Umbra

نموذج — اختبار اختراق خارجي لبنك أكمي

ملخص تنفيذي

أُعدّ لصالح	ACME Bank
التاريخ	2026-11-06
التصنيف	سري

نظرة عامة على المخاطر

مستوى الخطورة العام: حرج · إجمالي النتائج: 19 · مؤكدة: 6

الخطورة	النتائج
حرج	3
مرتفع	4
متوسط	6
منخفض	4
معلوماتي	2
غير مصنف	0

الملخص

External infrastructure and web application assessment of internet-facing banking services.

أبرز النتائج

- مكوّن برمجي قديم يحتوي على ثغرات معروفة: يعمل التطبيق ببرمجيات قديمة تحتوي على ثغرات أمنية معروفة للعموم.
- حقن SQL: يستطيع المهاجم عبر الإنترنت قراءة قاعدة بيانات التطبيق أو تعديلها، بما في ذلك بيانات العملاء.
- المرجع المباشر غير الآمن للكائنات: يستطيع أي عميل الاطلاع على السجلات الخاصة بعملاء آخرين بتغيير رقم في الطلب.
- غياب التحديثات الأمنية لنظام التشغيل أو البرمجيات: تفتقد عدة أنظمة تحديثات أمنية لثغرات يستغلها المهاجمون فعليًا.
- البرمجة النصية عبر المواقع المخزنة: يستطيع أحد المستخدمين زرع شيفرة تعمل في متصفحات المستخدمين الآخرين، ومنهم المسؤولون.

نطاق الاختبار

العميل: ACME Bank

فترة الاختبار: –

ضمن النطاق	نوع الاختبار
netbanking.acme-bank.example	domain
loans.acme-bank.example	domain
10.20.0.0/24	cidr

خارج النطاق	نوع الاختبار
10.20.9.0/24	cidr

تغطية المنهجية

قائمة التحقق	تم اختباره	ناجح	فاشل	%
OWASP Top 10 (2021)	7/24	4	3	29

ملخص النتائج

#	الاسم	الخطورة	الحالة	الأصل المتأثر
1	مكوّن برمجي قديم يحتوي على ثغرات معروفة	حرج	مفتوحة	10.20.0.21
2	حقن SQL	حرج	مفتوحة	10.20.0.10
3	SQL injection in login form	حرج	مفتوحة	10.20.0.10
4	المرجع المباشر غير الآمن للكائنات	مرتفع	مفتوحة	10.20.0.10
5	Outdated OpenSSH	مرتفع	مغلقة	10.20.0.5
6	غياب التحديثات الأمنية لنظام التشغيل أو البرمجيات	مرتفع	مفتوحة	10.20.0.5
7	البرمجة النصية عبر المواقع المخزنة	مرتفع	مفتوحة	10.20.0.10
8	واجهة إدارية مكشوفة على الإنترنت	متوسط	مفتوحة	10.20.1.40
9	غياب ترويسات أمان HTTP	متوسط	مغلقة	10.20.0.30
10	عدم اشتراط توقيع SMB	متوسط	مفتوحة	10.20.2.15
11	كشف أسماء المستخدمين	متوسط	مفتوحة	10.20.0.10
12	Weak password policy	متوسط	مفتوحة	10.20.0.10
13	دعم إصدارات قديمة من بروتوكولات SSL/TLS	متوسط	مفتوحة	10.20.0.30
14	ملف تعريف الارتباط للجلسة دون خصائص Secure أو HttpOnly أو SameSite	منخفض	مغلقة	10.20.0.30
15	Directory listing enabled	منخفض	مفتوحة	portal.acme.example
16	تفعيل عرض محتويات المجلدات	منخفض	مفتوحة	10.20.0.30
17	رسائل أخطاء تفصيلية وتتبع المكدس	منخفض	مفتوحة	10.20.0.21
18	إتاحة سطح المكتب البعيد (RDP) على الإنترنت	معلوماتي	مفتوحة	10.20.2.15
19	كشف إصدار البرمجيات في لافتات الخدمات	معلوماتي	مفتوحة	10.20.0.5