PENTROPIC.

REPORT DI ESEMPIO · DATI DIMOSTRATIVI

PENETRATION TEST REPORT

Valutazione di sicurezza applicativa, API & AI

Sample Cloud S.p.A. — piattaforma SaaS multi-tenant

AMBIENTE stage.sample-cloud.example	MODALITÀ Grey-box autenticato	PERIODO gg/mm/aaaa
CLASSIFICAZIONE Riservato	VERSIONE 1.0	A CURA DI Pentropic — Security Hub

DOCUMENT CONTROL

Controllo del documento

DOCUMENTO	Penetration Test Report — Sample Cloud S.p.A.
CLASSIFICAZIONE	Riservato — distribuzione limitata al committente
DESTINATARI	Team di sviluppo / responsabile IT / management
VERSIONE	1.0 — emissione iniziale
AUTORE	Pentropic (Security Hub S.r.l.)
RISERVATEZZA	Dati de-identificati in elaborazione; VM cifrata in Italia; distruzione entro 24h dalla conferma di ricezione

INDICE

Contenuti

01 — SINTESI ESECUTIVA

In breve

La valutazione su **Sample Cloud** ha identificato **10 vulnerabilità**, di cui **1 critica** che consente a qualunque utente registrato di ottenere privilegi di amministratore. Il filo conduttore è ricorrente: **controlli di autorizzazione applicati lato client, nel prompt o assenti** anziché imposti lato server, mass-assignment nei serializer e isolamento multi-tenant verificato solo parzialmente.

Quattro vulnerabilità (privilege escalation, lettura cross-tenant di dati personali, risorsa API anonima con credenziali in chiaro, recupero documenti non autorizzati via assistente AI) hanno impatto diretto su **riservatezza e GDPR** e vanno affrontate prima del rilascio. Le rimanenti riducono superficie d'attacco ed esposizione a brute force.

1	4	4	1
CRITICA	ALTE	MEDIE	BASSA

Come leggere questo report. Ogni vulnerabilità è documentata con prova tecnica (richiesta/risposta, evidenze), impatto e remediation, ed è marcata **Confermato** (riprodotta e verificata) o **Da validare** (indizio forte, da confermare col team). La sezione *Controlli verificati robusti* elenca ciò che **non** è risultato vulnerabile.

Sintesi dei findings

ID	SEVERITÀ	VULNERABILITÀ	CATEGORIA	CVSS	CWE
F1	CRITICA	Privilege escalation via mass-assignment	Authz / API	9.1	CWE-915
F2	ALTA	Lettura cross-tenant di dati personali (BOLA)	Authz / SaaS	7.7	CWE-639
F3	ALTA	Risorsa API anonima con credenziali in chiaro	Authn / API	7.5	CWE-306
F4	ALTA	Assistente AI: recupero documenti fuori perimetro	AI / LLM	7.1	CWE-285
F5	ALTA	Mass-assignment e bypass del workflow di approvazione	Logica / API	7.0	CWE-915
F6	MEDIA	Assenza di rate limiting / lockout sul login	Authn	5.9	CWE-307
F7	MEDIA	CORS misconfiguration (origin riflesso + credentials)	Config	5.4	CWE-942
F8	MEDIA	User enumeration via password reset	Authn	5.3	CWE-204
F9	MEDIA	Export anonimo con enumerazione dei token	Authz / API	5.0	CWE-639
F10	BASSA	Header di sicurezza mancanti (HSTS, CSP)	Config	3.1	CWE-693

02 — METODOLOGIA & APPROCCIO

Come abbiamo lavorato

Attività condotta in modalità **grey-box autenticata** con due utenze su due organizzazioni distinte, per verificare concretamente la segregazione dei dati tra clienti. Un penetration tester umano ha definito la strategia, validato e firmato i risultati; una struttura di agenti AI ha eseguito la copertura in parallelo sull'intera superficie. Traffico controllato, nessuna azione distruttiva.

1. **Ricognizione & mappatura**
   Enumerazione di domini, endpoint web e API, ruoli e flussi applicativi; costruzione della superficie d'attacco e del modello di autorizzazione atteso.

2. **Test di autenticazione & sessione**
   Robustezza dei token (firma, scadenza, claim), gestione delle sessioni, recupero password, rate limiting e lockout.

3. **Autorizzazione per ruolo & tenant**
   BOLA/BFLA, privilege escalation, isolamento multi-tenant in lettura e scrittura, con test incrociati tra le due utenze.

4. **Logica applicativa & injection**
   Mass-assignment, bypass dei workflow, business logic, injection, SSRF, esposizione dei dati e configurazioni (CORS, header).

5. **Funzioni AI**
   Assistente conversazionale e retrieval: autorizzazione sulle tool call, isolamento dei dati, prompt injection e data leakage.

6. **Validazione & reporting**
   Riproduzione di ogni finding, raccolta evidenze, classificazione CVSS 3.1, marcatura Confermato/Da validare e stesura remediation.

Standard di riferimento

OWASP WSTG · OWASP ASVS · OWASP API Top 10 · OWASP MASVS · PTES · CVSS 3.1 · CWE

Legenda severità (CVSS 3.1)

CRITICA	9.0–10.0 — sfruttabile, impatto sistemico
ALTA	7.0–8.9 — impatto grave su dati o accessi
MEDIA	4.0–6.9 — impatto circoscritto o condizionato
BASSA	0.1–3.9 — hardening / riduzione superficie

03 — DETTAGLIO DELLE VULNERABILITÀ

Findings

F1 **CRITICA** CVSS 9.1 CWE-915 Confermato

Privilege escalation via mass-assignment su `PATCH /api/v1/account/me`

RUOLO

Qualsiasi utente autenticato (riprodotto con profilo standard `cliente`).

DESCRIZIONE

Il serializer del profilo espone come **scrivibili** i campi `role` e `is_admin`. L'endpoint self-service `/account/me` li accetta in PATCH e li persiste senza controllo, permettendo all'utente di **promuoversi ad amministratore**.

RIPRODUZIONE

```
# richiesta
PATCH /api/v1/account/me HTTP/2
Authorization: Bearer <token-utente-standard>
Content-Type: application/json

{"is_admin": true}

# risposta  HTTP/2 200
prima:  is_admin=false  role=cliente
dopo:   is_admin=true   role=cliente   # accesso pannello admin
```

IMPATTO

Compromissione totale: accesso ai dati di **tutti i tenant**, pannello amministrativo, modifica e cancellazione arbitraria.

REMEDIATION

Campi privilegiati **read-only** nel serializer dell'utente finale; serializer dedicato e minimale per `/account/me`; serializer separato e protetto per le operazioni admin; verifica server-side che l'utente non possa elevare i propri privilegi.

F2 **ALTA** CVSS 7.7 CWE-639 Confermato

Lettura cross-tenant di dati personali (BOLA) su `/api/v1/orgs/{orgId}/employees`

DESCRIZIONE

Il token di sessione **non contiene** l'identificativo dell'organizzazione: il backend si fida dell'`orgId` nell'URL senza verificare l'appartenenza dell'utente.

RIPRODUZIONE

```
GET /api/v1/orgs/ORG-0042/employees   # org NON dell'utente
HTTP/2 200  count: 318
  → nome, codice fiscale, data di nascita, email, ruolo
```

IMPATTO

Esposizione di **PII di altri clienti** (codici fiscali, date di nascita, email). Violazione grave di riservatezza e GDPR.

REMEDIATION

Validare il tenant **lato server** ad ogni accesso; includere l'`orgId` nel token e confrontarlo con quello richiesto; centralizzare il controllo in un middleware.

F3 ALTA CVSS 7.5 CWE-306 Confermato

Risorsa API anonima con disclosure di credenziali su `/api/v1/meetings`

DESCRIZIONE

L'intera risorsa è esposta **senza autenticazione**: un anonimo legge tutte le sessioni con **password moderatore in chiaro** e può crearne/cancellarne (CRUD anonimo).

RIPRODUZIONE

```
GET /api/v1/meetings   # nessun header Authorization
HTTP/2 200
 id=37 room=mtg-37 moderator_password=xvPb9MuRi
 id=38 room=mtg-38 moderator_password=NE8njLbF7
```

IMPATTO

Un anonimo può **entrare come moderatore** in sessioni riservate e manomettere i meeting reali.

REMEDIATION

`IsAuthenticated` + autorizzazione per tenant sulla ViewSet; **non restituire mai** i segreti; proteggere i callback macchina-a-macchina con token/HMAC.

F4 ALTA CVSS 7.1 CWE-285 Confermato

Assistente AI «AskSample»: recupero documenti fuori dal perimetro dell'utente

DESCRIZIONE

L'assistente integrato con la knowledge base può invocare strumenti di ricerca documentale senza controllo server-side sufficiente sul perimetro dell'utente: si affida al **prompt** anziché all'**autorizzazione applicativa**. Manipolando il contesto si inducono ricerche su contenuti non pertinenti al ruolo.

RIPRODUZIONE

Conversazione in cui l'assistente, sollecitato a riassumere «le procedure dell'area amministrazione», restituisce estratti di documenti non assegnati al ruolo di test. Contenuti **realmente presenti** nei sistemi collegati (non allucinazioni). *Evidenze conversazionali allegate.*

IMPATTO

Accesso a documenti riservati (procedure interne, contratti, ticket, riferimenti a dati personali). Rischio GDPR e bypass dei controlli d'accesso.

REMEDIATION

Autorizzazione lato server su **ogni tool call**; retrieval vincolato all'identità e separazione dei tenant; logging delle invocazioni; test ricorrenti di prompt injection e data leakage.

LIMITE

Verificato: **nessuna esecuzione di codice**, nessun accesso diretto al database tramite l'assistente.

F5 ALTA CVSS 7.0 CWE-915 Confermato

Mass-assignment e bypass del workflow di approvazione su `POST /api/v1/invoices`

DESCRIZIONE

L'endpoint di creazione accetta campi che dovrebbero essere gestiti server-side — `status` e `owner_id`. È possibile creare un record già in stato **approvato** (saltando il flusso di validazione) e **assegnarlo ad un altro utente**.

RIPRODUZIONE

```
POST /api/v1/invoices
{"amount":1200,"status":"approved","owner_id":"USR-0007"}
HTTP/2 201   # creata approvata, intestata ad altri
```

IMPATTO

Alterazione dei processi di business, frode interna, ripudio: record approvati senza controllo e attribuiti a terzi.

REMEDIATION

Whitelist dei campi accettati in input; `status` governato solo dalla macchina a stati server-side; `owner_id` derivato dall'utente autenticato, non dal payload.

F6 MEDIA CVSS 5.9 CWE-307 Confermato

Assenza di rate limiting / lockout su `POST /api/v1/auth/login`

DESCRIZIONE

Nessun limite ai tentativi né lockout progressivo: brute force e credential stuffing ad alta frequenza senza ostacoli.

IMPATTO

Compromissione di account con password deboli o riutilizzate; abuso delle risorse.

REMEDIATION

Rate limiting per IP/account, lockout progressivo, CAPTCHA dopo N tentativi, allerta sui pattern anomali e, dove possibile, **MFA**.

F7 MEDIA CVSS 5.4 CWE-942 Confermato

CORS misconfiguration — riflessione dell'origin con credenziali

DESCRIZIONE — Il backend riflette qualsiasi `Origin` in `Access-Control-Allow-Origin` mantenendo `Allow-Credentials: true`.

IMPATTO — Un sito malevolo può effettuare richieste autenticate cross-origin per conto della vittima e leggerne le risposte.

REMEDIATION — Whitelist esplicita di origin fidati; mai abbinare wildcard e credenziali; preflight rigoroso.

F8 MEDIA CVSS 5.3 CWE-204 Confermato

User enumeration via password reset su `POST /api/v1/auth/password/reset`

DESCRIZIONE — La risposta differisce per account esistenti e inesistenti (messaggio e tempo di risposta), consentendo di **enumerare gli utenti** registrati.

IMPATTO — Costruzione di liste di email valide per phishing mirato e credential stuffing.

REMEDIATION — Risposta **identica** a prescindere dall'esistenza dell'account; tempi di risposta uniformi; rate limiting sull'endpoint.

F9 MEDIA CVSS 5.0 CWE-639 Confermato

Export anonimo con enumerazione dei token su `GET /api/v1/exports/{token}`

DESCRIZIONE — I file di export sono raggiungibili **senza autenticazione** tramite token sequenziale/prevedibile: è possibile enumerarli e scaricare export generati da altri utenti.

IMPATTO — Esposizione di dati esportati (anagrafiche, report) di altri tenant.

REMEDIATION — Autenticazione e autorizzazione sull'endpoint; token non prevedibili (UUID/firma) e a scadenza; binding del file all'utente proprietario.

F10 BASSA CVSS 3.1 CWE-693 Confermato

Header di sicurezza mancanti (HSTS, CSP, X-Content-Type-Options)

DESCRIZIONE — Le risposte non includono header difensivi chiave, aumentando l'esposizione a downgrade, sniffing del content-type e classi di XSS.

REMEDIATION — Aggiungere `Strict-Transport-Security`, una `Content-Security-Policy` restrittiva, `X-Content-Type-Options: nosniff` e `Referrer-Policy`.

04 — TABELLA ENDPOINT

Riepilogo chiamate & esito

Estratto rappresentativo degli endpoint testati e dell'esito del controllo di autorizzazione/autenticazione.

METODO	ENDPOINT	AUTH RICHIESTA	ESITO	RIF.
PATCH	`/api/v1/account/me`	Utente	Privilege escalation	F1
GET	`/api/v1/orgs/{orgId}/employees`	Utente	BOLA cross-tenant	F2
GET/POST	`/api/v1/meetings`	Nessuna ⚠	Anonimo + segreti	F3
POST	`/api/v1/assistant/query`	Utente	Retrieval fuori scope	F4
POST	`/api/v1/invoices`	Utente	Mass-assignment	F5
POST	`/api/v1/auth/login`	Nessuna	No rate limiting	F6
POST	`/api/v1/auth/password/reset`	Nessuna	User enumeration	F8
GET	`/api/v1/exports/{token}`	Nessuna ⚠	Export enumerabile	F9
POST	`/api/v1/orgs/{orgId}/employees`	Utente	Bloccato (corretto)	—
GET	`/api/v1/invoices/{id}` (FK altrui)	Utente	Scoping corretto	—

05 — CONTROLLI VERIFICATI ROBUSTI

Cosa NON è risultato vulnerabile

Verificato e **non sfruttabile** nel perimetro testato. In un report serio vale sapere cosa regge quanto cosa cede.

`Firma JWT (segreto robusto)` `Write-IDOR via foreign-key` `Scoping oggetti finanziari/utente/file` `SQL injection` `XXE` `Stored XSS sui campi nome (validati)` `Open redirect` `Azioni cross-account in scrittura (bloccate)`

06 — PRIORITÀ DI INTERVENTO

Roadmap di remediation

QUANDO	AZIONE	FINDINGS
Subito (pre-rilascio)	Chiudere privilege escalation, isolamento multi-tenant e risorse API anonime con segreti	F1, F2, F3
Breve termine	Autorizzazione sulle tool call dell'assistente; whitelist dei campi e workflow server-side; rate limiting/MFA	F4, F5, F6
Medio termine	Uniformare le risposte (enumeration), proteggere gli export, correggere CORS	F7, F8, F9
Hardening	Header di sicurezza e configurazione difensiva	F10

Retest. A correzioni applicate eseguiamo un re-test mirato sui finding chiusi, con aggiornamento dello stato (Risolto / Parziale / Aperto) e nuova evidenza. Disponibili piani periodici per verificare le regressioni nel tempo.

07 — SCOPE, REGOLE D'INGAGGIO & RISERVATEZZA

Perimetro e modalità

In scope	Web app `stage.sample-cloud.example` · API `api.stage.sample-cloud.example` · assistente AI «AskSample»
Fuori scope	Produzione, infrastruttura di rete, sistemi di terze parti integrati
Modalità	Grey-box autenticato — 2 utenze su 2 organizzazioni distinte
Esclusioni	DDoS, stress test, flooding e ogni attività che comprometta la disponibilità
Autorizzazione	Attività avviate previa autorizzazione scritta e regole d'ingaggio concordate

Riservatezza del dato. I dati del cliente sono de-identificati (Microsoft Presidio) prima di ogni elaborazione AI; l'attività è condotta su VM cifrata dedicata, ospitata in Italia, con accesso a token. A conferma della ricezione del report la VM e gli artefatti temporanei vengono distrutti entro 24 ore lavorative. Non viene conservata copia del report né documentazione relativa al cliente, salvo quanto concordato nelle regole d'ingaggio.

Documento dimostrativo. «Sample Cloud S.p.A.», gli endpoint, le evidenze e i dati riportati sono **fittizi** e costruiti a partire da un insieme di pattern ricorrenti, a solo scopo illustrativo dell'output di un penetration test Pentropic. Nessun cliente reale è rappresentato.