Web Application Security Testing

Safeguard your web applications from potential threats with tailored testing solutions.

Contact Us

Web Application Security Testing

We offer tailored Web Application Security Testing services to safeguard your applications against vulnerabilities and threats:

Automated Web Application Vulnerability Scanning

- Fast, automated scanning to detect potential vulnerabilities.
- Price: €450 | Duration: 1.5 day (including report writing).
- Receive a detailed vulnerability report analyzed by experts, with actionable insights.

Black-Box Web Application Penetration Testing

- Emulates real-world attacks with minimal upfront knowledge, testing from an external attacker's perspective.
- Price: €600 + €300/additional day depending on complexity | Duration: 2 days minimum.
- A comprehensive mix of automated and manual testing, delivering a full vulnerability report with exploit paths and remediation recommendations.

Gray-Box Web Application Penetration Testing

- Combines user-level access with advanced manual testing to simulate insider threats and discover deeper vulnerabilities.
- Price: €900 + €300/additional day | Duration: 3 days minimum (scope defined in kick-off meeting).
- Provides in-depth security insights into business logic, privilege escalation, insider threats, and complex workflows.

Order Now

Explore Service Details

	Automated Vulnerability Scanning	Black-Box Penetration Testing	Gray-Box Penetration Testing
Prerequisites	URL/IP Address	URL/IP Address	URL/IP Address, User Credentials, Application Insights
Test Type	Automated	Automated and Manual	Automated and Manual with Internal Knowledge
Actions	Identify and Report vulnerabilities	Identify, Exploit and Report vulnerabilities	Identify, Exploit and Report vulnerabilities
Used Tools	Primarily automated scanning tools (industry-standard vulnerability and web application scanners)	Automated scanners + manual penetration testing techniques, leveraging exploitation frameworks and custom scripts	Full toolset including automated scanners, manual exploitation, custom scripts, and in-depth analysis with insider knowledge
Covered Vulnerabilities	• Vulnerable and outdated components • Broken authentication and session management • Sensitive data exposure • Injection flaws (SQL, XSS, OS, NoSQL, LDAP, HTML, JSON, XPath, XML) • Security misconfigurations • Insecure direct object references • Server-side request forgery (SSRF) • Broken Authorization • Unvalidated redirects and forwards • XML External Entities (XXE)	Includes all vulnerabilities from Automated Vulnerability Scanning, plus advanced issues discovered through manual exploitation: • Cross-site request forgery (CSRF) • Business logic flaws • Side-channel attacks • Design flaws • Zero-day vulnerabilities • Insecure deserialization	Includes all vulnerabilities from Black-Box Testing, with deeper insight enabled by authenticated access and application knowledge: • Privilege escalation paths (horizontal & vertical) • Insider threat scenarios • Complex application workflow flaws • Chained attack paths (multi-step exploitation combining several weaknesses) • Data access/control flaws beyond standard authorization • Advanced misconfigurations only visible with credentials

Reporting	Comprehensive Report with Automated findings with expert review and remediation guidance.	Comprehensive Report with vulnerability details, exploit paths, risk assessment, and Remediation Recommendations.	Comprehensive Report with vulnerability details, exploit paths, risk assessment, and Remediation Recommendations.
Duration	1.5 days	2 days minimum (depending on complexity)	3 days minimum (scope defined in kick-off meeting)
Price	**€450**	**€600 + €300/additional day**	**€900 + €300/additional day**
	Order Now	Order Now	Order Now

Step-by-Step Process

1. Order Service Request

The client orders a "Service Request" by completing the contact form, providing the details of the resources in scope, a brief project description, and contact information.

2. Scope Review & Kick-Off (if applicable)

We review the Service Request and, if necessary, schedule a 30-minute kick-off meeting to discuss the effort estimation, project timeline, and details regarding the in-scope resources. For Black-Box tests, we can proceed directly to the next step.

3. Contract and Payment

Once the details are agreed upon, we send the client a contract and invoice. After the contract is signed and payment is received, we begin the testing phase.

4. Testing Execution

Our expert team conducts a combination of automated and manual tests, simulating real-world attack scenarios to uncover vulnerabilities and assess security posture.

5. Report Delivery

Upon completion, you'll receive a comprehensive report detailing identified vulnerabilities, their severity levels, and actionable recommendations to enhance your security.

Subscribe to our newsletter

Email address

Your email address

Submit

Contact

Email: office@ethicsec.com

Socials:

Contact Us