ARICOMA

Automatizované penetračné testy webových aplikácií

Efektívna identifikácia zneužiteľných zraniteľností
s podporou umelej inteligencie

Naša služba Penetračné testovanie webových aplikácií pomocou AI je navrhnutá ako efektívny a rýchly nástroj pre overovanie bezpečnostnej odolnosti verejne dostupných webových aplikácií - najmä tých bez nutnosti prihlásenia. Využívame automatizované skenovanie v kombinácii s výkonnými lokálnymi AI modelmi na overenie, stanovenie priorít a kontextové hodnotenie nájdených zraniteľností. Tým sa výrazne redukuje množstvo irelevantných nálezov z bežných nástrojov a zvyšuje sa presnosť a užitočnosť výsledných výstupov.

Čo testujeme

- Detekcia zraniteľností, ako napr. SQL injection, XSS, LFI, IDOR a ďalšie
- Overenie správneho nasadenia bezpečnostných hlavičiek a politík
- Vyhľadávanie kontextových rizík v obsahu webu (napr. úniky citlivých informácií alebo konfigurácií)
- Detekcia používania zastaraných technológií alebo knižníc
- Detekcia kryptografických nedostatkov

Pre koho je služba určená

Služba je vhodná pro Webové aplikácie bez prihlásenia (rovnaký obsah pre prihlásených aj neprihlásených používateľov). Pro informačné portály, produktové weby, microsites, verejné časti väčších systémov. Dále pro prípady, keď potrebujete rýchly prehľad o zneužiteľnosti vrátane jasných odporúčaní, čo treba riešiť.

Naopak - služba je nevhodná pro interné systémy a časti webov za prihlasovacím formulárom, komplexné aplikácie s business logikou a rolami používateľov nebo aplikácie s netypickým alebo dynamickým chovaním, ktoré si vyžadujú podrobné manuálne testovanie.

Ako testovanie prebieha

1. Automatizovaný sken aplikácie pomocou nami vybraných nástrojov.

2. AI analýza výstupov - identifikácia, deduplikácia a vyhodnotenie závažnosti.

3. Validácia expertom - výsledky AI overujeme manuálne.

4. Výstupný report v českom alebo anglickom jazyku obsahujúci: zoznam zneužiteľných zraniteľností, vysvetlenie rizík a dopadov, konkrétne odporúčania, ako tento problém riešiť.

Kľúčové prínosy

- **Validácia nájdených zraniteľností** - len overené a relevantné zistenia bez zahltenia zbytočnosťami
- **Prehľadový report** - zameraný na relevantné zistenia, bez balastu automatizovaných výstupov
- **Vlastný lokálny model** - vaše dáta neopustia testovaciu infraštruktúru, garancia súkromia
- **Expert-in-the-loop prístup** - každý výstup je finálne overený naším expertom
- **Odporúčania a riziká na mieru** - ku každému zisteniu pripravíme návrh opatrení
- **Rýchly a cenovo výhodný variant penetračného testu pre verejné weby**

Prečo nestačí obyčajný skener?

Bežné skenovacie Vulnerability Management nástroje generujú stovky hlásení - často bez ohľadu na to, či sú zistenia skutočne zneužiteľné. Naše riešenia kombinujú silu viacerých nástrojov, vlastnú analytiku a umelú inteligenciu, aby sme poskytli zmysluplné výsledky, nielen dlhý zoznam podozrení.

Funkcia	Naše penetračné testy s AI	Bežný sken
Rôznorodosť nástrojov	Používa viacero špecializovaných nástrojov	Jeden engine s rozsiahlou databázou zraniteľností
Validácia pomocou AI	Overuje nálezy, eliminuje false positives, zameriava sa na skutočne zneužiteľné hrozby	Statická logika pluginov vedúca k zahlteniu nepodstatnými zisteniami
Hĺbka analýzy	Napodobňuje správanie skúseného pentestera (napr. fuzzing, dynamická interakcia)	Automatické kontroly známych CVE a chybných konfigurácií
Presnosť výsledkov	Dodáva len relevantné zistenia prostredníctvom korelácie dát a práce AI	Výstupy sú obsiahle a vyžadujú ručnú filtráciu
Zameranie	Kontextovo zameraný pohľad	Plošné pokrytie zraniteľností bez ohľadu na kontext

Prečo zvoliť Aricomu?

- Spájame silu AI a ľudskej odbornosti - žiadna slepá dôvera v automatiku
- Dokážeme premýšľať nad kontextom - neanalyzujeme len technické zistenia, ale aj ich vplyv na vaše podnikanie
- Skúsený tím 20 etických hackerov s 30 ročnými skúsenosťami a vlastnými nástrojmi
- Rýchle dodanie výsledkov a možnosť opakovaného testovania