

اليوم 1

Day 1

اليوم 1 — حدود الثقة في الخادم وإعداد المحاكاة

Day 1 — Server trust boundary and mock setup

الأهداف

Objectives

اشرح مسؤوليات المتصفح والخادم والمزود
وأثبت أن المحاكاة تبدأ بلا مفتاح وأن الإعداد
الفعلي الناقص يمنع التشغيل.

Explain browser/server/provider
responsibilities and prove mock startup
needs no key while incomplete live
configuration fails closed.

المتطلبات المسبقة

Prerequisites

أكمل API المختبرة من الأسبوع الثامن وإعداد
البيئة المحلية المستبعدة أو مسار الدعم المتفق
عليه.

Complete the Week 8 tested API and ignored
local environment setup, or the agreed
supported route.

استخدم Python 3.11 أو أحدث واعتماديات
المحاكاة المثبتة. ابدأ

بـ `MODEL_MODE=mock`؛ لا تحتاج مفتاحاً أو
حساباً مدفوعاً أو قاعدة للعمل دون اتصال.

Use Python 3.11+ and the pinned mock
dependencies. Start with

`MODEL_MODE=mock`: no key, paid account
or database is needed for offline work.

الشروحات

Explanations

الإعداد ليس إذنًا

Configuration is not permission

يرسل المتصفح الإعلان الخيالي المقدم لا المفاتيح. يتحقق الخادم منه قبل الاتصال بالمزود. يبدأ MODEL_MODE بالمحاكاة ويتجاهل مفاتيح الاتصال الفعلي. يحتاج الوضع الفعلي مفتاحاً ونموذجاً صريحاً وعلم موافقة لكن العلم لا يمنح موافقة بشرية ولا يفرض ميزانية. استبعد الإعدادات المحلية واحجب الأدلة؛ لا يُحمّل env. تلقائياً.

The browser sends the supplied fictional notice, never credentials. The server validates it before a provider call. MODEL_MODE defaults to mock and ignores live credentials. Live mode requires key, explicit model and approval flag, but the flag alone cannot grant human approval or enforce a budget. Keep local settings ignored and redact evidence; .env is not loaded automatically.

أمثلة

Examples

محاكاة بلا مفتاح تعني بدء التشغيل؛ وضع فعلي بلا مفتاح أو نموذج أو موافقة يمنع التشغيل قبل الشبكة. المفتاح ليس حقل متصفح.

mock + no key → startup succeeds; live + missing key/model/approval → startup stops before network access. A key must never become a browser field.

التدريب الموجّه

Guided practice

ارسم حدود الثقة الثلاثة وحدد موضع تحقق المدخل والمفاتيح والسجلات التشغيلية. توقع حالات الإعداد الناقص قبل اختبارات الإعداد.

Draw the three trust boundaries; identify where input validation, secrets and operational logs belong. Predict every missing-configuration case before running setup tests.

ورقة العمل

Worksheet

قدّم مخطط الحدود وجدول الإعداد وفحص الاستبعاد وشرح لماذا لا تعني اختبارات البداية الناجحة اكتمال التكامل.

Submit the boundary diagram, configuration matrix, ignored-file check and explanation of why a green starter suite is not a completed model integration.

w9d1-evidence

خطوات المختبر

Lab steps

افحص الإعلان المقدم وعقد العينة وتوقع النتيجة والرمز وعدد المحاولات.

Inspect the supplied notice and fixture contract; predict result, status and attempt count.

أنشئ بيئة Python 3.11 أو أحدث وثبّت اعتماديات المحاكاة وشغّل فحوص الإعداد التسعة. افحص

model_settings.py و env.example دون مفتاح حقيقي والتقط الوضع وحقائق النجاح والفشل الآمنة فقط.

Create a Python 3.11+ environment, install pinned mock dependencies and run the nine setup checks.

Inspect model_settings.py and .env.example without adding a real key. Capture only safe mode and pass/fail facts.

حدد أول حد فاشل وأصلحه وأعد الاختبار مع حجب الشبكة. لا تستخدم إعادة مدفوعة كحلقة تصحيح.

Find the first failing boundary, repair it and rerun with network access blocked. Never use a paid retry as a debugging loop.

احفظ الدليل بعد الحجب وملاحظة استخدام الذكاء الاصطناعي أو عدمه وميّز دليل المحاكاة من الفعلي.

Save redacted evidence and an AI-use or non-use note; label mock and live evidence separately.

الحالات الاصطناعية

Synthetic cases

النوع المتوقع	الإدخال المقدم
Expected kind	Supplied input
accepted	approved fictional notice + valid mock → 200; strict category/summary, manual source check
rejected	blank/wrong type/extra field/over 800/unapproved notice → 422; zero provider calls, no input echo
rejected	malformed/extra/missing/wrong type/enum/blank/over 160/refusal/incomplete → 502
rejected	timeout → 504; rate limit → 429; unavailable → 503; generic details only
rejected	two concurrent calls → one outbound attempt, one 429; zero retries including timeout; no restart bypass
accepted	approved real call + validated result + redacted limits/usage/cost/faithfulness record; mock-only remains pending

قائمة الأدلة

Evidence checklist

- ☐ قدّم مخطط الحدود وجدول الإعداد وفحص الاستبعاد وشرح لماذا لا تعني اختبارات البداية الناجحة اكتمال التكامل.

Submit the boundary diagram, configuration matrix, ignored-file check and explanation of why a green starter suite is not a completed model integration.

w9d1-evidence

مسرد الإنجليزية التقنية

Technical English glossary

server-side يعمل داخل الخادم لا المتصفح

environment قيمة إعداد خارج الكود
variable

fail closed المنع عند غياب شرط الأمان

الخصوصية

Privacy

استخدم الإعلان الخيالي المقدم فقط. أبقِ المفاتيح والترويسات وأخطاء المزود الخام والمدخلات والسجلات الحقيقية والرسائل الخاصة خارج السجلات واللقطات والأدلة المشتركة. لا ترسل محتويات القاعدة للنموذج وأبقِ المختبر محلياً.

Use only the supplied fictional notice. Keep keys, headers, raw provider errors, prompts, real records and private messages out of logs, captures and shared evidence. The model must never receive database contents. Keep the lab on localhost.

الذكاء الاصطناعي المسؤول

Responsible AI

يمكن للذكاء الاصطناعي مراجعة عينة فاشلة بعد حجبها وإعادة إنتاجها. عليك تنفيذ الإصلاح واختباره وشرحه. لا تطلب كود التحقق الكامل ولا ترسل بيانات حقيقية. يحتاج أي اتصال بالمزود في هذا التمرين شرط الاتصال الفعلي المنفصل.

AI may review a redacted failing fixture after you reproduce it. You must implement, test and explain the repair. Do not request complete checkpoint code or send real data. Any provider call in this exercise requires the separate live gate.

الاستدراك

Recovery

خلال أسبوع أصلح حداً فاشلاً وأعد تقديم دليل اليوم 1. ابدأ بالمحاكاة. إذا تعذر الوصول أو التمويل فسجل الدليل الفعلي معلقاً ورّتب محاولة بإشراف وموافقة جديدة ولا تقبل دليلاً مختلقاً أو محاكاة بدلاً من الفعلي.

Within one week, repair one failing boundary and resubmit the Day 1 evidence. Use mocks first. If access or budget is unavailable, record live evidence pending and arrange one newly approved supervised attempt; never accept fabricated or mock-only real-call proof.

الأخطاء الشائعة

Common errors

يوضع مفتاح في كود المتصفح أو لقطة أو مخرجات استثناء خام.

A key is placed in browser code, a screenshot or raw exception output.

يُحلل JSON لكن تُقبل الزوائد والتحويلات الضمنية والرفض أو التوليد الناقص.

JSON parses but extra fields, coercions, refusal or incomplete generation are accepted.

تتجاوز الإعادة التلقائية أو الطلبات المتزامنة محاولة واحدة أو تُسمّى المحاكاة اتصالاً فعلياً.

Automatic retries or concurrent calls exceed one attempt; a mock result is labelled live.

اليوم 2 — مدخل صارم ونتيجة منظّمة

Day 2 — Strict input and structured result

الأهداف

Objectives

عرّف نماذج طلب ونتيجة صارمة وارفض حالات البنية التالفة والحقول الزائدة والناقصة والنوع والتصنيف والطول.

Define strict request/result models and reject every malformed, extra-field, missing-field, type, enum and length fixture.

المتطلبات المسبقة

Prerequisites

أكمل API المختبرة من الأسبوع الثامن وإعداد البيئة المحلية المستبعدة أو مسار الدعم المتفق عليه.

Complete the Week 8 tested API and ignored local environment setup, or the agreed supported route.

استخدم Python 3.11 أو أحدث واعتماديات المحاكاة المثبتة. ابدأ

بـ `MODEL_MODE=mock`؛ لا تحتاج مفتاحاً أو حساباً مدفوعاً أو قاعدة للعمل دون اتصال.

Use Python 3.11+ and the pinned mock dependencies. Start with

`MODEL_MODE=mock`: no key, paid account or database is needed for offline work.

الشروحات

Explanations

JSON الصالح هو الفحص الأول فقط

Valid JSON is only the first check

يقبل POST /analyse الحقل notice فقط كنص صارم بطول 1-800 بعد إزالة الفراغات مع رفض الزوائد ومطابقة public_notice.json تماماً. تحتوي النتيجة category بقيمة workshop أو meeting أو other summary وكنص صارم بطول 1-160 بلا زوائد. تحليل JSON والتحقق من المخطط والأمانة للمصدر فحوص منفصلة. الرفض والاستجابة الناقصة ليسا ملخصاً ناجحاً.

POST /analyse accepts only notice: a strict string stripped to 1-800 characters, with extra fields forbidden and exact matching to public_notice.json. The result has category workshop/meeting/other and a strict stripped summary of 1-160 characters, no extras. JSON parsing, schema validation and factual faithfulness are separate checks. Refusals and incomplete responses cannot be treated as successful summaries.

أمثلة

Examples

{category:"workshop","summary":42} هو JSON صالح لكن بياناته غير صالحة. الملخص ذو البنية السليمة الذي يخلق مكاناً يحتاج أيضاً رفضاً بالمراجعة البشرية للمصدر. {"category":"workshop","summary":42} is valid JSON but invalid data. A well-shaped summary inventing a location also needs rejection by the human source check.

التدريب الموجّه

Guided practice

توقع الحالات الثلاث عشرة بجدول الحقل والقاعدة والنتيجة وميّز فشل التحليل والمخطط والرفض والتوليد الناقص.

Predict all thirteen adapter fixtures using a field/rule/outcome table. Contrast parsing failure, schema failure, refusal and incomplete generation.

ورقة العمل

Worksheet

قدّم جدولي المخطط ونتائج الحالات الثلاث عشرة المتوقعة والفعلية وفحص أمانة منفصلاً مقابل المصدر الخيالي.

Submit both schema tables, thirteen expected/actual fixture outcomes and a separate faithfulness check against the fictional source.

w9d2-evidence

Lab steps

افحص الإعلان المقدم وعقد العينة وتوقع النتيجة والرمز وعدد المحاولات.

Inspect the supplied notice and fixture contract; predict result, status and attempt count.

أكمل NoticeRequest و NoticeResult واختبر الفراغات والتحويل الضمني والحقول الناقصة والزائدة والتصنيفات المجهولة وحدود الطول. أثبت رفض المدخل غير المعتمد قبل الوصول للنموذج.

Complete NoticeRequest and NoticeResult. Test whitespace, coercion, missing and extra fields, unknown categories and exact boundary lengths. Prove unapproved input is rejected before model access.

حدد أول حد فاشل وأصلحه وأعد الاختبار مع حجب الشبكة. لا تستخدم إعادة مدفوعة كحلقة تصحيح.

Find the first failing boundary, repair it and rerun with network access blocked. Never use a paid retry as a debugging loop.

احفظ الدليل بعد الحجب وملاحظة استخدام الذكاء الاصطناعي أو عدمه وميّز دليل المحاكاة من الفعلي.

Save redacted evidence and an AI-use or non-use note; label mock and live evidence separately.

الحالات الاصطناعية

Synthetic cases

النوع المتوقع	الإدخال المقدم
Expected kind	Supplied input
accepted	approved fictional notice + valid mock → 200; strict category/summary, manual source check
rejected	blank/wrong type/extra field/over 800/unapproved notice → 422; zero provider calls, no input echo
rejected	malformed/extra/missing/wrong type/enum/blank/over 160/refusal/incomplete → 502
rejected	timeout → 504; rate limit → 429; unavailable → 503; generic details only
rejected	two concurrent calls → one outbound attempt, one 429; zero retries including timeout; no restart bypass
accepted	approved real call + validated result + redacted limits/usage/cost/faithfulness record; mock-only remains pending

Evidence checklist

- ☐ قدّم جدولّي المخطط ونتائج الحالات الثلاث عشرة المتوقعة والفعلية وفحص أمانة منفصلاً مقابل المصدر الخيالي.

Submit both schema tables, thirteen expected/actual fixture outcomes and a separate faithfulness check against the fictional source.

w9d2-evidence

مسرد الإنجليزية التقنية

Technical English glossary

structured output نتيجة تتبع مخطط حقول محدداً

schema قواعد الحقول والأنواع والقيود

refusal امتناع النموذج عن تقديم النتيجة

الخصوصية

Privacy

استخدم الإعلان الخيالي المقدم فقط. أبقِ المفاتيح والترويسات وأخطاء المزود الخام والمدخلات والسجلات الحقيقية والرسائل الخاصة خارج السجلات واللقطات والأدلة المشتركة. لا ترسل محتويات القاعدة للنموذج وأبقِ المختبر محلياً.

Use only the supplied fictional notice. Keep keys, headers, raw provider errors, prompts, real records and private messages out of logs, captures and shared evidence. The model must never receive database contents. Keep the lab on localhost.

الذكاء الاصطناعي المسؤول

Responsible AI

يمكن للذكاء الاصطناعي مراجعة عينة فاشلة بعد حجبها وإعادة إنتاجها. عليك تنفيذ الإصلاح واختباره وشرحه. لا تطلب كود التحقق الكامل ولا ترسل بيانات حقيقية. يحتاج أي اتصال بالمزود في هذا التمرين شرط الاتصال الفعلي المنفصل.

AI may review a redacted failing fixture after you reproduce it. You must implement, test and explain the repair. Do not request complete checkpoint code or send real data. Any provider call in this exercise requires the separate live gate.

الاستدراك

Recovery

خلال أسبوع أصلح حداً فاشلاً وأعد تقديم دليل اليوم 2. ابدأ بالمحاكاة. إذا تعذر الوصول أو التمويل فسجل الدليل الفعلي معلقاً ورّتب محاولة بإشراف وموافقة جديدة ولا تقبل دليلاً مختلقاً أو محاكاة بدلاً من الفعلي.

Within one week, repair one failing boundary and resubmit the Day 2 evidence. Use mocks first. If access or budget is unavailable, record live evidence pending and arrange one newly approved supervised attempt; never accept fabricated or mock-only real-call proof.

الأخطاء الشائعة

Common errors

يوضع مفتاح في كود المتصفح أو لقطة أو مخرجات استثناء خام.

A key is placed in browser code, a screenshot or raw exception output.

يُحلل JSON لكن تُقبل الزوائد والتحويلات الضمنية والرفض أو التوليد الناقص.

JSON parses but extra fields, coercions, refusal or incomplete generation are accepted.

تتجاوز الإعادة التلقائية أو الطلبات المتزامنة محاولة واحدة أو تُسمّى المحاكاة اتصالاً فعلياً.

Automatic retries or concurrent calls exceed one attempt; a mock result is labelled live.

اليوم 3 — عميل المحاكاة وأعطال HTTP الآمنة

Day 3 — Mock client and safe HTTP failures

الأهداف

Objectives

نفّذ حدود النموذج وPOST /analyse بنجاح
متحقق منه وأعطال آمنة 422 و502 و429 و504
و503 دون اتصال بالشبكة.

Implement the model boundary and POST
/analyse with validated success and safe
422/502/429/504/503 failures, without
network access.

المتطلبات المسبقة

Prerequisites

أكمل API المختبرة من الأسبوع الثامن وإعداد
البيئة المحلية المستبعدة أو مسار الدعم المتفق
عليه.

Complete the Week 8 tested API and ignored
local environment setup, or the agreed
supported route.

استخدم Python 3.11 أو أحدث واعتماديات
المحاكاة المثبتة. ابدأ

بـMODEL_MODE=mock؛ لا تحتاج مفتاحاً أو
حساباً مدفوعاً أو قاعدة للعمل دون اتصال.

Use Python 3.11+ and the pinned mock
dependencies. Start with

MODEL_MODE=mock: no key, paid account
or database is needed for offline work.

الشروحات

Explanations

مخرجات المزود مدخل غير موثوق

Provider output is untrusted input

استخدم غلاف العينة المبسط داخل طبقة الربط؛ فهو ليس استجابة OpenAI الشبكية. حوّل الطلب غير الصالح إلى 422 والنتيجة غير الصالحة أو المرفوضة أو الناقصة إلى 502 وحد الطلب أو المعدل إلى 429 والمهلة إلى 504 وتعدّر الخدمة إلى 503. أعد رسائل عامة موثقة فقط وعدّل أخطاء تحقق الطلب لمنع صدى المدخل. أبقِ اختيار الحالة داخلياً ولا تنفذ نص النموذج.

Use the supplied simplified fixture envelope inside the adapter; it is not an OpenAI wire response. Map invalid request to 422, invalid/refused/incomplete result to 502, rate or attempt limit to 429, timeout to 504 and unavailable service to 503. Return only documented generic detail strings. Override request validation errors so rejected input is not echoed. Keep case selection internal and never execute model text.

أمثلة

Examples

عينة انتهاء المهلة تعطي 504 ورسالة Model request timed out. لا يظهر الاستثناء الخام أو المدخل أو الترويسة أو المفتاح في الجسم أو السجلات.

timeout fixture → 504 Model request timed out. No raw exception, prompt, header or key appears in the body or logs.

التدريب الموجّه

Guided practice

تتبع الطلب وقائمة السماح وطبقة الربط والتحقق والرد وحد أول نقطة توقف للمدخل غير الصالح والرفض والمهلة.

Trace request → allowlist → adapter → result validation → HTTP response. Mark the earliest stop point for invalid input, refusal and timeout.

ورقة العمل

Worksheet

قدّم توثيق المسار والنجاح الاصطناعي المتحقق منه وكل رموز الفشل واختبار حجب يثبت غياب المفاتيح والمدخل من الأخطاء والسجلات.

Submit endpoint documentation, validated synthetic success, all failure statuses and a redaction test proving secrets and input are absent from errors and logs.

w9d3-evidence

Lab steps

افحص الإعلان المقدم وعقد العينة وتوقع النتيجة والرمز وعدد المحاولات.

Inspect the supplied notice and fixture contract; predict result, status and attempt count.

أكمل analyse_with_model وسجّل المسار. اختبر الحالات الثلاث عشرة وافحص الرسائل العامة وأثبت عدم استدعاء المزود مع 422. سجّل النتيجة والوضع والعدد والمدة الآمنة فقط.

Complete analyse_with_model and register the route. Exercise all thirteen fixtures through tests, check generic details and assert zero provider access on 422. Use safe outcome/mode/count/duration logs only.

حدد أول حد فاشل وأصلحه وأعد الاختبار مع حجب الشبكة. لا تستخدم إعادة مدفوعة كحلقة تصحيح.

Find the first failing boundary, repair it and rerun with network access blocked. Never use a paid retry as a debugging loop.

احفظ الدليل بعد الحجب وملاحظة استخدام الذكاء الاصطناعي أو عدمه وميّز دليل المحاكاة من الفعلي.

Save redacted evidence and an AI-use or non-use note; label mock and live evidence separately.

الحالات الاصطناعية

Synthetic cases

النوع المتوقع	الإدخال المقدم
Expected kind	Supplied input
accepted	approved fictional notice + valid mock → 200; strict category/summary, manual source check
rejected	blank/wrong type/extra field/over 800/unapproved notice → 422; zero provider calls, no input echo
rejected	malformed/extra/missing/wrong type/enum/blank/over 160/refusal/incomplete → 502
rejected	timeout → 504; rate limit → 429; unavailable → 503; generic details only
rejected	two concurrent calls → one outbound attempt, one 429; zero retries including timeout; no restart bypass
accepted	approved real call + validated result + redacted limits/usage/cost/faithfulness record; mock-only remains pending

Evidence checklist

- ☐ قدّم توثيق المسار والنجاح الاصطناعي المتحقق منه وكل رموز الفشل واختبار حجب يثبت غياب المفاتيح والمدخل من الأخطاء والسجلات.

Submit endpoint documentation, validated synthetic success, all failure statuses and a redaction test proving secrets and input are absent from errors and logs.

w9d3-evidence

الخصوصية

Privacy

استخدم الإعلان الخيالي المقدم فقط. أبقِ المفاتيح والترويسات وأخطاء المزود الخام والمدخلات والسجلات الحقيقية والرسائل الخاصة خارج السجلات واللقطات والأدلة المشتركة. لا ترسل محتويات القاعدة للنموذج وأبقِ المختبر محلياً.

Use only the supplied fictional notice. Keep keys, headers, raw provider errors, prompts, real records and private messages out of logs, captures and shared evidence. The model must never receive database contents. Keep the lab on localhost.

الذكاء الاصطناعي المسؤول

Responsible AI

يمكن للذكاء الاصطناعي مراجعة عينة فاشلة بعد حجبها وإعادة إنتاجها. عليك تنفيذ الإصلاح واختباره وشرحه. لا تطلب كود التحقق الكامل ولا ترسل بيانات حقيقية. يحتاج أي اتصال بالمزود في هذا التمرين شرط الاتصال الفعلي المنفصل.

AI may review a redacted failing fixture after you reproduce it. You must implement, test and explain the repair. Do not request complete checkpoint code or send real data. Any provider call in this exercise requires the separate live gate.

الاستدراك

Recovery

خلال أسبوع أصلح حداً فاشلاً وأعد تقديم دليل اليوم 3. ابدأ بالمحاكاة. إذا تعذر الوصول أو التمويل فسجل الدليل الفعلي معلقاً ورّتب محاولة بإشراف وموافقة جديدة ولا تقبل دليلاً مختلقاً أو محاكاة بدلاً من الفعلي.

Within one week, repair one failing boundary and resubmit the Day 3 evidence. Use mocks first. If access or budget is unavailable, record live evidence pending and arrange one newly approved supervised attempt; never accept fabricated or mock-only real-call proof.

مسرد الإنجليزية التقنية

Technical English glossary

adapter طبقة تترجم بين عقد التطبيق والمزود

timeout انتهاء مهلة انتظار الطلب

sanitized error رسالة خطأ خالية من التفاصيل الحساسة

الأخطاء الشائعة

Common errors

يوضع مفتاح في كود المتصفح أو لقطة أو مخرجات استثناء خام.

A key is placed in browser code, a screenshot or raw exception output.

يُحلل JSON لكن تُقبل الزوائد والتحويلات الضمنية والرفض أو التوليد الناقص.

JSON parses but extra fields, coercions, refusal or incomplete generation are accepted.

تتجاوز الإعادة التلقائية أو الطلبات المتزامنة محاولة واحدة أو تُسمّى المحاكاة اتصالاً فعلياً.

Automatic retries or concurrent calls exceed one attempt; a mock result is labelled live.

اليوم 4 — حدود التكلفة والتحقق دون اتصال

Day 4 — Cost bounds and offline verification

الأهداف

Objectives

أثبت محاولة خارجية واحدة وصفر إعادة وحدوداً ثابتة بناقل وهمي وجهاز ميزانية مراجعة لاتصال فعلي دون طلب غير معتمد.

Prove one outbound attempt, zero retries and fixed limits with a fake transport; prepare a reviewed real-call budget without making an unapproved request.

المتطلبات المسبقة

Prerequisites

أكمل API المختبرة من الأسبوع الثامن وإعداد البيئة المحلية المستبعدة أو مسار الدعم المتفق عليه.

Complete the Week 8 tested API and ignored local environment setup, or the agreed supported route.

استخدم Python 3.11 أو أحدث واعتماديات المحاكاة المثبتة. ابدأ

بـ `MODEL_MODE=mock`؛ لا تحتاج مفتاحاً أو حساباً مدفوعاً أو قاعدة للعمل دون اتصال.

Use Python 3.11+ and the pinned mock dependencies. Start with

`MODEL_MODE=mock`: no key, paid account or database is needed for offline work.

الشروحات

Explanations

انتهاء المهلة لا يلغي حدوث الطلب

A timeout does not undo a request

استخدم 800 حرف للمدخل و256 رمزاً للمخرجات ومهلة 10 ثوانٍ وصفر إعادة تلقائية. احجز المحاولة الوحيدة ذرياً قبل الشبكة واحسبها حتى عند الفشل واختبر الطلبات المتزامنة. يُعاد عداد الذاكرة عند التشغيل وليس ميزانية دائمة. التعليقات والمخطط يستهلكان رموز مدخل أيضاً وحد المخرجات وحده لا يحد التكلفة. قد تُحتسب المهلة مالياً. توقف عند الفشل واطلب موافقة جديدة.

Use 800 input characters, 256 output tokens, a 10-second timeout and zero automatic retries. Count and reserve the single attempt atomically before I/O, including failure. Test simultaneous requests. An in-memory guard resets on restart and is not a durable budget. Full instructions and schema also consume input tokens; output limits alone do not cap cost. A timeout may still be billed. Stop after failure and seek renewed approval.

أمثلة

Examples

طلبان متزامنان يعنيان محاولة خارجية محجوزة واحدة ورد 429 للثاني. لا تؤدي مهلة المحاولة الأولى إلى إعادة خفية.

Two simultaneous requests → one reserved outbound attempt and one 429. A timed-out first attempt must not trigger a hidden retry.

التدريب الموجّه

Guided practice

افحص مراجع Responses والنتائج المنظّمة الرسمية في البداية وميّز تحليل اكتمال المزود ورفضه عن غلاف المحاكاة المبسط وقدر تكلفة الطلب كاملة بأسعار حالية يقدمها المدرب.

Inspect the official Responses and Structured Outputs references in the starter. Distinguish provider completion/refusal parsing from the simplified mock envelope; estimate full request cost with trainer-supplied current prices.

ورقة العمل

Worksheet

قدّم تشغيلين دون اتصال ودليل منع الإعادة والتزامن وتقدير التكلفة الكاملة مع النموذج ومصدر الأسعار وتاريخها وحالة الاتصال المعلقة أو المعتمدة بوضوح.

Submit two offline test runs, no-retry/concurrency evidence, full cost estimate with model/pricing source/date and explicit pending or approved live status.

w9d4-evidence

Lab steps

افحص الإعلان المقدم وعقد العينة وتوقع النتيجة والرمز وعدد المحاولات.

Inspect the supplied notice and fixture contract; predict result, status and attempt count.

أكمل مجموعات الاختبار الأربع وشغلها مرتين مع حجب الشبكة. افحص الحدود والتزامن بنقل فعلي وهمي وأكمل cost-and-failure-checklist.md واترك الاستخدام الفعلي فارغاً حتى الطلب المعتمد. أبقِ المختبر محلياً بعامل واحد.

Complete four test groups and run twice with networking blocked. Use a fake live transport to inspect limits and concurrency. Fill cost-and-failure-checklist.md; leave actual usage blank until an approved live request. Keep the lab local with one worker.

حدد أول حد فاشل وأصلحه وأعد الاختبار مع حجب الشبكة. لا تستخدم إعادة مدفوعة كحلقة تصحيح.

Find the first failing boundary, repair it and rerun with network access blocked. Never use a paid retry as a debugging loop.

احفظ الدليل بعد الحجب وملاحظة استخدام الذكاء الاصطناعي أو عدمه وميّز دليل المحاكاة من الفعلي.

Save redacted evidence and an AI-use or non-use note; label mock and live evidence separately.

الحالات الاصطناعية

Synthetic cases

النوع المتوقع	الإدخال المقدم
Expected kind	Supplied input
accepted	approved fictional notice + valid mock → 200; strict category/summary, manual source check
rejected	blank/wrong type/extra field/over 800/unapproved notice → 422; zero provider calls, no input echo
rejected	malformed/extra/missing/wrong type/enum/blank/over 160/refusal/incomplete → 502
rejected	timeout → 504; rate limit → 429; unavailable → 503; generic details only
rejected	two concurrent calls → one outbound attempt, one 429; zero retries including timeout; no restart bypass
accepted	approved real call + validated result + redacted limits/usage/cost/faithfulness record; mock-only remains pending

Evidence checklist

- ☐ قدّم تشغيلين دون اتصال ودليل منع الإعادة والتزامن وتقدير التكلفة الكاملة مع النموذج ومصدر الأسعار وتاريخها وحالة الاتصال المعلقة أو المعتمدة بوضوح.

Submit two offline test runs, no-retry/concurrency evidence, full cost estimate with model/pricing source/date and explicit pending or approved live status.

w9d4-evidence

الخصوصية

Privacy

استخدم الإعلان الخيالي المقدم فقط. أبقِ المفاتيح والترويسات وأخطاء المزود الخام والمدخلات والسجلات الحقيقية والرسائل الخاصة خارج السجلات واللقطات والأدلة المشتركة. لا ترسل محتويات القاعدة للنموذج وأبقِ المختبر محلياً.

Use only the supplied fictional notice. Keep keys, headers, raw provider errors, prompts, real records and private messages out of logs, captures and shared evidence. The model must never receive database contents. Keep the lab on localhost.

الذكاء الاصطناعي المسؤول

Responsible AI

يمكن للذكاء الاصطناعي مراجعة عينة فاشلة بعد حجبها وإعادة إنتاجها. عليك تنفيذ الإصلاح واختباره وشرحه. لا تطلب كود التحقق الكامل ولا ترسل بيانات حقيقية. يحتاج أي اتصال بالمزود في هذا التمرين شرط الاتصال الفعلي المنفصل.

AI may review a redacted failing fixture after you reproduce it. You must implement, test and explain the repair. Do not request complete checkpoint code or send real data. Any provider call in this exercise requires the separate live gate.

الاستدراك

Recovery

خلال أسبوع أصلح حداً فاشلاً وأعد تقديم دليل اليوم 4. ابدأ بالمحاكاة. إذا تعذر الوصول أو التمويل فسجل الدليل الفعلي معلقاً ورّتب محاولة بإشراف وموافقة جديدة ولا تقبل دليلاً مختلقاً أو محاكاة بدلاً من الفعلي.

Within one week, repair one failing boundary and resubmit the Day 4 evidence. Use mocks first. If access or budget is unavailable, record live evidence pending and arrange one newly approved supervised attempt; never accept fabricated or mock-only real-call proof.

مسرد الإنجليزية التقنية

Technical English glossary

token budget حد رموز المدخل والمخرجات المخطط

retry محاولة إرسال أخرى بعد الفشل

atomic حجز لا تستطيع الطلبات reservation المتزامنة تجاوزه

Common errors

يوضع مفتاح في كود المتصفح أو لقطة أو مخرجات استثناء خام.

A key is placed in browser code, a screenshot or raw exception output.

يُحلل JSON لكن تُقبل الزوائد والتحويلات الضمنية والرفض أو التوليد الناقص.

JSON parses but extra fields, coercions, refusal or incomplete generation are accepted.

تتجاوز الإعادة التلقائية أو الطلبات المتزامنة محاولة واحدة أو تُسمّى المحاكاة اتصالاً فعلياً.

Automatic retries or concurrent calls exceed one attempt; a mock result is labelled live.

اليوم 5 — تحقق فردي من الاتصال المحدود

Day 5 — Individual bounded-call checkpoint

الأهداف

Objectives

اعرض مجموعة المحاكاة المتحقق منها واتصالاً فعلياً محدوداً يوافق عليه المدرب واطرح الأمان والتكلفة أو سجل بوضوح الدليل الفعلي المتبقي وموعد الاستدراك.

Demonstrate the validated mock suite and one trainer-approved bounded real call, explain safety and cost, or explicitly record the remaining live evidence and recovery appointment.

المتطلبات المسبقة

Prerequisites

أكمل API المختبرة من الأسبوع الثامن وإعداد البيئة المحلية المستبعدة أو مسار الدعم المتفق عليه.

Complete the Week 8 tested API and ignored local environment setup, or the agreed supported route.

استخدم Python 3.11 أو أحدث واعتماديات المحاكاة المثبتة. ابدأ

بـ `MODEL_MODE=mock`؛ لا تحتاج مفتاحاً أو حساباً مدفوعاً أو قاعدة للعمل دون اتصال.

Use Python 3.11+ and the pinned mock dependencies. Start with

`MODEL_MODE=mock`: no key, paid account or database is needed for offline work.

الشروحات

Explanations

نجاح المحاكاة لا يثبت التكامل الفعلي

Mock success does not prove live integration

بعد الاختبارات دون اتصال وموافقة الميزانية البشرية نفذ طبقة الربط الفعلية داخل الخادم بنموذج مدعوم صريح وإصدار SDK مثبت. راجع text.format و max_output_tokens ومعالجة الاكتمال والرفض و store=false؛ لا يضمن الأخير انعدام احتفاظ المزود. اعرض استجابة فعلية متحققاً منها وقارنها بالمصدر وسجل الاستخدام عند توفره. غياب التمويل أو الوصول يبغي شرط الاتصال معلقاً ولا يعني اختلاق دليل أو فشل التعلم.

After offline tests and human budget approval, implement the server-only live adapter with an explicit supported model and pinned SDK. Review current Responses text.format, max_output_tokens, completion/refusal handling and store=false; the latter does not promise zero provider retention.

Demonstrate one validated real response, compare it with the source and record usage when available. No funding or access means the real-call requirement remains pending, not failed learning or invented evidence.

أمثلة

Examples

حالات الدليل: محاكاة ناجحة؛ فعلي لم يُحاول أو متعذر أو فاشل أو متحقق منه. النتيجة الفعلية المتحقق منها وحدها تكمل شرط الاتصال.

Evidence labels: mock passed; live not attempted / blocked / attempted-failed / validated. Only validated real output completes the real-call requirement.

التدريب الموجّه

Guided practice

راجع معيار التحقق وافصل أدلة المصدر والاختبارات والإعداد والتكلفة والاتصال الفعلي و اشرح نتيجة غير صالحة دون إجابات مكتملة.

Review the checkpoint rubric and separate source/test/configuration/cost/real-call evidence. Explain one invalid result without looking at completed answers.

ورقة العمل

Worksheet

قدّم المصدر الفردي ونتائج الحالات الثلاث عشرة والاختبارات المكررة والإعداد المحجوب ودليل الاتصال وحدود المدخل والمخرج والطلبات وملاحظة التكلفة والفشل ومراجعة الأمانة والشرح المباشر وحدد أي دليل فعلي غير مكتمل.

Submit individual source, thirteen fixture outcomes, repeated tests, redacted setup and real-call evidence, input/output/request limits, cost/failure note, faithfulness review and live explanation. Clearly identify unfinished live evidence.
w9d5-evidence

خطوات المختبر

Lab steps

افحص الإعلان المقدم وعقد العينة وتوقع النتيجة والرمز وعدد المحاولات.

Inspect the supplied notice and fixture contract; predict result, status and attempt count.

أكمل واشرح مسارك ومخططاتك وطبقة الربط بنفسك. شغل كل الاختبارات دون اتصال وخذ موافقة المدرب قبل المحاولة الفعلية الوحيدة والتقط نتيجة متحققاً منها بعد الحجب وعرض فشل آمن وقدم ملاحظة التكلفة وسجل استخدام الذكاء الاصطناعي. توقف بعد المحاولة الفاشلة.

Complete and explain your own route, schemas and adapter. Run all offline tests, obtain trainer approval before the single bounded live attempt, capture a redacted validated result and a safe failure demonstration, and submit the cost note and AI-use record. Stop after a failed attempt.

حدد أول حد فاشل وأصلحه وأعد الاختبار مع حجب الشبكة. لا تستخدم إعادة مدفوعة كحلقة تصحيح.

Find the first failing boundary, repair it and rerun with network access blocked. Never use a paid retry as a debugging loop.

احفظ الدليل بعد الحجب وملاحظة استخدام الذكاء الاصطناعي أو عدمه وميّز دليل المحاكاة من الفعلي.

Save redacted evidence and an AI-use or non-use note; label mock and live evidence separately.

الحالات الاصطناعية

Synthetic cases

النوع المتوقع	الإدخال المقدم
Expected kind	Supplied input
accepted	approved fictional notice + valid mock → 200; strict category/summary, manual source check
rejected	blank/wrong type/extra field/over 800/unapproved notice → 422; zero provider

النوع المتوقع	الإدخال المقدّم
Expected kind	Supplied input
	calls, no input echo
rejected	malformed/extra/missing/wrong type/enum/blank/over 160/refusal/incomplete → 502
rejected	timeout → 504; rate limit → 429; unavailable → 503; generic details only
rejected	two concurrent calls → one outbound attempt, one 429; zero retries including timeout; no restart bypass
accepted	approved real call + validated result + redacted limits/usage/cost/faithfulness record; mock-only remains pending

قائمة الأدلة

Evidence checklist

- ☐ قدّم المصدر الفردي ونتائج الحالات الثلاث عشرة والاختبارات المكررة والإعداد المحجوب ودليل الاتصال وحدود المدخل والمخرج والطلبات وملاحظة التكلفة والفشل ومراجعة الأمانة والشرح المباشر وحدد أي دليل فعلي غير مكتمل.

Submit individual source, thirteen fixture outcomes, repeated tests, redacted setup and real-call evidence, input/output/request limits, cost/failure note, faithfulness review and live explanation. Clearly identify unfinished live evidence.

w9d5-evidence

الخصوصية

Privacy

استخدم الإعلان الخيالي المقدم فقط. أبقِ المفاتيح والترويسات وأخطاء المزود الخام والمدخلات والسجلات الحقيقية والرسائل الخاصة خارج السجلات واللقطات والأدلة المشتركة. لا ترسل محتويات القاعدة للنموذج وأبقِ المختبر محلياً.

Use only the supplied fictional notice. Keep keys, headers, raw provider errors, prompts, real records and private messages out of logs, captures and shared evidence. The model must never receive database contents. Keep the lab on localhost.

الذكاء الاصطناعي المسؤول

Responsible AI

يمكن للذكاء الاصطناعي مراجعة عينة فاشلة بعد حجبها وإعادة إنتاجها. عليك تنفيذ الإصلاح واختباره وشرحه. لا تطلب كود التحقق الكامل ولا ترسل بيانات حقيقية. يحتاج أي اتصال بالمزود في هذا التمرين شرط الاتصال الفعلي المنفصل.

AI may review a redacted failing fixture after you reproduce it. You must implement, test and explain the repair. Do not request complete checkpoint code or send real data. Any provider call in this exercise requires the separate live gate.

الاستدراك

Recovery

خلال أسبوع أصلح حداً فاشلاً وأعد تقديم دليل اليوم 5. ابدأ بالمحاكاة. إذا تعذر الوصول أو التمويل فسجل الدليل الفعلي معلقاً ورّتب محاولة بإشراف وموافقة جديدة ولا تقبل دليلاً مختلقاً أو محاكاة بدلاً من الفعلي.

Within one week, repair one failing boundary and resubmit the Day 5 evidence. Use mocks first. If access or budget is unavailable, record live evidence pending and arrange one newly approved supervised attempt; never accept fabricated or mock-only real-call proof.

مسرد الإنجليزية التقنية

Technical English glossary

live evidence دليل اتصال فعلي لا محاكاة

faithfulness التزام الملخص بما يقوله المصدر

recovery مسار لإكمال الدليل الناقص بإشراف

Common errors

يوضع مفتاح في كود المتصفح أو لقطة أو مخرجات استثناء خام.

A key is placed in browser code, a screenshot or raw exception output.

يُحلل JSON لكن تُقبل الزوائد والتحويلات الضمنية والرفض أو التوليد الناقص.

JSON parses but extra fields, coercions, refusal or incomplete generation are accepted.

تتجاوز الإعادة التلقائية أو الطلبات المتزامنة محاولة واحدة أو تُسمّى المحاكاة اتصالاً فعلياً.

Automatic retries or concurrent calls exceed one attempt; a mock result is labelled live.