PENETRAČNÉ TESTOVANIE MOBILNÝCH APLIKÁCIÍ

S rastúcim trhom na poli mobilných zariadení, mnohé spoločnosti sprístupňujú svoje služby a dáta pomocou mobilných aplikácií.

Tieto aplikácie môžu byť zraniteľné na rôzne typy útokov, ktoré môžu viesť nielen k úniku dát, ale aj k spusteniu nechceného kódu na zariadeniach alebo príslušných serveroch.

Náš tím profesionálnych penetračných testerov je pripravený pomôcť firmám zabezpečiť aplikácie na platformách iOS, Android alebo Windows Mobile.

VŠEOBECNÝ PREHĽAD SLUŽBY

Cieľom penetračného testu mobilných aplikácií je odhaliť zraniteľnosti v aplikáciách a ich komunikačných rozhraniach, demonštrovať zneužitie nájdených chýb, určiť ich riziko a odporučiť riešenia ako eliminovať nájdené zraniteľnosti.

Výsledkom penetračného testu je report, ktorý neobsahuje žiadne "false-positive" nálezy, ale len overené zraniteľnosti.

Penetračný test môže byt vykonaný pomocou metódy BLACK BOX (zdrojový kód aplikácie nie je dostupný), GRAY BOX (čiastočné informácie o testovanej aplikácií) alebo WHITE BOX (zdrojové kódy aplikácie sú poskytnuté na začiatku testovania).

Cena penetračného testu záleží od veľkosti a komplexnosti testovanej aplikácie. Táto cena je určená po konzultácii so zákazníkom, v ktorom sa určí rozsah, typ testu a ďalšie požiadavky od zákazníka.

DETAILNÝ PREHĽAD SLUŽBY A METODOLÓGIA

Binary House používa metodológiu založenú na OWASP Top 10 Mobile Risks s ohľadom na súčasný výskum na poli mobilných platforiem. V prípade záujmu vieme test prispôsobiť podľa metodológií OWASP Mobile Security Testing Guide, OWASP Mobile Application Security Verification Standard (ASVS). Testovanie je vykonávané za pomoci špecializovaných nástrojov s dodatočnou manuálnou kontrolou zdrojového kódu.

Testovanie zahŕňa obsiahlu škálu testov zameraných na lokálne bežiacu aplikáciu, komunikáciu so serverom ale aj testovanie služieb na serveri (REST API, SOAP...).

Kombinujúc techniky statickej a dynamickej analýzy spolu so špecifickým technikami fuzzingu, naše testovanie pokrýva všetky kategórie z OWASP Top 10 Mobile Risks:

- M1 - Improper Platform Usage
- M2 - Insecure Data Storage
- M3 - Insecure Communication
- M4 - Insecure Authentication
- M5 - Insufficient Cryptography
- M6 - Insecure Authorization
- M7 - Poor Code Quality
- M8 - Code Tampering
- M9 - Reverse Engineering
- M10 - Extraneous Functionality