تقرير تدقيق الأمان: تحليل البنية التحتية لـ example.com

أخصائي أمن المعلومات

2025-12-17

الملخص التنفيذي

تم إجراء تدقيق شامل لأمان الموقع الإلكتروني example.com باستخدام أدوات المسح الحديثة (Nmap، SSLScan). تم تحديد ثغرات أمنية حرجة في التكوين تتطلب معالجة فورية. التقييم العام للأمان: **6/10** - يتطلب تدخلاً عاجلاً.

> ⚠ **تحذير حرج**: تم اكتشاف منافذ غير معيارية مفتوحة (8080، 8443) ونقاط هجوم محتملة على لوحة إدارة WordPress.

هدف الاختبار

المعامل	القيمة
النطاق	example.com
عناوين IP	192.0.2.1
CDN/WAF	Cloudflare
نظام إدارة المحتوى	WordPress 6.9
تاريخ التدقيق	17 ديسمبر 2025

منهجية الاختبار

تم إجراء التدقيق وفقاً لمنهجية NIST Cybersecurity Framework وشمل:

- **مسح المنافذ** (Nmap 7.94SVN)
- **تحليل SSL/TLS** (SSLScan 2.1.2)
- **مراجعة تكوين خادم الويب**
- **تحليل رؤوس الأمان**
- **تقييم أمان WordPress**

هندسة النظام

المستخدم → Cloudflare CDN → الخادم الأصلي
↓
المنافذ: 80، 443، 8080، 8443
↓
WordPress 6.9

المكونات الرئيسية: - Cloudflare كوكيل عكسي على جميع المنافذ - شهادة SSL من Google Trust Services (WE1) - شهادة Wildcard (*.example.com) - دعم HTTP/2 و HTTP/3

نتائج المسح

المنافذ والخدمات المفتوحة

المنفذ	البروتوكول	الحالة	الخدمة	ملاحظات
80	HTTP	مفتوح	Cloudflare proxy	إعادة توجيه إلى HTTPS
443	HTTPS	مفتوح	Cloudflare proxy	الموقع الرئيسي
8080	HTTP	⚠ مفتوح	Cloudflare proxy	منفذ غير معياري
8443	HTTPS	× خطأ 523	Cloudflare proxy	الأصل غير متاح

تكوين SSL/TLS

الجوانب الإيجابية: - دعم TLS 1.3 (بروتوكول حديث) - TLS 1.2 مع خوارزميات تشفير آمنة - Perfect Forward Secrecy (ECDHE) - تعطيل البروتوكولات القديمة (SSL 2.0/3.0، TLS 1.0/1.1) - منحنيات إهليلجية حديثة (x25519، secp256r1)

المناطق المشكلة: ⚠ دعم خوارزميات CBC (عرضة لـ BEAST، Lucky13) - ⚠ فترة صلاحية قصيرة للشهادة (90 يوماً) ⚠ تكوين متطابق على جميع المنافذ

تحليل WordPress

المكون	الحالة	المخاطر
الإصدار	WordPress 6.9	عالي
لوحة الإدارة	/wp-admin/ متاحة	حرج
Robots.txt	يكشف الهيكل	◍ متوسط
المولد	الإصدار مكشوف	◍ متوسط

الثغرات المحددة

المستوى الحرج (CVSS 7.0-10.0)

1. خطأ تكوين المنفذ 8443

- **الوصف**: المنفذ 8443 مكون في Cloudflare لكن الخادم الأصلي غير متاح (HTTP 523)
- **المخاطر**: تجاوز حماية Cloudflare، تسريب المعلومات
- **نقاط CVSS**: 7.5
- **التوصية**: إغلاق المنفذ فوراً أو إصلاح التكوين

2. منفذ غير معياري مفتوح 8080

- **الوصف**: نقطة دخول بديلة يمكن استخدامها لتجاوز WAF
- **المخاطر**: تجاوز سياسات الأمان، هجمات القوة الغاشمة
- **نقاط CVSS**: 7.2
- **التوصية**: إغلاق المنفذ أو تقييد الوصول

🔵 المستوى العالي (CVSS 4.0-6.9)

3. لوحة إدارة WordPress

- **الوصف**: الإصدار مكشوف، /wp-admin/ مذكور في robots.txt
- **المخاطر**: هجمات القوة الغاشمة، استغلال الثغرات
- **نقاط CVSS**: 6.8
- **التوصية**: إخفاء الإصدار، حماية لوحة الإدارة

4. غياب رؤوس الأمان الحرجة

- **الوصف**: غياب HSTS، X-Frame-Options، CSP
- **المخاطر**: Clickjacking، هجمات التراجع، XSS
- **نقاط CVSS**: 5.5
- **التوصية**: إضافة الرؤوس المفقودة

🟡 المستوى المتوسط (CVSS 2.0-3.9)

5. خوارزميات CBC في TLS 1.2

- **الوصف**: دعم خوارزميات CBC القديمة
- **المخاطر**: هجمات BEAST، Lucky13
- **نقاط CVSS**: 3.7
- **التوصية**: تعطيل خوارزميات CBC

توصيات المعالجة

الإجراءات الفورية (24 ساعة)

1. **إغلاق المنفذ 8443**

```
# تعطيل في لوحة تحكم Cloudflare
# أو إغلاق على الخادم الأصلي
server {
    listen 8443;
    return 444;  # إغلاق الاتصال
}
```

2. **تقييد الوصول للمنفذ 8080**

```
server {
    listen 8080;
    # الشبكة الداخلية فقط
    allow 192.168.0.0/16;
    deny all;
}
```

3. **حماية لوحة إدارة WordPress**

```
# .htaccess في /wp-admin/
AuthType Basic
AuthName "Admin Area"
AuthUserFile /path/to/.htpasswd
Require valid-user
```

التحسينات قصيرة المدى (7 أيام)

4. **إضافة رؤوس الأمان**

```
add_header Strict-Transport-Security "max-age=31536000; includeSubDomains; preload";
add_header X-Frame-Options "DENY";
add_header Content-Security-Policy "default-src 'self'";
add_header X-Content-Type-Options "nosniff";
```

5. **تحسين SSL/TLS**

```
# تعطيل خوارزميات CBC
ssl_ciphers "ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384";
ssl_protocols TLSv1.2 TLSv1.3;
```

6. **تكوين Cloudflare WAF**
   - حجب الوصول إلى /wp-admin/ للعناوين غير المصرح بها
   - إعداد تحديد المعدل لـ /wp-login.php
   - تفعيل Bot Fight Mode

الإجراءات طويلة المدى (30 يوماً)

7. **المراقبة والأتمتة**
   - تجديد شهادات SSL تلقائياً
   - مراقبة محاولات الوصول للموارد المحمية
   - مسح الثغرات بانتظام
8. **تقوية WordPress**
   - تثبيت إضافات الأمان (Wordfence، iThemes Security)
   - المصادقة الثنائية
   - إخفاء إصدار WordPress
   - التحديثات المنتظمة

مصفوفة المخاطر

الأولوية	المخاطر العامة	التأثير	الاحتمالية	الثغرة
P0	حرج	عالي	عالية	خطأ المنفذ 8443
P1	🟠 عالي	عالي	متوسطة	المنفذ 8080 مفتوح
P1	🟠 عالي	متوسط	عالية	إدارة WordPress
P2	🟡 متوسط	متوسط	متوسطة	رؤوس الأمان

الأولوية	المخاطر العامة	التأثير	الاحتمالية	الثغرة
P3	منخفض 🟢	منخفض	منخفضة	خوارزميات CBC

خطة المعالجة

المرحلة 1: الإصلاحات الحرجة (1-2 يوم)

- ☐ إغلاق المنفذ 8443 في Cloudflare
- ☐ تقييد الوصول للمنفذ 8080
- ☐ حماية لوحة إدارة WordPress
- ☐ إضافة رؤوس الأمان الأساسية

المرحلة 2: تحسينات الأمان (أسبوع واحد)

- ☐ تحسين تكوين SSL/TLS
- ☐ تكوين قواعد Cloudflare WAF
- ☐ تثبيت إضافات أمان WordPress
- ☐ إعداد المراقبة

المرحلة 3: الإجراءات طويلة المدى (شهر واحد)

- ☐ أتمتة التحديثات
- ☐ تدقيقات أمنية منتظمة
- ☐ تدريب الموظفين
- ☐ توثيق الإجراءات

الامتثال للمعايير

المعيار	الحالة الحالية	الإجراءات المطلوبة
NIST CSF	جزئي	تحسين وظائف الحماية والكشف
ISO 27001	غير متوافق	تنفيذ عمليات ISMS
PCI DSS	يتطلب تقييماً	تعزيز حماية البيانات
GDPR	مستوى أساسي	إضافة رؤوس الخصوصية

الخلاصة

كشف التدقيق عن مشاكل أمنية خطيرة تتطلب اهتماماً فورياً. المخاطر الرئيسية مرتبطة بالتكوين غير الصحيح للمنافذ وعدم كفاية حماية لوحة إدارة WordPress.

النتائج الرئيسية: - **الثغرات الحرجة**: 2 (تتطلب معالجة فورية) - 🟠 **المخاطر العالية**: 2 (تخطيط المعالجة) - 🟡 **المخاطر المتوسطة**: 1 معالجة خلال أسبوع)

الخطوات التالية الموصى بها: 1. إغلاق المنافذ المشكلة فوراً 2. تعزيز حماية WordPress 3. إضافة رؤوس الأمان المفقودة 4. تنفيذ مراقبة أمنية منتظمة

مع التنفيذ الصحيح للتوصيات، يمكن تحسين التقييم العام للأمان إلى **8-9/10** خلال 30 يوماً.

.

تم إعداد التقرير وفقاً لأفضل الممارسات في الصناعة ومعايير Microsoft Security Development Lifecycle (SDL).