NEMZETI KÖZSZOLGÁLATI EGYETEM
LUDOVIKA

Az új OWASP Top 10

Dr. Tóth András

Infokommunikáció 2021

2021. november 10.

„Az MTA Bolyai János Kutatási Ösztöndíj, valamint Innovációs és Technológiai Minisztérium ÚNKP-21-5-NKE-149 kódszámú Új Nemzeti Kiválóság Programjának szakmai támogatásával készült.”

Új Nemzeti Kiválóság Program

Tartalom

I • Kutatási célok, kérdések, témaválasztás

II • Módszertan

III • Az OWASP Top 10

IV • Az új OWASP Top 10

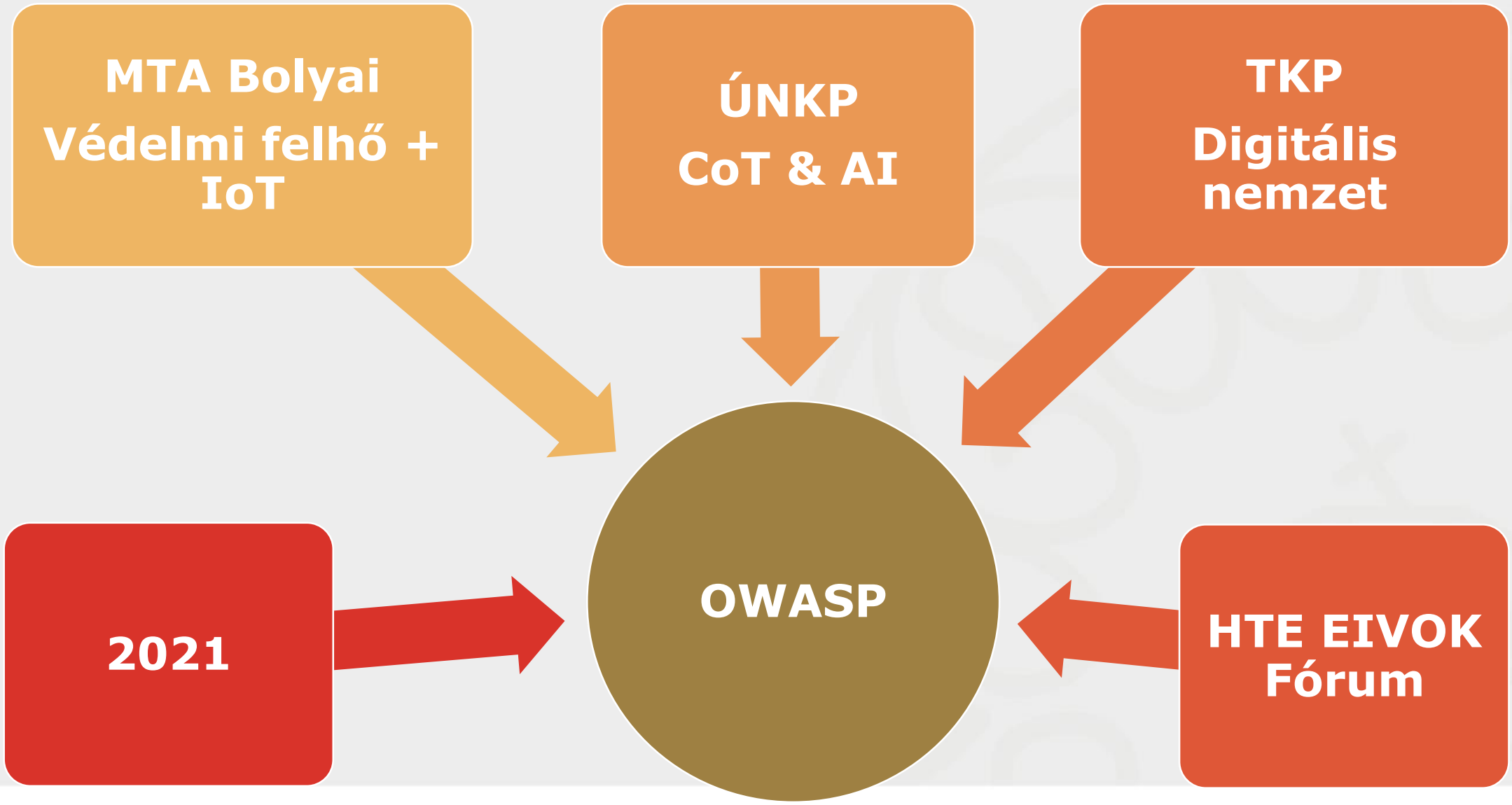
V • Következtetések

I. Kutatási célok, kérdések

RQ1 Hogyan változtak meg a jellemző sérülékenységek az elmúlt 4 évben?

RQ2 Mennyire vannak hatással ezek a jelentések a biztonsági környezeteinkre?

I. Témaválasztás



II. Módszertan

- OWASP Top 10 jelentés megvizsgálása, összehasonlítása a korábbi verziókkal;
- Releváns szakmai jelentések elemzése.

III. Az OWASP Top 10

Open Web Application Security Project

- az alkalmazásbiztonság ügyét segítő nemzetközi szervezet;
- az AppSec ügye: a hackereknek ellenállóbb szoftverek fejlesztése alkalmazás

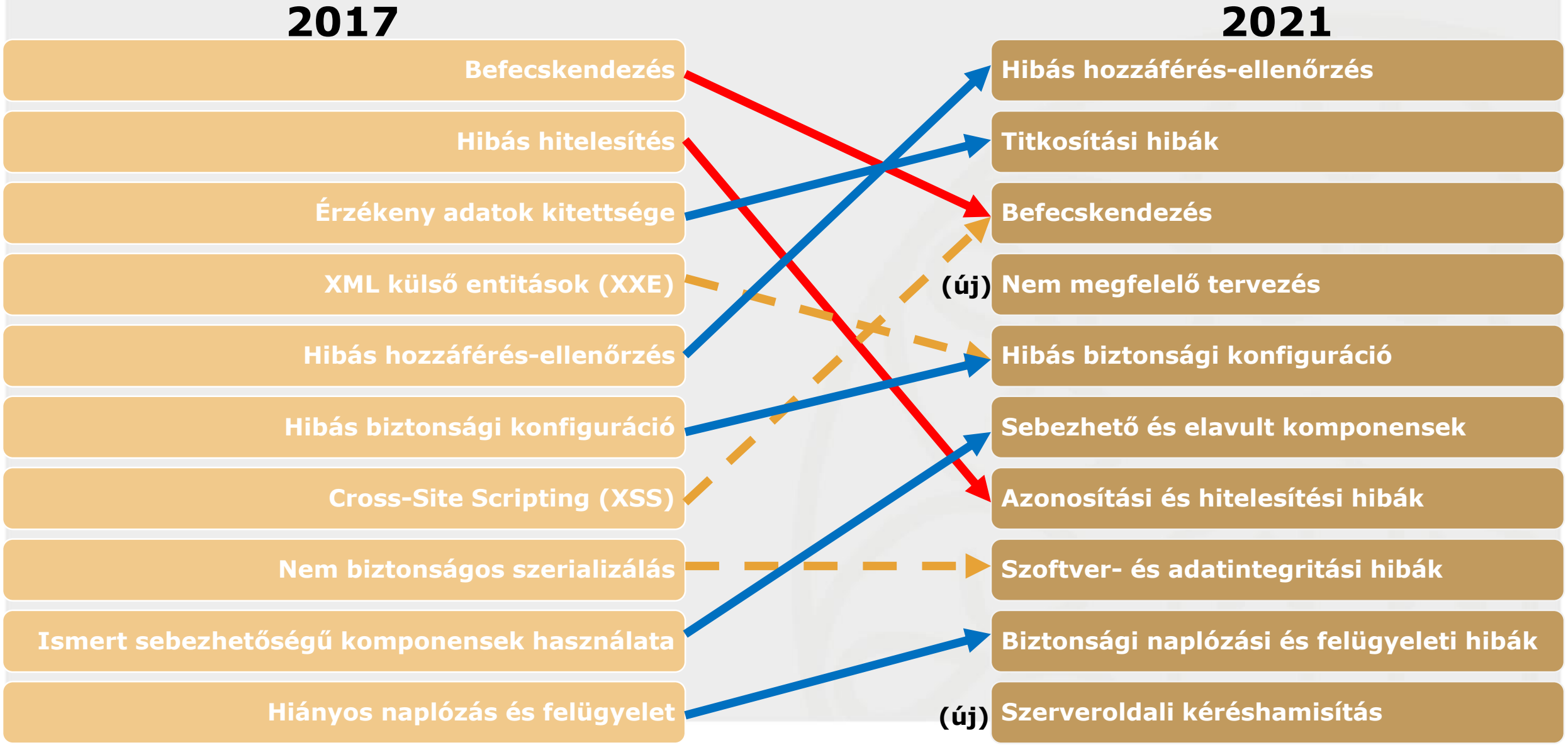
OWASP Top 10

A fejlesztők és a webalkalmazások biztonságának szabványos tudatossági dokumentuma. Széles körű konszenzust képvisel a webes alkalmazásokat érintő legkritikusabb biztonsági kockázatokról.

IV/1. Az új OWASP Top10

A01:2021-Broken Access Control	Hibás hozzáférés-ellenőrzés
A02:2021-Cryptographic Failures	Titkosítási hibák
A03:2021-Injection	Befecskendezés
A04:2021-Insecure Design	Nem megfelelő tervezés
A05:2021-Security Misconfiguration	Hibás biztonsági konfiguráció
A06:2021-Vulnerable and Outdated Components	Sebezhető és elavult komponensek
A07:2021-Identification and Authentication Failures	Azonosítási és hitelesítési hibák
A08:2021-Software and Data Integrity Failures	Szoftver- és adatintegritási hibák
A09:2021-Security Logging and Monitoring Failures	Biztonsági naplózási és felügyeleti hibák
A10:2021-Server-Side Request Forgery	Szerveroldali kéréshamisítás

IV/2. Az új OWASP Top10



IV/3. Az új OWASP Top10

Név	Összes CWE	Előfordulás alkalmazások-ban	Súlyozott kihasználás	Súlyozott hatás	Összes előfordulás	Összes CVE
Hibás hozzáférés-ellenőrzés	34	3,81%	6,92	5,93	**318 487**	19 013
Titkosítási hibák	29	4,49%	7,29	6,81	233 788	3 075
Befecskendezés	33	3,37%	7,25	7,15	274 228	32 078
Nem megfelelő tervezés	**40**	3%	6,46	6,78	262 407	2 691
Hibás biztonsági konfiguráció	20	4,51%	8,12	6,56	208 387	**789**
Sebezhető és elavult komponensek	3	**8,77%**	5	5	30 457	0
Azonosítási és hitelesítési hibák	22	2,55%	7,4	6,5	132 195	3 897
Szoftver- és adatintegritási hibák	10	2,05%	6,96	**7,96**	47 972	1 152
Biztonsági naplózási és felügyeleti hibák	4	6,51%	6,87	4,99	53 615	242
Szerveroldali kéréshamisítás	1	2,72%	**8,28**	6,72	9 503	385

A01:2021 – Broken Access Control
Hibás hozzáférés-ellenőrzés

- CWE-200 Érzékeny információk jogosulatlan szereplőnek való kiszolgáltatása
- CWE-201 Érzékeny információk nyilvánosságra hozatala az elküldött adatokon keresztül
- CWE-275 Jogosultsági problémák
- CWE-276 Nem megfelelő alapértelmezett hozzáférési jogosultságok
- CWE-284 Nem megfelelő hozzáférés-szabályozás
- CWE-285 Nem megfelelő engedélyezés

A Travis CI sebezhetősége potenciálisan nyilvánosságra hozhatta a platformon lévő publikus nyílt forráskódú projektek titkos adatait.

- **2021 szeptemberében** egy olyan hibát fedeztek fel a Travis CI nevű szoftvertesztelési megoldásban, amelynek következtében a build-tárhelyekkel kapcsolatos **titkos adatok hozzáférhetővé váltak** (privát kulcsok, API-k) minden olyan projekt számára, amely klónozta az adott tárhelyet.

A02:2021 – Cryptographic Failures
Titkosítási hibák

- CWE-261 Gyenge kódolás a jelszóhoz
- CWE-310 Titkosítási problémák
- CWE-319 Érzékeny információk egyszerű szöveges továbbítása
- CWE-321 Keményen kódolt kriptográfiai kulcs használata
- CWE-322 Kulcscsere entitás-hitelesítés nélkül

A VeryFitPro nevű androidos fitneszalkalmazásról kiderült, hogy érzékeny adatokat továbbít egyszerű szöveges formában.

- **2021 júniusában** jelentették, hogy egy körülbelül 10 millió letöltéssel rendelkező androidos fitneszalkalmazás **egyszerű szövegben küldte el az általa kezelt adatokat**. Ez a kriptográfiai hiba egyik legjobb példája, amely potenciálisan érzékeny adatokat, köztük jelszavakat szivárogtatott ki a támadóknak.

A03:2021 – Injection
Befecskendezés

- CWE-20 Helytelen bemeneti hitelesítés
- CWE-79 A bemenet nem megfelelő hatástalanítása a weboldal létrehozása során ("Cross-site Scripting")
- CWE-89 SQL-parancsban használt speciális elemek nem megfelelő semlegesítése ("SQL Injection")
- CWE-94 A kód létrehozásának nem megfelelő ellenőrzése ("Code Injection")
- CWE-116 A kimenet helytelen kódolása vagy kikerülése

SQL befecskendezési sebezhetőségeket találtak a Sophos Cyberoam termékeiben.

•2020 decemberében a Sophos javításokat adott ki a Cyberoam termékeiben található SQL-injekciós sebezhetőségek javítására. Ez a sebezhetőség **lehetővé tette a támadók számára, hogy távolról fiókokat adjanak hozzá az** ezeken az eszközökön futó **operációs rendszerhez**, ha az eszköz adminisztrációs felülete nyilvánosan hozzáférhető volt.

A04:2021 – Insecure Design
Nem megfelelő tervezés

- CWE-73 A fájlnév vagy elérési útvonal külső vezérlése
- CWE-235 Extra paraméterek helytelen kezelése
- CWE-256 Hitelesítő adatok nem védett tárolása
- CWE-257 Jelszavak helyreállítható formátumban történő tárolása
- CWE-266 Helytelen jogosultságkiosztás
- CWE-269 Nem megfelelő jogosultságkezelés
- CWE-311 Érzékeny adatok titkosításának hiánya

A Kaseya virtuális rendszergazda (VSA) hibái miatt a REvil zsarolóprogram elterjedése.

- 2021. július 2-án jelentések láttak napvilágot arról, hogy számos olyan vállalat, amelynek hálózatait a Kaseya Virtual System Administrator (VSA) kezelte, nagyszabású zsarolóprogram-támadás áldozatává vált. A támadók a Kaseya VSA-ban található hibákat használták fel a REvil zsarolóprogram terjesztésére.

A05:2021 – Security Misconfiguration
Hibás biztonsági konfiguráció

- CWE-15 A rendszer vagy a konfiguráció beállításának külső vezérlése
- CWE-260 Jelszó a konfigurációs fájlban
- CWE-315 Érzékeny információk egyértelmű szövegű tárolása sütikben
- CWE-520 .NET hibás konfiguráció: Megszemélyesítés használata
- CWE-526 Érzékeny információk felfedése környezeti változókon keresztül

Egy felhőalapú adatbázis hibás konfigurációja több mint egymillió rekord nyilvános közzétételéhez vezetett.

- 2021 szeptemberében jelentették, hogy az indonéziai Hírközlési és Informatikai Minisztérium **nem megfelelően konfigurálta felhőalapú adatbázisát**. Ez azt eredményezte, hogy az ország COVID-19 karanténkezelő rendszerének **egymillió rekordja nyilvánosan hozzáférhetővé vált az interneten**.

A06:2021 – Vulnerable and Outdated Components
Sebezhető és elavult komponensek

- CWE-937 OWASP Top 10 2013: Ismert sebezhetőségekkel rendelkező komponensek használata
- CWE-1035 2017 Top 10 A9: Ismert sebezhetőségű komponensek használata
- CWE-1104 Nem karbantartott harmadik féltől származó komponensek használata

Az Equifax egy sebezhető Apache Struts könyvtáron keresztül szenvedett el egy drága, nagy nyilvánosságot kapott támadást.

- 2017 szeptemberében az Equifax értesítette ügyfeleit arról, hogy adatvédelmi incidens történt. A jogsértés kiváltó oka az volt, hogy az Equifax egy **sebezhető** Apache Struts **könyvtárat használt**. Becslések szerint az incidens akár 1,38 milliárd dollárjába is kerülhetett a vállalatnak.

A07:2021 – Identification and Authentication Failures
Azonosítási és hitelesítési hibák

- CWE-255 Hitelesítési adatok kezelésének hibái
- CWE-259 Keményen kódolt jelszó használata
- CWE-287 Helytelen hitelesítés
- CWE-288 Hitelesítés megkerülése alternatív útvonal vagy csatorna használatával
- CWE-290 Hitelesítés megkerülése hamisítással
- CWE-295 Nem megfelelő tanúsítvány-hitelesítés
- CWE-521 Gyenge jelszókövetelmények

Az Apple egyszeri bejelentkezési rendszerében (SSO) szolgáltatásának hibája lehetővé tette a teljes fiókátvételt.

•2020 májusában hibát találtak az Apple SSO bejelentkezési szolgáltatásában. A hiba az e szolgáltatás részeként használt JSON Web Token (JWT) ellenőrzésében volt jelen, ami lehetővé tette, hogy egy személy **úgy módosítsa a meglévő JWT-t, hogy az egy másik felhasználó e-mail címét tartalmazza.** Ez a sebezhetőség **lehetővé tette az áldozat fiókjainak teljes körű átvételét**.

A08:2021 – Software and Data Integrity Failures
Szoftver- és adatintegritási hibák

- CWE-345 Az adatok hitelességének nem megfelelő ellenőrzése
- CWE-353 Hiányzó támogatás az integritásellenőrzéshez
- CWE-426 Nem megbízható keresési útvonal
- CWE-565 Validálás és integritásellenőrzés nélküli cookie-kra való támaszkodás
- CWE-784 Validálás és integritásellenőrzés nélküli cookie-kra való hagyatkozás biztonsági döntésben

Több száz ügyfélhálózatot érintett a Codecov adatvédelmi incidense a nem megfelelő hitelesítési ellenőrzések miatt.

- 2021 áprilisában a CodeCov kódelemzőt biztonsági incidens érte, amelynek következtében az ügyfelek által használt bash szkriptet manipulálták. A kódrészletek feltöltésére használt Bash Uploader szkripthez ismeretlen személyek illetéktelenül hozzáfértek és úgy módosították, hogy az az ügyfelek által feltöltött adatokat a cég hálózatán kívülre exportálja.

A09:2021 – Security Logging and Monitoring Failures
Biztonsági naplózási és felügyeleti hibák

- CWE-117 Helytelen kimeneti semlegesítés a naplókhoz
- CWE-223 Biztonsági szempontból fontos információk kihagyása
- CWE-532 Érzékeny információk beillesztése a naplófájlba
- CWE-778 Elégtelen naplózás

A megfelelő biztonsági naplózás és nyomon követés elmulasztása vezetett az Egyesült Királyság kormányzati webhelyei elleni cryptojacking támadáshoz.

•2018 februárjában egy kriptobányász program került be a Browsealoud nevű szolgáltatásba. Ez számos webhelyet érintett, köztük az Egyesült Királyság kormányzati webhelyeit is. A szolgáltatást használó webhelyek közül sokan **nem engedélyezték a megfelelő naplózást** egy olyan vezérlőn keresztül, mint például a tartalombiztonsági politika (CSP), amely a problémát észlelte volna és figyelmeztetett volna rá. Ehelyett manuálisan azonosították a problémát.

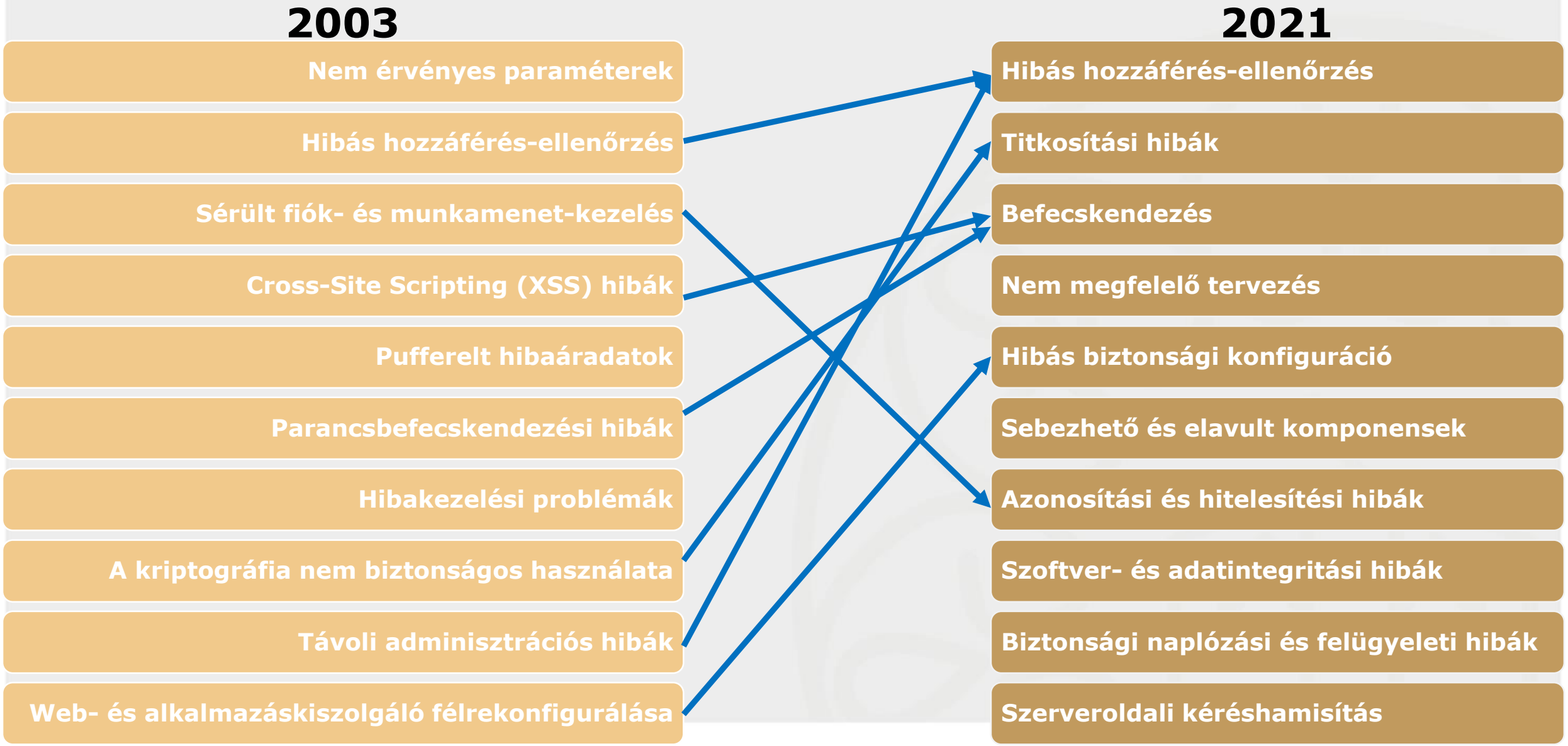
A10:2021 – Server-Side Request Forgery (SSRF)
Szerveroldali kéréshamisítás

CWE-918 Kiszolgálóoldali kéréshamisítás (SSRF)

A GitLab SSRF-je lehetővé tette a támadók számára, hogy kéréseket küldjenek belső szerverekre és szolgáltatásokra.

- A GitLab 2021 júniusában **SSRF sebezhetőséget talált** a CLI Lint API könyvtárában, amely a kódkezelésért és a fejlesztői munkafolyamatok kezeléséért volt felelős. Ez **lehetővé tette, hogy egy támadó kéréseket küldjön a szervezet belső szervereihez és szolgáltatásaihoz**.

Következtetések



KÖSZÖNÖM A FIGYELMET!

uni-nke.hu