

ZKRÁCENÝ BEZPEČNOSTNÍ REPORT

Penetrační test webové aplikace a API

Sedmistránkový výtah z plného modelového reportu v1.7. Ukazuje rozhodnutí pro vedení, přesný stav nálezů a jeden zkrácený modelový nález včetně důkazů, nápravy a retestu.

KLIENT FakturaCloud fiktivní modelový klient	SLUŽBA TORCH-WEB grey-box pentest webu a API	ROZSAH app.fakturacloud.test REST API v2
TEST 2.-6. 3. 2026 retest 24. 3. 2026	TESTOVALI Bezpečnostní tým Torch Labs technická kontrola Jan Marval	DOKUMENT TL-FC-2026-03-PREVIEW odvozeno z v1.7-model

Tohle je veřejná ukázka. Klient, systém, termíny, nálezy, účty, důkazy i výsledky retestu jsou smyšlené. Doména .test a všechny identifikátory jsou vyhrazené pro modelový dataset.

00 **Obsah**

01 · Shrnutí pro vedení	3
02 · Přehled nálezů	3
03 · Zkrácený modelový nález	4
TCH-001 · Čtení faktur jiného tenanta přes API	4
TCH-001 · Reprodukce a důkazy	5
TCH-001 · Náprava a retest	6
04 · Rozsah, metodika a výstup	7

CO JE V UKÁZCE

Preview zachovává rozhodnutí, přehled všech šesti nálezů a jeden zkrácený detail TCH-001. Plný report obsahuje všech šest detailů, úplnou mapu pokrytí, retest protokol, plán nápravy a evidence index.

01

Shrnutí pro vedení

RELEASE BLOCKER · TCH-004

NEVYDÁVAT

Důvod:

TCH-004 nebyl opraven ani retestován. Před vydáním je nutná oprava a PASS retest, nebo písemná výjimka schválená vlastníkem rizika.

OPRAVENO A OVĚŘENO

TCH-001 až TCH-003 + TCH-005

ZBÝVÁ

TCH-004 · release blocker

FOLLOW-UP

TCH-005 rozsah · TCH-006 správa API

TCH-004: NÍZKÁ závažnost · RELEASE BLOCKER · P0 interní priorit. Jde o tři různé osy. Dopad je omezený, ale okamžitá revokace tokenů je explicitní klientské kritérium vydání.

NÁLEZY CELKEM

6

OPRAVY OVĚŘENY

4/5

OTEVŘENÁ ZRANITELNOST

1

OTEVŘENÉ INFO

1

PROVEDENÉ KONTROLY

19/19

02

Přehled nálezů

ID	NÁLEZ	ZÁVAŽNOST	STAV
TCH-001	Čtení faktur jiného tenanta přes API Broken Object-Level Authorization	VYSOKÁ	OPRAVA OVĚŘENA
TCH-002	Klient může změnit interní stav úhrady Broken Object Property-Level Authorization	STŘEDNÍ	OPRAVA OVĚŘENA
TCH-003	Uložené XSS v komentáři faktury Stored Cross-Site Scripting	STŘEDNÍ	OPRAVA OVĚŘENA
TCH-004	Access token zůstává po změně hesla platný Nízká závažnost, ale nesplněné klientské kritérium vydání	NÍZKÁ	OTEVŘENO RELEASE BLOCKER P0 interní · retest neproveden
TCH-005	PDF faktury zůstává v cache prohlížeče Service worker a CDN mimo ověřený rozsah	NÍZKÁ	OVĚŘENO V ROZSAHU
TCH-006	Neúplný inventář veřejných API verzí Nebyl prokázán únik ani slabší autorizace	INFO	DOPORUČENÍ

Retest: 19/19 provedených kontrol PASS · 1 nález nebyl retestován · 1 informační doporučení retest nevyžaduje. Cílený retest není nový kompletní pentest.

03 · ZKRÁCENÝ MODELOVÝ NÁLEZ

03 TCH-001 · Čtení faktur jiného tenanta přes API

TCH-001 · **VYSOKÁ** OPRAVA OVĚŘENA

Broken Object-Level Authorization

Po změně ID v požadavku API vrátilo fakturu mimo tenant přihlášeného uživatele. Klient tenanta acme proto získal fakturu tenanta beta-corp.

CVSS 4.0: 7.1 · CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N
Míra jistoty: POTVRZENO · reprodukcí důkaz
CWE-639 · OWASP API1:2023 · WSTG-ATHZ-04 · COV-API-AUTHZ-0BJ-001

Dopad na byznys

V tomto scénáři mohl zákazník číst faktury jiné firmy. Pro B2B SaaS jde o přímé riziko porušení tenant isolation a důvěrnosti zákaznických dat. Sekvenční ID umožňovala útok opakovat; rozsah nebyl kvůli minimalizaci dat ověřován hromadnou enumerací.

Technický dopad

V doložené původní reprodukci obdržela role client HTTP 200 pro objekt mimo svůj tenant. Důkaz se vztahuje k uvedenému GET endpointu; role accountant a admin byly ověřeny až při retestu opravy.

Ověřený scénář



Dotčený povrch	
AKTIVUM	A-API-01
BASE URL	app.fakturacloud.test/api/v2
ENDPOINT	GET /api/v2/invoices/{id}
PŮVODNĚ PROKÁZÁNO	role client
TENANTY	acme, beta-corp
TESTOVACÍ KONTEXT	
PŮVODNÍ BUILD	fc-api-2.18.0
RETEST BUILD	fc-api-2.18.3
RETESTOVANÉ ROLE	client, accountant, admin

- Předpoklady scénáře
- Platný účet role client a bearer token.
 - Znalost nebo odhad číselného ID faktury; v modelu jsou ID sekvenční.
 - Žádný administrátorský přístup ani speciální nástroj.

TCH-001 - Reprodukce a důkazy

Kroky k reprodukci

1. Přihlaste se účtem `client-acme@example.test`.
2. Ověřte vlastní objekt požadavkem `GET /api/v2/invoices/8401`; odpověď je `HTTP 200` s tenantem `acme`.
3. Změňte pouze ID na 8412, které v datasetu patří tenantovi `beta-corp`.
4. Původní build vrátí `HTTP 200` a pole `tenant:beta-corp`.
5. Kontrolní požadavek bez tokenu vrátí 401 a neexistující ID 999999 vrátí 404.

DŮKAZNÍ REŽIM

Syntetická a redigovaná data. Ukázky důkazů jsou přímo v reportu. Toto veřejné PDF neobsahuje přílohy.

EV-TCH-001-HTTP-01

POŽADAVEK

```
GET /api/v2/invoices/8412 HTTP/1.1
Host: app.fakturacloud.test
Authorization: Bearer <MODEL_TOKEN_REDACTED>
Role: client
Tenant: acme
```

Skutečné: Požadavek s rolí `client` pokračoval ke zpracování objektu mimo tenant.

Očekávané: API má objekt mimo tenant vyhodnotit jako neexistující a vrátit 404.

Redigovaný transkript; všechny identifikátory jsou testovací.

EV-TCH-001-HTTP-02

200 OK

```
HTTP/1.1 200 OK
Content-Type: application/json

{"id":8412,"tenant":"beta-corp",
 "customer":"N••••••• s.r.o.", "total_czk":48200}
```

Skutečné: API vrátilo fakturu tenanta `beta-corp` uživateli `acme`.

Očekávané: 404 bez informace, zda cizí objekt existuje.

Redigovaný obsah; žádné pole nepochází od reálného klienta.

Rozsah původního důkazu

Původní reprodukce dokládá jeden bezpečně zvolený cizí objekt pro roli `client` a kontrolní odpovědi 401/404. Hromadná enumerace nebyla kvůli minimalizaci dat provedena.

Jak číst dvojici artefaktů

První artefakt zachycuje přesný požadavek, druhý odpověď s objektem jiného tenanta.

- Mezi vlastní a cizí fakturou se změnilo pouze invoice ID.
- Role `accountant` a `admin` jsou doloženy až v EV-TCH-001-RT-01.
- Hodnoty jsou redigované a výhradně syntetické.

TCH-001 - Náprava

EV-TCH-001-CTRL-01401 / 404 NEGATIVNÍ KONTROLY Skutečné: Kontroly potvrdily autentizaci i standardní 404 větev. Očekávané: Stejná 404 větev také pro objekt mimo tenant.	EV-TCH-001-RT-01404 NOT FOUND RETEST ROLE × TENANT Skutečné: Retest vrátil jednotné 404 pro všechny cross-tenant kombinace. Očekávané: Cizí objekty nejsou rozlišitelné; vlastní zůstávají dostupné.
--	--

Pravděpodobná příčina · bez ověření zdrojového kódu

Pozorování odpovídá dotazu podle invoice ID bez omezení na tenant. Doporučení míří na společnou autorizační vrstvu.

Dočasná mitigace

- Do opravy zablokovat endpoint pro roli client nebo použít allowlist faktur.
- Monitorovat opakované dotazy na cizí a neexistující ID bez citlivých payloadů.

Trvalá oprava

- Načítat objekt kombinací ID a tenantId ze serverové session.
- Centralizovat objektovou autorizaci pro všechny endpointy a metody.
- Pro objekt mimo tenant vracet stejnou 404 jako pro neexistující objekt.
- Přidat do CI matici role × tenant × objekt.

Ověřovací kritéria · cílový stav

- Každá role obdrží pro cizí invoice ID odpověď 404.
- Vlastní objekty zůstanou dostupné podle role.
- Tělo, délka a časování významně nerozliší cizí a neexistující ID.
- Regresní test pokryje GET i související metody.

● OPRAVA OVĚŘENA	2026-03-24 · fc-api-2.18.3	EV-TCH-001-RT-01
Cross-tenant kombinace vracely jednotné 404 a vlastní objekty zůstaly dostupné. Výsledek platí pro uvedený endpoint a build. Reziduální riziko: Nízké pouze pro retestovaný endpoint a build; nejde o nový kompletní pentest.		

CO VÍME - Původní build vrátil cizí objekt s HTTP 200. - Opravený build prošel 5 popsánymi kontrolami. - Důkazy mají stabilní ID; tato ukázka uvádí jejich obsah přímo v reportu.	CO NETVRDÍME - Nebyla provedena hromadná enumerace faktur. - Nebyl potvrzen řetězec více nálezu. - Cílený retest není nový kompletní pentest ani záruka všech metod.
---	--

Reference: OWASP API Security Top 10 2023 · API1 Broken Object Level Authorization · CWE-639 · OWASP WSTG 4.2 · WSTG-ATHZ-04. Přesné syntetické artefakty: EV-TCH-001-HTTP-01, HTTP-02, CTRL-01 a RT-01.

04 Rozsah, metodika a výstup

V rozsahu

- Stagingová webová aplikace `app.fakturacLOUD.test`.
- REST API v2: účty, fakturace a export.
- Role admin, accountant a client ve dvou testovacích tenantech.
- Autentizace, relace, tenant isolation, business logika a vstupy.

Mimo rozsah

- Produkce a data reálných zákazníků.
- Zdrojový kód, DoS, zátěžové a destruktivní testy.
- Phishing, kancelářská síť a koncová zařízení.
- CDN a service worker mimo výslovně popsany retest TCH-005.

Jak vzniká ověřitelný závěr

01 · ROZSAH

Schválená pravidla, aktiva, role, tenanty a časové omezení.

02 · MANUÁLNÍ TEST

OWASP WSTG, API Top 10 a omezené podpůrné nástroje.

03 · DŮKAZ

Reprodukce, negativní kontrola, evidence ID a redigovaný artefakt.

04 · RETEST

Přesný build, ověřovací kritéria, PASS/FAIL a reziduální riziko.

Hodnocení bez falešné přesnosti. CVSS 4.0 popisuje technické charakteristiky. Klientská závažnost, interní priorita, release blocker a reziduální riziko jsou vedeny odděleně. Referenční rámce mapují pokrytí; nejsou prohlášením compliance.

Plný ukázkový report v1.7

- 33 stran a všech 6 nálezů v plném znění.
- Business a technický dopad, reprodukce, kontroly, náprava, ověřovací kritéria a retest.
- Mapa pokrytí, plán nápravy, řízení dokumentu a přesná omezení závěrů.
- 21 syntetických evidence souborů, 4 vložené přílohy, manifest, coverage a retest matice, SHA-256 a QA protokol.

Co obsahuje tento preview PDF

Krátká verze je výtah, nikoli náhrada plného reportu. Přesto zachovává auditní návaznost u modelového TCH-001.

STRAN
7

DŮKAZY
4

PŘÍLOHY
0

PUBLIC PREVIEW uvádí syntetické ukázky důkazů TCH-001 přímo v reportu. PDF neobsahuje vložené soubory; úplné přílohy a jejich kontrolní součty patří k plnému reportu.

Chcete vidět plný report nebo probrat vlastní aplikaci?

Plná veřejná ukázka ukazuje všechna omezení, důkazy i release rozhodnutí. Hovor není podmínkou.

torchlabs.cz
hello@torchlabs.cz

Metodika: OWASP Web Security Testing Guide 4.2 · OWASP API Security Top 10 2023 · OWASP ASVS 5.0.0 pro mapování pokrytí · CVSS 4.0. Test dokumentuje stav známého rozsahu v daném čase; negarantuje nalezení všech chyb.