work flow patterns
Trojan shell script	Information Leakage	Verify bypass flaws
Cross site scripting in path	Exception handling	Verify flaws in user access rights

E Com Security Solutions Customer Support Engineers provide enterprise-class software support. You can access customer support by email, phone, or the Customer Support Portal.

Service Level Comparisons

Web Application Penetration Testing / Web APP & API Vulnerability Scan

	Web Application Penetration Test	**Web App / API Vulnerability Scan**
	For production websites that are mission-critical, with multistep forms and rigorous compliance requirements. All Vulnerability scan and business logic testing is included.	Foundational solution that covers all your website assets and protects basic, less-critical sites. It is a massively scalable "best value" solution designed to fit any environment.
	Service Benefits: Unlimited Support through out the annual subscription.	
Application Vulnerability Scan	Included	
Multi Scanners Usage	✓	✖
Validation Of Scan Results	✓	✓
Manual Verification of Scan Completeness	✓	✓
Manual Exploitation of findings	✓	✖
Verified, prioritized results eliminate false positives	✓	✓
Continuous assessment	✓	✓
PCI DSS Compliance	✓	✓
Highly scalable across the enterprise	✓	✓
Access to E Com Security Experts	✓	✓
Production safe	✓	✓
Scanner configuration and continuous tuning	✓	✓
Business logic testing	✓	✖
Proof of concepts for vulnerabilities	✓	✖
Video Evidence Demonstrations	✓	✖
Multi-level authentication testing	✓	✖
Findings Report	✓	✓
Prioritization guidance report	✓	✖
Platinum Support with a dedicated expert	✓	✓
Post-Test Debrief	✓	✓

E Com Security Solutions data centers are audited and certified regularly to assure compliance, including PCI DSS, ISO 27001 and SSAE 16 audited to keeping your data, secure.

Service Level Comparisons

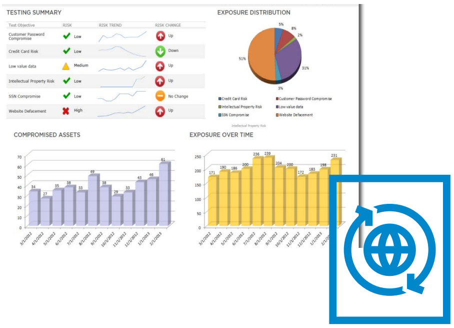
Source Code Security Assessment / Mobile App Security Assessment

	Source Code Security	Mobile App Security
	Assess source code directly, giving developers accurate vulnerability data and enabling them to fix code continuously throughout software development lifecycle (SDLC).	Enables enterprises to identify and remediate security vulnerabilities in any mobile application across all stages of the Mobile software development life cycle (SDLC).
	Service Benefits: Unlimited Support throughout the annual subscription.	
Verified, prioritized vulnerability results eliminate false positives	✓	✓
Preserves Intellectual Property	✓	✓
Detailed vulnerabilities reporting	✓	✓
Early risk remediation	✓	✓
Highly scalable across the enterprise	✓	✓
Unlimited assessments	✓	✓
Ease of use	✓	✓
Flexible assessment configuration	✓	✓
Broad repository support	✓	✓
Multi-level authentication testing	✓	✓
PCI DSS Compliance	✓	✓

Research-driven assessment methodologies that incorporate with the following standards

OWASP | Web Application Security Consortium | SANS | NIST National Institute of Standards and Technology U.S. Department of Commerce | CERT | the CENTER for INTERNET SECURITY

Strategic Recommendations and Reporting Functionalities

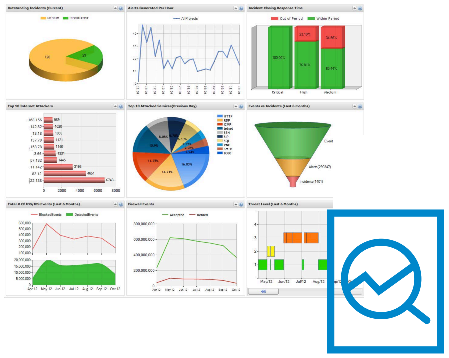


Test Objective	Risk	Risk Trend	Risk Change
Customer Password Compromise	Low		Up
Credit Card Risk	Low		Down
Low value data	Medium		Up
Intellectual Property Risk	Low		Up
SSN Compromise	Low		No Change
Website Defacement	High		Up

Powerful Reporting Features

E Com Security Solutions offers a variety of reporting functions to help meet internal reporting, audit, compliance and other needs, including:

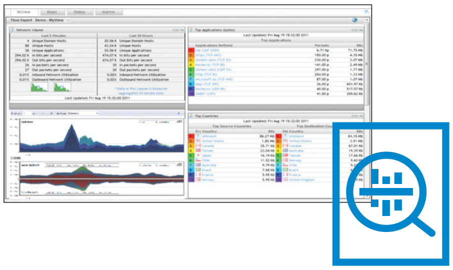
- Comprehensive Penetration test report consisting of Executive Summary and detailed vulnerability analysis, recommendations with prioritized action plan along with the Image and video based evidences will be delivered.
- Online Reporting and Metrics: Vulnerability data is captured through the portal, including risk, remediation status, data compromised and status across projects or for individual tests.
- Complete historical access to test results for trend analysis, providing insight into an organization’s security posture over time.
- Pre-set Reports: Online reporting includes executive summary, summary recommendations, detailed test methodology and findings.
- Custom Reporting: Users can build custom reports in a number of different ways such as by risk, by finding status, across a mix of projects, by custom fields, individual tests and test types.
- Common Vulnerability Scoring System (CVSSv2) Values for All Vulnerabilities: CVSS provides a standard method for risk ranking and prioritizing security vulnerabilities to streamline the remediation process.
- Multi-format Reports: Export report data in PDF, Excel, XML, CSV and HTML.


Outstanding Incidents (Current)
Alerts Generated Per Hour
Incident Closing Response Time
Top 10 Internet Attackers
Top 10 Attacked Services(Previous Day)
Events vs Incidents (Last 6 months)
Total # Of IDS/IPS Events (Last 6 Months)
Firewall Events
Threat Level (Last 6 Months)

Centralized Dashboard powered by Jira for ticketing functionality

Simplify the management of penetration tests, with at-a-glance views of project and test status and findings.

- Project and Test Drill Down: Display the relationship between projects and tests to easily organize enterprise security programs.
- Detailed Findings: Evidence including images and videos offers detailed walkthroughs of vulnerabilities. Slideshow presentation views explain security risks to key personnel in the organization.
- Attack Sequence Reporting: Graphically displays the relationships between multiple vulnerabilities and simplifies attack scenarios for easy understanding.
- Real-time Notification: E-mail alerts are sent instantly when tests change status and findings are identified or remediated.
- Secure Document Transfer: Securely share sensitive files such as code, network diagrams, media, etc.



Understand all findings and recommendations

A strong understanding of engagement findings and recommendations enables you to address the risks to your organization effectively. Security engagements often span multiple organizational groups and involve stakeholders outside of security and IT staff who do not understand the “native language” of IT security.

We understand this and provides jargon-free communication that is easily understood by nontechnical business leaders and auditors. Our consultants are “bilingual” and provide their findings and recommendations in language appropriate for all stakeholders, ensuring that risks are understood and properly addressed.

E Com Security®
Solutions

We would welcome the opportunity to discuss your security governance, risk management and compliance needs, and how we can help address your security management challenges. To set up an appointment, please contact your nearest E Com Security Solutions office.

MIDDLE EAST ASIA AUSTRALIA EUROPE AMERICAS

For further information visit: **www.ecomsecurity.org**