Easy Gara
Volt AI Dynamics S.R.L.

Report di sicurezza

Sintesi pubblica del penetration test della piattaforma — novembre 2026

Oggetto: applicazione web app.easygara.it **Eseguito da:** DifesaLab.it

Test eseguiti: 15 e 17 novembre 2026 **Stato aggiornato al:** 18 novembre 2026 **Versione:** 1.0

In sintesi: nessuna vulnerabilità critica o alta.

Il test ha cercato di entrare senza credenziali, di superare i permessi con un account ordinario e di leggere dati di altri clienti. Nessuno di questi tentativi è riuscito.

I rilievi emersi sono di gravità media o bassa, riguardavano soprattutto la gestione delle sessioni e non mettevano a rischio nessun account o dato. Tutti i rilievi che comportavano un rischio sono stati corretti; gli altri sono stati valutati come rischio accettabile e non mettono in pericolo la sicurezza dei dati e degli utenti.

0	3	15	300+
vulnerabilità critiche o alte	rilievi corretti dopo il test	famiglie di attacco verificate senza esito	richieste di prova inviate

1. Perché questo documento

Easy Gara custodisce documenti di gara, offerte tecniche e dati aziendali dei propri clienti. Abbiamo fatto verificare la piattaforma con un penetration test, eseguito da DifesaLab.it, e pubblichiamo qui i risultati, compresi i punti da migliorare e le correzioni fatte. Il documento non contiene dettagli che possano aiutare un attacco: nessun indirizzo interno, nessun dato di account, nessuna istruzione per riprodurre i rilievi.

2. Perimetro e metodo

Fase	Cosa è stato fatto
Esterna, senza credenziali 15 novembre 2026	Mappatura della superficie esposta, prove di iniezione su tutti i campi pubblici (accesso, registrazione, recupero password, rinnovo della sessione), ricerca di file e cartelle esposti, analisi del codice JavaScript pubblicato, prove sui token di autenticazione.
Interna, con un account ordinario 17 novembre 2026	Account di prova dedicato, con i permessi di un normale cliente. Prove di falsificazione della sessione, di accesso alle funzioni di amministrazione, di lettura o modifica di dati di altri clienti, di modifica di campi riservati, di aggiramento dei controlli contrattuali, di iniezione sui campi del profilo.

Il test è stato condotto da DifesaLab.it ed è stato **non distruttivo**: nessun dato reale è stato letto o alterato, e l'account di prova è stato riportato allo stato iniziale. L'impostazione segue le categorie di rischio più diffuse per le applicazioni web (OWASP Top 10).

3. Le difese che hanno retto

Per ognuna di queste famiglie di attacco il test non ha trovato alcun punto debole.

Area	Cosa è stato tentato	Esito
Iniezione nel database	Iniezione SQL (per errore, booleana, temporale) e NoSQL con operatori, su tutti i campi pubblici e del profilo	**Nessuna vulnerabilità**
Iniezione di template e comandi	Espressioni di template lato server e comandi di sistema nei campi	**Nessuna vulnerabilità**
Cross-site scripting	Codice HTML e script nei campi e negli indirizzi	**Nessuna vulnerabilità**
Falsificazione della sessione	Token senza firma, confusione di algoritmo, firme con segreti deboli, sostituzione dell'identità dell'utente	**Nessuna vulnerabilità**

Area	Cosa è stato tentato	Esito
Accesso alle funzioni di amministrazione	Rotte riservate con parametri, intestazioni e metodi alterati	**Nessuna vulnerabilità**
Isolamento fra clienti	Lettura o sovrascrittura dei dati di un altro account o di un'altra organizzazione	**Nessuna vulnerabilità**
Elevazione dei privilegi	Invio di ruolo, piano o organizzazione nei salvataggi del profilo	**Nessuna vulnerabilità**
Controlli contrattuali	Aggiramento del blocco «contratto da firmare» con varianti di indirizzo e codifica	**Nessuna vulnerabilità**
File esposti	Attraversamento di cartelle, file di configurazione, sorgenti, elenchi di directory	**Nessuna vulnerabilità**
Caricamento di file	Accesso senza credenziali alle funzioni di caricamento e importazione	**Tutte protette**
Scoperta degli account	Capire dalle risposte di accesso e registrazione se un'email è cliente	**Risposte identiche**
Credenziali deboli	Password comuni e predefinite su indirizzi plausibili	**Nessun accesso**
Forza bruta	Tentativi ripetuti di accesso	**Bloccati**
Segreti nel codice pubblico	Chiavi e credenziali nel codice JavaScript scaricato dal browser	**Nessuno trovato**
Documentazione tecnica esposta	Pagine di debug, documentazione delle API, endpoint di sviluppo	**Nessuna esposta**

Configurazione confermata dal test

- **Connessione cifrata** con TLS 1.3 e HSTS: il browser non accetta mai una connessione in chiaro.
- **Content Security Policy rigorosa**: il browser esegue solo il codice della piattaforma, non script inseriti da terzi, e la pagina non può essere incorniciata da altri siti.

- **Cookie di sessione protetto** (`HttpOnly`, `Secure`, `SameSite=Strict`): non leggibile da script e non inviato da siti esterni, quindi le richieste contraffatte da altri siti (CSRF) non possono usarlo.
- **Sessioni brevi**: il token di accesso dura 4 ore ed è firmato e verificato a ogni richiesta.
- **Limiti di frequenza** a più livelli, più stretti su accesso, registrazione e funzioni costose.
- **Messaggi d'errore neutri**: nessuna traccia tecnica, nessun dettaglio sul database.

4. Rilievi e piano d'azione

Ogni rilievo riporta la gravità assegnata dal test e lo stato al momento della pubblicazione. Le correzioni sono in produzione dal 18 novembre 2026 e sono accompagnate da test automatici che verificano che il problema non si ripresenti.

R1 · Uscita dall'account e rinnovo della sessione

Gravità media · Corretto

Cosa: quando si esce dall'account il browser cancella la sessione, ma il server non la invalida. Chi avesse già sottratto un token di sessione potrebbe continuare a usarlo fino alla scadenza.

Quanto pesa: serve prima sottrarre il token, che è custodito in un cookie non leggibile dagli script e trasmesso solo su connessione cifrata. Il rilievo riguarda quindi la capacità di chiudere una sessione già compromessa, non la possibilità di comprometterla.

Correzione: ogni sessione ha ora un identificativo che il server può revocare. All'uscita la sessione viene chiusa subito anche sul server; al rinnovo la sessione precedente smette di valere; cambiare o reimpostare la password, o disattivare un account, chiude tutte le sessioni aperte.

R2 · Tempi di risposta del recupero password

Gravità media · Corretto

Cosa: la pagina «Password dimenticata» risponde con lo stesso messaggio a tutti, ma impiega più tempo quando l'email appartiene a un cliente. Misurando i tempi si può capire se un indirizzo è registrato.

Quanto pesa: non dà accesso a nulla; può aiutare chi prepara campagne di phishing mirate. La pagina resta soggetta ai limiti di frequenza.

Correzione: la risposta parte subito e identica per tutti, prima di qualunque verifica; la ricerca dell'account e l'invio dell'email avvengono dopo.

R3 · Valori di tipo inatteso nei campi di accesso

Gravità bassa · Corretto

Cosa: inviando al posto dell'email un oggetto o un numero, il server risponde con un errore generico invece che con un messaggio di dato non valido. Nessuna informazione trapela e nessun controllo viene aggirato: il test lo conferma come prova che quei valori non arrivano mai al database.

Correzione: i campi di accesso, registrazione e recupero password verificano il tipo del dato e rispondono «dato non valido».

R4 · Blocco dei tentativi di accesso per indirizzo di rete

Gravità bassa · Rischio accettato

Cosa: dopo vari accessi falliti, la piattaforma blocca per alcuni minuti i tentativi dallo stesso indirizzo di rete. In un ufficio che esce su Internet con un unico indirizzo, i tentativi sbagliati di una persona possono bloccare per poco tempo anche i colleghi.

Valutazione: è il prezzo di una protezione efficace contro i tentativi a tappeto di indovinare le password. Il blocco è breve e si sblocca da solo.

R5 · Controlli di formato su alcuni campi del profilo

Gravità bassa · Rischio accettato

Cosa: alcuni campi compilati dal cliente (denominazione, partita IVA, chiave di un servizio esterno) accettano testo libero e lo conservano così com'è.

Valutazione: i valori sono visibili solo all'organizzazione che li ha scritti e vengono codificati quando si mostrano a video e nei documenti esportati; la Content Security Policy impedisce comunque l'esecuzione di script inseriti nei dati. Il test non ha trovato modo di sfruttarli.

R6 · Osservazioni informative

Informativo | Nessuna azione

- Dalle risposte del server si deducono il nome del cookie di sessione e l'esistenza delle rotte di amministrazione: sono informazioni senza valore senza un token valido, e le rotte sono protette.
- Il collegamento di reimpostazione della password dice solo se è valido o scaduto: è casuale, lungo, monouso e dura un'ora, quindi non può essere indovinato.
- Il collegamento per la firma del contratto inviato a un firmatario funziona come una chiave personale: non è enumerabile e risponde allo stesso modo a ogni valore sbagliato.

5. Misure di sicurezza strutturali

Oltre a quanto verificato dal test, la piattaforma adotta queste misure.

Isolamento per organizzazione
Ogni cliente vede solo i propri dati; i ruoli dei collaboratori (proprietario, editor, revisore, lettore) sono applicati dal server, non solo dall'interfaccia.

Password protette
Conservate con hash bcrypt, mai in chiaro; chiavi di servizi esterni cifrate nel database.

Database non esposti
Raggiungibili solo dall'interno dell'infrastruttura, mai da Internet.

Backup giornalieri
Copie del database ogni giorno, con rotazione.

AI senza conservazione dei dati
Fornitori di intelligenza artificiale con conservazione zero dei dati dove disponibile, dichiarati nell'informativa privacy.

Controlli prima dell'export
I documenti di gara non escono con dichiarazioni incoerenti con i dati dell'impresa.

Lettura sicura dei siti web

L'import del profilo aziendale legge solo indirizzi pubblici, mai risorse interne.

6. Segnalazioni

Chi individua un possibile problema di sicurezza può scrivere a info@easygara.it. Chiediamo di non divulgare il problema prima che sia stato corretto; risponderemo indicando i tempi previsti.

Easy Gara è un prodotto di Volt AI Dynamics S.R.L. · Report di sicurezza v1.0 · stato al 18 novembre 2026. Penetration test eseguito da DifesaLab.it. Questo documento sintetizza i risultati del test e delle correzioni; non contiene dati personali né informazioni tecniche utili a un attacco.