ARICOMA

Automatizované penetrační testy webových aplikací

Efektivní identifikace zneužitelných zranitelností
s podporou umělé inteligence

Naše služba Penetrační testy webových aplikací pomocí AI je navržena jako efektivní a rychlý nástroj pro ověření bezpečnostní odolnosti veřejně dostupných webových aplikací - především těch bez nutnosti přihlášení. Využíváme automatizované skenování kombinované s výkonnými lokálními AI modely, které se postarají o validaci, prioritizaci a kontextové hodnocení nalezených zranitelností. Tím se výrazně redukuje množství nerelevantních nálezů z běžných nástrojů a zvyšuje se přesnost a přínosnost výsledných výstupů.

Co testujeme

- Detekce zranitelností jako SQL injekce, XSS, LFI, IDOR a další
- Ověření správného nasazení bezpečnostních hlaviček a politik
- Hledání kontextových rizik v obsahu webu (např. úniky citlivých informací nebo konfigurací)
- Detekce použití zastaralých technologií nebo knihoven
- Detekce kryptografických nedostatků

Pro koho je služba určena

Služba je vhodná pro webové aplikace bez přihlášení (stejný obsah pro přihlášeného i nepřihlášeného uživatele). Pro informační portály, produktové weby, microsite, veřejné části větších systémů. Dále pro případy, kdy potřebujete rychlý přehled zneužitelností včetně jasného doporučení, co řešit.

Naopak - služba je nevhodná pro interní systémy a části webů za přihlašovacím formulářem, komplexní aplikace s business logikou a rolemi uživatelů nebo aplikace s netypickým nebo dynamickým chováním, které vyžaduje detailní manuální testování.

Jak testování probíhá

1. Automatizovaný scan aplikace pomocí námi vybraných nástrojů.

2. AI analýza výstupů - identifikace, deduplikace a vyhodnocení závažnosti.

3. Validace expertem - výsledky AI ověřujeme manuálně.

4. Výstupní report v českém nebo anglickém jazyce obsahující: seznam zneužitelných zranitelností, vysvětlení rizik a dopadů, konkrétní doporučení, jak problém řešit

Klíčové přínosy

- **Validace nalezených zranitelností** - jen ověřené a relevantní nálezy bez zahlcení zbytečnostmi
- **Přehledný report** - zaměřeno na podstatné nálezy, bez balastu z automatizovaných výstupů
- **Vlastní lokální model** - vaše data neopouští testovací infrastrukturu, garance soukromí
- **Expert-in-the-loop přístup** - každý výstup je finálně validován naším expertem
- **Doporučení a rizika na míru** - ke každému nálezu připravíme návrh opatření
- **Rychlá a nákladově efektivní varianta penetračního testu pro veřejné weby**

Proč nestačí obyčejný skener?

Běžné skenovací Vulnerability Management nástroje generují stovky hlášení - často bez ohledu na to, zda jsou nálezy opravdu zneužitelné. Naše řešení kombinujeme sílu několika nástrojů, vlastní analytiku a umělou inteligenci, abychom poskytli smysluplné výsledky, ne jen dlouhý seznam podezření.

Funkce	Naše penetrační testy s AI	Běžný sken
Různorodost nástrojů	Využívá více specializovaných nástrojů	Jeden engine s rozsáhlou databází zranitelností
Validace pomocí AI	Ověřuje nálezy, eliminuje false positives, zaměřuje se na skutečně zneužitelné hrozby	Statická logika pluginů vedoucí k zahlcení nepodstatnými nálezy
Hloubka analýzy	Napodobuje chování zkušeného pentestera (např. fuzzing, dynamická interakce)	Automatické kontroly známých CVE a chybné konfigurace
Přesnost výsledků	Dodává jen relevantní nálezy díky korelaci dat a práci AI	Výstupy jsou obsáhlé a vyžadují ruční filtraci
Zaměření	Kontextově zaměřený pohled	Plošné pokrytí zranitelností bez ohledu na kontext

Proč zvolit Aricomu?

- Spojujeme sílu AI a lidské expertízy - žádná slepá důvěra v automatiku
- Umíme přemýšlet nad kontextem - neanalyzujeme jen technické nálezy, ale i jejich dopad na vaše podnikání
- Zkušený tým 20 etických hackerů s 30letitou praxí a vlastními nástroji
- Rychlá dodávka výsledků a možnost opakovaného testování