PENETRAČNÝ TEST WEBOVÝCH APLIKÁCIÍ

Webové aplikácie zohrávajú dôležitú úlohu v dnešnom biznise. Tieto aplikácie bývajú často zraniteľné na mnohé typy útokov, ktoré môžu mať za následok ukradnuté dáta, či spustenie cudzieho (škodlivého) kódu s právami webservera.

Náš tím profesionálov má skúsenosti s testovaním všetkých druhov web aplikácii. Od malých prezentačných webov, e-shopov, CMS, e-commerce, API služieb, Web Services až po internetový banking a robustné veľké portály.

Ponúkame viacero druhov penetračných testov webových aplikácií, ktoré sa líšia rozsahom a hĺbkou vykonaného testu. Po diskusii so zákazníkom odporučíme typ a rozsah vhodného testu pre konkrétnu aplikáciu.

VŠEOBECNÝ PREHĽAD SLUŽBY

Cieľom penetračného testu webových aplikácií je odhaliť zraniteľnosti vo webových aplikáciách, 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 byť vykonaný pomocou metódy BLACK BOX (žiadne informácie o testovanom prostredí), GREY BOX (čiastočné informácie o testovanom prostredí) alebo WHITE BOX (úplne informácie o testovanom prostredí, vrátane zdrojových kódov aplikácie).

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.

V prípade záujmu vieme test prispôsobiť podľa metodológií/štandardov CWE/SANS Top 25, ASVS, WASC 26 Classes Testing.

PENETRAČNÝ TEST WEBOVÝCH APLIKÁCIÍ PODĽA METODOLÓGIE OWASP TESTING GUIDE V4.0

Hĺbkový penetračný test podľa metodológie OWASP testing guide v4.0 je určený pre tých, ktorí chcú komplexne preveriť bezpečnosť svojej aplikácie do detailov. Je vhodný pre veľké projekty, kritické web aplikácie a tam kde je kladený veľký dôraz na bezpečnosť. Test je vykonaný pomocou komerčných a open source nástrojov, skriptov a nástrojov napísaných v rámci firmy.

Penetračný test podľa metodológie OWASP testing guide v4.0 pozostáva z:

- Information Gathering
- Configuration and Deployment Management Testing
- Identity Management Testing
- Authentication Testing
- Authorization Testing

- Session Management Testing
- Input Validation Testing
- Testing for Error Handling
- Testing for weak Cryptography
- Business Logic Testing
- Client Side Testing

PENETRAČNÝ TEST WEBOVÝCH APLIKÁCIÍ PODĽA REBRÍČKA OWASP TOP 10 2017

Rebríček OWASP Top 10 obsahuje 10 kategórií zraniteľností, ktoré sa najčastejšie vyskytujú vo webových aplikáciách. Tieto zraniteľnosti sa zvyčajne dajú ľahšie identifikovať a zneužiť. Tieto chyby predstavujú nebezpečenstvo, kedže pomocou nich môže útočník ukradnúť dáta z databázy alebo súborov, získať kontrolu nad používateľským kontom, alebo spustiť svoj (škodlivý) kód s právami webservera.

Penetračný test podľa rebríčka OWASP TOP 2017 pozostáva z:

- A1 – Injection
- A2 - Broken Authentication
- A3 - Sensitive Data Exposure
- A4 - XML External Entities (XXE)
- A5 - Broken Access Control
- A6 - Security Misconfiguration
- A7 - Cross-Site Scripting (XSS)
- A8 - Insecure Deserialization
- A9 - Using Components with Known Vulnerabilities
- A10 - Insufficient Logging & Monitoring

AUTOMATIZOVANÝ TEST

Test je vykonaný pomocou automatizovaných nástrojov (skenerov). Po skončení automatizovaného testu sa manuálne preveria výsledky a odstránia sa false-postive nálezy. Automatizované testy preveria len základnú bezpečnosť a preto sú vhodné len pre web aplikácie, ktoré nie sú kritické z pohľadu biznisu. Tento typ testu slúži ako prevencia pred útokmi neskúsenými útočníkmi (script-kiddies), alebo nástrojmi, ktoré neustále skenujú webové aplikácie na internete a snažia sa zneužiť nájdené zraniteľnosti.

AUTOMATIZOVANÝ TEST S MANUÁLNYM TESTOVANÍM

Test je vykonaný pomocou automatizovaných nástrojov (skenerov). Po skončení automatizovaného testu sa manuálne preveria výsledky a odstránia sa false-postive nálezy. Na rozdiel od "Automatizovaného testu" je to len prvá fáza testu. V druhej fáze testu sa hľadajú (manuálne) zraniteľnosti z rebríčka OWASP TOP10 2017 v limitovanom časovom horizonte, podľa veľkosti aplikácie. Tento typ testu slúži ako prevencia pred útokmi neskúsenými útočníkmi (script-kiddies) až mierne skúsenými útočníkmi, alebo nástrojmi, ktoré neustále skenujú webové aplikácie na internete a snažia sa zneužiť nájdene zraniteľnosti. Tento test je vhodný pre nekritické web aplikácie.

MIKROTEST (BLESKOVÝ) TEST

Jedná sa o rýchly a časovo obmedzený test v rozsahu niekoľko hodín až dní, pričom záleží od veľkosti a funkcionality aplikácie. Počas penetračného testu sa hľadajú zraniteľnosti z rebríčka OWASP TOP10 2017 - spôsobom "nájdi čo naviac zraniteľností za krátky čas". Cieľom testu je rýchle zhodnotenie bezpečnosti aplikácie.

DLHODOBÝ TEST (DOPLNKOVÁ SLUŽBA

Keďže sa neustále objavujú nové vektory útokov, zraniteľnosti a nové techniky obchádzania zabezpečenia, ponúkame po skončení penetračného testu doplnkovú službu "dlhodobý test". Dlhodobý test pozostáva z krátkodobého intenzívneho testu (napríklad jeden deň) vykonávaného každý mesiac počas trvania služby.