AI Pentest

Detailed scope of work:

№	Service	Scope of work
1	**Passive reconnaissance**	**Data collection using AI agents from publicly available sources:** • Collecting information from the Internet, basic network queries; • Collecting domain information: WHOIS, DNS, IP, SPF/DKIM/DMARC, etc., identifying subdomains; • Reviewing metadata and HTML comments; • Identifying applications on the web server: Wappalyzer, BuiltWith, WhatWeb, Nikto; • Taking “fingerprints” of web applications and frameworks.
2	**AI Active Reconnaissance**	**Obtaining information about the target system:** • Port scanning: Nmap, Masscan, Nessus; • Banner grabbing.
3	**Automatic scanning**	**Automated scanning using AI agents** – identifying and assessing vulnerabilities in a manner similar to traditional tools (OWASP ZAP, Burp Suite, Nessus, Nikto, Acunetix, Nuclei, Naabu) using autonomous AI agents.
4	**Testing by AI agents**	**Technical testing conducted by AI agents** that fully simulate the actions of an experienced hacker, following a detailed checklist (including coverage of the **OWASP Top 10**): • **SDLC configuration and deployment management.** • **Identity management:** Verification of roles, registration, and account monitoring. • **Authentication:** Verification of password policies, lockout mechanisms, bypass attempts, etc. • **Session management:** Verification of cookies, CSRF, login bypass, etc. • **Input validation:** Search for injections (SQL, LDAP, XML, OS, NoSQL), XSS. • **Error handling:** Error analysis, tracing.

№	Service	Scope of work
	Testing by AI agents	**Testing internal accounts and authorization domains using AI agents:** • **Authentication:** Verifying authentication mechanisms, including: JWT (JSON Web Tokens), OAuth, Basic Auth. • **Authorization:** Testing for privilege escalation and bypassing authentication logic. • **Client-side logic:** Testing interactions with the client-side. • **Business logic:** Verifying the correct implementation of business logic, request routing, integrity checks, file uploads, and data flow bypasses. **CRLF Injection and HTTP Request Testing Smuggling Desync Attacks** **Testing File Upload Attacks:** • Checking restrictions on file types and content • Checking for bypassed checks • Checking file metadata processing **RCE, RFI, LFI, and XXE Testing:** • Identifying injection points • Testing server behavior when executing damaging commands **Password Attacks:** • Checking configuration files • Searching for configuration files • Brute-force attacks (weak passwords) **Testing internal and external APIs:** • Checking internal APIs for vulnerabilities that could be exploited to attack the internal infrastructure; • Checking authentication mechanisms and their resistance to attacks; • Injection protection testing; • Testing HTTP methods (including REST and other APIs); • Testing API responses to non-standard HTTP methods; • Testing for potential bypasses of resource access controls
5	**Report**	**Preparation of a report** that includes a detailed description of vulnerabilities and recommendations for addressing them.