yof

تقرير الأمان: كامل

فحص مستقل لتطبيق ويب

shop.example

https://shop.example/

نموذج: موقع مُختلَق

نموذج: موقع مُختلَق. هذا تقرير نموذجي لـ shop.example، وهو موقع غير موجود. كل النتائج فيه مُختلَقة.

نوع التقرير	تقرير الأمان: كامل
التطبيق	shop.example
تاريخ الإصدار	2026-11-07
رقم التقرير	5a3b1e00-0000-4000-8000-000000000000
الإصدار	1

أعده yof على yof.io

تحقق من هذا التقرير
yof.io/verify/5a3b1e00-0000-4000-8000-000000000000
بصمة SHA-256: fb9ff4c2ff530d7b8b05f4622d7e389ab732e25f51676dc2cd21e1f34878fee5

سري: أُعد لمالك shop.example

بيانات الوثيقة

سجل الإصدارات

v1 الإصدار 1، صدر في 2026-11-07

النطاق

shop.example: the outside of the app, the code of example-shop/storefront, attack results from the owner's CI.

الجهة الطالبة

مالك shop.example، عبر تطبيق yof (الطلب 00000000).

التوزيع

سري. أُعد لمالك shop.example، وله أن يشاركه مع من يحتاجه مثل المدققين أو شركات التأمين أو العملاء. يستطيع كل من يحمل نسخة أن يتحقق منها برمز QR.

التوقيع

الخوارزمية	none (sample, not signed) (yof-report/v1 sample)
معرّف المفتاح	-
بصمة SHA-256	fb9ff4c2ff530d7b8b05f4622d7e389ab732e25f51676dc2cd21e1f34878fee5
قيمة التوقيع	Sample report: not signed and not in yof's register.

طريقة التحقق

1. امسح رمز QR على الغلاف أو افتح العنوان المطبوع تحته. تتحقق الصفحة من توقيع yof في السجل.
2. للتحقق من ملف وصلك، اختره في تلك الصفحة: يحسب متصفحك بصمة SHA-256 ويقارنها، ولا يُرفع الملف.
3. مع توقيع Ed25519 يستطيع أي شخص أيضًا التحقق دون اتصال بمفتاح yof العام، على رقم التقرير والإصدار وتاريخ الإصدار وبصمة المحتوى.

yof.io/verify/5a3b1e00-0000-4000-8000-000000000000

ما هو هذا التقرير وما ليس هو

هذا التقرير فحص لـ shop.example في لحظة واحدة، بحسب الحال في 2026-11-07. يشمل المستودع والحزم التابعة والعناوين الحية المذكورة في قسم النطاق، ولا شيء غير ذلك.

أُعدّ بقواعد واختبارات آلية. بحسب النطاق، قرأ yof الشيفرة وفحص الحزم واختبر الموقع الحي، وأجرى اختبارات هجوم بموافقة المالك. يذكر قسم النطاق بالضبط ما تم وما لم يتم.

هذا التقرير دليل يدعم عملك في الأمان والامتثال. ليس شهادة ولا تقييم مطابقة ولا استشارة قانونية، ولا يقيّم الحوكمة أو السياسات أو الإجراءات أو أي التزامات أخرى غير تقنية.

النتيجة الخالية من الملاحظات لا تعني أن التطبيق خالٍ من الثغرات. لا تستطيع الفحوص الآلية أن تجد كل خلل. قد تبقى ثغرات لم يعرفها أحد بعد (ثغرات اليوم الصفري)، وأخطاء في منطق العمل، وكل ما هو خارج النطاق، وقد يتغير التطبيق بعد التاريخ المذكور.

في الحدود التي يسمح بها القانون، تقتصر مسؤولية yof عن هذا التقرير على الثمن المدفوع مقابله. قد لا يسمح قانون حماية المستهلك في بلدك ببعض هذه الحدود، وحيث لا يسمح بها فلا تنطبق عليك.

هذه ترجمة لتقرير yof ذي التوقيع الرقمي 5a3b1e00-0000-4000-8000-000000000000. النسخة الأصلية الموقعة بالإنجليزية، وبصمة SHA-256 الخاصة بها أدناه. التفاصيل التقنية (الإصلاحات والخطوات والمراجع) بالإنجليزية.

المحتويات

بيانات الوثيقة 2
ما هو هذا التقرير وما ليس هو 2
الملخص التنفيذي 4
النطاق 5
الملاحظات (5) 6
الملحق A: المخاطر المقبولة وأسبابها 9
الملحق B: المنهجية والأدوات 10
الملحق C: مسرد المصطلحات 11
الملحق D: ملخص قائمة مكونات البرمجيات (SBOM) 12
الملحق E: طريقة التحقق 13

الملخص التنفيذي

النتيجة العامة

مرتفع

مرتفع: مشكلة واحدة على الأقل يجب إصلاحها الآن.

النتائج المفتوحة حسب الأولوية

أصلحه الآن	أصلحه هذا الأسبوع	يُستحسن	للعلم	المخاطر المقبولة
4	0	0	0	2

أهم المخاطر بكلمات بسيطة

F-001 حزمة يثبّتها تطبيقك فيها ثغرة خطيرة معروفة

الثغرة منشورة ولها إصلاح متاح. يبحث المهاجمون عن التطبيقات التي ما زالت تستخدم الإصدار القديم.

أصلحه الآن | package-lock.json:812 (example-shop/storefront at 0f1e2d3c4b5a)

F-002 مفتاح Stripe السري موجود في كود صفحتك

يستطيع أي شخص استخدامه لتحصيل المدفوعات وإصدار المبالغ المستردة وقراءة بيانات الدفع الخاصة بعملائك.

أصلحه الآن | https://shop.example/assets/app.js

F-003 أي شخص يستطيع قراءة جدول في قاعدة بياناتك

يستطيع غريب تنزيل صفوف هذا الجدول، مثل أسماء عملائك أو بريدهم أو طلباتهم، دون تسجيل الدخول.

أصلحه الآن | https://shop.example/

ضمن النطاق

من الخارج, داخل الشيفرة, اختبارات الهجوم

التغطية: 45% من الأجزاء التي يمكن لـ yof فحصها.

خارج النطاق

- لم تُختبر الصفحات التي تتطلب تسجيل الدخول: لا يسجّل yof الدخول إلا من خلال اختبارات الهجوم التي يشغّلها المالك بنفسه.
- قُرئت الصفحات الأولى فقط؛ ولم يُقرأ باقي الموقع.
- مساعد الذكاء الاصطناعي: لم يُختبر في هذا التقرير.

النطاق

التغطية: 45% من الأجزاء التي يمكن لـ yof فحصها.
- من الخارج: فُحص جزئيًا
- داخل الشيفرة: فُحص بالكامل
- صفحات خلف تسجيل الدخول: لم يُفحص
- اختبارات الهجوم: فُحص بالكامل
- مساعد الذكاء الاصطناعي: لم يُفحص
- كل الصفحات: لم يُفحص

لم يُفحص

- لم تُختبر الصفحات التي تتطلب تسجيل الدخول: لا يسجّل yof الدخول إلا من خلال اختبارات الهجوم التي يشغّلها المالك بنفسه.
- قُرئت الصفحات الأولى فقط؛ ولم يُقرأ باقي الموقع.
- مساعد الذكاء الاصطناعي: لم يُختبر في هذا التقرير.

ما الذي فُحص وما الذي لم يُفحص

هذا هو نطاق هذا التقرير. الجزء الذي لم يُفحص لا يُفترض أبدًا أنه سليم.

تم فحصه
- من الخارج: فُحص جزئيًا
- داخل الشيفرة: فُحص بالكامل
- اختبارات الهجوم: فُحص بالكامل

لم يُفحص، والسبب
- لم تُختبر الصفحات التي تتطلب تسجيل الدخول: لا يسجّل yof الدخول إلا من خلال اختبارات الهجوم التي يشغّلها المالك بنفسه.
- قُرئت الصفحات الأولى فقط؛ ولم يُقرأ باقي الموقع.
- مساعد الذكاء الاصطناعي: لم يُختبر في هذا التقرير.

لا تغطيه الفحوص الآلية أبدًا
- عيوب في منطق العمل، مثل سعر أو خطوة يمكن لشخص تخطيها.
- نقاط ضعف لا يعرفها أحد بعد (ثغرات اليوم صفر).
- الأشخاص والإجراءات: التصيّد، وكلمات المرور المتبادلة يدويًا، ومن لديه صلاحية الوصول.
- كل ما هو خارج النطاق المذكور في هذا التقرير، وأي تغيير بعد تاريخه.

مدى ثقة yof في كل نتيجة

لكل نتيجة حكم واحد. لا يُحسب إلا النتائج المؤكدة والنتائج التي تحتاج إلى تحقق. ملاحظات التقوية والنتائج المرفوضة مذكورة على حدة ولا تُحسب أبدًا.
- مؤكدة: رأى yof الأثر يحدث، أو لديه الدليل الدقيق (مثل المفتاح الذي كان يُقدَّم للجميع، أو الإصدار المثبت الذي تذكره نشرة أمنية).
- تحتاج إلى تحقق: مرجّحة لكنها غير مُثبتة: رأى yof النمط ولم يستطع إثبات الأثر. يحتاج الأمر إلى شخص أو اختبار أعمق لتأكيده.
- مرفوضة: دحضها فحص ثانٍ منفصل. محفوظة للسجل، ولا تُحسب.

معنى كل درجة خطورة
- حرجة: فقط لنتيجة مؤكدة رأى yof حدوثها: بيانات أو تحكم يخص شخصًا آخر (سجلات شخص آخر، جدول كامل، مفتاح بصلاحيات كاملة يُقدَّم للجميع)، أو حزمة معروف أنها مُستغلة أو خبيثة.
- عالية: ضرر جسيم مرجّح إذا استغلها أحد: كشف مؤكد لكنه محدود، أو مشكلة مرجّحة لم يستطع yof إثباتها. النتيجة غير المؤكدة لا تتجاوز درجة عالية.
- متوسطة: تجعل الهجوم أسهل أو ضرره أكبر، بشروط مثل تسجيل الدخول أو نقرة من المستخدم أو إعداد محدد.
- منخفضة: ضرر صغير بحد ذاته، أو لا يمكن الوصول إليها إلا في أدوات التطوير والاختبار.
- معلومة: من المفيد معرفتها، ولا ضرر منها بحد ذاتها.

الملاحظات (5)

أصلحه الآن | CVSS 9.3 | مفتوح

F-001 حزمة يثبّتها تطبيقك فيها ثغرة خطيرة معروفة

الحكم: مؤكدة. الخطورة: عالية. السبب: يحتوي المستودع على الدليل الدقيق. لم يرها yof في التطبيق المباشر، لذا لا تتجاوز درجة عالية.

الثغرة منشورة ولها إصلاح متاح. يبحث المهاجمون عن التطبيقات التي ما زالت تستخدم الإصدار القديم.

CVSS 4.0: CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N

CWE: CWE-1395

المكان: package-lock.json:812 (example-shop/storefront at 0f1e2d3c4b5a)

خطوات رؤيته:

1. افتح package-lock.json:812 (example-shop/storefront at 0f1e2d3c4b5a).
2. المتوقع بدلًا من ذلك: الإصدار المثبّت من minimist هو 1.2.6 أو أحدث.

الأثر على العمل: قد تُستغل ثغرة منشورة في أحد المكوّنات ضد التطبيق.

الحزمة: minimist (npm)

الإصدار المثبّت: 1.2.5

التنبيهات: GHSA-xvch-5gv4-984h https://github.com/advisories/GHSA-xvch-5gv4-984h, CVE-2021-44906 https://nvd.nist.gov/vuln/detail/CVE-2021-44906

أول إصدار مُصلَح: 1.2.6

lockfile: package-lock.json:812

مذكورة في: package.json

الإصلاح: رقّي minimist من 1.2.5 إلى 1.2.6 أو أحدث (التنبيهات: GHSA-xvch-5gv4-984h, CVE-2021-44906). حدّث package-lock.json بمدير الحزم لديك بدلًا من التعديل اليدوي، وشغّل التثبيت والاختبارات، وتحقّق مما إذا كانت الترقية تحتاج إلى تغييرات في الكود.

المراجع:

GHSA-xvch-5gv4-984h (https://github.com/advisories/GHSA-xvch-5gv4-984h)

CVE-2021-44906 (https://nvd.nist.gov/vuln/detail/CVE-2021-44906)

CWE-1395: Dependency on Vulnerable Third-Party Component (https://cwe.mitre.org/data/definitions/1395.html)

OWASP A06:2021: Vulnerable and Outdated Components

الحالة: مفتوح. أول ظهور: 2026-10-30

أصلحه الآن | CVSS 9.3 | مفتوح

F-002 مفتاح Stripe السري موجود في كود صفحتك

الحكم: مؤكدة. الخطورة: حرجة. السبب: رأى yof ذلك في التطبيق المباشر.

يستطيع أي شخص استخدامه لتحصيل المدفوعات وإصدار المبالغ المستردة وقراءة بيانات الدفع الخاصة بعملائك.

CVSS 4.0: CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:N/VA:N/SC:H/SI:H/SA:H

CWE: CWE-798

المكان: https://shop.example/assets/app.js

الدليل (مخفي جزئيًا): sk_live_****9f2a

خطوات رؤيته:

1. افتح https://shop.example/assets/app.js من دون تسجيل الدخول.
2. ما رآه yof (مع إخفاء البيانات): sk_live_****9f2a
3. المتوقع بدلًا من ذلك: لا يظهر مفتاح Stripe السري الحي (live) في الكود الذي يستطيع الزوار تنزيله.

الأثر على العمل: قد يسجّل شخص الدخول باسم شخص آخر أو يحتفظ بجلسة لا ينبغي أن تكون له.

الإصلاح: أزِل المفتاح السري لـ Stripe (يبدأ بـ sk_live_) من كل كود المتصفح ومن أي متغيّر بيئة يستطيع المتصفح قراءته. أنشئ المدفوعات على الخادم فقط (مسار API أو server action أو Supabase Edge Function) وأرسل إلى المتصفح فقط الـ client secret الخاص بالدفعة. يجب ألا يرى المتصفح إلا المفتاح القابل للنشر (pk_live_). لا تلصق المفتاح الحقيقي في هذه المحادثة أبدًا، ولا تطبعه أبدًا، ولا تخترع مفتاحًا بديلًا. أخبرني عندما لا يعود الكود يحتوي عليه، حتى أُنشئ مفتاحًا جديدًا في لوحة تحكم المزوّد وأحذف القديم (فالقديم كان مكشوفًا للعامة، لذا يجب استبداله).

المراجع:

CWE-798: Use of Hard-coded Credentials (https://cwe.mitre.org/data/definitions/798.html)
OWASP A07:2021: Identification and Authentication Failures
الحالة: مفتوح. أول ظهور: 2026-10-30

أصلحه الآن | CVSS 8.7 | مفتوح

F-003 أي شخص يستطيع قراءة جدول في قاعدة بياناتك

الحكم: مؤكدة. الخطورة: عالية. السبب: رأى yof ذلك في التطبيق المباشر.

يستطيع غريب تنزيل صفوف هذا الجدول، مثل أسماء عملائك أو بريدهم أو طلباتهم، دون تسجيل الدخول.

CVSS 4.0: CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N
CWE: CWE-862
المكان: https://shop.example/
الدليل (مخفي جزئيًا): table orders: 3 rows readable without signing in

خطوات رؤيته:

1. افتح https://shop.example/ من دون تسجيل الدخول.
2. ما رآه yof (مع إخفاء البيانات): table orders: 3 rows readable without signing in
3. المتوقع بدلًا من ذلك: لا يستطيع الزوار غير المسجّلين الدخول قراءة هذا الجدول.

الأثر على العمل: قد يتمكن أشخاص من رؤية بيانات تخص غيرهم أو تغييرها.

الإصلاح: يمكن لأي شخص يملك مفتاح anon العام قراءة جدول في Supabase. فعّل Row Level Security لهذا الجدول (ولكل جدول آخر)، ثم أضف سياسات بحيث لا يستطيع الشخص المسجّل الدخول قراءة إلا صفوفه هو (مثلًا باستخدام auth.uid() = user_id). احذف أي سياسة تسمح لدور anon بقراءة كل شيء. اكتب لي أوامر SQL واشرح ما تسمح به كل سياسة. لا تلصق أبدًا بيانات عملاء حقيقية أو مفاتيح في هذه المحادثة.

```
-- for each table the browser can reach
alter table public.your_table enable row level security;
create policy "own rows" on public.your_table
  for select using (auth.uid() = user_id);
```

المراجع:

CWE-862: Missing Authorization (https://cwe.mitre.org/data/definitions/862.html)
OWASP A01:2021: Broken Access Control
الحالة: مفتوح. أول ظهور: 2026-10-30

أصلحه الآن | CVSS 7.1 | مفتوح

F-004 يستطيع مستخدم قراءة سجلات مستخدم آخر بتغيير المعرّف

الحكم: مؤكدة. الخطورة: عالية. السبب: رأى yof ذلك في التطبيق المباشر.

فتح حساب تجريبي سجلًا لحسابك التجريبي الآخر باستخدام معرّفه فقط، لذا يستطيع المستخدمون الحقيقيون قراءة بيانات بعضهم.

CVSS 4.0: CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N
CWE: CWE-639
المكان: GET /api/orders/{id} (as user b)
الدليل (مخفي جزئيًا): 200 with another customer's order

خطوات رؤيته:

1. سجّل الدخول بصفة مستخدم الاختبار b.
2. أرسل GET /api/orders/{id} مع معرّف يخص مستخدمًا آخر أو دورًا آخر.
3. ما رآه yof (مع إخفاء البيانات): 200 with another customer's order
4. المتوقع بدلًا من ذلك: لا يستطيع الحساب أن يفتح إلا سجلاته؛ ومعرّف حساب آخر يُجاب بالرمز 404 أو 403.

الأثر على العمل: قد يتمكن أشخاص من رؤية بيانات تخص غيرهم أو تغييرها.

الإصلاح: في تطبيقي، يستطيع المستخدم B قراءة سجل يخص المستخدم A بوضع معرّف سجل A في العنوان (أو يراه في قائمة). على الخادم، يجب أن يُرشِّح كل استعلام لسجل أو لقائمة حسب المستخدم المسجّل الدخول (أو مساحة عمله)، مثلًا `where id = :id and owner_id = :currentUser`، وأن يجيب بـ 404 عندما لا يكون السجل له. إذا كانت قاعدة البيانات تدعم row-level security، ففعّلها مع سياسة لا تسمح إلا للمالك. لا تعتمد على صعوبة تخمين المعرّفات.

المراجع:

CWE-639: Authorization Bypass Through User-Controlled Key (https://cwe.mitre.org/data/definitions/639.html)
OWASP A01:2021: Broken Access Control
OWASP API1:2023: Broken Object Level Authorization
الحالة: مفتوح. أول ظهور: 2026-10-30

أصلحه هذا الأسبوع | CVSS 5.1 | تم إصلاحه

F-005 نطاقك لا يملك قاعدة للبريد المزيف

الحكم: تحتاج إلى تحقق. الخطورة: متوسطة. السبب: لم يحتفظ الفحص بالدليل اللازم لتأكيدها.

مزودو البريد لا يعرفون ماذا يفعلون بالرسائل التي تنتحل اسمك، فيصل كثير منها.

CVSS 4.0: CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:N/VA:N/SC:L/SI:L/SA:N

CWE: CWE-290

المكان: https://shop.example/

خطوات رؤيته:

1. اطّلع على سجلات DNS TXT الخاصة بالنطاق (مثلًا: dig TXT shop.example).
2. المتوقع بدلًا من ذلك: ينشر النطاق سياسة DMARC بقيمة quarantine أو reject.

الأثر على العمل: أحد الإعدادات يترك ثغرة يسهل العثور عليها.

الإصلاح: لا يوجد للنطاق سجلّ DMARC. أضف سجلّ TXT يكون اسمه (host) هو _dmarc بالضبط، وليس @ (فسجلّ DMARC عند الجذر يُتجاهَل)، وابدأ بالمراقبة: v=DMARC1; p=none; rua=mailto:<an address you read> (ضع مكان ذلك عنوانًا تقرأه). بعد بضعة أسابيع من التقارير السليمة، انتقل إلى p=quarantine ثم إلى p=reject.

```
_dmarc.shop.example.  TXT  "v=DMARC1; p=quarantine; rua=mailto:dmarc@shop.example"
```

المراجع:

CWE-290: Authentication Bypass by Spoofing (https://cwe.mitre.org/data/definitions/290.html)

OWASP A05:2021: Security Misconfiguration

الحالة: تم إصلاحه. أول ظهور: 2026-10-30

النتائج المفتوحة فقط، حسب الحكم: مؤكدة (4)، تحتاج إلى تحقق (0). وعلى حدة: ملاحظات التقوية (1)، مرفوضة (0).

ملاحظات التقوية (لا تُحسب كنتائج)

ممارسات جيدة تضيف طبقة حماية. لم يُثبت yof أي خطر، لذا فهي ليست نتائج ولا تدخل في أي عدد.

- H-001 المتصفحات لا تُبلَّغ باستخدام https دائمًا: https://shop.example/

أضف الترويسة Strict-Transport-Security إلى كل استجابة، مثلًا: Strict-Transport-Security: max-age=31536000; includeSubDomains. اضبطها في إعدادات الترويسات في الاستضافة أو إطار العمل.

```
// vercel.json (or the same header in your host's settings)
{
  "headers": [
    { "source": "/(.*)", "headers": [ { "key": "Strict-Transport-Security", "value": "max-a
ge=63072000; includeSubDomains" } ] }
  ]
}
```

- H-002 لا توجد قاعدة تحدد أي سكربتات يمكن تشغيلها: https://shop.example/

أضف ترويسة Content-Security-Policy تحدّد المصادر المسموح أن تأتي منها السكربتات والأنماط والصور والاتصالات. ابدأ بوضع Report-Only، وتحقّق من أن التطبيق ما زال يعمل، ثم فعّل التطبيق الفعلي للسياسة.

```
// vercel.json (or the same header in your host's settings)
{
  "headers": [
    { "source": "/(.*)", "headers": [ { "key": "Content-Security-Policy", "value": "default
-src 'self'; frame-ancestors 'self'; object-src 'none'; base-uri 'self'" } ] }
  ]
}
```

الملحق A: المخاطر المقبولة وأسبابها

راجع المالك هذه النتائج وقرر قبول خطرها للسبب المذكور. لا تُحتسب ضمن النتائج المفتوحة، وهي مذكورة هنا كي لا يُخفى شيء.

H-002 لا توجد قاعدة تحدد أي سكربتات يمكن تشغيلها
المكان: https://shop.example/
السبب: The payment widget needs inline scripts until its next version; we review this in January.
قبلها: owner@shop.example, 2026-11-05
قُبلت في: تطبيق yof

مفتاح Stripe السري التجريبي موجود في كود صفحتك
المكان: tests/fixtures/payments.ts
السبب: A Stripe test key in a test fixture; it cannot take real payments.
قبلها: Sam (developer), 2026-11-02
قُبلت في: المستودع (yof/accepted.json.)

الملحق B: المنهجية والأدوات

شغّل yof قواعده واختباراته الخاصة: فحص التطبيق الحي من الخارج، وقراءة المستودع المرتبط وحزمه، واختبارات الهجوم التي يجريها المالك، ومع الموافقة اختبارات ثابتة لمساعد الذكاء الاصطناعي. يتبع كل فحص المنهج المنشور المذكور بجانبه.

لم يحكم أي ماسح خارجي أو نموذج ذكاء اصطناعي على النتائج. تُخفى الأدلة قبل حفظها، وكل طلب أرسله yof مدرج في قائمة الإثبات.

المناهج والمعايير المشار إليها

ASVS V14.1, ASVS V14.2.1, ASVS V14.3, ASVS V14.4, ASVS V2.10.4, ASVS V4.1, ASVS V5, ASVS V6.4.1, OWASP A06:2021, OWASP API Top 10 2023, RFC 6376 (DKIM), RFC 7208 (SPF), RFC 7489 (DMARC), WSTG-ATHN-04, WSTG-ATHZ-01, WSTG-ATHZ-02, WSTG-ATHZ-04, WSTG-CLNT-09, WSTG-CONF-03, WSTG-CONF-04, WSTG-CONF-05, WSTG-CONF-06, WSTG-CONF-07, WSTG-CONF-12, WSTG-INFO-05, WSTG-INPV, WSTG-SESS-01

الملحق C: مسرد المصطلحات

النتيجة
شيء رآه yof قد يسمح بدخول مهاجم أو يكشف بيانات، مع مكانه وطريقة رؤيته.

الأولوية
ترتيب yof البسيط للعمل: أصلح الآن، هذا الأسبوع، من الجيد إصلاحه، للعلم.

CVSS 4.0
نظام التقييم الشائع لمدى خطورة الثغرة من 0 إلى 10، مع المتجه الذي يشرح الدرجة.

CWE
القائمة الشائعة لأنواع الثغرات؛ تذكر كل نتيجة نوعها.

التغطية
مقدار ما اختُبر في هذا التقرير من الأجزاء الستة التي يستطيع yof فحصها.

خطر مقبول
نتيجة قرر المالك الإبقاء عليها مع ذكر السبب. تُذكر ولا تُحتسب مفتوحة.

SBOM
قائمة مكونات البرمجيات: الحزم التي بُني منها التطبيق.

البصمة
بصمة SHA-256 لمحتوى التقرير. أي تغيير في التقرير يغيرها.

الملحق D: ملخص قائمة مكونات البرمجيات (SBOM)

الحزم في ملف SBOM المرفق بالتقرير: 640. وعليها تحذير معروف: 1.

- example-shop/storefront @ 0f1e2d3c4b5a
- npm: 640
- package-lock.json

SHA-256 5a5a5a5a5a5a5a5a5a5a5a5a5a5a5a5a5a5a5a5a5a5a5a5a5a5a5a5a5a5a5a5a5a5a5a5a5a5a5a5a5a5a5a5a5a

الملحق E: طريقة التحقق

1. امسح رمز QR على الغلاف أو افتح العنوان المطبوع تحته. تتحقق الصفحة من توقيع yof في السجل.
2. للتحقق من ملف وصلك، اختره في تلك الصفحة؛ يحسب متصفحك بصمة SHA-256 ويقارنها، ولا يُرفع الملف.
3. مع توقيع Ed25519 يستطيع أي شخص أيضًا التحقق دون اتصال بمفتاح yof العام، على رقم التقرير والإصدار وتاريخ الإصدار وبصمة المحتوى.

- امسح رمز QR أو افتح https://yof.io/verify/5a3b1e00-0000-4000-8000-000000000000. تتحقق الصفحة من توقيع yof وتعرض فقط ما اختار صاحب التقرير مشاركته.

تحقق من هذا التقرير
yof.io/verify/5a3b1e00-0000-4000-8000-000000000000
بصمة SHA-256: fb9ff4c2ff530d7b8b05f4622d7e389ab732e25f51676dc2cd21e1f34878fee5

الحدود

- يعرض التقرير أدلة على ما تم فحصه في التواريخ أعلاه. وليس وعدًا بشأن ما لم يُفحص أو بشأن التغييرات اللاحقة.
- الأدلة مخفية جزئيًا: لا تُطبع المفاتيح والرموز وكلمات المرور وعناوين البريد كاملة أبدًا.