PENETRAČNÉ TESTOVANIE NATÍVNYCH APLIKÁCIÍ

Mnohé firmy využívajú na podporu svojich interných a biznis procesov natívne aplikácie. Tieto aplikácie sú zvyčajne spustené v klientskom prostredí a pripájajú sa k aplikačnému serveru alebo v niektorých prípadoch priamo k databázovému serveru.

Bezpečnosť natívnych aplikácií by nemala byť podceňovaná vzhľadom na to, že úspešné zneužitie zraniteľnosti môže znamenať kompromitáciu klientskej stanice a s tým spojený únik dát. Zraniteľné bývajú aj koncové body API služieb, kam sa daná aplikácia pripája.

Náš tím profesionálnych testerov je pripravený pomôcť firmám zabezpečiť aplikácie na rôznych platformách.

VŠEOBECNÝ PREHĽAD SLUŽBY

Cieľom penetračného testu natívnych 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

Natívne aplikácie si vďaka ich jedinečnej povahe vyžadujú špecifický prístup. Mnoho z nich používa proprietárne komunikačné protokoly, má unikátny dizajn, z čoho vyplýva, že nie je možné efektívne použiť automatizované skenery.

Testovanie zahŕňa obsiahlu škálu testov zameraných na lokálne bežiacu aplikáciu, jej správanie sa v systéme, komunikáciu so serverom ale aj preverenie služieb na serveri (REST API, SOAP, proprietárne protokoly,...).

Komplexné preverenie bezpečnosti natívnej aplikácie pozostáva zo statickej a dynamickej analýzy. Statická analýza sa vykonáva najmä pomocou revízie zdrojového kódu alebo reverzného inžinierstva s následným manuálnym alebo automatizovaným hľadaním zraniteľností.

Dynamická analýza je vykonaná pomocou inštrumentácie aplikácií (debuggingu) na bežiacom systéme pričom sa testeri sústredia nielen na možné klientske problémy, ale aj problémy na strane servera. Dynamické testovanie zahŕňa aj hľadanie zraniteľností pomocou rôznych fuzzing techník. Binary House kombinuje techniky statickej a dynamickej analýzy, čo umožňuje efektívne hľadanie a overovanie zraniteľností.