SÉRÜLÉKENYSÉGVIZSGÁLATI METODIKÁK

Külső rendszerek vizsgálata

v 1.0

Hatályos:

Digitálisan aláírta: Kiss Tamás László
Dátum: 2026.10.12 07:31:33 +02'00'

Kiss Tamás László
Nemzetbiztonsági Szakszolgálat
Nemzeti Kiberbiztonsági Intézet
Sérülékenységvizsgálati Főosztály

Figyelem! A dokumentum érzékeny információkat tartalmazhat!

1. Vizsgálatok összefoglaló leírása

A **külső irányultság** keretében az alkalmazások ellenőrzése az **External Attack Surface Assessment (EASA)** módszertana szerint történik. A vizsgálatok alapját automatizált sérülékenység-felderítő eszközök eredményei képezik, amelyeket a vizsgált alkalmazás technológiai sajátosságainak megfelelő, célzott manuális biztonsági tesztelés egészít ki.

A vizsgálat az EASA módszertanának megfelelően az alábbi fő tesztelési területekre terjed ki:

- Információgyűjtés;
- Rendszer- és szolgáltatáskonfiguráció vizsgálata;
- Hitelesítés vizsgálata;
- Jogosultságkezelés vizsgálata;
- Hibakezelés vizsgálata;
- Kriptográfiai mechanizmusok vizsgálata;

Az EASA módszertana által lefedett vizsgálati területeken túl az alkalmazott technológiák, keretrendszerek és komponensek sajátosságainak értékelése a vonatkozó gyártói dokumentációk, biztonsági útmutatók és iparági ajánlások alapján történik.

2. Vizsgálatok részletes műszaki leírása

2.1 Kereső által tárolt információk felderítése - (OUT-INFO-001)

Annak vizsgálata, hogy az alkalmazással kapcsolatban milyen eltárolt adatok térképezhetők fel a keresőmotorokból, valamint a nyílt adatbázisokból.

2.2 Rendszer információk felderítése - (OUT-INFO-002)

Annak vizsgálata, hogy az alkalmazást futtató rendszerrel kapcsolatban milyen információk tárhatók fel.

2.3 Metafájl információk felderítése - (OUT-INFO-003)

Annak vizsgálata, hogy az alkalmazás metafájlai alapján milyen információk ismerhetők meg.

2.4 Erőforrások felderítése - (OUT-INFO-004)

Annak vizsgálata, hogy az alkalmazás milyen erőforrásokat szolgál ki (rendszerfeltérképezés).

2.5 Komment és egyéb tartalmi információk felderítése - (OUT-INFO-005)

Annak vizsgálata, hogy az alkalmazás kódjában lévő kommentek, illetve a rendszer állományai tartalmaznak-e potenciálisan érzékeny információkat.

2.6 Kiinduló pontok felderítése - (OUT-INFO-006)

Annak vizsgálata, hogy az alkalmazás kiinduló felülete milyen elérési utakon hívható meg.

2.7 Végrehajtási utak felderítése - (OUT-INFO-007)

Annak vizsgálata, hogy az alkalmazás egy tipikus kérése során mely végrehajtási utak és kérések ismerhetők meg, illetve kerülnek végrehajtása.

2.8 Keretrendszer információk felderítése - (OUT-INFO-008)

Annak vizsgálata, hogy az alkalmazás keretrendszerével kapcsolatban milyen információk tárhatók fel

2.9 Szoftverkomponens információk felderítése - (OUT-INFO-009)

Annak vizsgálata, hogy az alkalmazás milyen szoftverkomponenseket használ.

2.10 Rendszerstruktúra felderítése - (OUT-INFO-010)

Annak vizsgálata, hogy az alkalmazás szerkezeti felépítése feltérképezhető-e, illetve ez milyen sérülékenységeket tartalmaz.

2.11 Hálózat és infrastruktúra konfigurációjának vizsgálata - (OUT-CONF-001)

Annak vizsgálata, hogy az alkalmazás milyen hálózati kapcsolatokkal és infrastruktúrával rendelkezik, valamint ezek milyen hatással vannak a rendszer biztonságára nézve.

2.12 Alkalmazás platform konfigurációjának vizsgálata - (OUT-CONF-002)

Annak vizsgálata, hogy az alkalmazás keretrendszerének, illetve szerverének mely alapértelmezetten telepített fájlai, mappái, konfigurációs állományai és beállításai térképezhetők fel szabadon.

2.13 Fájlkiterjesztések kezelésének vizsgálata - (OUT-CONF-003)

Annak vizsgálata, hogy az alkalmazás megfelelően kezeli-e a felületéről elérhető fájlok típusát, valamint kiterjesztéseit, illetve megkerülhetők-e ezen beállítások.

2.14 Régi, backup és nem hivatkozott fájlok vizsgálata - (OUT-CONF-004)

Annak vizsgálata, hogy az alkalmazás felületén megtalálhatók-e dinamikus szkriptek (backup fájlok, esetleg régebbi verziók állományai) vagy potenciálisan érzékeny tartalmú adatok.

2.15 Infrastruktúra és alkalmazás adminisztrátori interfészek vizsgálata - (OUT-CONF-005)

Annak vizsgálata, hogy az alkalmazás működése szempontjából kritikus felületek szabadon hozzáférhetők-e.

2.16 HTTP metódusok vizsgálata - (OUT-CONF-006)

Annak vizsgálata, hogy az alkalmazás webszervere milyen HTTP metódusokat támogat és azok megfelelően vannak-e konfigurálva.

2.17 HTTP Strict Transport Security vizsgálata - (OUT-CONF-007)

Annak vizsgálata, hogy az alkalmazás megfelelően használja-e a HSTS eljárást az adatai védelme érdekében.

2.18 Fájl jogosultságok vizsgálata - (OUT-CONF-008)

Annak vizsgálata, hogy az alkalmazás konfigurációs állományainak hozzáférési jogosultságai megfelelően vannak-e beállítva.

2.19 Aldomain átvétel vizsgálata - (OUT-CONF-009)

Annak vizsgálata, hogy az alkalmazás valamely aldomainje felett átvehető-e az irányítás.

2.20 Felhőtárhely vizsgálata - (OUT-CONF-010)

Annak vizsgálata, hogy az alkalmazás felhő szolgáltatásai megfelelően vannak-e konfigurálva.

2.21 Content Security Policy vizsgálata - (OUT-CONF-011)

Annak vizsgálata, hogy az alkalmazás CSP beállításai megfelelően vannak-e konfigurálva.

2.22 Elérési útvonal-zavar vizsgálata - (OUT-CONF-012)

Annak vizsgálata, hogy az alkalmazás válaszokat szolgáltat-e a kétértelmű URL-ekre.

2.23 Egyéb biztonsági fejléc-hibák vizsgálata - (OUT-CONF-013)

Annak vizsgálata, hogy az alkalmazás biztonsági fejlécei megfelelően vannak-e beállítva, illetve feltárható-e velük kapcsolatban konfigurációs probléma.

2.24 Alapértelmezett hitelesítési adatok vizsgálata - (OUT-AUTN-001)

Annak vizsgálata, hogy az alkalmazás telepítésekor használt fiókok léteznek-e a rendszerben.

2.25 Kizárási házirend vizsgálata - (OUT-AUTN-002)

Annak vizsgálata, hogy az alkalmazás szankcionálja-e a helytelen bejelentkezési kísérleteket.

2.26 Hitelesítési séma megkerülésének vizsgálata - (OUT-AUTN-003)

Annak vizsgálata, hogy az alkalmazás felhasználóinak beléptetését végző felület tervezési vagy megvalósítási hibáin keresztül lehetséges-e a rendszerbe jogosulatlanul belépni.

2.27 Jelszómegjegyző funkció vizsgálata - (OUT-AUTN-004)

Annak vizsgálata, hogy az alkalmazásban található-e olyan jelszómegjegyző funkció, ami nem megfelelően tárolja el a bejelentkezési adatokat.

2.28 Böngésző gyorsítótárazás vizsgálata - (OUT-AUTN-005)

Annak vizsgálata, hogy az alkalmazásba történő sikeres hitelesítés után elérhető adatok helyileg is hozzáférhetők maradnak-e kijelentkezés után a webböngésző gyorsítótárában.

2.29 Hitelesítési módszerek vizsgálata - (OUT-AUTN-006)

Annak vizsgálata, hogy az alkalmazás fiókjainak hitelesítő adatait szabályzó házirend kellően biztonságos-e.

2.30 Biztonsági kérdések és válaszok vizsgálata - (OUT-AUTN-007)

Annak vizsgálata, hogy az alkalmazás lehetőséget biztosít-e a gyenge biztonsági kérdések, illetve válaszok használatára.

2.31 Jelszóváltoztató és visszaállító funkciók vizsgálata - (OUT-AUTN-008)

Annak vizsgálata, hogy az alkalmazás felhasználói visszaélhetnek-e a jelszóváltoztató és visszaállító funkciók gyengeségeivel.

2.32 Alternatív csatornákon keresztüli gyengébb hitelesítés vizsgálata - (OUT-AUTN-009)

Annak vizsgálata, hogy az alkalmazásban léteznek-e alternatív autentikációs mechanizmusok, valamint ezek létező hitelesítési adatokkal kihasználhatók-e.

2.33 Többfaktoros hitelesítés vizsgálata - (OUT-AUTN-010)

Annak vizsgálata, hogy az alkalmazás többfaktoros autentikációja megfelelően van-e konfigurálva.

2.34 Könyvtárbejárás és fájl beszúrás vizsgálata - (OUT-AUTZ-001)

Annak vizsgálata, hogy az alkalmazás által kezelt fájlok elérési útjáról lehetséges-e átlépni a kiszolgáló rendszerfájljai felé.

2.35 Jogosultságkezelési séma megkerülésének vizsgálata - (OUT-AUTZ-002)

Annak vizsgálata, hogy az alkalmazás bizonyos jogosultsági szint birtokában elérhető funkciói hozzáférhetők-e az elvártnak nem megfelelő jogosultsági szint birtokában.

2.36 Jogosultság kiterjesztés vizsgálata - (OUT-AUTZ-003)

Annak vizsgálata, hogy az alkalmazás felhasználói hozzájuthatnak-e a számukra kiosztottnál bővebb jogosultságokhoz.

2.37 Közvetlen objektum referenciák kezelésének vizsgálata - (OUT-AUTZ-004)

Annak vizsgálata, hogy az alkalmazáson belül más felhasználók által kezelt állományokhoz hozzá lehet-e férni.

2.38 OAuth implementáció vizsgálata - (OUT-AUTZ-005)

Annak vizsgálata, hogy az alkalmazás OAuth implementációja megfelelően biztonságos-e.

2.39 OAuth jogosultságkezelési szerver vizsgálata - (OUT-AUTZ-005-1)

Annak vizsgálata, hogy az alkalmazás OAuth hitelesítő szerverének bizonyos jogosultsági szint birtokában elérhető funkciói hozzáférhetők-e az elvártnak nem megfelelő jogosultsági szint birtokában.

2.40 OAuth kliens vizsgálata - (OUT-AUTZ-005-2)

Annak vizsgálata, hogy az alkalmazás OAuth kliensei hozzájuthatnak-e a számukra kiosztottnál bővebb jogosultságokhoz.

2.41 Hibaüzenetek és hibaállapotok kezelésének vizsgálata - (OUT-ERRH-001)

Annak vizsgálata, hogy az alkalmazás miként kezeli a felmerülő hibaüzeneteket és hibaállapotokat.

2.42 Gyenge SSL/TLS konfiguráció vizsgálata - (OUT-CRYP-001)

Annak vizsgálata, hogy az alkalmazás SSL/TLS protokolljai, titkosítási algoritmusai és kapcsolódó kriptográfiai paraméterei megfelelnek-e az aktuális biztonsági követelményeknek.

2.43 Padding Oracle vizsgálata - (OUT-CRYP-002)

Annak vizsgálata, hogy az alkalmazás megfelelően védett-e a Padding Oracle technikák használatával szemben.

2.44 Nyílt csatorna feletti érzékeny adattovábbítás vizsgálata - (OUT-CRYP-003)

Annak vizsgálata, hogy az alkalmazás megfelelően konfigurált és titkosított hálózati csatornát használ-e az adatainak továbbítására.

2.45 Gyenge titkosítás vizsgálata - (OUT-CRYP-004)

Annak vizsgálata, hogy az alkalmazás megfelelően biztonságos kriptográfiai algoritmusokat használ-e.