Umbra

SAMPLE — Acme Bank external penetration test

Technical Report / تقرير فني

Prepared for / أُعدّ لصالح	ACME Bank
Date / التاريخ	2026-11-06
Classification / التصنيف	Confidential

Risk Overview / نظرة عامة على المخاطر

Overall risk: Critical · Total findings: 19 · Confirmed: 6

Severity	Findings
Critical / حرج	3
High / مرتفع	4
Medium / متوسط	6
Low / منخفض	4
Info / معلوماتي	2
Unclassified / غير مصنف	0

Summary / الملخص

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

Key findings / أبرز النتائج

• Remote code execution in Apache Struts (S2-066): The application runs outdated software with publicly known security flaws.

• مكوّن برمجي قديم يحتوي على ثغرات معروفة: يعمل التطبيق ببرمجيات قديمة تحتوي على ثغرات أمنية معروفة للعموم.

• SQL injection in /api/accounts/search: An attacker on the internet can read or change the application's database, including customer data.

• حقن SQL: يستطيع المهاجم عبر الإنترنت قراءة قاعدة بيانات التطبيق أو تعديلها، بما في ذلك بيانات العملاء.

• Broken access control: view any customer's statements: Any customer can view other customers' private records by changing a number in the request.

• المرجع المباشر غير الآمن للكائنات: يستطيع أي عميل الاطلاع على السجلات الخاصة بعملاء آخرين بتغيير رقم في الطلب.

• Outdated OpenSSH with known vulnerabilities: Several systems are missing security updates for flaws that attackers actively exploit.

• غياب التحديثات الأمنية لنظام التشغيل أو البرمجيات: تفتقد عدة أنظمة تحديثات أمنية لثغرات يستغلها المهاجمون فعليًا.

• Stored cross-site scripting in support tickets: A user can plant code that runs in the browsers of other users, including administrators.

• البرمجة النصية عبر المواقع المخزنة: يستطيع أحد المستخدمين زرع شيفرة تعمل في متصفحات المستخدمين الآخرين، ومنهم المسؤولون.

Engagement scope / نطاق الاختبار

Client: ACME Bank

Testing period: –

In scope	Engagement type
netbanking.acme-bank.example	domain
loans.acme-bank.example	domain
10.20.0.0/24	cidr

Out of scope	Engagement type
10.20.9.0/24	cidr

Methodology coverage / تغطية المنهجية

Checklist	Tested	Passed	Failed	%
OWASP Top 10 (2021)	7/24	4	3	29

Findings summary / ملخص النتائج

#	Name	Severity	Status	Affected asset
1	Remote code execution in Apache Struts (S2-066) / مكوّن برمجي قديم يحتوي على ثغرات معروفة	Critical	Open	10.20.0.21
2	SQL injection in /api/accounts/search / حقن SQL	Critical	Open	10.20.0.10
3	SQL injection in login form	Critical	Open	10.20.0.10
4	Broken access control: view any customer's statements / المرجع المباشر غير الآمن للكائنات	High	Open	10.20.0.10
5	Outdated OpenSSH	High	Closed	10.20.0.5
6	Outdated OpenSSH with known vulnerabilities / غياب التحديثات الأمنية لنظام التشغيل أو البرمجيات	High	Open	10.20.0.5
7	Stored cross-site scripting in support tickets / البرمجة النصية عبر المواقع المخزنة	High	Open	10.20.0.10
8	Exposed Jenkins dashboard / واجهة إدارية مكشوفة على الإنترنت	Medium	Open	10.20.1.40
9	Missing HTTP security headers / غياب ترويسات أمان HTTP	Medium	Closed	10.20.0.30
10	SMB signing not required / عدم اشتراط توقيع SMB	Medium	Open	10.20.2.15
11	User enumeration on login page / كشف أسماء المستخدمين	Medium	Open	10.20.0.10
12	Weak password policy	Medium	Open	10.20.0.10
13	Weak TLS configuration (TLS 1.0/1.1 enabled) / دعم إصدارات قديمة من بروتوكولات SSL/TLS	Medium	Open	10.20.0.30

14	ملف تعريف الارتباط / Cookie without Secure flag للجلسة دون خصائص Secure أو HttpOnly أو SameSite	Low	Closed	10.20.0.30
15	Directory listing enabled	Low	Open	portal.acme.example
16	تفعيل عرض / Directory listing enabled on /static محتويات المجلدات	Low	Open	10.20.0.30
17	/ Verbose error messages disclose stack traces رسائل أخطاء تفصيلية وتتبع المكدس	Low	Open	10.20.0.21
18	إتاحة سطح / Open port 3389 (RDP) on jump host المكتب البعيد (RDP) على الإنترنت	Info	Open	10.20.2.15
19	كشف إصدار البرمجيات / Server version disclosure في لافتات الخدمات	Info	Open	10.20.0.5

Detailed findings / تفاصيل النتائج

1. Remote code execution in Apache Struts (S2-066)

مكوّن برمجي قديم يحتوي على ثغرات معروفة

Severity	CVSS v3	Status	Affected asset
Critical	9.8	Open	10.20.0.21 (https-alt 8443/tcp)

CVE: CVE-2023-50164

Description

The legacy loan-portal runs a vulnerable Apache Struts version that allows path traversal in file upload leading to remote code execution.

الوصف

يستخدم التطبيق إطار عمل أو مكتبة أو مكوّن خادم بإصدار يحتوي على ثغرات معروفة للعموم. يرد المكوّن المتأثر وإصداره في الأدلة.

الأثر

بحسب الثغرة، قد يستخدم المهاجم طرق استغلال منشورة لتنفيذ شيفرة أو قراءة البيانات أو تعطيل الخدمة. تُعد البرمجيات غير المحدّثة من أكثر أسباب الاختراقات شيوعًا.

Remediation

Upgrade Struts to 6.3.0.2 or later. Restrict upload handling until patched.

المعالجة

حدّث المكوّن إلى إصدار مدعوم يعالج الثغرات المذكورة. احتفظ بقائمة جرد للمكتبات المعتمدة، وتابع النشرات الأمنية، وأضف فحص المكتبات إلى عملية البناء ليُطبَّق التحديث الأمني بسرعة.

2. SQL injection in /api/accounts/search

حقن **SQL**

Severity	CVSS v3	Status	Affected asset
Critical	9.8	Open	10.20.0.10 (unknown 443/tcp)

Description

The `q` parameter of `/api/accounts/search` is concatenated into a SQL query. An unauthenticated attacker can read the full customer database.

الوصف

يبني التطبيق استعلامات قاعدة البيانات بدمج مدخلات المستخدم مباشرة في نص SQL. يستطيع المهاجم تغيير بنية الاستعلام بإرسال صيغة SQL في أحد المعاملات أو الترويسات أو قيمة ملف تعريف الارتباط. تم تأكيد الثغرة بتغيير منطق الاستعلام وملاحظة اختلاف الاستجابات أو زمنها.

الأثر

يستطيع المهاجم قراءة البيانات في قاعدة البيانات أو تعديلها أو حذفها، وتجاوز المصادقة، وفي بعض البيئات تنفيذ أوامر نظام التشغيل على خادم قاعدة البيانات.

Remediation

Use parameterised queries for all database access and add server-side input validation. Re-test after deployment.

المعالجة

استخدم الاستعلامات المهيأة (Prepared Statements) أو أداة ORM آمنة في جميع استدعاءات قاعدة البيانات، ولا تبنِ استعلامات SQL بدمج النصوص. طبّق التحقق من المدخلات كطبقة حماية إضافية، وشغّل التطبيق بحساب قاعدة بيانات وفق مبدأ الحد الأدنى من الصلاحيات، وأزل رسائل أخطاء قاعدة البيانات التفصيلية من الاستجابات.

3. SQL injection in login form

Severity	CVSS v3	Status	Affected asset
Critical	-	Open	10.20.0.10 (unknown 443/tcp)

CVE: CVE-2021-1111

Description

The username parameter is concatenated into SQL.

Remediation

Use parameterised queries.

References: https://owasp.org/Top10/A03_2021-Injection/

4. Broken access control: view any customer's statements

المرجع المباشر غير الآمن للكائنات

Severity	CVSS v3	Status	Affected asset
High	6.5	Open	10.20.0.10 (unknown 443/tcp)

Description

Changing the `accountId` in `/statements/{id}` returns statements of other customers (IDOR).

الوصف

يستخدم التطبيق معرّفات من الطلب، مثل رقم الحساب أو المستند، لتحميل السجلات دون التحقق من أنها تخص المستخدم الحالي. يؤدي تغيير المعرّف إلى إرجاع بيانات مستخدم آخر.

الأثر

يستطيع أي مستخدم مسجّل الدخول قراءة سجلات العملاء الآخرين، مثل الكشوف أو الفواتير أو البيانات الشخصية، وتعديلها في بعض الوظائف.

Remediation
Enforce object-level authorisation on every request; derive the account from the session, not the URL.

المعالجة

طبّق التحقق من التفويض على الخادم لكل كائن، وذلك بتحميل السجلات عبر استعلام مقيّد بالمستخدم أو الجهة الحالية مع الرفض افتراضيًا. استخدم معرّفات غير قابلة للتخمين كطبقة دفاع إضافية، وأضف اختبارات آلية للوصول بين الحسابات ضمن التحكم في الوصول.

5. Outdated OpenSSH

Severity	CVSS v3	Status	Affected asset
High	-	Closed	10.20.0.5 (unknown 22/tcp)

CVE: CVE-2016-6210, CVE-2018-15473

Description
OpenSSH 7.2 has known vulnerabilities.

Remediation
Upgrade OpenSSH.

6. Outdated OpenSSH with known vulnerabilities

غياب التحديثات الأمنية لنظام التشغيل أو البرمجيات

Severity	CVSS v3	Status	Affected asset
High	8.1	Open	10.20.0.5 (unknown 22/tcp)

CVE: CVE-2024-6387

Description
OpenSSH 8.9p1 on the VPN gateway is affected by the regreSSHion race condition.

الوصف

تفتقد الأجهزة تحديثات أمنية أصدرها المورّد منذ عدة أشهر، بما فيها إصلاحات لثغرات تتوفر لها طرق استغلال علنية. ترد التحديثات الناقصة والأجهزة المتأثرة في الأدلة.

الأثر

يستطيع المهاجمون استخدام طرق استغلال علنية لتنفيذ شيفرة أو تصعيد الصلاحيات أو التنقل بين الأنظمة. يُعد غياب التحديث الأمني من الأسباب الرئيسية لنجاح الهجمات.

Remediation
Upgrade OpenSSH to 9.8p1 or apply the vendor patch; set LoginGraceTime 0 as a temporary mitigation.

المعالجة

طبّق التحديثات الناقصة بدءًا بالأنظمة المتصلة بالإنترنت والثغرات المدرجة في فهرس CISA للثغرات المستغلة فعليًا. أنشئ عملية لإدارة التحديثات بجداول زمنية محددة حسب الخطورة، وقدّم تقارير عن الالتزام بها.

7. Stored cross-site scripting in support tickets

البرمجة النصية عبر المواقع المخزنة

Severity	CVSS v3	Status	Affected asset
High	7.6	Open	10.20.0.10 (unknown 443/tcp)

Description
Ticket subjects are rendered without output encoding in the agent console, allowing session theft of support staff.

الوصف

تُحفظ بيانات يدخلها أحد المستخدمين ثم تُعرض لاحقًا لمستخدمين آخرين دون ترميز المخرجات. يُنفَّذ أي نص برمجي يوضع في حقل مخزن، مثل اسم الملف الشخصي أو تعليق، في متصفح كل مستخدم يعرض الصفحة.

الأثر

يستطيع المهاجم التصرف باسم الضحايا داخل التطبيق، وسرقة رموز الجلسة المتاحة للنصوص البرمجية، وتغيير ما يراه المستخدمون، واستهداف المسؤولين الذين يعرضون المحتوى المخزن.

Remediation
Encode output by context and add a strict Content-Security-Policy.

المعالجة

طبّق ترميز المخرجات المناسب للسياق في كل موضع تُعرض فيه البيانات المخزنة باستخدام الترميز التلقائي في محرك القوالب. نقِّ النصوص المنسقة بأداة تنقية HTML محدّثة، وأضف سياسة أمان المحتوى (CSP) كطبقة ثانية، واضبط ملفات تعريف الارتباط الخاصة بالجلسة بخاصية HttpOnly.

8. Exposed Jenkins dashboard

واجهة إدارية مكشوفة على الإنترنت

Severity	CVSS v3	Status	Affected asset
Medium	6.5	Open	10.20.1.40 (http-proxy 8080/tcp)

Description
Jenkins is reachable from the internet with anonymous read access to job configuration.

الوصف

يمكن الوصول من الإنترنت إلى واجهات الإدارة، مثل لوحة إدارة التطبيق أو الواجهة الخلفية لنظام إدارة المحتوى أو وحدة تحكم قاعدة البيانات أو صفحة إدارة الخادم.

الأثر

تصبح هذه الواجهات هدفًا مباشرًا لتخمين كلمات المرور ولاستغلال ثغرات برمجيات الإدارة، ويمنح اختراقها سيطرة واسعة.

Remediation

Restrict access to the VPN and disable anonymous read.

المعالجة

قصر الوصول إلى الواجهات الإدارية على الشبكة الداخلية أو عبر VPN، واشترط المصادقة متعددة العوامل، واسمح بالوصول فقط من عناوين IP معروفة حيثما أمكن.

9. Missing HTTP security headers

غياب ترويسات أمان **HTTP**

Severity	CVSS v3	Status	Affected asset
Medium	5.4	Closed	10.20.0.30 (https 443/tcp)

Description

HSTS, Content-Security-Policy and X-Frame-Options are not set.

الوصف

لا تتضمن الاستجابات ترويسات الأمان الشائعة مثل Content-Security-Policy وX-Content-Type-Options: nosniff و Referrer-Policy. تضيف كل ترويسة أمان طبقة حماية في المتصفح.

الأثر

تقل حماية التطبيق من البرمجة النصية عبر المواقع ومن تخمين نوع المحتوى ومن تسريب الروابط إلى جهات خارجية إذا وُجدت ثغرة أخرى.

Remediation

Add the headers at the reverse proxy.

المعالجة

أضف Content-Security-Policy وX-Content-Type-Options: nosniff و-Referrer-Policy: strict-origin-when-cross origin وPermissions-Policy على خادم الويب أو في إطار العمل، واختبر السياسة قبل فرضها.

10. SMB signing not required

عدم اشتراط توقيع **SMB**

Severity	CVSS v3	Status	Affected asset
Medium	6.8	Open	10.20.2.15 (microsoft-ds 445/tcp)

Description

The file server does not require SMB signing, enabling NTLM relay attacks inside the network.

الوصف

تقبل أجهزة Windows اتصالات SMB دون توقيع الرسائل. يثبت التوقيع أن رسائل SMB صادرة عن الطرف المتوقع وأنها لم تُعدَّل.

الأثر

يستطيع المهاجم على الشبكة الداخلية تنفيذ هجوم الترحيل لمصادقة NTLM، بتمرير بيانات المصادقة الملتقطة إلى هذه الأجهزة لتنفيذ أوامر أو الوصول إلى الملفات باسم الضحية، مما يؤدي غالبًا إلى الحركة الجانبية.

Remediation

Enforce SMB signing through Group Policy.

المعالجة

اشترط توقيع SMB على جميع الخوادم ومحطات العمل عبر نهج المجموعة (Microsoft network server/client: Digitally sign communications (always))، بدءًا بوحدة التحكم بالمجال وخوادم الملفات.

11. User enumeration on login page

كشف أسماء المستخدمين

Severity	CVSS v3	Status	Affected asset
Medium	5.3	Open	10.20.0.10 (unknown 443/tcp)

Description

Different error messages reveal whether a username exists.

الوصف

تستجيب وظائف تسجيل الدخول أو التسجيل أو إعادة تعيين كلمة المرور بشكل مختلف حسب وجود الحساب، من خلال رسائل أو رموز حالة أو أزمنة استجابة مختلفة.

الأثر

يستطيع المهاجم بناء قائمة بأسماء المستخدمين أو عناوين البريد الصحيحة، مما يزيد فعالية تخمين كلمات المرور وإعادة استخدام بيانات الاعتماد والتصيد الموجّه.

Remediation
Return one generic error message and add rate limiting.

المعالجة

أعد الرسالة ورمز الحالة والزمن نفسه للحسابات الموجودة وغير الموجودة، مثل: "إذا كان الحساب موجودًا فقد أرسلنا رسالة بريد". وطبّق تحديد معدل الطلبات على هذه الوظائف.

12. Weak password policy

Severity	CVSS v3	Status	Affected asset
Medium	-	Open	10.20.0.10

Description
Domain allows 8 character passwords.

Remediation
Require 14 characters.

13. Weak TLS configuration (TLS 1.0/1.1 enabled)

دعم إصدارات قديمة من بروتوكولات **SSL/TLS**

Severity	CVSS v3	Status	Affected asset
Medium	5.9	Open	10.20.0.30 (https 443/tcp)

Description
The marketing site accepts TLS 1.0 and 1.1 and CBC cipher suites.

الوصف

تقبل الخدمة SSLv3 أو TLS 1.0 أو TLS 1.1. تحتوي هذه الإصدارات على نقاط ضعف معروفة ولم تعد مسموحة في المعايير الحالية مثل PCI DSS.

الأثر

قد يتمكن مهاجم في موقع يسمح باعتراض الحركة من إضعاف التشفير في بعض الجلسات أو كسره وقراءة البيانات أو تعديلها.

Remediation
Disable TLS < 1.2 and CBC suites; prefer TLS 1.3.

المعالجة

عطّل SSLv3 وTLS 1.0 وTLS 1.1 واسمح فقط بـ TLS 1.2 وTLS 1.3. تأكد قبل التغيير من دعم العملاء وتكاملات الشركاء لـ TLS 1.2.

14. Cookie without Secure flag

ملف تعريف الارتباط للجلسة دون خصائص **Secure** أو **HttpOnly** أو **SameSite**

Severity	CVSS v3	Status	Affected asset
Low	3.1	Closed	10.20.0.30 (https 443/tcp)

Description

The `lang` cookie is set without the Secure attribute.

الوصف

يُضبط ملف تعريف الارتباط الخاص بالجلسة دون خاصية حماية واحدة أو أكثر: Secure (يُرسل عبر HTTPS فقط)، وHttpOnly (لا تقرؤه النصوص البرمجية)، وSameSite (لا يُرسل مع الطلبات عبر المواقع).

الأثر

قد تنكشف الجلسة عبر اتصالات غير مشفرة، أو تُسرق عبر البرمجة النصية عبر المواقع، أو تُستخدم في هجمات تزوير الطلبات عبر المواقع.

Remediation

Set Secure and SameSite on all cookies.

المعالجة

اضبط ملف تعريف الارتباط الخاص بالجلسة بالخصائص Secure وHttpOnly وSameSite=Lax (أو Strict إذا سمحت مسارات العمل)، واستخدم البادئة __Host- حيثما أمكن.

15. Directory listing enabled

Severity	CVSS v3	Status	Affected asset
Low	-	Open	portal.acme.example (https 443/tcp)

Description

Directory listing shows internal files.

Remediation

Disable autoindex.

16. Directory listing enabled on /static

تفعيل عرض محتويات المجلدات

Severity	CVSS v3	Status	Affected asset
Low	-	Open	10.20.0.30 (https 443/tcp)

Description

Directory listing reveals file names.

الوصف

يعرض خادم الويب محتويات المجلدات التي لا تحتوي على صفحة فهرس، فتظهر جميع الملفات المخزنة فيها.

الأثر

يستطيع المهاجمون اكتشاف ملفات لم يُقصد ربطها مثل النسخ الاحتياطية أو ملفات التصدير أو السجلات أو الإعدادات، مما يؤدي إلى كشف المعلومات.

Remediation
Disable autoindex.

المعالجة

عطّل الفهرسة التلقائية للمجلدات في إعدادات خادم الويب (مثل Options -Indexes في Apache أو autoindex off في nginx)، واحذف الملفات التي لا يجب أن تكون عامة.

17. Verbose error messages disclose stack traces

رسائل أخطاء تفصيلية وتتبع المكدس

Severity	CVSS v3	Status	Affected asset
Low	5.3	Open	10.20.0.21 (https-alt 8443/tcp)

Description
Unhandled exceptions return full Java stack traces.

الوصف

تعرض صفحات الأخطاء تتبع المكدس أو صفحات تصحيح إطار العمل أو أخطاء SQL أو المسارات الداخلية أو إصدارات البرمجيات عند إرسال مدخلات غير متوقعة، وهذا نوع من كشف المعلومات.

الأثر

تساعد هذه التفاصيل المهاجم على معرفة التقنيات المستخدمة وإيجاد المكونات المعرّضة للثغرات وصياغة طرق استغلال فعالة بسرعة أكبر.

Remediation
Use generic error pages in production.

المعالجة

عطّل وضع التصحيح في بيئة الإنتاج، وأعد صفحات أخطاء عامة مع رقم مرجعي، وسجّل التفاصيل الكاملة على الخادم فقط.

18. Open port 3389 (RDP) on jump host

إتاحة سطح المكتب البعيد (**RDP**) على الإنترنت

Severity	CVSS v3	Status	Affected asset
Info	-	Open	10.20.2.15 (ms-wbt-server 3389/tcp)

Description
RDP is reachable from the internal user network.

الوصف

يمكن الوصول إلى بروتوكول سطح المكتب البعيد (TCP 3389) من الإنترنت على جهاز واحد أو أكثر.

الأثر

يُعد RDP المكشوف من أكثر طرق الوصول الأولي شيوعًا لدى مجموعات الفدية، عبر تخمين كلمات المرور وبيانات الاعتماد المسروقة وثغرات RDP.

Remediation
Limit RDP to the admin VLAN.

المعالجة

أزل RDP من الإنترنت ووفّر الوصول عبر VPN أو بوابة وصول عن بُعد مع المصادقة متعددة العوامل. اشترط Network Level Authentication وحافظ على تطبيق التحديث الأمني للأجهزة.

19. Server version disclosure

كشف إصدار البرمجيات في لافتات الخدمات

Severity	CVSS v3	Status	Affected asset
Info	-	Open	10.20.0.5 (unknown 22/tcp)

Description
The SSH banner discloses the exact version.

الوصف

تكشف الخدمات اسم المنتج وإصداره الدقيق في اللافتات والترويسات، مثل Server: Apache/2.4.49 أو سلسلة إصدار SSH.

الأثر

لا يمكن استغلال ذلك بمفرده، لكنه كشف المعلومات يتيح للمهاجمين مطابقة الخدمة بسرعة مع الثغرات المعروفة.

Remediation
Hide version banners where possible.

المعالجة

اضبط الخدمات لإخفاء تفاصيل الإصدار (مثل ServerTokens Prod في Apache أو server_tokens off في nginx)، والأهم من ذلك حافظ على تحديث البرمجيات.