الدليل الثالث

ربط الأتمتة وخطافات المتصفح الإلكتروني

التصميم، التوقيع، إعادة المحاولة، والأمان Webhooks:

أكاديمية التعليم التفاعلي — Arab Templates

إصدار 2026 · arabiatemplates.com

المفهوم	المعنى	مثال
Event	الحدث الذي يفعل الإرسال	order.created
Payload	بيانات الحدث بصيغة JSON	رقم الطلب والمبلغ
Endpoint	العنوان الذي يستقبل الرسالة	https://example.com/hooks/orders
Signature	توقيع يثبت أن المرسل نظامك	HMAC-SHA256

قاعدة التصميم

أرسل أقل قدر من البيانات يكفي لاتخاذ القرار. لا ترسل بيانات شخصية كاملة في الحمولة، وأرسل المعرف ليجلب المتلقي التفاصيل عند الحاجة.

> الإنجليزي Webhooks داخل الواجهات لأنه المصطلح المعتمد في أدوات المطورين، مع شرح عربي في الدروس.
> في منصة Arab Templates نستخدم المصطلح

الفصل الثاني: شكل الرسالة الصحيح

الغرض	النوع	الحقل
منع المعالجة المزدوجة	نص فريد	id
نوع الحدث	نص	type
ترتيب الأحداث	تاريخ ISO	created_at
بيانات الحدث	كائن	data
توافق الحمولة	رقم	version

التحقق من التوقيع

1. اجمع جسم الطلب الخام كما وصل، دون إعادة تنسيقه.
2. احسب HMAC-SHA256 بالسر المشترك.
3. قارن الناتج بالترويسة بطريقة آمنة ضد اختلاف التوقيت.
4. ارفض الطلب إن اختلف التوقيع أو تجاوز الوقت المسموح.
5. أعد 200 بسرعة، ثم عالج البيانات في الخلفية.

> الرد البطيء يجعل المرسل يعيد المحاولة، فتتكرر العمليات. استقبل، تحقق، ثم أعد الرد.

الفصل الثالث: الأحداث القياسية في المنصة

الحدث	يفعل عند	أثر نموذجي
invoice.created	إنشاء فاتورة	إرسال نسخة للعميل
invoice.paid	تأكيد السداد	تحديث الحساب وإشعار المبيعات
order.created	طلب جديد	خصم المخزون وتجهيز الشحنة
ticket.escalated	تصعيد تذكرة	إشعار المشرف
student.enrolled	تسجيل طالب	إصدار حساب ومنهج
payment.failed	فشل عملية دفع	متابعة آلية مع العميل

إعادة المحاولة

اعتمد ثلاث محاولات على الأقل بفواصل متزايدة: دقيقة، خمس دقائق، ثلاثون

- لا تعد المحاولة عند أخطاء 4xx إلا بعد تصحيح الطلب.
- أعد المحاولة عند 5xx وأخطاء الشبكة.
- احتفظ بالرسائل الفاشلة سبعة أيام على الأقل.

الفصل الرابع: الاختبار والأمان

النتيجة المتوقعة	الاختبار
استقبال 200 ومعالجة واحدة	حدث صحيح
تجاهل بلا أثر مالي	حدث مكرر
رفض 401 بلا معالجة	توقيع خاطئ
إعادة محاولة ثم طابور مراجعة	انقطاع المتلقي
رفض منظم أو قص للحقول غير اللازمة	حمولة كبيرة

أمان لا يتفاوض

- سر مشترك قوي لكل بيئة، ولا تشاركه بين الإنتاج والتجربة.
- HTTPS فقط، ورفض العناوين غير المشفرة.
- تقييد العناوين المسموح بها عند الإمكان.
- عدم تسجيل الحمولات الكاملة التي تحتوي بيانات شخصية.
- تدوير السر دوريا وتحديث المتلقي قبل التقديم.

> الملف الواحد لا يحتفظ بأسرار. ضع السر في بيئة الخادم أو خدمة الاستقبال، لا داخل HTML.

إلى المكان الصحيح. ابدأ بحدث واحد، راقبه أسبوعا، ثم أضف الثاني. القوالب في الأكاديمية جاهزة لهذا التدرج. الأتمتة الجيدة ليست كثرة الخطافات، بل حدث واحد واضح يصل في وقته