eSureITy

Web & Mobile Application Security Testing

Stop Vulnerabilities Before They Ship

Application Security Testing Built for Real-World Attacks, Not Just Checklists

Human-led web and mobile application testing that exposes privilege abuse, broken authorization, and data exposure before attackers or auditors do.

The Risk Your Software Development Lifetime Cycle Doesn’t Show You

Most teams rely on scanners, unit tests, and “happy path” QA. That stack catches bugs. It does not reliably catch the abuse paths attackers use:

- Users chaining “harmless” parameters to escalate privileges
- Forgotten debug endpoints that bypass authentication entirely
- Mobile apps leaking sensitive data in logs, caches, or backups
- Session and cookie issues that let attackers impersonate real users

As releases accelerate, the attack surface expands across web portals, APIs, and mobile apps. Your risk is no longer limited to “the app.” It’s:

- How the app handles identity, roles, and sessions
- How it enforces authorization across every function
- How it stores, transmits, and exposes sensitive data
- How it behaves in production, not just in a test lab

Attackers don’t care about your test plans. They care about the fastest path from “unauthenticated outsider” to “trusted insider with data access.”

Where Traditional App Testing Fails

Common breakdowns that leave teams exposed even when they believe they’re “covered”:

- Scanner-only testing – Automated tools flag noise and miss chained issues that require human interrogation.
- Permission blind spots – Features work in QA, but nobody tests what happens when a “basic user” changes parameters to act like an admin.
- Compliance without proof – Policies talk about secure coding, but there’s no evidence that production apps are tested for real-world exploit paths.
- Mobile as an afterthought – Web gets some testing; mobile gets almost none, despite holding tokens, keys, and cached data.

Result: vulnerabilities live in production for months. They’re discovered by attackers or external testers—not your team.

eSureity’s Web & Mobile Application Security Testing is built to surface those real-world failure paths, convert them into prioritized fixes, and give you defendable proof that applications have been tested where it matters: in production-like conditions, under adversarial pressure.

What You Get From an Engagement

A clear exploit narrative – How an attacker moves from “login page” to “data exposure,” step by step.

Prioritized remediation – Ranked by impact and exploitability, mapped to specific code and configuration changes.

Evidence you can show leadership and auditors – Screens, payloads, and logs that prove the risk and the fix.

Retest verification – Confirmation that high-risk issues are actually closed, not just “marked resolved” in a ticketing system.

Contact Us ✉ info@eSureITy.com 🌐 www.eSureITy.com

How We Test and Why It Matters

Web Application Security Testing

A Web Application Test is a focused series of security tests against your hosted application in a live or production-like environment. The goal: find the exact paths attackers would use to escalate privileges, exfiltrate data, or bypass controls.

Core Focus Areas

- **Application Security Review**
  - Architecture, roles, and trust boundaries
  - Authentication and session handling patterns
  - Input validation, output encoding, and error handling
- **Production Security Testing for Abuse Paths**
  - Privilege escalation and horizontal/vertical authorization abuse
  - Authorization creep across roles, modules, and tenants
  - Insecure input operations and business logic flaws
  - Security controls bypass via direct object references, forced browsing, or parameter manipulation

Technical Testing Components

- **Parameter Tampering Testing**
  - Manipulation of IDs, roles, pricing, and workflow parameters
  - Testing for forced browsing and insecure direct object references
- **Web Server Infrastructure Analysis**
  - Misconfigurations, default content, directory listings
  - Unsupported software, missing security headers, weak TLS configurations
- **Web Attack Signatures Testing**
  - Injection vectors (SQL, command, LDAP, template, XML)
  - Cross-site scripting (XSS), CSRF, deserialization attacks
- **Web Forms Vulnerabilities Testing**
  - Input validation and sanitization gaps
  - Authentication, password reset, and enrollment flows
- **Compliance-Oriented Analysis**
  - Alignment with secure coding and data handling expectations
  - Evidence to support internal policies and external assessments
- **Cookie Security Analysis**
  - Flags (Secure, HttpOnly, SameSite)
  - Session fixation and token exposure
- **File & Directory Exposure Checks**
  - Backup files, config files, logs, and temp artifacts exposed over HTTP
  - Access to admin panels, utilities, and dev endpoints

Mobile Application Security Testing

Modern mobile apps hold tokens, keys, and sensitive data that can be abused even without compromising the backend. eSureity's Mobile Security Testing targets both the app and its interactions with APIs and services.

How We Test

- Manual probing of app interfaces and flows
- Automated fuzzing of inputs and APIs
- Development of focused test datasets and harnesses
- Automated and assisted review of application code and behavior

Mobile Testing Scope

- **White Box (Full Disclosure) Mobile Testing**
  - Use of APK, IPA, or equivalent packages
  - Review with internal knowledge where beneficial to expose deeper issues
- **Mobile Application Exposure**
  - Data stored on the device (caches, logs, local databases, backups)
  - Credential, token, and key handling
- **Mobile Signature Attacks**
  - Tampering with requests, headers, and payloads
  - Replay and manipulation of signed or tokenized operations
- **Confidentiality Exposure Checks**
  - Leakage of sensitive information through logs, debug messages, and crash reports
  - Unencrypted storage and weak transport protections
- **Mobile Form Vulnerabilities**
  - Input validation and injection vectors
  - Authentication and session handling flows
- **Cookie and Token Exposure Checks**
  - WebView and browser integrations
  - Cross-app and cross-context token exposure
- **File & Directory Exposure Checks**
  - Insecure use of file storage and temporary directories
  - Artifacts that reveal environment details or user data

Why eSureity

- *Attacker-Mindset Testing* – Human-led testing focused on exploit paths, not just vulnerability lists.
- *Web + Mobile + API Perspective* – Applications are tested as part of an ecosystem, not in isolation.
- *Clear, Executable Output* – Findings written for both executives and engineers, with concrete remediation steps.
- *Security-First, Vendor-Neutral* – eSureity does not sell software. The outcome is a more secure application, not a product upsell.

Book a Web & Mobile Application Security Assessment with eSureity

Align testing with real-world threat behavior and convert your web and mobile apps from high-risk attack surface into defended assets.