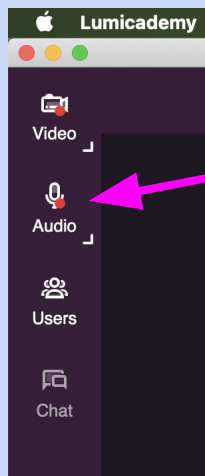
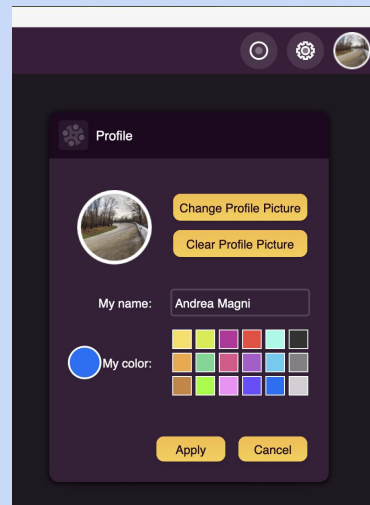


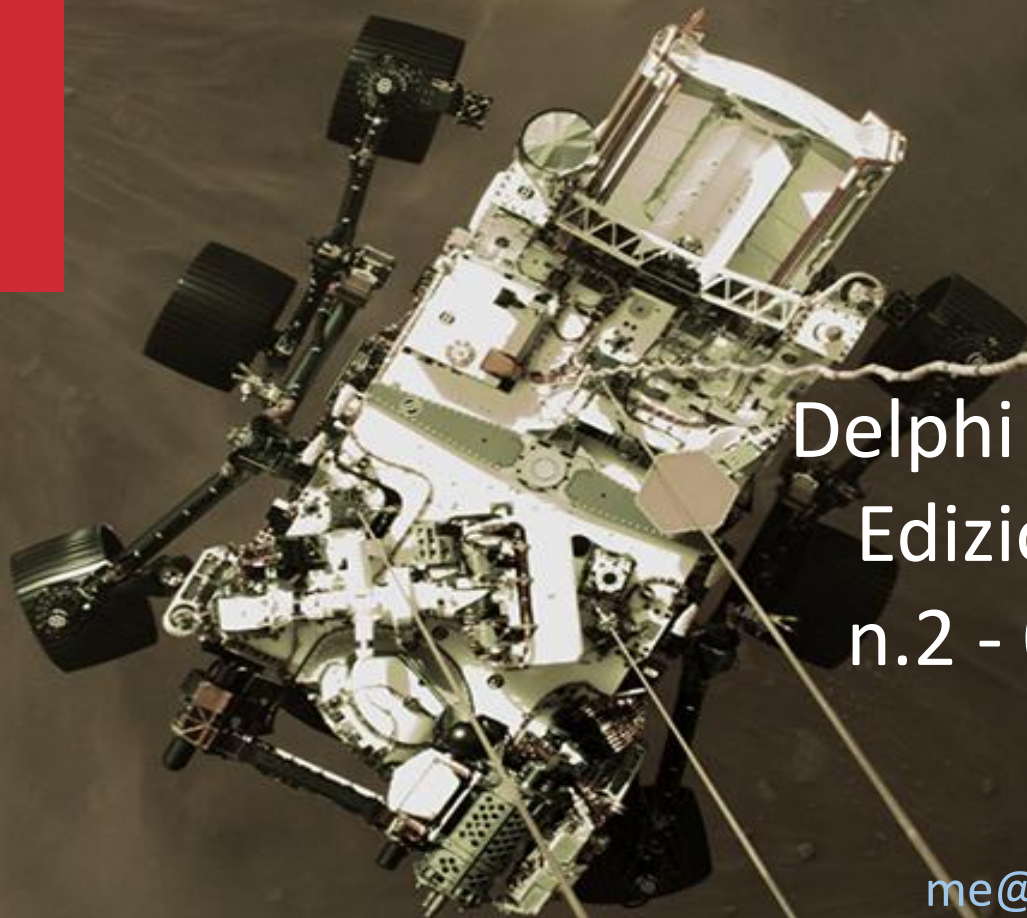
- La piattaforma permette ai partecipanti di condividere la vostra webcam e il microfono
 - Per cortesia, aprite il microfono solo per fare domande
- Per accedere alla chat Slack:
 - <https://andreamagni.eu/live.html>



Pallino rosso = spento, click per attivare
(vale per Video e Audio)



Potete impostare
il vostro nome
utente, se volete



Delphi Live - Italia Edizione 2021 n.2 - 01 Marzo

Andrea Magni
me@andreamagni.eu

Andrea Magni

Ingegnere informatico, Monza

Sviluppatore, Formatore, Consulente

Desktop, Server, Web, Mobile e IoT

- TFrameStand, TFormStand, FMXER (FMX)
- MARS-Curiosity (REST Library)
- Delphi GUI Programming with FireMonkey (Book)



<https://andreamagni.eu>

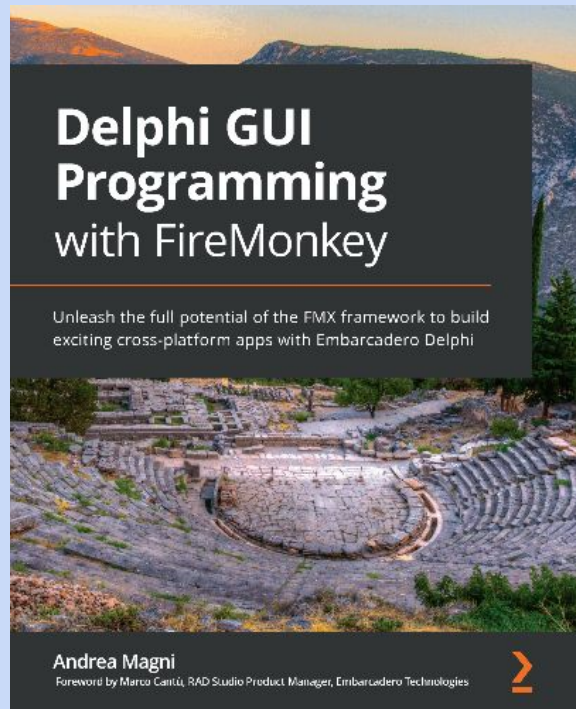
Piattaforma

- <https://www.lumicademy.com/>
- <https://blog.grijjy.com/>
 - Allen Drennan
 - Erik van Bilsen
- Applicazioni FMX
 - Desktop: Windows e OS X
 - con integrazioni a basso livello (GPU, video, audio)
 - chat



Sponsor

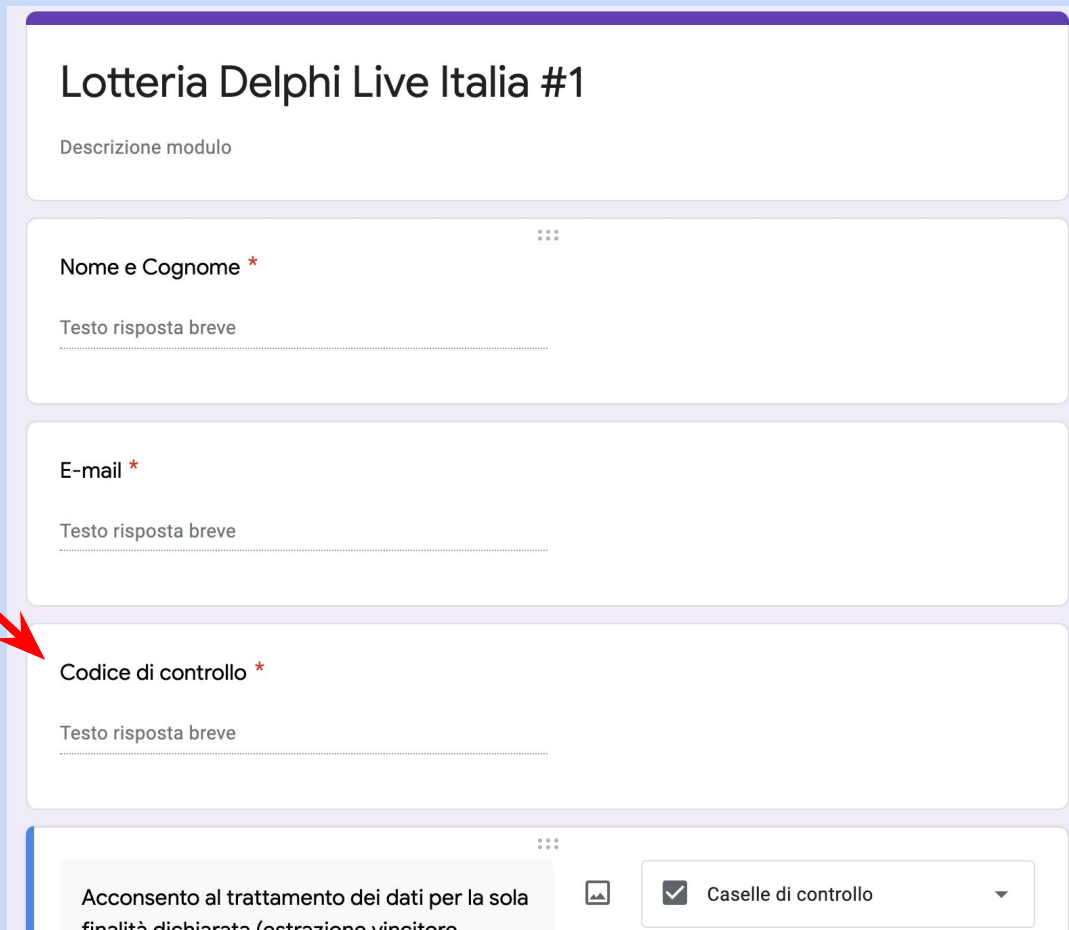
- <https://www.packtpub.com/>
- 1 printed copy of my FMX book
- discounts (also on other books)



Packt>

Lotteria

Fate attenzione:
durante la sessione
comunicheremo il
codice di controllo
da inserire nel modulo
per partecipare
all'estrazione.



Lotteria Delphi Live Italia #1

Descrizione modulo

Nome e Cognome *

Testo risposta breve

E-mail *

Testo risposta breve

Codice di controllo *

Testo risposta breve

Acconsento al trattamento dei dati per la sola
finalità dichiarata (estrazione vincitore)

☒ Caselle di controllo

La sicurezza nella gestione delle credenziali nelle applicazioni distribuite



JWT

Cesare Bacci
cesare.bacci@generazioneinformatica.it

Cesare Bacci

Generazione Informatica S.r.l. - Firenze



<https://www.autenticazione Sicura.it>

<https://www.geninfo.it>

Agenda

- Generazione Informatica: 25 anni di Delphi
- Case history: l'occasione del GDPR per un salto di qualità nella sicurezza
- La sicurezza nel processo di autenticazione
- La sicurezza nel dialogo (l'utilizzo di token)
- Esempio pratico: autenticazione "convenzionale" su un applicativo di test
- Esempio pratico: autenticazione biometrica su un applicativo di test
- La Strong Authentication (2FA) per un livello di sicurezza maggiore
- Feedback e domande

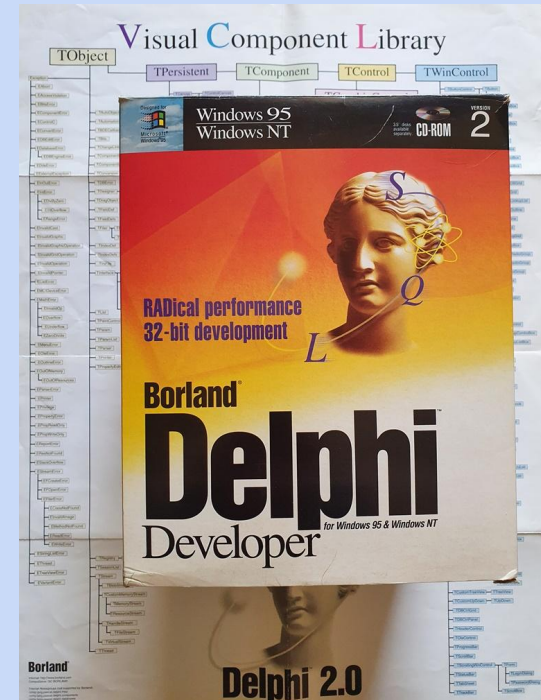
Generazione Informatica: 25 anni di Delphi

Generazione Informatica è nata nel 1996...

È più giovane di Delphi solo di 1 anno

Con le varie versioni di Delphi:

- applicativi client/server
- servizi
- applicativi web
- webservice
- App
- etc.



Iniziamo con una domanda

Vi è mai stato posto dai vostri clienti (o avete voi mai avvertito) il problema di come rendere più sicuro l'uso dei vostri applicativi?

- rispondere sinteticamente in chat

Come è nata l'esigenza...

- **Cliente:** Cassa di Assistenza bancaria
- **Oggetto:** Erogazione rimborsi per attività di tipo sanitario
- **Strumento:** Nostro applicativo web e nostra app
- **Dati trattati:** Anagrafiche, domande di rimborso, estratti conto, ecc.

Come è nata l'esigenza...

- **Richiesta del Cliente:** Mettersi in regola col GDPR
- **Necessità:** Scorporare le credenziali degli utenti dalle tabelle anagrafiche
- **Opportunità:** Aumentare anche la sicurezza
 - sia nel processo di autenticazione
 - sia nel dialogo tra client e server

Come è nata l'esigenza...

Analisi della soluzione

- Intervento sul DB
 - modifica delle tabelle (estrapolazione delle credenziali)
 - creazione di un database separato
 - ...magari anche su un server differente
- Problematiche connesse
 - ingegnerizzazione della gestione delle password
 - implementazione protocollo sicuro
 - difesa da tentativi di personificazione del soggetto
 - difesa da attacchi brute-force

Come è nata l'esigenza...

Ipotesi di lavoro

- Utilizzare qualche soluzione presente sul mercato

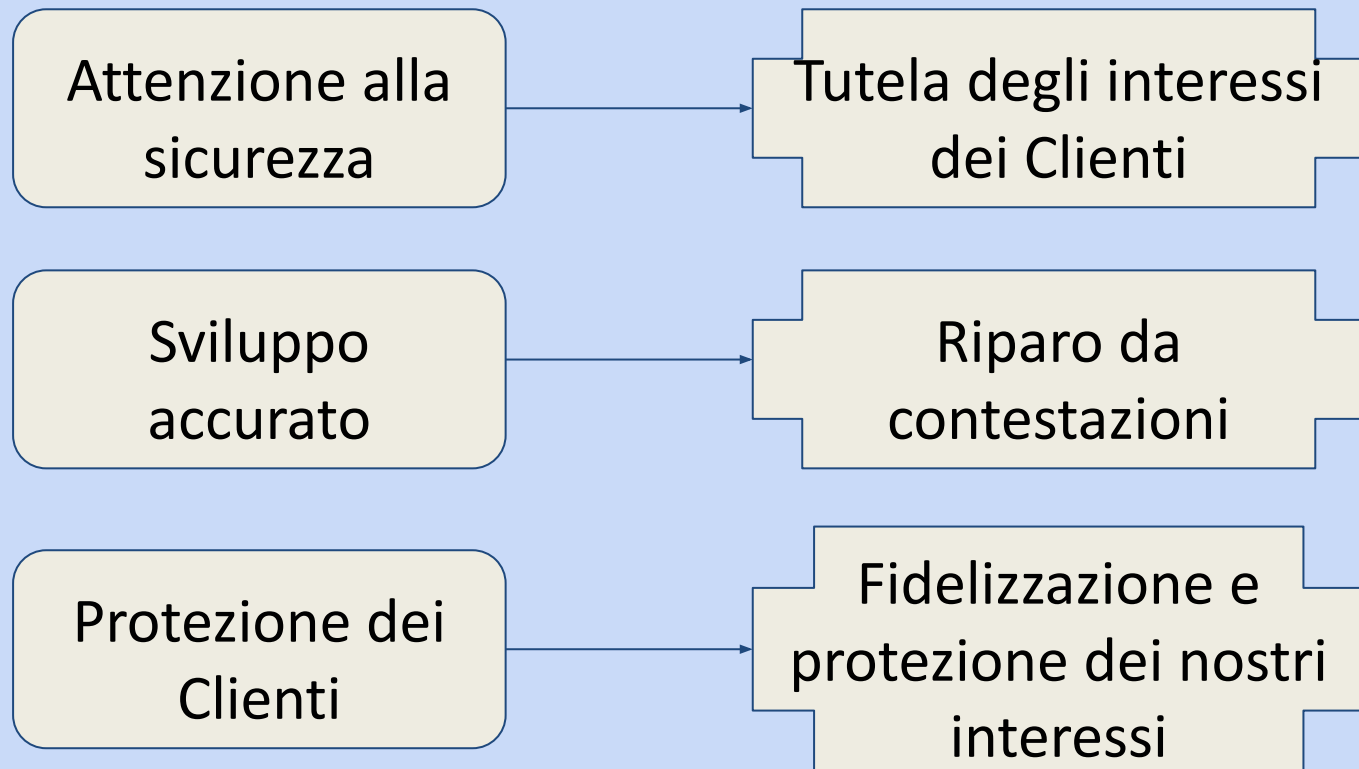
Ricerca soluzione

- Gestione password: non trovato prodotti adatti
- Sicurezza: uso dei token JWT

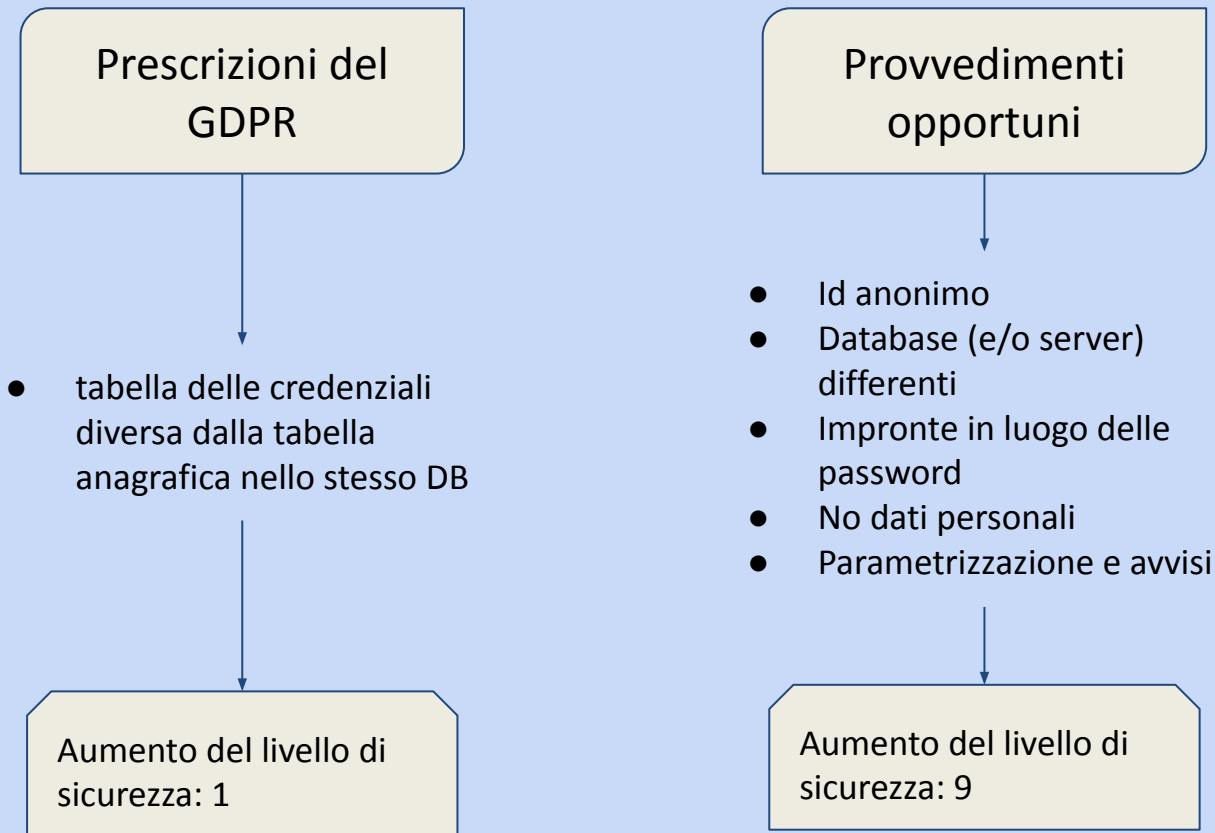
La nascita di Autentica

- ❖ L'esigenza del nostro cliente
 - valenza generale
- ❖ Necessità specifiche di sicurezza
 - necessità per tutti gli applicativi distribuiti
- ❖ Riconoscere con certezza i propri utenti
 - esigenza di tutti coloro che gestiscono profili utente
- ❖ Tutelare dati più o meno riservati
 - rapporto fiduciario con i nostri Clienti

La nascita di Autentica



La sicurezza nell'autenticazione



Diamo i numeri!

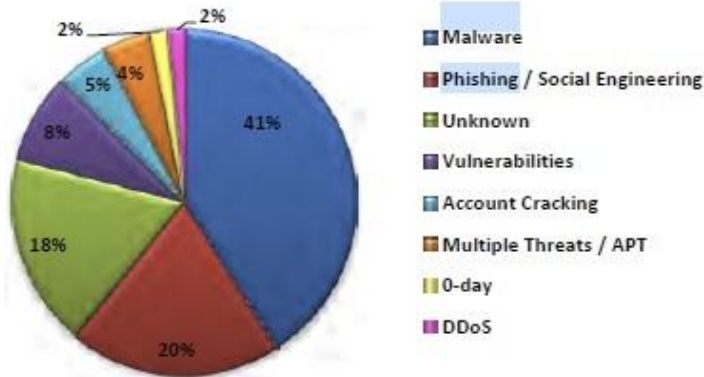
Secondo voi, quante email finalizzate alla sottrazione di credenziali (phishing) sono state bloccate nel 2019?

- rispondere sinteticamente in chat

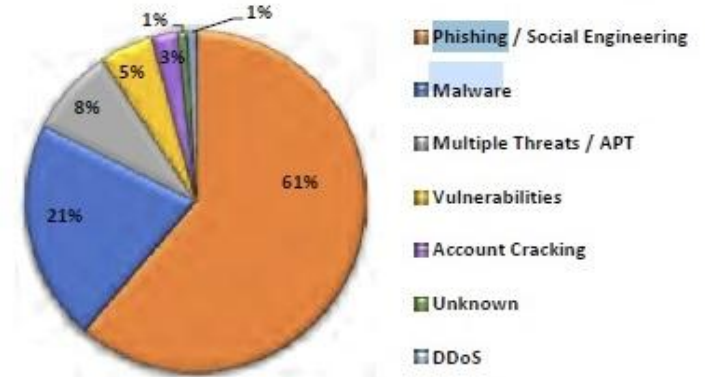
Diamo i numeri!

Nel 2019 sono state bloccate oltre **13 miliardi di email** nocive e sospette. (fonte Digital Defense Report di Microsoft)

Tipologia e distribuzione delle tecniche d'attacco (1H 2020)



Distribuzione % delle tecniche - tema COVID-19 (1H 2020)



**Esempi di integrazione
disponibili su
github.com/cebacci**

**Un esempio di
autenticazione
“convenzionale” in
un applicativo di test**

I token JWT

Un token JWT è un insieme di informazioni codificate in Json, non riservate, verificate e attendibili perché firmate digitalmente.

- Diversi livelli di sicurezza
- Diversi strumenti di verifica

Esempio di composizione di un JWT con jwt.io

La sicurezza nel dialogo con l'uso dei token

- Al momento dell'autenticazione andata a buon fine, viene “staccato” un gettone
- Questo gettone deve essere fornito insieme ad ogni successiva richiesta

Esempio di utilizzo di un JWT con Mars-Curiosity

**Un esempio di
autenticazione
con credenziali
biometriche in un
applicativo di test**

Si può ulteriormente aumentare la sicurezza?

- Utilizzo delle restrizioni
 - limiti sugli indirizzi ip da cui si accettano richieste
 - limiti sui domini da cui si accettano richieste
 - limiti sulla validità (durata) dei token
- Utilizzo di autenticazione a due fattori:
 - uso di un pin scelto dall'utente
 - uso di una OTP inviata via sms

Riepilogo

- Percezione della sicurezza e della protezione
- Da una richiesta di un Cliente può nascere un'opportunità di business
- Con Delphi abbiamo creato un prodotto che non esisteva sul mercato
- Il vantaggio per il Cliente è anche tutela dei nostri interessi aziendali



AUTENTICA

<https://www.autenticazione Sicura.it>

<https://www.geninfo.it>

Un ringraziamento concreto

A tutti coloro che hanno partecipato al seminario e hanno resistito fino alla fine, registrandosi su Autentica entro la settimana, verrà riconosciuto un upgrade gratuito per un anno dalla versione Cherry (gratuita, 1 progetto, 5 utenti) alla versione Apricot (219,99€/anno, 3 progetti, 25 utenti)



<https://www.autenticazione Sicura.it>

<https://www.geninfo.it>



Feedback & demande



Grazie