TOKODI
SOFTWARE

Alkalmazás-szintű intézkedési tételek felmérése

> **MINTA — fiktív adatokkal.** A megrendelő, a rendszer és a megállapítások kitaláltak. A dokumentum azt mutatja meg, mit kap a megrendelő egy felmérés végén. A valós dokumentumban minden tételnél fix ár szerepel.

Megrendelő	Minta Kereskedelmi Zrt. *(fiktív)*
Rendszer	Ügyfél- és rendelésportál — ASP.NET MVC (.NET Framework 4.6.1), SQL Server 2016, saját fejlesztés 2017-ből, az eredeti fejlesztő már nem elérhető
Forrás	2026. szeptemberi penetrációs teszt jelentés (P-01…P-03) és NIS2 intézkedési terv (IT-07, IT-11)
Hozzáférés a felméréshez	Olvasási jog a forráskódhoz, a tesztkörnyezethez és a telepítési leíráshoz. Éles adathoz nem volt hozzáférés.
Felmérés ideje	2026. október, 6 munkanap
Készítette	Tokodi Software Kft. · Tokodi Lajos

MINTA

1. Vezetői összefoglaló

Az auditjelentés **5 megállapítása** érinti a portál saját kódját.

	TÉTEL	SÚLYOSSÁG	MEGOLDÁS	MÉRET
F1	Jelszavak és API-kulcs a konfigurációban és a kódtárban	Kritikus	Kódból	M
F2	Más ügyfél rendelése lekérdezhető (IDOR)	Magas	Kódból	S
F3	Nincs biztonsági napló	Magas	Kódból	M
F4	Nincs MFA az adminfelületen, gyenge jelszótárolás	Magas	Kódból	L
F5	Támogatás nélküli komponensek	Közepes	**Részben kódból, részben kompenzáló kontrollal**	M

Méret: S = legfeljebb 2 munkanap · M = 3–5 munkanap · L = 6–10 munkanap.

A legfontosabb döntés: az F5-ben szereplő riportkomponens cseréje a portál nyomtatási funkciójának újraírását jelentené. Ezt **nem javasoljuk most** — a kockázat kompenzáló kontrollal arányosan kezelhető, a csere a következő nagyobb fejlesztéssel együtt olcsóbb (3. fejezet, F5).

Javasolt ütemezés: négy hullámban, kb. 5–6 hét alatt (4. fejezet). Az F1 kulcscseréje nem várhat a többire: azt a megrendelés napján elvégezzük.

2. A felmérés módja

1. **A megállapításokból indultunk, nem a teljes kódból.** Tételenként megkerestük, hol él a hiba, és mi a gyökéroka.

2. **Megnéztük, hogyan épül és települ a rendszer.** A javítás kockázata itt sokszor nagyobb, mint a kódban: ennél a portálnál a telepítés kézi fájlmásolással történik, verziózott kiadás nélkül. Ezt minden tételnél figyelembe vettük.
3. **Tételenként leírtuk:** mi a javítás, mekkora, mi a kockázata, és milyen bizonyítékot kap a megrendelő a következő auditra.

Nem része a felmérésnek: infrastruktúra (hálózat, TLS-beállítás, tűzfal), szabályzatok, és a javítás utáni **ellenőrző újrateszt — ezt a pentestet végző fél végzi**, nem a javítást végző.

---

3. Tételek

F1 — Jelszavak és API-kulcs a konfigurációban és a kódtárban

Forrás: IT-07 · **Súlyosság:** kritikus · **Méret:** M

Hol él	`Web.config` (adatbázis-kapcsolati sztring `sa` felhasználóval), `PaymentClient.cs` (fizetési szolgáltató API-kulcsa beégetve). Mindkettő a git-előzményben is, 2017 óta.
Gyökérok	Nincs titokkezelés; a fejlesztői és az éles konfiguráció ugyanaz a fájl.
Javítás	1. **Azonnal:** az érintett jelszó és API-kulcs cseréje (a régiek érvénytelenítése). 2. A titkok kulcstárolóba kerülnek (Azure Key Vault), az alkalmazás onnan olvassa. 3. Az `sa` helyett saját, legkisebb jogosultságú adatbázis-felhasználó. 4. Titokszivárgás-ellenőrzés a kódtárban.
Amit nem javaslunk	A git-előzmény átírását. A kiszivárgott titok attól nem lesz titok, hogy eltüntetjük — a csere a valódi javítás.
Kockázat	Kulcscserénél rövid kiesés lehetséges → karbantartási ablakban, visszaállítási tervvel.
Bizonyíték az auditra	Kulcscsere-jegyzőkönyv (mi, mikor, ki), a kulcstároló hozzáférési listája, a titokszivárgás-ellenőrzés tiszta eredménye.

F2 — Más ügyfél rendelése lekérdezhető (IDOR)

Forrás: P-01 · **Súlyosság:** magas · **Méret:** S

Hol él	`OrdersController.Details(int id)` és `InvoicesController.Download(int id)` : az azonosító alapján bármely rendelés és számla megnyílik, ha a felhasználó be van jelentkezve.
Gyökérok	A jogosultság-ellenőrzés csak a bejelentkezést nézi, a tulajdonost nem. Ugyanez a minta 7 további végponton is megvan — ezeket a pentest nem jelezte, a felmérés találta meg.
Javítás	Tulajdonos-ellenőrzés a lekérdezés szintjén, **mind a 9 végponton**, közös szűrővel. Automatikus teszt minden végpontra: idegen azonosítóval 404-et kell adnia.
Kockázat	Alacsony. Az ügyfélszolgálati szerepkör jogosan lát mindent — ezt külön szerepként kezeljük, hogy ne törjön el.
Bizonyíték az auditra	A tesztek listája és eredménye; a javított végpontok jegyzéke.

MINTA

F3 — Nincs biztonsági napló

Forrás: IT-11 · **Súlyosság:** magas · **Méret:** M

Hol él	A portál csak hibákat naplóz, helyi fájlba, 7 napos megőrzéssel. Bejelentkezés, sikertelen próbálkozás, jogosultság-változás, adatexport nem kerül naplóba.
Javítás	Strukturált biztonsági napló (ki, mit, mikor, honnan, milyen eredménnyel) a fenti eseményekre. Központi gyűjtés, a megrendelő SIEM-jébe továbbítható formátumban. Megőrzés a megrendelő szabályzata szerint.
Miért ez a második hullám	Az F4 (MFA) eseményei már ebbe a naplóba kerülnek, így az a javítás is bizonyítható lesz.
Kockázat	Alacsony. Személyes adat a naplóba nem kerül (jelszó, kártyaadat soha), az IP-cím és a felhasználói azonosító igen — ezt az adatkezelési tájékoztatóban jelezni kell.
Bizonyíték az auditra	Mintanapló a tesztkörnyezetből minden eseménytípusra; a naplózott események jegyzéke.

F4 — Nincs MFA az adminfelületen, gyenge jelszótárolás

Forrás: P-02, IT-07 · **Súlyosság:** magas · **Méret:** L

Hol él	Saját fejlesztésű bejelentkezés; a jelszavak sózatlan SHA-1 hash-sel tárolva; az `/admin` útvonal ugyanazzal a jelszóval érhető el, mint az ügyféloldal.
Javítás	1. Az adminisztrátorok a megrendelő Entra ID-jával lépnek be (SSO, a céges MFA-val). 2. Az ügyfélfiókoknál a jelszó a következő bejelentkezéskor korszerű, lassú hash-re (PBKDF2) migrálódik — jelszócsere kikényszerítése nélkül. 3. Fiókzárolás ismételt sikertelen próbálkozás után.
Kockázat	Közepes: egy hibás SSO-beállítás kizárhatja az adminokat. → Egy dokumentált, széfben tartott vészhelyzeti fiók, amelynek minden használata naplózódik (F3).
Bizonyíték az auditra	Az Entra ID alkalmazásregisztráció és a feltételes hozzáférési szabály; a migrált jelszóhash-ek aránya; a vészhelyzeti fiók eljárása.

F5 — Támogatás nélküli komponensek

Forrás: P-03 · **Súlyosság:** közepes · **Méret:** M

KOMPONENS	ÁLLAPOT	JAVASLAT
.NET Framework 4.6.1	A támogatás 2022-ben megszűnt	**Kódból:** emelés 4.8.1-re. Kis kockázatú, a kód szinte változatlan. *.NET 8-ra migrálni nem szükséges az auditponthoz — az egy külön, jóval nagyobb döntés.*
jQuery 1.12	Ismert XSS-sérülékenységek	**Kódból:** emelés 3.x-re, a 4 érintett oldal tesztelésével
Riportkomponens (számlanyomtatás), 2013-as runtime	Nem támogatott; a cseréje a nyomtatási funkció újraírása	**Kompenzáló kontroll:** a riportgenerálás külön, csak belső hálózatból elérhető szolgáltatásba kerül; bemenetét szigorúan ellenőrizzük; a kockázatot a megrendelő írásban elfogadja, a csere a következő nagyobb fejlesztés része

Bizonyíték az auditra: komponensjegyzék (SBOM) a javítás után; a riportkomponens kockázatelfogadó nyilatkozata, határidővel.

MINTA

4. Javasolt sorrend

HULLÁM	TÉTELEK	MIÉRT EBBEN A SORRENDBEN	IDŐ
0	F1 kulcscsere	A kiszivárgott titok most is használható	a megrendelés napja
1	F1 titokkezelés, F2	Kicsik, és azonnali kockázatot zárnak	1. hét
2	F3	A többi javítás bizonyítéka erre épül	2. hét
3	F4	A legnagyobb tétel; a naplózásra támaszkodik	3–4. hét
4	F5	A legkisebb sürgősségű	5–6. hét

Minden hullám **verziózott kiadással** zárul, visszaállítási tervvel. A telepítési folyamatot az első hullámban egyszerű, megismételhető kiadásra alakítjuk — enélkül minden további javítás kockázatosabb.

5. Amit a megrendelőtől kérünk

- Írási jogot a kódtárhoz és a tesztkörnyezethez; az élesítést a megrendelő üzemeltetője hagyja jóvá.
- Egy technikai kapcsolattartót, aki a kódfelülvizsgálatot jóváhagyja.
- Karbantartási ablakokat a 0., 3. és 4. hullámhoz.
- Az Entra ID-ban egy alkalmazásregisztrációs jogot (F4).

6. Ár és ütemezés

TÉTEL	MÉRET	ÁR
F1	M	*[fix ár]*
F2	S	*[fix ár]*
F3	M	*[fix ár]*
F4	L	*[fix ár]*
F5	M	*[fix ár]*
Összesen		***[fix ár]***

A valós dokumentumban itt tételenkénti fix ár, fizetési ütemezés és a hullámok naptári dátuma szerepel. A megrendelő tételenként is dönthet: ha egy tételt saját fejlesztővel vagy kompenzáló kontrollal zár, azt nem számlázzuk.

Tokodi Software Kft. · 6423 Kelebia, Bajcsy-Zsilinszky utca 40. · Cg. 03-09-140638 · hello@tokodisoftware.com · tokodisoftware.com

MINTA