SÉRÜLÉKENYSÉGVIZSGÁLATI METODIKÁK

Alkalmazásvizsgálat

Webalkalmazás

v 1.0

Hatályos:

Digitálisan aláírta: Kiss Tamás László
Dátum: 2026.10.12 07:35:05 +02'00'

Kiss Tamás László
Nemzetbiztonsági Szakszolgálat
Nemzeti Kiberbiztonsági Intézet
Sérülékenységvizsgálati Főosztály

Figyelem! A dokumentum érzékeny információkat tartalmazhat!

1. Vizsgálatok összefoglaló leírása

Az alkalmazásvizsgálati irányultság keretében a **webalkalmazások** ellenőrzése az **OWASP Web Security Testing Guide (WSTG) v5** módszertana szerint történik. A vizsgálatok alapját automatizált sérülékenység-felderítő eszközök eredményei képezik, amelyeket a vizsgált webalkalmazás technológiai sajátosságainak megfelelő, célzott manuális biztonsági tesztelés egészít ki.

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

- Információgyűjtés;
- Konfiguráció- és telepítésmenedzsment vizsgálata;
- Identitáskezelés vizsgálata;
- Hitelesítés vizsgálata;
- Jogosultságkezelés vizsgálata;
- Munkamenet-kezelés vizsgálata;
- Bemenet-ellenőrzés vizsgálata;
- Hibakezelés vizsgálata;
- Kriptográfiai mechanizmusok vizsgálata;
- Üzleti logika vizsgálata;
- Kliensoldali mechanizmusok vizsgálata;
- API-k vizsgálata.

Az OWASP WSTG 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 - (WEB-INFO-001)

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

2.2 Webszerver információk felderítése - (WEB-INFO-002)

Annak vizsgálata, hogy a webalkalmazást futtató webszerverrel kapcsolatban milyen információk tárhatók fel.

2.3 Webszerver metafájlok információszivárgásának felderítése - (WEB-INFO-003)

Annak vizsgálata, hogy a webalkalmazás metafájlai alapján milyen információk ismerhetők meg.

2.4 Webszerveren lévő alkalmazások felderítése - (WEB-INFO-004)

Annak vizsgálata, hogy a webalkalmazást futtató webszerver milyen erőforrásokat szolgál ki (rendszerfeltérképezés).

2.5 Weboldal-tartalmak információszivárgásának felderítése - (WEB-INFO-005)

Annak vizsgálata, hogy a webalkalmazás forrásában lévő kommentek, illetve felületéről elérhető állományok tartalmaznak-e potenciálisan érzékeny információkat.

2.6 Webalkalmazás kiinduló pontjainak felderítése - (WEB-INFO-006)

Annak vizsgálata, hogy a webalkalmazás kiinduló felülete milyen elérési utakon hívható meg.

2.7 Webalkalmazáson belüli végrehajtási utak felderítése - (WEB-INFO-007)

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

2.8 Webalkalmazás-keretrendszer információk felderítése - (WEB-INFO-008)

Annak vizsgálata, hogy a webalkalmazást betöltő keretrendszerrel kapcsolatban milyen információk tárhatók fel.

2.9 Webalkalmazás-szoftverkomponens információk felderítése - (WEB-INFO-009)

Annak vizsgálata, hogy a webalkalmazás milyen szoftverkomponenseket használ.

2.10 Webalkalmazás szerkezetének felderítése - (WEB-INFO-010)

Annak vizsgálata, hogy a webalkalmazás szerkezeti felépítése feltérképezhető-e, illetve ez milyen sérülékenységeket tartalmaz.

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

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

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

Annak vizsgálata, hogy a webalkalmazás keretrendszerének, illetve webszerverének mely alapértelmezetten telepített fájlai, mappái, konfigurációs állományai és beállításai térképezhetők fel szabadon.

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

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

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

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

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

Annak vizsgálata, hogy a webalkalmazás működése szempontjából kritikus felületek szabadon hozzáférhetők-e.

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

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

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

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

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

Annak vizsgálata, hogy a webalkalmazás konfigurációs állományainak hozzáférési jogosultságai megfelelően vannak-e beállítva.

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

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

2.20 Felhőtárhely vizsgálata - (WEB-CONF-010)

Annak vizsgálata, hogy a webalkalmazás felhő szolgáltatásai megfelelően vannak-e konfigurálva.

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

Annak vizsgálata, hogy a webalkalmazás CSP beállításai megfelelően vannak-e konfigurálva.

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

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

2.23 Egyéb HTTP biztonsági fejléc-hibák vizsgálata - (WEB-CONF-013)

Annak vizsgálata, hogy a webalkalmazás HTTP biztonsági fejlécei megfelelően vannak-e beállítva, illetve feltárható-e velük kapcsolatban konfigurációs probléma.

2.24 Szerepkör definíciók vizsgálata - (WEB-IDNT-001)

Annak vizsgálata, hogy a webalkalmazásban mely szerepkörök vannak definiálva, ezek hogyan működnek, valamint megfelelő hozzáférést biztosítanak-e a rendszer funkcionalitásához és információihoz.

2.25 Felhasználói regisztráció vizsgálata - (WEB-IDNT-002)

Annak vizsgálata, hogy a webalkalmazás leendő felhasználói miként juthatnak jogosultságokhoz.

2.26 Felhasználói hozzáférés létrehozásának vizsgálata - (WEB-IDNT-003)

Annak vizsgálata, hogy a webalkalmazást használók képesek-e új fiókokat hozzáadni a rendszerhez vagy módosítani a már meglévő felhasználókat.

2.27 Felsoroltatható és könnyen kitalálható felhasználói hozzáférések vizsgálata - (WEB-IDNT-004)

Annak vizsgálata, hogy a webalkalmazás egyes funkcióinak felhasználásával felderíthetők-e a beregisztrált felhasználók belépési azonosítói, illetve ezek általánosan és gyakran használt felhasználói hozzáférések-e.

2.28 Felhasználónév házirend vizsgálata - (WEB-IDNT-005)

Annak vizsgálata, hogy a webalkalmazás fiókjainak felhasználónév követelményeit szabályzó házirend kellően biztonságos-e.

2.29 Alapértelmezett hitelesítési adatok vizsgálata - (WEB-AUTN-001)

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

2.30 Kizárási házirend vizsgálata - (WEB-AUTN-002)

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

2.31 Hitelesítési séma megkerülésének vizsgálata - (WEB-AUTN-003)

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

2.32 Jelszómegjegyző funkció vizsgálata - (WEB-AUTN-004)

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

2.33 Böngésző gyorsítótárazás vizsgálata - (WEB-AUTN-005)

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

2.34 Hitelesítési módszerek vizsgálata - (WEB-AUTN-006)

Annak vizsgálata, hogy a webalkalmazás fiókjainak hitelesítő adatait szabályzó házirend kellően biztonságos-e.

2.35 Biztonsági kérdések és válaszok vizsgálata - (WEB-AUTN-007)

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

2.36 Jelszóváltoztató és visszaállító funkciók vizsgálata - (WEB-AUTN-008)

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

2.37 Alternatív csatornákon keresztüli gyengébb hitelesítés vizsgálata - (WEB-AUTN-009)

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

2.38 Többfaktoros hitelesítés vizsgálata - (WEB-AUTN-010)

Annak vizsgálata, hogy a webalkalmazás többfaktoros autentikációja megfelelően van-e konfigurálva.

2.39 Könyvtárbejárás és fájl beszúrás vizsgálata - (WEB-AUTZ-001)

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

2.40 Jogosultságkezelési séma megkerülésének vizsgálata - (WEB-AUTZ-002)

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

2.41 Jogosultság kiterjesztés vizsgálata - (WEB-AUTZ-003)

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

2.42 Közvetlen objektum referenciák kezelésének vizsgálata - (WEB-AUTZ-004)

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

2.43 OAuth implementáció vizsgálata - (WEB-AUTZ-005)

Annak vizsgálata, hogy a webalkalmazás OAuth implementációja megfelelően biztonságos-e.

2.44 OAuth jogosultságkezelési szerver vizsgálata - (WEB-AUTZ-005-1)

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

2.45 OAuth kliens vizsgálata - (WEB-AUTZ-005-2)

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

2.46 Munkamenet-kezelési séma megkerülhetőségének vizsgálata - (WEB-SESS-001)

Annak vizsgálata, hogy a webalkalmazás munkamenet-kezelési sémája biztonságos-e, illetve ezzel kapcsolatban felderíthetők-e potenciális sérülékenységek.

2.47 Süti védelem vizsgálata - (WEB-SESS-002)

Annak vizsgálata, hogy a webalkalmazás munkamenet változóira (sütijeire) mely biztonsági beállítások kerültek konfigurálásra.

2.48 Munkamenet-hitelesítés megkerülhetőségének vizsgálata - (WEB-SESS-003)

Annak vizsgálata, hogy a webalkalmazás munkamenete eltéríthető-e a rendszer nem megfelelő hitelesítési folyamata következtében.

2.49 Védtelen munkamenet-változók kezelésének vizsgálata - (WEB-SESS-004)

Annak vizsgálata, hogy a webalkalmazás működését érzékenyen befolyásoló paraméterek kerülnek-e eltárolásra a kliensoldalon.

2.50 Cross Site Request Forgery vizsgálata - (WEB-SESS-005)

Annak vizsgálata, hogy a webalkalmazásba bejelentkezett felhasználók rávehetők-e a tudtuk és szándékuk nélkül arra, hogy olyan tevékenységet végezzenek a saját nevükben, amit nem áll szándékukban.

2.51 Kijelentkezés vizsgálata - (WEB-SESS-006)

Annak vizsgálata, hogy a webalkalmazás lehetőséget ad-e a befejezett munkamenetek szerveroldalon történő érvénytelenítésére.

2.52 Munkamenet lejárat vizsgálata - (WEB-SESS-007)

Annak vizsgálata, hogy a webalkalmazás aktuális (bejelentkeztetett) munkamenetei érvénytelenítésre kerülnek-e észszerű időn belül.

2.53 Munkamenet változók túlterhelhetőségének vizsgálata - (WEB-SESS-008)

Annak vizsgálata, hogy a webalkalmazás munkamenet változói túlterhelhetők-e, illetve ez a rendszer sérülékenységéhez vezethet-e.

2.54 Munkamenet eltéríthetőségének vizsgálata - (WEB-SESS-009)

Annak vizsgálata, hogy a webalkalmazás munkamenetei eltéríthetők-e a munkamenet változók (sütik) megszerzésének következtében.

2.55 JSON Web Tokenek vizsgálata - (WEB-SESS-010)

Annak vizsgálata, hogy a webalkalmazás JSON Web Tokenjei megfelelően védettek-e.

2.56 Egyidejű munkamenetek vizsgálata - (WEB-SESS-011)

Annak vizsgálata, hogy a webalkalmazás egyidejű munkamenetei megfelelően biztonságosan vannak-e kezelve.

2.57 Reflected Cross Site Scripting vizsgálata - (WEB-INPV-001)

Annak vizsgálata, hogy a webalkalmazás felületébe lehetséges-e ideiglenesen kártékony, kliensoldali kódot juttatni.

2.58 Stored Cross Site Scripting vizsgálata - (WEB-INPV-002)

Annak vizsgálata, hogy a webalkalmazás felületébe lehetséges-e maradandóan kártékony, kliensoldali kódot juttatni.

2.59 HTTP Verb Tampering vizsgálata - (WEB-INPV-003)

Annak vizsgálata, hogy a webalkalmazás szerverén lehetséges-e alternatív HTTP metódusokat kihasználni.

2.60 HTTP paraméter többszörös értékátadásának vizsgálata - (WEB-INPV-004)

Annak vizsgálata, hogy a webalkalmazás felületén lehetséges-e azonos nevű HTTP paramétereknek többszörösen értéket adni.

2.61 SQL befecskendezés vizsgálata - (WEB-INPV-005)

Annak vizsgálata, hogy a webalkalmazás felületén lehetséges-e a rendszer által az adatbázis-kiszolgáló(k)nak küldött utasítások módosítása.

2.62 Oracle sérülékenységek vizsgálata - (WEB-INPV-005-1)

Annak vizsgálata, hogy a webalkalmazás PL/SQL adatbázisa rendelkezik-e kihasználható sérülékenységekkel.

2.63 MySQL sérülékenységek vizsgálata - (WEB-INPV-005-2)

Annak vizsgálata, hogy a webalkalmazás MySQL adatbázisa rendelkezik-e kihasználható sérülékenységekkel.

2.64 SQL Server sérülékenységek vizsgálata - (WEB-INPV-005-3)

Annak vizsgálata, hogy a webalkalmazás Microsoft SQL Server adatbázisa rendelkezik-e kihasználható sérülékenységekkel.

2.65 PostgreSQL sérülékenységek vizsgálata - (WEB-INPV-005-4)

Annak vizsgálata, hogy a webalkalmazás PostgreSQL adatbázisa rendelkezik-e kihasználható sérülékenységekkel.

2.66 MS Access sérülékenységek vizsgálata - (WEB-INPV-005-5)

Annak vizsgálata, hogy a webalkalmazás Microsoft Access adatbázisa rendelkezik-e kihasználható sérülékenységekkel.

2.67 NoSQL befecskendezés vizsgálata - (WEB-INPV-005-6)

Annak vizsgálata, hogy a webalkalmazás NoSQL adatbázisa rendelkezik-e kihasználható sérülékenységekkel.

2.68 ORM befecskendezés vizsgálata - (WEB-INPV-005-7)

Annak vizsgálata, hogy a webalkalmazás ORM adatbázisa rendelkezik-e kihasználható sérülékenységekkel.

2.69 Kliensoldali befecskendezés vizsgálata - (WEB-INPV-005-8)

Annak vizsgálata, hogy a webalkalmazás Web SQL DB adatbázisa rendelkezik-e kihasználható sérülékenységekkel.

2.70 LDAP befecskendezés vizsgálata - (WEB-INPV-006)

Annak vizsgálata, hogy a webalkalmazás LDAP komponense rendelkezik-e kihasználható sérülékenységekkel.

2.71 XML befecskendezés vizsgálata - (WEB-INPV-007)

Annak vizsgálata, hogy a webalkalmazás XML komponense rendelkezik-e kihasználható sérülékenységekkel.

2.72 SSI befecskendezés vizsgálata - (WEB-INPV-008)

Annak vizsgálata, hogy a webalkalmazás SSI komponense rendelkezik-e kihasználható sérülékenységekkel.

2.73 XPath befecskendezés vizsgálata - (WEB-INPV-009)

Annak vizsgálata, hogy a webalkalmazás XPath komponense rendelkezik-e kihasználható sérülékenységekkel.

2.74 IMAP/SMTP befecskendezés vizsgálata - (WEB-INPV-010)

Annak vizsgálata, hogy a webalkalmazás IMAP/SMTP komponense rendelkezik-e kihasználható sérülékenységekkel.

2.75 Kód befecskendezés vizsgálata - (WEB-INPV-011)

Annak vizsgálata, hogy a webalkalmazás felületére lehetséges-e olyan adatot berögzíteni, amelyet a rendszer szerveroldalon feldolgoz majd lefuttat.

2.76 Fájlbeszúrás vizsgálata - (WEB-INPV-011-1)

Annak vizsgálata, hogy a webalkalmazás felületéről meghívhatók-e csak helyileg elérhető fájlok, illetve szerveroldalról betölthetők-e távoli tárterületen lévő állományok.

2.77 Parancs befecskendezés vizsgálata - (WEB-INPV-012)

Annak vizsgálata, hogy a webalkalmazás bemeneti paramétereibe lehetséges-e a kiszolgáló operációs rendszerén keresztül futtatható parancsokat beszúrni.

2.78 Formázó karakter befecskendezés vizsgálata - (WEB-INPV-013)

Annak vizsgálata, hogy a webalkalmazás megfelelően védett-e a formázó karakter túlcsordulásos technikák használatával szemben.

2.79 Lappangó sérülékenység vizsgálata - (WEB-INPV-014)

Annak vizsgálata, hogy a webalkalmazás megfelelően védett-e a perzisztens technikák használatával szemben.

2.80 HTTP Response Splitting vizsgálata - (WEB-INPV-015)

Annak vizsgálata, hogy a webalkalmazás megfelelően védett-e a HTTP válaszok szerkezetét manipuláló technikák használatával szemben.

2.81 HTTP Request Smuggling vizsgálata - (WEB-INPV-016)

Annak vizsgálata, hogy a webalkalmazás megfelelően védett-e a beérkező HTTP kérésekbe rejtett további HTTP kérések becsempészésével szemben.

2.82 Host fejléc befecskendezés vizsgálata - (WEB-INPV-017)

Annak vizsgálata, hogy a webalkalmazás megfelelően védett-e a hoszt fejléceket érintő befecskendezéses technikák használatával szemben.

2.83 Szerveroldali sablon befecskendezés vizsgálata - (WEB-INPV-018)

Annak vizsgálata, hogy a webalkalmazás megfelelően védett-e a szerveroldali sablonokba való befecskendezéses technikák használatával szemben.

2.84 Szerveroldali kérés hamisítás vizsgálata - (WEB-INPV-019)

Annak vizsgálata, hogy a webalkalmazás megfelelően védett-e a jogosultság nélkül meghívott szerveroldali műveletek használatával szemben.

2.85 Mass Assignment vizsgálata - (WEB-INPV-020)

Annak vizsgálata, hogy a webalkalmazás megfelelően védett-e a jogosultság nélkül meghívott adatmódosító funkcióival történő extra paramétereket feldolgozó műveletek használatával szemben.

2.86 CSV befecskendezés vizsgálata - (WEB-INPV-021)

Annak vizsgálata, hogy a webalkalmazásból kiexportálható CSV fájlokba lehetséges-e olyan adatot berögzíteni, amelyet a táblázatkezelő programok képletként értelmeznek, majd végrehajtanak.

2.87 Hibaüzenetek és hibaállapotok kezelésének vizsgálata - (WEB-ERRH-001)

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

2.88 Gyenge SSL/TLS konfiguráció vizsgálata - (WEB-CRYP-001)

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

2.89 Padding Oracle vizsgálata - (WEB-CRYP-002)

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

2.90 Nyílt csatorna feletti érzékeny adattovábbítás vizsgálata - (WEB-CRYP-003)

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

2.91 Gyenge titkosítás vizsgálata - (WEB-CRYP-004)

Annak vizsgálata, hogy a webalkalmazás megfelelően biztonságos kriptográfiai algoritmusokat használ-e.

2.92 Üzleti logikai adatvalidáció vizsgálata - (WEB-BUSL-001)

Annak vizsgálata, hogy a webalkalmazás megfelelően érvényesíti-e az üzleti logikához kapcsolódó adatellenőrzési szabályokat.

2.93 Kérések hamisíthatóságának vizsgálata - (WEB-BUSL-002)

Annak vizsgálata, hogy a webalkalmazás megfelelően kezeli-e a módosított vagy hamisított kéréseket, illetve megakadályozza-e azok jogosulatlan felhasználását.

2.94 Integritás tesztek vizsgálata - (WEB-BUSL-003)

Annak vizsgálata, hogy a webalkalmazás megfelelően kezeli-e a rejtett vagy nem szerkeszthető mezők és paraméterek adatait.

2.95 Folyamatidőzítések vizsgálata - (WEB-BUSL-004)

Annak vizsgálata, hogy a webalkalmazás megfelelően védett-e a rendszerfolyamatok és a HTTP kérések válaszidejére vonatkozó rendszerhibákkal szemben.

2.96 Folyamat többszöri felhasználhatóságának vizsgálata - (WEB-BUSL-005)

Annak vizsgálata, hogy a webalkalmazás megfelelően korlátozza-e a folyamatainak többszörös felhasználhatóságát.

2.97 Munkafolyamatok kijátszásának vizsgálata - (WEB-BUSL-006)

Annak vizsgálata, hogy a webalkalmazás megfelelően szabályozza-e a munkafolyamatainak szabályos végrehajtódásától való eltérést.

2.98 Alkalmazással való visszaélés elleni védelem vizsgálata - (WEB-BUSL-007)

Annak vizsgálata, hogy a webalkalmazás megfelelően védett-e a funkcióinak rendeltetésszerűtől eltérő használatával szemben.

2.99 Nem engedélyezett fájltípusok feltöltésének vizsgálata - (WEB-BUSL-008)

Annak vizsgálata, hogy a webalkalmazás megakadályozza-e a nem engedélyezett, váratlan vagy manipulált fájlok feltöltését és feldolgozását.

2.100 Kártékony fájlok feltöltésének vizsgálata - (WEB-BUSL-009)

Annak vizsgálata, hogy a webalkalmazás megakadályozza-e a kártékony vagy végrehajtható fájlok feltöltését és feldolgozását.

2.101 Fizetési funkciók vizsgálata - (WEB-BUSL-010)

Annak vizsgálata, hogy a webalkalmazás megfelelően kezeli-e a fizetési folyamatokat, illetve megakadályozza-e azok jogosulatlan manipulálását.

2.102 DOM-Based Cross Site Scripting vizsgálata - (WEB-CLNT-001)

Annak vizsgálata, hogy a webalkalmazás Document Object Model struktúrájába lehetséges-e ideiglenesen kártékony, kliensoldali kódot juttatni.

2.103 JavaScript kódfuttatás vizsgálata - (WEB-CLNT-002)

Annak vizsgálata, hogy a webalkalmazás JavaScript állományainak felületébe lehetséges-e ideiglenesen kártékony, kliensoldali kódot juttatni.

2.104 HTML befecskendezés vizsgálata - (WEB-CLNT-003)

Annak vizsgálata, hogy a webalkalmazás felületébe lehetséges-e tetszőleges kliensoldali HTML kódokat juttatni.

2.105 Kliensoldali URL átirányítás vizsgálata - (WEB-CLNT-004)

Annak vizsgálata, hogy a webalkalmazás felhasználói átirányíthatók-e külső URL címekre.

2.106 CSS befecskendezés vizsgálata - (WEB-CLNT-005)

Annak vizsgálata, hogy a webalkalmazás felületébe lehetséges-e tetszőleges kliensoldali CSS kódokat juttatni.

2.107 Kliensoldali erőforrás-manipuláció vizsgálata - (WEB-CLNT-006)

Annak vizsgálata, hogy a webalkalmazás megfelelően kezeli-e a kliensoldali erőforrások hivatkozásainak módosítását, illetve megakadályozza-e azok jogosulatlan manipulálását.

2.108 Cross Origin Resource Sharing vizsgálata - (WEB-CLNT-007)

Annak vizsgálata, hogy a webalkalmazás tetszőleges domain címeket is elfogad-e, mint HTTP kérést indító weboldal.

2.109 Cross Site Flashing vizsgálata - (WEB-CLNT-008)

Annak vizsgálata, hogy a webalkalmazás felületébe lehetséges-e tetszőleges ActionScript kódokat juttatni.

2.110 Clickjacking vizsgálata - (WEB-CLNT-009)

Annak vizsgálata, hogy a webalkalmazás felülete beágyazható-e egy másik rendszer weboldalába.

2.111 WebSocketek vizsgálata - (WEB-CLNT-010)

Annak vizsgálata, hogy a webalkalmazás WebSocket protokolt használó funkciói megfelelően biztonságos mechanizmusokkal rendelkeznek-e.

2.112 Web Messaging vizsgálata - (WEB-CLNT-011)

Annak vizsgálata, hogy a webalkalmazás megfelelően ellenőrzi-e a Web Messaging mechanizmuson keresztül érkező üzenetek forrását és tartalmát.

2.113 Böngésző tárolók vizsgálata - (WEB-CLNT-012)

Annak vizsgálata, hogy a webalkalmazás biztonságosan kezeli-e a böngészőben tárolt adatokat.

2.114 Cross Site Script Inclusion vizsgálata - (WEB-CLNT-013)

Annak vizsgálata, hogy a webalkalmazásba bejelentkezett felhasználók nevében és jogosultságaival, de tudtuk és szándékuk nélkül, valamely szoftverkomponens képes-e adatokat kinyerni a rendszerből.

2.115 Reverse Tabnabbing vizsgálata - (WEB-CLNT-014)

Annak vizsgálata, hogy a webalkalmazás nem megfelelően konfigurált linkjeivel megnyitott új ablakokat manipulálva, van-e lehetőség phising weboldalakra való átirányításra.

2.116 Kliensoldali sablon befecskendezés vizsgálata - (WEB-CLNT-015)

Annak vizsgálata, hogy a webalkalmazás megfelelően védett-e a kliensoldali sablonokba való befecskendezéses technikák használatával szemben.

2.117 API információk felderítése - (WEB-APIT-001)

Annak vizsgálata, hogy a webalkalmazás API végpontjaival, funkcióival és működésével kapcsolatban milyen információk tárhatók fel.

2.118 API objektum szintű jogosultságkezelés vizsgálata - (WEB-APIT-002)

Annak vizsgálata, hogy a webalkalmazás API végpontjai megakadályozzák-e a más felhasználókhoz vagy erőforrásokhoz tartozó objektumok jogosulatlan elérését.

2.119 API túlzott adatkitettség vizsgálata - (WEB-APIT-003)

Annak vizsgálata, hogy a webalkalmazás API végpontjai a működéshez szükségesnél több adatot szolgáltatnak-e vissza.

2.120 API jogosulatlan funkcióelérés vizsgálata - (WEB-APIT-004)

Annak vizsgálata, hogy a webalkalmazás API végpontjai megfelelően korlátozzák-e a felhasználók hozzáférését a jogosultsági szintjüknek nem megfelelő funkciókhoz.

2.121 GraphQL vizsgálata - (WEB-APIT-005)

Annak vizsgálata, hogy a webalkalmazás GraphQL API funkciói megfelelően kezelik-e a hozzáférés-szabályozást, a lekérdezések korlátozását és a bemeneti adatok ellenőrzését.

2.122 SQL Wildcard támadás vizsgálata - (WEB-DOST-001)

Annak vizsgálata, hogy a webalkalmazásban előidézhető-e SQL adatbázisok helyettesítő karaktereit tartalmazó lekérdezésekkel való CPU, valamint az adatfeldolgozás terhelés következtében történő rendszerleállás.

2.123 Felhasználói fiókok zárolásának vizsgálata - (WEB-DOST-002)

Annak vizsgálata, hogy a webalkalmazásból ki lehet-e zárni úgy a felhasználókat, hogy ennek hatására ne tudjanak bejelentkezni.

2.124 Buffer túlcsordulás vizsgálata - (WEB-DOST-003)

Annak vizsgálata, hogy a webalkalmazásban előidézhető-e adatstruktúrák kérelmekkel való „csordultig” töltése következtében rendszerleállás.

2.125 Felhasználó általi objektum létrehozás vizsgálata - (WEB-DOST-004)

Annak vizsgálata, hogy a webalkalmazásban előidézhető-e a nem megfelelően korlátozott felhasználói bemenet alapján létrehozott objektumok következtében erőforrás-kimerítés.

2.126 Felhasználói bemenet ciklusvezérlésének vizsgálata - (WEB-DOST-005)

Annak vizsgálata, hogy a webalkalmazásban előidézhető-e nagy számítást igénylő ciklusok vagy iterációk végrehajtódásából eredő rendszerleállás.

2.127 Felhasználók által generált adatok tárolásának vizsgálata - (WEB-DOST-006)

Annak vizsgálata, hogy a webalkalmazásban előidézhető-e nagy mennyiségű műveletből generált adatokkal történő rendszerleállás.

2.128 Erőforrás-felszabadítás hibáinak vizsgálata - (WEB-DOST-007)

Annak vizsgálata, hogy a webalkalmazásban előidézhető-e a nem megfelelően felszabadított erőforrások és objektumok következtében erőforrás-kimerülés.

2.129 Munkamenet túlterhelés vizsgálata - (WEB-DOST-008)

Annak vizsgálata, hogy a webalkalmazásban előidézhető-e nagy mennyiségű adatokkal való feladat-végrehajtás következtében történő rendszerleállás.