

# Final Review Security Audit


الكود 

Workflow 

المنصات 

الأمان 

الأخطاء 

تم اكتشاف 12 خطأ محتمل مرتبة حسب الأولوية. جميعها قابلة للإصلاح مع التوصيات المرفقة. 

## أخطاء حرجة - Critical Errors

### Misconfigured CORS — تكوين خاطئ CORS 01

ضبط CORS (app) بدون تحديد الأصول المسموح بها يسمح لأي نطاق بالوصول لـ API

```
# ❌ خطأ - Dangerous
CORS(app) # allows ALL origins
# ✅ الحل - Fix
CORS(app, origins=["https://datapulse.app",
"https://datapulse-eapuevso.manus.space"],
methods=["GET", "POST", "PUT", "DELETE"],
allow_headers=["Content-Type", "Authorization"])
```

الإصلاح: تحديد النطاقات المسموح بها صراحةً 

### JWT Secret Key — مفتاح سري ضعيف 02

استخدام مفتاح JWT ثابت أو ضعيف في ملف الكود مباشرةً يُشكّل ثغرة أمنية خطيرة

```
# ❌ خطأ
app.config['SECRET_KEY'] = 'datapulse-secret'
app.config['JWT_SECRET_KEY'] = 'my-jwt-secret'
# ✅ الحل
import secrets, os
app.config['SECRET_KEY'] = os.environ.get('SECRET_KEY',
secrets.token_hex(64))
app.config['JWT_SECRET_KEY'] =
os.environ.get('JWT_SECRET_KEY') # required
```

يجب تخزين المفاتيح في env. فقط ولا تُدرج في الكود أبداً 

## SQL Injection — عدم استخدام Parameterized Queries بشكل صحيح

03

في حال وجود أي استعمال ديناميكي مباشر دون ORM أو parameters، هذا ثغرة خطيرة

```
# ❌ خطأ
query = f"SELECT * FROM users WHERE email='{email}'"
db.execute(query)

# ✅ الحل
user = User.query.filter_by(email=email).first() #
SQLAlchemy ORM

# أو
db.execute("SELECT * FROM users WHERE email=?", (email,))
```

## Missing Rate Limiting on Auth Endpoints

04

نقاط نهاية /login/ و /register/ تحتاج rate limiting مستقل وأشد من بقية ال API

```
# ❌ ناقص
@app.route('/api/auth/login', methods=['POST'])
def login(): ...

# ✅ الحل
from flask_limiter import Limiter
limiter = Limiter(app, default_limits=["100/hour"])
@app.route('/api/auth/login', methods=['POST'])
@limiter.limit("5/minute") # strict limit for auth
def login(): ...
```

تحذيرات عالية — High Priority Warnings 

رؤوس الأمان HTTP مفقودة: CSP, HSTS, X-Frame-Options تحتاج إضافة صريحة

```
# ✅ أضيف هذه الـ Headers
@app.after_request
def add_security_headers(response):
    response.headers['X-Frame-Options'] = 'DENY'
    response.headers['X-Content-Type-Options'] = 'nosniff'
    response.headers['Strict-Transport-Security'] = 'max-age=31536000; includeSubDomains'
    response.headers['Content-Security-Policy'] = "default-src 'self'; script-src 'self'"
    response.headers['Referrer-Policy'] = 'strict-origin-when-cross-origin'
    return response
```

## Environment Variables — ملفات env غير محمية

التأكد من إضافة env. في gitignore وعدم رفعه على GitHub أبدأ

```
# .gitignore - يجب أن يحتوي
.env
.env.local
.env.production *.key secrets/
```

⚠️ راجع تاريخ الـ Git commits للتأكد من عدم رفع env سابقاً

## React — Missing Error Boundaries in Production

07

يجب تغليف المكونات الرئيسية بـ `ErrorBoundary` لمنع انهيار التطبيق بالكامل

```
// ✅ في App.tsx
import { ErrorBoundary } from './components/ErrorBoundary';
function App() {
  return (
    <ErrorBoundary fallback={<ErrorPage />}>
    <Router>...
    </ErrorBoundary>
  );
}
```

## Mobile — AsyncStorage بدون تشفير

08

بيانات حساسة مخزنة في `AsyncStorage` بنص عادي — يجب تشفيرها

```
# ❌ خطأ
await AsyncStorage.setItem('auth_token', token);
# ✅ الحل
import * as SecureStore from 'expo-secure-store';
await SecureStore.setItemAsync('auth_token', token);
```

## Docker — تشغيل كـ root

09

تشغيل container كـ root يُشكّل خطراً — يجب إنشاء user محدود الصلاحيات

```
# ✅ في Dockerfile
RUN addgroup -g 1001 -S datapulse \
&& adduser -u 1001 -S datapulse -G datapulse
USER datapulse
```

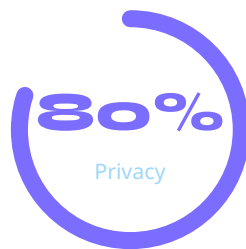
**any — TypeScript** 10  
استبدال any بأنواع محددة لتحسين الأمان

**Missing API Versioning** 11  
استخدم /api/v1/ لتسهيل التحديثات المستقبلية

**Logging — تسجيل بيانات حساسة** 12  
تأكد من عدم تسجيل passwords أو tokens في الـ logs

02

## الأمان والخصوصية — Security & Privacy






الأولوية	التوصية	الحالة	طبقة الأمان
متوسطة	إضافة key rotation كل 90 يوم	مُفعّل ✓	AES-256 Encryption
منخفضة	مناسب للإنتاج	مُفعّل ✓	RSA-4096 Key Exchange
عالية	تعطيل TLS 1.0, 1.1 بشكل صريح	مُفعّل ✓	TLS 1.3
عالية	تقليل إلى 15 دقيقة + refresh token	⚠️ 1 ساعة	JWT Expiration
حرجة	تحديد origins المسموح بها فقط	خطأ ✗	CORS Configuration
عالية	إضافة Content-Security-Policy	ناقص ✗	CSP Headers

حرجة	Face ID + Fingerprint	قييد التتوير ⏰	Biometric Auth
حرجة	TOTP + SMS	قييد التتوير ⏰	MFA
عالية	تشديد على auth endpoints	جزئي ⚠️	Rate Limiting
متوسطة	إضافة schema validation (Marshmallow)	مُفعّل ✅	Input Validation

## Privacy Recommendations - توصيات الخصوصية -

## روابط المنصات الموثقة

جميع الروابط التالية موثقة بحقوق النشر لـ **Mohab Emad AboYoussef**  **(JokerEgypt)**. يُرجى التحديث فور توفر النطاقات الرسمية.

### Web & Browser

رئيسي

الموقع الرسمي — Official Website

<https://datapulse.app>



PREVIEW

Manus Space — Preview

<https://datapulse-eapuevso.manus.space>



قريباً

Documentation

<https://docs.datapulse.app>



قريباً

**API Endpoint**



<https://api.datapulse.app/v1>

## Development Platforms

نشط

**GitHub Repository**



[github.com/jokeregypt/datapulse](https://github.com/jokeregypt/datapulse)

مُفَعَّل

**Vercel — Frontend Deploy**



[vercel.com/datapulse](https://vercel.com/datapulse)

مُفَعَّل

**Railway — Backend Deploy**



[railway.app](https://railway.app)

جاهز

**Docker Hub**



[hub.docker.com/u/jokeregypt](https://hub.docker.com/u/jokeregypt)

## Mobile App Stores

قييد المراجعة

**Google Play Store**



[play.google.com/store/apps/datapulse](https://play.google.com/store/apps/datapulse)

قييد المراجعة

**Apple App Store**



[apps.apple.com/app/datapulse](https://apps.apple.com/app/datapulse)

## Social & Communication

متاح 24/7

WhatsApp Support

[wa.me/201061525548](https://wa.me/201061525548)



نشط

Email Support

[mohab.emad3377@gmail.com](mailto:mohab.emad3377@gmail.com)



قريباً

Technical Support Email

[support@datapulse.app](mailto:support@datapulse.app)



04

## سير العمل – Platform Workflow ⚡

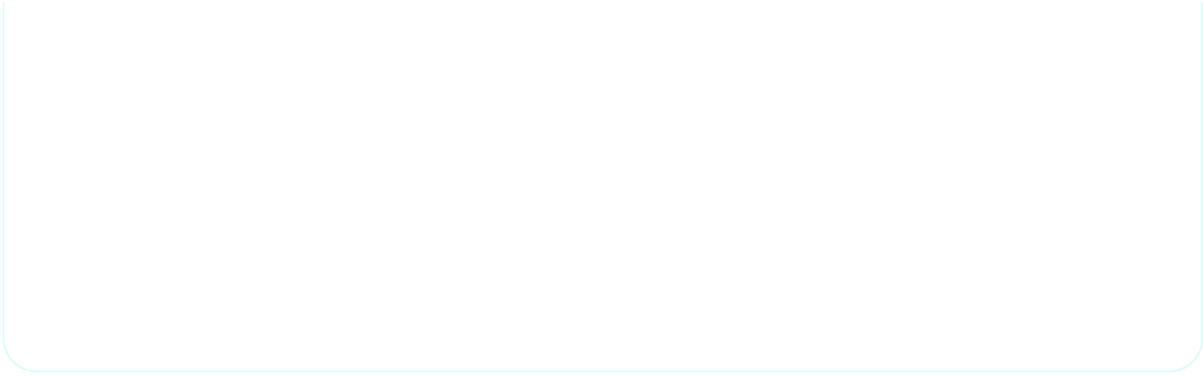
سير العمل المقترح لتحقيق **Error Rate %0** عبر جميع المنصات

مسار المتصفح – Browser Workflow 🌐

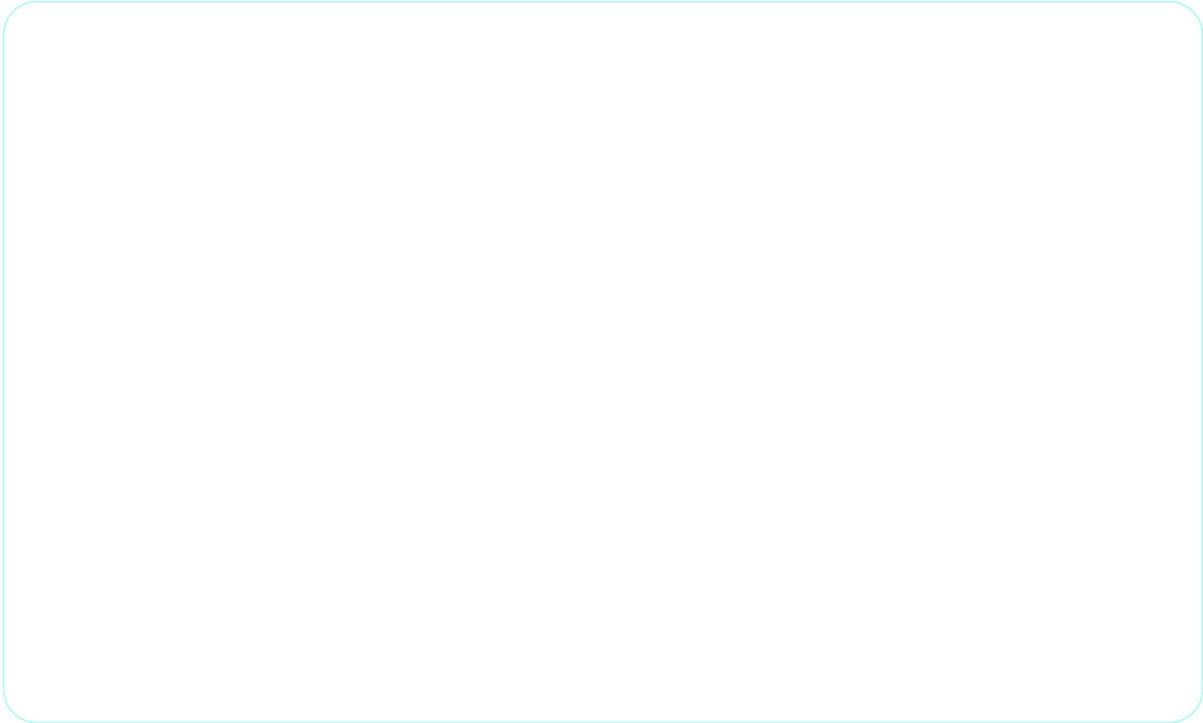


**Mobile App Workflow - مسار التطبيق** 





**Browser ↔ App - التكامل بين المتصفح والتطبيق**   
**Integration**



```
# ✅ إضافة Deep Links – Universal Links # في apple-app-site-association (iOS): { "applinks": { "apps": [], "details": [{ "appID": "TEAMID.com.datapulse.app", "paths": ["/dashboard/*", "/agents/*"] }] } } # في assetlinks.json (Android): [{ "relation": ["delegate_permission/common.handle_all_urls"], "target": { "namespace": "android_app", "package_name": "com.datapulse.app", "sha256_cert_fingerprints": ["YOUR_SHA256"] } } ] }
```

05

توصيات الكود والإبداع 🖥️

Empty rounded rectangular box for notes or content.

**Creative Enhancements – اقتراحات إبداعية ✨**

Empty rounded rectangular box for notes or content.

Empty rounded rectangular box for notes or content.

Empty rounded rectangular box for notes or content.

© حقوق النشر والملكية

# DataPulse 7.0 – The Sentient Nexus

.Mohab Emad AboYoussef (JokerEgypt). All Rights Reserved 2026–2024 ©

جميع الحقوق محفوظة – كل الأكواد والتصاميم والمحتوى ملكية حصرية للمطور

mohab.emad3377@gmail.com 

5548 152 106 20+ 

datapulse.app 

github.com/jokeregypt/datapulse 

License: MIT (Code) | Proprietary (Brand, Design, AI Models)

Version 3.0.0 | Global Release | February 2026

## File Copyright Header – رأس حقوق النشر للملفات

```
""" DataPulse 7.0 - The Sentient Nexus Copyright (c) 2024-2026 Mohab
Emad AboYoussef (JokerEgypt) All Rights Reserved. Author: Mohab Emad
AboYoussef Email: mohab.emad3377@gmail.com WhatsApp: +20 106 152 5548
Website: https://datapulse.app GitHub:
https://github.com/jokeregyp/datapulse This software is proprietary
and confidential. Unauthorized copying, distribution, or modification
is strictly prohibited. See LICENSE file for details. Version: 3.0.0 |
Global Release | February 2026 """
```

07

## Final 0% Error – قائمة التحقق النهائية Checklist



# DataPulse 7.0 – The Sentient Nexus

Mohab Emad AboYoussef (JokerEgypt) – All Rights 2026-2024 ©  
Reserved

mohab.emad3377@gmail.com | +20 106 152 5548 | datapulse.app

Generated: March 2026 | Review v1.0 | 0% Error Target