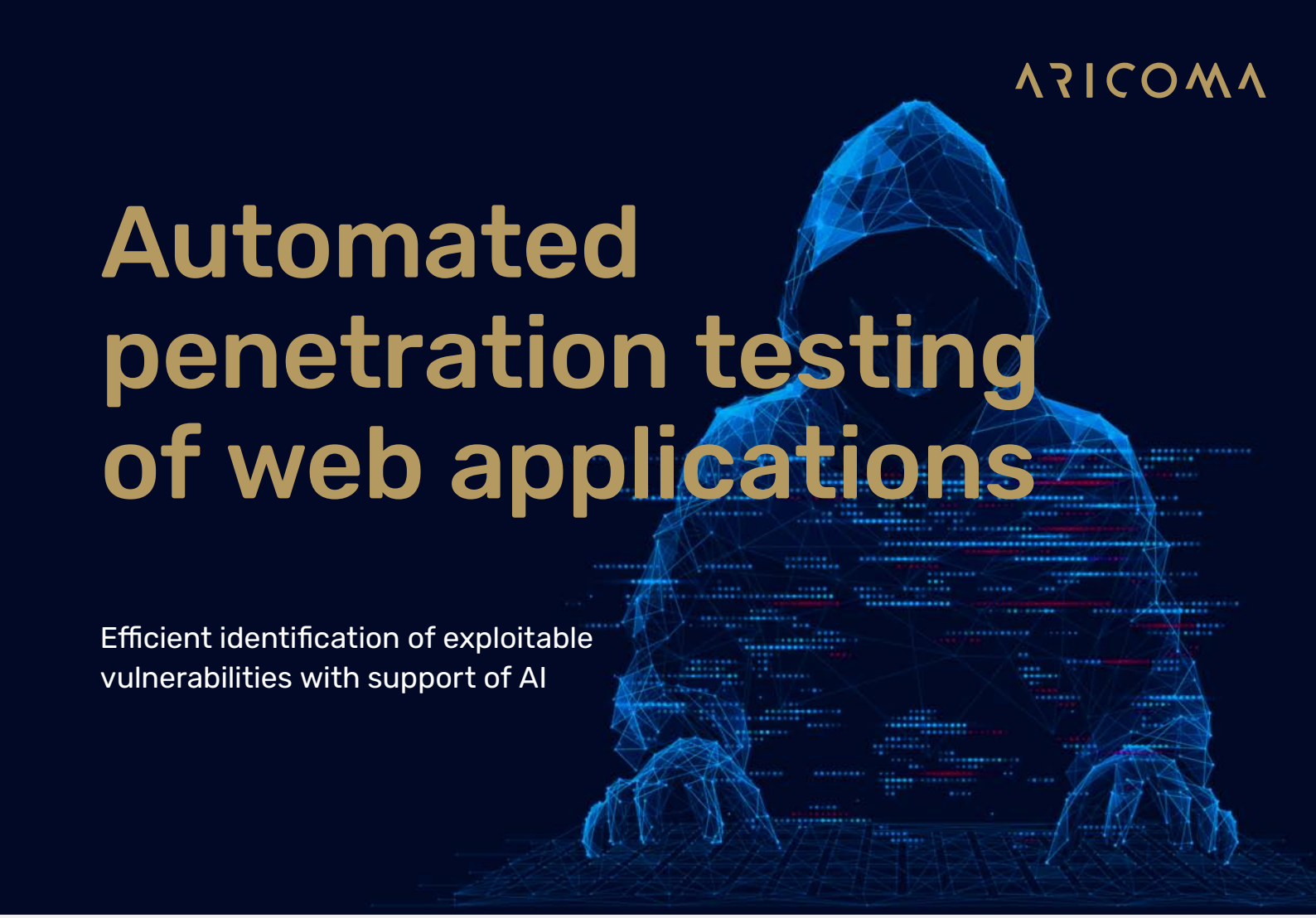
ARICOMA

Automated penetration testing of web applications



Efficient identification of exploitable vulnerabilities with support of AI

Our AI Web Application Penetration Testing service is designed as an efficient and fast tool for verifying the security resilience of publicly accessible web applications - especially those without authentication. We leverage advanced automated scanning combined with powerful on-premise AI models to validate, prioritize, and contextualize vulnerabilities-enabling faster, smarter, and more effective threat response. This significantly reduces the amount of irrelevant findings from common tools and increases the accuracy and value of the resulting outputs.

What we test

- Vulnerabilities such as SQL injection, XSS, LFI, IDOR and more
- Correct deployment of security headers and policies
- Contextual risks (e.g., leaks of sensitive information or configurations)
- Detection of outdated technologies and vulnerable libraries
- Cryptographic weaknesses and insecure implementations

Who is the service for

This service is suitable for web applications without login (same content for logged in and not logged in user). For information portals, product websites, microsites, public parts of larger systems. Also for cases when you need a quick overview of exploits including clear recommendations on what to address.

Conversely - the service is unsuitable for internal systems and parts of sites behind a login form, complex applications with business logic and user roles, or applications with atypical or dynamic behavior that require detailed manual testing.

How testing works

1. Automated scan of the application using our selected tools.

2. AI-driven analysis of scan results - identification, deduplication and severity assessment.

3. Validation by an expert - we manually verify the AI results.

4. Output report in Czech or English containing: list of exploitable vulnerabilities, explanation of risks and impacts, specific recommendations onremedation.

Key Benefits

- **Validation of vulnerabilities found** - ensures only relevant and confirmed findings, eliminating redundancy and noise
- **Clear report** - delivers focused insights without unnecessary automated clutter
- **Custom on-premise AI model** - guarantees, that your data remains within the testing infrastructure, ensuring full privacy
- **Expert-in-the-loop approach** - every output is validated by our expert
- **Tailored recommendations and risks** - we prepare a proposal for action for each finding
- **A fast and cost-effective penetration test option for public-facing websites.**

Why isn‘t an ordinary scanner enough?

Conventional scanning Vulnerability Management tools generate hundreds of reports - often without considering whether the findings are actually exploitable. Our solutions combine the power of multiple tools, proprietary analytics, and artificial intelligence to provide meaningful results, not just a long list of detections.

Features	Our AI penetration tests	Common scan
Tool diversity	Uses multiple specialized tools	One engine with a large vulnerability database
AI validation	Verifies findings, eliminates false positives, focuses on truly exploitable threats	Static plugin logics leading to overwhelm with irrelevant findings
Depth analysis	Mimics the behaviour of an experienced pentester	Automatic checks for known CVEs and misconfigurations
Accuracy of results	Delivers only relevant finding due to data correlation and AI work	Outputs are voluminous and require manual filtering
Focus	Context-aware view	Broad coverage of vulnerabilities regardless of context

Why choose Aricoma?

- We combine the power of AI and human expertise - avoiding blind trust in automation
- We know how to think about context - we don‘t just analyse technical findings, we analyse their impact on your business
- Experienced team of 20 ethical hackers with 30 years of experience and proprietary tools
- Fast delivery of results and the ability to retest