Xalgorix: أداة اختبار اختراق مفتوحة المصدر بالذكاء الاصطناعي تضيف وكيلًا ثانياً للتحقق من النتائج



تعتمد أداة Xalgorix المجانية المفتوحة المصدر على وكيل ثانٍ يعيد استغلال كل ثغرة قبل اعتمادها. ولم تُنشر نتائج قياس أداء، وتعمل حاوية Docker بصلاحيات الجذر.

- يبدأ وكيل التحقق من سياق جديد بأدوات للقراءة فقط، وعليه إعادة استغلال كل ثغرة يجدها الوكيل الأول.
- لا تُسقَط النتائج غير المثبتة تلقائياً، بل تُحال إلى المراجعة اليدوية ما لم يثبت بطلانها.
- تشغّل الأداة Nmap وNucleig وSQLmap، وتعمل مع سبعة مزوّدي نماذج لغوية منها النماذج المحلية عبر Ollama، وفيها حارس نطاق يقيّد الأهداف.
- لم ينشر المطوّرون نتائج قياس أداء، ولم يكتمل بعد تشغيل اختبارات XBOW كاملة.
- تعمل حاوية Docker بصلاحيات الجذر وتتطلب --privileged أو صلاحيات إضافية، ولذلك تُعامل كبيئة معزولة قابلة للتخلص منها.

Xalgorix أداة مجانية مفتوحة المصدر لاختبار الاختراق، صادرة برخصة Apache-2.0. يعمل فيها وكيل قائم على نموذج لغوي مزوّد بمتصفح وطرفية وفق خطة اختبار من 22 مرحلة، من الاستطلاع حتى التقرير النهائي، مستعيناً بأدوات معروفة مثل Nmap وNucleig وSQLmap. ويمنع حارس النطاق أي استدعاء لأجهزة خارج الأهداف المحددة ونطاقاتها الفرعية.

آلية التحقق من النتائج

عندما يجد الوكيل الرئيسي ثغرة، يتولى وكيل تحقق مستقل إعادة استغلالها. يبدأ هذا الوكيل من سياق جديد، ويتعامل مع إثبات الوكيل الأول على أنه غير موثوق، ويملك أدوات للقراءة فقط، وكل فحص محدود بثماني جولات وثلاث دقائق. ويختلف معيار القبول حسب نوع الثغرة: ففي XSS يجب أن ينفَّذ السكربت فعلًا، وفي SSRF يلزم استدعاء من خادم الهدف إلى رمز جديد. وإذا أقرّ النموذج بالتأكيد دون إعادة اختبار ناجحة، يخفّض الكود الحكم إلى غير حاسم. ولا تُسقَط النتيجة إلا بإثبات بطلانها، وما عداها يُحال إلى المراجعة اليدوية.

حدود ينبغي الانتباه إليها

يذكر مؤسس المشروع أن لديهم اختبارات داخلية، منها مقارنة تطبيقات هشّة بنسخ آمنة، وثغرات CVE حقيقية مقابل إصدارات مصحَّحة، لكن لا نتائج منشورة. كما بدأ العمل على اختبارات XBOW دون تشغيلها كاملة. وقد أعطى Claude Opus 5.5 أفضل النتائج، بينما تحتاج النماذج المحلية إلى إشراف أكبر في الفحوص الطويلة.

تعمل حاوية Docker بصلاحيات الجذر وتتطلب --privileged أو صلاحيات إضافية، وينصح المطوّرون باستخدامها كبيئة معزولة قابلة للتخلص منها على شبكة منفصلة.

بالنسبة للجهات الخاضعة للتنظيم، تستحق الأداة تقييماً دقيقاً قبل اعتمادها، لا الاكتفاء بما يُعلن عنها.

ما يجب فعله الآن

1. عند تجربة Xalgorix، شغّلها في شبكة مختبر معزولة فقط، كما ينصح المطوّرون بسبب صلاحيات الجذر في الحاوية.
2. اقصر الأهداف المضبوطة على أنظمة تملكها أو لديك تفويض كتابي باختبارها، وتأكد من عمل حارس النطاق كما هو متوقع.
3. اختبر الأداة على نسخ هشّة وأخرى مصحَّحة من تطبيقاتك لقياس الإيجابيات الكاذبة بنفسك، إذ لا توجد نتائج منشورة.
4. عيّن مسؤولًا لمراجعة النتائج المحالة إلى قائمة المراجعة اليدوية.
5. لا تعتمد على مخرجات أدوات الذكاء الاصطناعي بديلًا عن اختبارات الاختراق المصرّح بها التي تتطلبها أطر الجهة المنظِّمة.