تقرير الامتثال لمعايير الأمان: تحليل موقع example.com

أخصائي أمن المعلومات

2025-12-31

الملخص التنفيذي

يقدم هذا التقرير تحليلاً شاملاً لامتثال موقع https://example.com للمعايير الدولية للأمان بما في ذلك OWASP Top 10 2021، وإطار عمل الأمن السيبراني NIST 2.0، وتوصيات Microsoft Security Baseline. يستند التحليل إلى نتائج المسح الأمني الآلي الذي تم تنفيذه في 30 ديسمبر 2025 باستخدام OWASP ZAP (Zed Attack Proxy) الإصدار 2.17.0 من Checkmarx.

يتطلب تدخلاً فورياً! - (PII) **تحذير حرج**: تم اكتشاف تسريب للمعلومات الشخصية

النتائج الرئيسية:

- تم تحديد **29 تنبيهاً أمنياً** عبر مستويات خطورة مختلفة
- (PII) تم اكتشاف **ثغرة أمنية حرجة** في تسريب المعلومات الشخصية
- **غياب آليات الحماية الأساسية** لتطبيق الويب
- الموقع **غير متوافق** مع المتطلبات الأساسية للمعايير الدولية للأمان

جدول المحتويات

منهجية التحليل

معاملات المسح

- **الأداة**: OWASP ZAP 2.17.0 من Checkmarx [1]
- **تاريخ ووقت المسح**: 30 ديسمبر 2025، 19:00:53
- **المورد المستهدف**: https://example.com
- **إجمالي نقاط النهاية**: 290
- **السياقات**: جميع السياقات مشمولة افتراضياً
- **مستويات المخاطر**: عالي، متوسط، منخفض، معلوماتي
- **مستويات الثقة**: مؤكد من المستخدم، عالي، متوسط، منخفض

إحصائيات نتائج المسح

مستوى المخاطر	العدد	النسبة المئوية	مستوى الثقة
عالي	1	3.4%	عالي
متوسط 🟠	3	10.3%	عالي/متوسط
منخفض	4	13.8%	عالي/متوسط/منخفض
معلوماتي ℹ	21	72.4%	متوسط/منخفض
المجموع	**29**	**100%**	-

المكدس التقني

التقنيات المكتشفة على الموقع:

- **نظام إدارة المحتوى**: WordPress مع Block Editor
- **خادم الويب**: LiteSpeed مع LiteSpeed Cache
- **شبكة توصيل المحتوى**: Cloudflare مع Browser Insights
- **لغة البرمجة**: PHP
- **المكونات الإضافية**:
  - Blocksy (قالب WordPress)
  - Stackable (إضافة WordPress)
  - Gravatar (خدمة الصور الرمزية)
  - Google Font API
- **البروتوكولات**: HTTP/3، HSTS، RSS، Priority Hints

التحليل التفصيلي للثغرات الأمنية

الثغرات الحرجة (مخاطر عالية)

1. تسريب المعلومات الشخصية (PII)

مستوى الثقة: عالي | CWE-359 | WASC-13

انتهاك حرج: تم اكتشاف تسريب للبيانات الشخصية للمستخدمين

الوصف التقني:

- المعلومات الشخصية للمستخدمين متاحة دون تفويض
- انتهاك لمبادئ سرية البيانات
- انتهاك مباشر لمتطلبات GDPR

التأثير على الأعمال:

- **المخاطر التنظيمية**: غرامات GDPR تصل إلى 4% من الإيرادات السنوية للشركة
- **الأضرار السمعية**: ضرر جسيم لثقة العملاء
- **العواقب القانونية**: دعاوى قضائية محتملة من المتضررين
- **المخاطر التشغيلية**: ضرورة إخطار الجهات التنظيمية خلال 72 ساعة

الثغرات متوسطة المخاطر

2. غياب Subresource Integrity (SRI)

العدد: 5 حالات | مستوى الثقة: عالي | CWE-345 | WASC-15

الوصف: تحميل الموارد الخارجية دون التحقق من سلامتها، مما يخلق مخاطر هجمات سلسلة التوريد.

الموارد المتأثرة:

- Google Font API
- موارد Cloudflare CDN
- مكتبات JavaScript الخارجية

3. غياب Content Security Policy (CSP)

العدد: 5 حالات | مستوى الثقة: عالي | CWE-693 | WASC-15

الوصف: غياب سياسة أمان المحتوى يجعل الموقع عرضة لهجمات XSS وحقن أخرى.

4. غياب الحماية من Clickjacking

العدد: 5 حالات | مستوى الثقة: متوسط | CWE-1021 | WASC-15

الوصف: غياب رؤوس X-Frame-Options أو CSP frame-ancestors يسمح بتضمين الموقع في iframe لتنفيذ هجمات clickjacking.

الثغرات منخفضة المخاطر

5. مشاكل أمان النقل

- **رأس Strict-Transport-Security غير مُعيَّن** (حالة واحدة، CWE-319)
- **أمان النقل الصارم معطل** (5 حالات، CWE-319)

6. غياب X-Content-Type-Options

مستوى الثقة: متوسط | CWE-693 | WASC-15

الوصف: غياب الحماية من هجمات MIME-sniffing.

7. تسريب Unix timestamp

العدد: 4 حالات | مستوى الثقة: منخفض | CWE-497 | WASC-13

الوصف: تم اكتشاف تسريب للطوابع الزمنية، مما قد يكشف معلومات عن توقيت إنشاء المحتوى.

التنبيهات المعلوماتية

تم تحديد 21 تنبيهاً معلوماتياً، بما في ذلك:

- اكتشاف التقنيات (WordPress، PHP، Cloudflare، إلخ)
- مشاكل التخزين المؤقت (5 حالات)
- عدم تطابق ترميز الأحرف
- تعليقات مشبوهة في الكود (58 حالة)

تحليل الامتثال لـ OWASP Top 10 2021

A01:2021 – كسر التحكم في الوصول

الحالة: ✗ **عدم امتثال حرج**

المشاكل المحددة:

- انتهاك مباشر لمبادئ التحكم في الوصول - **تسريب PII**
- غياب آليات حماية المعلومات الحساسة
- انتهاك مبدأ "الرفض افتراضياً"

توصيات OWASP:

- تنفيذ ضوابط وصول صارمة
- تسجيل محاولات الوصول الفاشلة
- تحديد معدل طلبات API
- مراجعة دورية لحقوق الوصول

A03:2021 – الحقن

الحالة: **متوافق** (بناءً على نتائج المسح)

النتيجة: لم يتم اكتشاف ثغرات من نوع SQL أو NoSQL. أو حقن أوامر نظام التشغيل.

A05:2021 – سوء تكوين الأمان

الحالة: ✗ **عدم امتثال حرج**

المشاكل المحددة:

- غياب CSP (5 حالات)
- غياب الحماية من clickjacking (5 حالات)
- تكوين خاطئ لرؤوس الأمان
- غياب X-Content-Type-Options
- مشاكل في تكوين HSTS

A06:2021 – المكونات الضعيفة والقديمة

الحالة: ⚠ **يتطلب التحقق**

المكونات المحددة:

- WordPress (الإصدار غير محدد)
- PHP (الإصدار غير محدد)
- خادم ويب LiteSpeed
- إضافات متعددة: Blocksy، Stackable، LiteSpeed Cache

التوصيات: مطلوب مراجعة تفصيلية لإصدارات جميع المكونات.

A08:2021 – فشل سلامة البرمجيات والبيانات

الحالة: ✗ **غير متوافق**

المشاكل:

- غياب Subresource Integrity للموارد الخارجية (5 حالات)
- مخاطر الاختراق عبر CDN والمكتبات الخارجية
- غياب التحقق من سلامة التحديثات

A09:2021 – فشل التسجيل والمراقبة الأمنية

الحالة: × **غير متوافق**

المشاكل:

- لا توجد معلومات عن أنظمة التسجيل
- حالة مراقبة الأمان غير معروفة
- غياب أنظمة اكتشاف الشذوذ

الامتثال لإطار عمل NIST 2.0 للأمن السيبراني

GOVERN (الحوكمة) - 20% امتثال

GV.OC-01: الأمن السيبراني التنظيمي

- × لا توجد أدلة على سياسة أمان رسمية

GV.RM-01: إدارة المخاطر

- × لم يتم تنفيذ إجراءات إدارة مخاطر الأمن السيبراني

GV.SC-01: إدارة سلسلة التوريد

- × غياب ضوابط سلامة الموارد الخارجية

IDENTIFY (التحديد) - 60% امتثال

ID.AM-02: جرد أصول البرمجيات

- مكتمل جزئياً - تم تحديد المكونات الرئيسية

ID.RA-01: تقييم الثغرات

- مكتمل - تم إجراء مسح أمني

ID.RA-02: تحليل التهديدات

- × غياب تحليل منهجي للتهديدات

PROTECT (الحماية) - 15% امتثال

PR.AC-01: إدارة الهوية والمصادقة

- × بيانات غير كافية للتقييم

PR.DS-01: حماية البيانات في حالة السكون

- × تم اكتشاف تسريب PII

PR.DS-02: حماية البيانات أثناء النقل

- ⚠ أمنفذ جزئي (HTTPS، لكن مشاكل في HSTS)

PR.PT-01: المراجعة/التسجيل

- × معلومات غير كافية عن أنظمة المراجعة

DETECT (الاكتشاف) - 0% امتثال

DE.CM-01: مراقبة الشبكة

- × لا توجد أدلة على المراقبة

DE.AE-01: اكتشاف الشذوذ

- × غياب أنظمة اكتشاف الشذوذ

RESPOND (الاستجابة) - 0% امتثال

RS.RP-01: تخطيط الاستجابة

- × لا توجد أدلة على خطة استجابة

RS.CO-01: الاتصالات

- × غياب إجراءات إخطار الحوادث

RECOVER (الاستعادة) - 0% امتثال

RC.RP-01: تخطيط الاستعادة

- × لا توجد أدلة على خطة استعادة

RC.CO-01: اتصالات الاستعادة

- × غياب إجراءات الاتصال أثناء الاستعادة

الامتثال لمعايير Microsoft Security Baseline

أمان النقل

× أوجه قصور حرجة:

- رأس Strict-Transport-Security (حالة واحدة) غير مُعيَّن
- أمان النقل الصارم معطل (5 حالات)
- الإجباري لجميع الموارد HTTPS غياب فرض

حماية المحتوى

× أوجه قصور حرجة:

- رأس X-Content-Type-Options مفقود
- Content Security Policy (5 حالات) مفقود
- لا توجد حماية من هجمات MIME-sniffing
- غياب الحماية من clickjacking

سلامة الموارد

مخاطر متوسطة: ×

- غياب خاصية Subresource Integrity (5 حالات) للموارد الخارجية
- مخاطر اختراق المكتبات الخارجية من Google Font API وCloudflare وCDN أخرى
- غياب التحقق من سلامة تحميل الموارد

إدارة البيانات

مخاطر حرجة: ×

- تم اكتشاف تسريب للبيانات الشخصية
- غياب تصنيف البيانات
- لا توجد ضوابط وصول للمعلومات الحساسة

خطة معالجة الثغرات الأمنية

المرحلة الأولى: الإصلاحات الحرجة (0-7 أيام)

الأولوية الأولى: معالجة تسريب PII (0-3 أيام)

- ☐ **اليوم الأول**: التحديد الفوري وحجب مصادر تسريب PII
- ☐ **اليوم الثاني**: تنفيذ إخفاء/تشفير البيانات الحساسة
- ☐ **اليوم الثالث**: نشر ضوابط وصول صارمة للبيانات الشخصية
- ☐ **اليوم الثالث**: إخطار الجهات التنظيمية وفقاً لمتطلبات GDPR (72 ساعة)

الأولوية الثانية: رؤوس الأمان الأساسية (4-7 أيام)

- ☐ تنفيذ **اليوم 4-5**: Content Security Policy

```
Content-Security-Policy: default-src 'self';
script-src 'self' 'unsafe-inline' https://cdnjs.cloudflare.com https://fonts.googleapis.com;
style-src 'self' 'unsafe-inline' https://fonts.googleapis.com;
img-src 'self' data: https: https://secure.gravatar.com;
frame-ancestors 'none';
base-uri 'self';
```

- ☐ تكوين الحماية من clickjacking: **اليوم السادس**

```
X-Frame-Options: DENY
```

- ☐ تكوين: **اليوم السادس** HSTS

```
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
```

- ☐ **اليوم السابع**: اختبار والتحقق من التغييرات

المرحلة الثانية: الإصلاحات متوسطة الأولوية (8-30 يوماً)

الأسبوع الثاني: Subresource Integrity

- ☐ تنفيذ SRI لجميع الموارد الخارجية

```
<link
href="https://fonts.googleapis.com/css2?family=Roboto:wght@300;400;700&display=swap"
```

```
    rel="stylesheet"
    integrity="sha384-hash"
    crossorigin="anonymous">
<script src="https://cdnjs.cloudflare.com/ajax/libs/jquery/3.6.0/jquery.min.js"
     integrity="sha384-
vtXRMe3mGCbOeY7l30aIg8H9p3GdeSe4IFlP6G8JMa7o7lXvnz3GFKzPxzJdPfGK"
     crossorigin="anonymous"></script>
```

الأسبوع الثالث: رؤوس أمان إضافية

- ☐ تنفيذ X-Content-Type-Options

```
X-Content-Type-Options: nosniff
```

- ☐ تكوين رؤوس إضافية

```
X-XSS-Protection: 1; mode=block
Referrer-Policy: strict-origin-when-cross-origin
Permissions-Policy: geolocation=(), microphone=(), camera=()
```

الأسبوع الرابع: مراجعة المكونات

- ☐ التحقق من إصدارات WordPress وPHP وجميع الإضافات
- ☐ تحديث المكونات القديمة
- ☐ إزالة الإضافات والقوالب غير المستخدمة
- ☐ تكوين التحديثات الأمنية التلقائية

المرحلة الثالثة: التحسينات طويلة المدى (31-90 يوماً)

الشهر الثاني: المراقبة والتسجيل

- ☐ تنفيذ نظام مراقبة أمنية (SIEM)
- ☐ تكوين التسجيل المركزي
- ☐ إنشاء لوحات معلومات أمنية
- ☐ إعداد تنبيهات للأنشطة المشبوهة

الشهر الثالث: الإجراءات والسياسات

- ☐ تطوير سياسة أمن المعلومات
- ☐ إنشاء إجراءات الاستجابة للحوادث
- ☐ تطوير خطة الاستعادة بعد الحوادث
- ☐ تدريب الموظفين على أساسيات الأمن السيبراني
- ☐ اختبارات اختراق دورية

الخلاصة

كشف تحليل أمان موقع https://example.com مع **غير متوافق** في حماية المعلومات. الموقع **أوجه قصور حرجة** عن المتطلبات الأساسية للمعايير الدولية للأمان OWASP Top 10 2021 وNIST CSF 2.0 ومعايير Microsoft Security Baseline.

تقييم المخاطر الحرج:

- **مستوى المخاطر الحالي: حرج**

- **التهديد الأساسي**: تسريب البيانات الشخصية للمستخدمين
- **المخاطر التنظيمية**: غرامات GDPR (تصل إلى 4% من الإيرادات السنوية) عالية
- **المخاطر السمعية**: فقدان جسيم لثقة العملاء
- **المخاطر التشغيلية**: إمكانية تعليق الأعمال

الامتثال للمعايير:

المعيار	مستوى الامتثال	المشاكل الحرجة
OWASP Top 10 2021	20%	A01, A05, A08, A09
NIST CSF 2.0	19%	جميع الوظائف عدا التحديد الجزئي
Microsoft Security Baseline	15%	النقل، المحتوى، البيانات

التوصيات الرئيسية:

1. **المعالجة الفورية** لتسريب البيانات الشخصية (0-3 أيام)
2. **تنفيذ آليات الحماية الأساسية** لتطبيق الويب (4-7 أيام)
3. **التحديث المنتظم** لجميع مكونات النظام
4. **إنشاء إجراءات** للمراقبة والاستجابة للحوادث
5. **تدريب الموظفين** على أساسيات أمن المعلومات

توقعات التحسن:

- **بعد المرحلة الأولى**: تقليل المخاطر إلى 🟡 **متوسط** (إزالة الثغرات الحرجة)
- **بعد المرحلة الثانية**: تقليل المخاطر إلى **منخفض** (الحماية الأساسية)
- **بعد المرحلة الثالثة**: تحقيق مستوى أمان 🟢 **مقبول** (امتثال للمعايير)

الخطوات التالية: يُوصى **بالبدء فوراً** في تنفيذ المرحلة الأولى من خطة معالجة الثغرات، مع إيلاء اهتمام خاص لإزالة تسريب البيانات الشخصية وإخطار الجهات التنظيمية وفقاً لمتطلبات GDPR.

المراجع

[1] مؤسسة OWASP. (2024). *OWASP Zed Attack Proxy (ZAP)*. https://zaproxy.org

[2] مؤسسة OWASP. (2021). *OWASP Top 10:2021*. https://owasp.org/Top10/2021/

[3] NIST. (2024). *إطار عمل NIST للأمن السيبراني (CSF) 2.0*. https://www.nist.gov/publications/nist-cybersecurity-framework-csf-20