صائد الثغرات

THAGHARAT

تقرير اختبار الاختراق

اختبار اختراق تطبيق الويب وواجهات برمجة التطبيقات لبوابة العملاء

أُعدّ لـ	شركة المثال التجارية
تاريخ التقرير	27 أكتوبر 2026
الإصدار	1.1
المرجع	TH-2026-000
وثيقة نطاق العمل	TH-2026-000، 3 سبتمبر 2026

تقرير نموذجي: العميل والأنظمة والنتائج الواردة فيه غير حقيقية.

يعرض هذا النموذج التقرير الذي يتسلّمه كل عميل لدى «صائد الثغرات». وشركة المثال التجارية غير موجودة، فأنظمتها والنتائج الواردة هنا كُتبت لأغراض هذا النموذج، وقد حُذفت أسماء الأشخاص.

شركة صائد الثغرات · س.ت 7055275007 · الرياض · info@thagharat.com

ضبط المستند

الإصدار	التاريخ	الوصف	المُعِد
1.0	20 سبتمبر 2026	التقرير النهائي	قائد المشروع
1.1	27 أكتوبر 2026	إضافة نتائج إعادة الاختبار (القسم 7)	قائد المشروع

قائمة التوزيع

الاسم	الجهة	الدور
يُذكر في نسخة العميل	شركة المثال التجارية	مدير تقنية المعلومات
يُذكر في نسخة العميل	شركة صائد الثغرات	قائد المشروع

فريق المشروع

الاسم	الدور	المؤهلات
يُذكر في نسخة العميل	قائد المشروع	تُذكر في نسخة العميل
يُذكر في نسخة العميل	مختبِر	تُذكر في نسخة العميل

التسليم	سُلّم عبر بوابة الملفات الآمنة لدى العميل بتاريخ 27 أكتوبر 2026، وأُبلغت كلمة المرور بشكل منفصل إلى مدير تقنية المعلومات هاتفياً. ويُسلَّم مع التقرير جدول بالنتائج لاستخدامه في نظام متابعة الطلبات لديكم.
مراجعة الجودة	راجعه مراجِع يُذكر اسمه في نسخة العميل، ولم يشارك في تنفيذ الاختبار، بتاريخ 26 أكتوبر 2026.
التداول	يصف هذا التقرير نقاط ضعف في أنظمتكم، فلا تشاركوه إلا مع من يحتاج إليه لمعالجتها أو لتقييم الامتثال، واحفظوه مشفّراً. وتُتلف «صائد الثغرات» بيانات المشروع بعد 30 يوماً من إصدار خطاب الإغلاق.
التواصل	قائد المشروع لدى «صائد الثغرات»، info@thagharat.com، +966 50 601 6914

المحتويات

ضبط المستند 2

1. الملخص التنفيذي 4

2. النطاق والمنهجية 5

3. ملخص النتائج 5

4. تفاصيل النتائج 6

TH-01 يستطيع أي عميل تنزيل فواتير جميع العملاء الآخرين 6

TH-02 رسائل إعادة تعيين كلمة المرور قد تحمل رابطاً إلى موقع المهاجم 7

TH-03 تسجيل الدخول يقبل عدداً غير محدود من محاولات تخمين كلمة المرور 9

TH-04 رابط مُعدّ يشغّل شيفرة المهاجم داخل البوابة 11

TH-05 يستطيع أي عميل الاطلاع على قائمة حسابات الموظفين بعناوين بريدهم وأدوارهم 12

TH-06 تسجيل الخروج لا يُنهي الجلسة في الخادم 14

TH-07 ترويسات الحماية الخاصة بالمتصفح غير مفعّلة 15

5. خطة المعالجة 17

6. ربط النتائج بالأطر 17

7. نتائج إعادة الاختبار 17

8. الخطوات التالية 18

الملحق (أ): تصنيف مستوى الخطر 19

الملحق (ب): الجدول الزمني للاختبار 20

الملحق (ج): تغطية الاختبار 20

نموذج

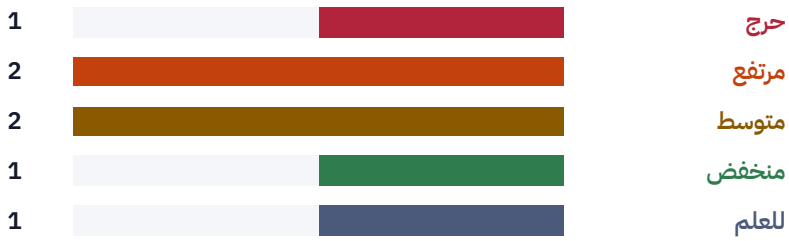
1. الملخص التنفيذي

كلّفت شركة المثال التجارية «صائد الثغرات» باختبار بوابة العملاء لديها وواجهات برمجة التطبيقات التابعة لها خلال الفترة من 13 سبتمبر 2026 إلى 15 سبتمبر 2026، بهدف تقييم أمن البوابة والبيانات الشخصية التي تحتفظ بها. وجرى الاختبار وفق النطاق وقواعد الاشتباك المتفق عليها في وثيقة نطاق العمل TH-2026-000.

مستوى الخطر العام	**حرج**: يستطيع أي عميل تنزيل فواتير جميع العملاء الآخرين، بما فيها الأسماء والعناوين وأرقام الجوال (TH-01).
نتائج إعادة الاختبار	تمت المعالجة: 4 · معالجة جزئية: 1 · لم تُعالج: 1 · خطر مقبول: 1 (القسم 7)

النتائج بإيجاز

مستوى الخطر	عدد النتائج
حرج	1
مرتفع	2
متوسط	2
منخفض	1
للعلم	1
الإجمالي	7



أبرز المخاطر

- يستطيع أي عميل تنزيل فواتير جميع العملاء الآخرين بتغيير رقم في العنوان، وتتضمن كل فاتورة الاسم والعنوان ورقم الجوال والمشتريات (TH-01).
- يستطيع المهاجم السيطرة على أي حساب، ومنها حسابات الموظفين، بطريقتين: أن ينقر صاحب الحساب رابط إعادة تعيين كلمة المرور الذي ترسله البوابة نفسها (TH-02)، أو أن يخمّن المهاجم كلمة المرور دون حد لعدد المحاولات (TH-03).
- رابط يُرسَل إلى عميل مسجّل الدخول يشغّل شيفرة المهاجم داخل البوابة، فتعمل بصفة ذلك العميل (TH-04).

ما يجب إصلاحه أولاً

- التحقق في الخادم من أن الفاتورة تخص العميل الذي سجّل دخوله قبل إعادتها (TH-01).
- بناء روابط إعادة تعيين كلمة المرور من عنوان ثابت، وتحديد عدد محاولات تسجيل الدخول لكل حساب ولكل عنوان مصدر (TH-02، TH-03).
- ترميز نص البحث قبل عرضه، وحصر قائمة الموظفين في الموظفين (TH-04، TH-05).

ما يعمل بصورة جيدة

- جميع الاتصالات تجري عبر HTTPS بإعدادات TLS حديثة، ويُحوَّل HTTP غير المشفّر إليها تلقائياً.
- الطلبات محمية، فلم يستطع العميل قراءة طلب عميل آخر ولا تغييره.
- خطوة الدفع لا تتعامل مع أرقام البطاقات داخل البوابة، بل تنتقل إلى الصفحة التي يستضيفها مزوّد خدمة الدفع.
- لم تُظهر البوابة رسائل أخطاء من قاعدة البيانات أو من الخادم عند إرسال مدخلات غير سليمة، ولم يُعثر على حقن SQL في أي مُدخل جرى اختباره.

2. النطاق والمنهجية

#	الهدف	النوع	البيئة
1	https://portal.example.com	تطبيق ويب	بيئة الإنتاج
2	https://api.example.com	واجهة برمجة التطبيقات	بيئة الإنتاج

خارج النطاق	صفحة الدفع التي يستضيفها مزوّد خدمة الدفع، واختبارات توافر الخدمة.
نافذة الاختبار	من 13 إلى 15 سبتمبر 2026، من 09:00 إلى 17:00
عناوين IP المصدر	203.0.113.24
الأسلوب	صندوق رمادي، حسابات الاختبار: حسابا عميل وحساب موظف، أنشأتها شركة المثال التجارية لأغراض الاختبار

المنهجية

جرى اختبار تطبيقات الويب وفق دليل OWASP WSTG، وتطبيقات الهواتف وفق OWASP MASVS و MASTG، واتّبع الاختبار المراحل الأربع في NIST SP 800-115: التخطيط والاستكشاف والهجوم وإعداد التقرير. وتستعين «صائد الثغرات» بأدوات ذكاء اصطناعي تعمل على أجهزتها الخاصة في حصر سطح الهجوم وفرز مخرجات أدوات الفحص ومراجعة الشيفرة، وقد أكّد مختبِر كل نتيجة وردت في هذا التقرير.

حدود الاختبار

هذا تقييم للأنظمة المشمولة بالنطاق خلال نافذة الاختبار، ولا يضمن اكتشاف جميع الثغرات ولا أمن الأنظمة. وقد وصل حساب الموظف في اليوم الثاني، فاقتصر اختبار قسم الموظفين على يومي 14 و15 سبتمبر.

3. ملخص النتائج

الرقم	النتيجة	الخطر	CVSS	الأصل	الحالة
TH-01	يستطيع أي عميل تنزيل فواتير جميع العملاء الآخرين	حرج	6.5	واجهة برمجة التطبيقات	تمت المعالجة
TH-02	رسائل إعادة تعيين كلمة المرور قد تحمل رابطاً إلى موقع المهاجم	مرتفع	8.1	واجهة برمجة التطبيقات	تمت المعالجة
TH-03	تسجيل الدخول يقبل عدداً غير محدود من محاولات تخمين كلمة المرور	مرتفع	7.4	واجهة برمجة التطبيقات	معالجة جزئية
TH-04	رابط مُعدّ يشغّل شيفرة المهاجم داخل البوابة	متوسط	6.1	البوابة	تمت المعالجة
TH-05	يستطيع أي عميل الاطلاع على قائمة حسابات الموظفين بعناوين بريدهم وأدوارهم	متوسط	4.3	واجهة برمجة التطبيقات	تمت المعالجة
TH-06	تسجيل الخروج لا يُنهي الجلسة في الخادم	منخفض	4.8	واجهة برمجة التطبيقات	خطر مقبول
TH-07	ترويسات الحماية الخاصة بالمتصفح غير مفعّلة	للعلم	0.0	البوابة	لم تُعالج

4. تفاصيل النتائج

TH-01 يستطيع أي عميل تنزيل فواتير جميع العملاء الآخرين

الخطر	**حرج**: الاحتمالية مرتفعة، والأثر على الأعمال مرتفع (الملحق أ)
CVSS 3.1	6.5 (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N)
الاحتمالية	مرتفعة: لا تتطلب سوى حساب عميل يستطيع أي شخص إنشاءه، وأرقام الفواتير متسلسلة.
الأثر على الأعمال	مرتفع: يكشف اسم كل عميل وعنوانه ورقم جواله ومشترياته، وهي بيانات شخصية بكميات كبيرة.
الأصل المتأثر	https://api.example.com/v1/invoices/{number}/pdf
التصنيف	OWASP Top 10 2025 A01: Broken Access Control، و OWASP API Security Top 10 2023 API1: Broken Object Level Authorization، و CWE-639
تاريخ الاكتشاف	13 سبتمبر 2026
جهد الإصلاح	منخفض
الحالة	**تمت المعالجة**

الوصف

تُعيد واجهة الفواتير ملف أي فاتورة يَرِد رقمها في العنوان. وهي تتحقق من أن الطلب يحمل جلسة صالحة، لكنها لا تتحقق من أن الفاتورة تخص العميل الذي سجّل دخوله. وأرقام الفواتير متسلسلة، فلا يفصل فاتورة العميل التالي عن سابقتها سوى رقم واحد.

الأثر

يستطيع كل من يسجّل في البوابة تنزيل جميع الفواتير التي أصدرتها الشركة. وتتضمن كل فاتورة اسم العميل وعنوان التسليم ورقم الجوال وما اشتراه.

وهذا كشف لبيانات شخصية بكميات كبيرة، قد يستوجب إشعار الجهة المختصة والعملاء المتضررين وفق نظام حماية البيانات الشخصية، ويضر بثقة العملاء.

وقد أثبت الفريق ذلك بحسابَي الاختبار فقط، ولم يطلب فاتورة أي عميل حقيقي.

خطوات إعادة الاختبار

1. سجّلوا الدخول بصفة العميل التجريبي (أ) وافتحوا إحدى فواتيره، فيطلب المتصفح `/v1/invoices/104217/pdf` .
2. أعيدوا إرسال الطلب نفسه بعد تغيير الرقم إلى `104218` ، وهو رقم فاتورة تخص العميل التجريبي (ب).
3. تُعيد الاستجابة فاتورة العميل التجريبي (ب).

الأدلة

```
GET /v1/invoices/104218/pdf HTTP/1.1
Host: api.example.com
Authorization: Bearer (token of test customer A, ending 9f3c)

HTTP/1.1 200 OK
Content-Type: application/pdf
Content-Disposition: attachment; filename="invoice-104218.pdf"
```

الملف المُعاد هو فاتورة العميل التجريبي (ب)، وقد أُنشئ الحسابان لأغراض هذا الاختبار.

التوصية

تحقّقوا في الخادم، قبل إعادة أي فاتورة، من أنها تخص العميل الذي سجّل دخوله. وأعيدوا الرد `404` للفاتورة غير الموجودة وللفاتورة التي تخص عميلاً آخر على السواء، حتى لا يكشف الرد الأرقام المستخدمة.

- طبّقوا التحقق نفسه على كل عنوان يستقبل رقم فاتورة أو طلب أو عميل.
- أضيفوا اختباراً آلياً يطلب فاتورة حساب آخر ويتوقع الرد `404` .
- راجعوا سجلات الوصول بحثاً عن حسابات طلبت أرقام فواتير كثيرة، لأن الثغرة كانت متاحة فعلياً.

المراجع

- OWASP API Security Top 10 2023, API1 Broken Object Level Authorization: https://owasp.org/API-Security/editions/2023/en/0xa1-broken-object-level-authorization/
- OWASP Insecure Direct Object Reference Prevention Cheat Sheet: cheatsheetseries.owasp.org/cheatsheets/Insecure_Direct_Object_Reference_Prevention_Cheat_Sheet.html
- CWE-639: https://cwe.mitre.org/data/definitions/639.html

الربط بالأطر

- PDPL: المادة 19 (حماية البيانات الشخصية)
- NCA ECC: 2-2, 2-15 (إدارة هويات الدخول والصلاحيات، وحماية تطبيقات الويب)
- ISO 27001: A.8.3 (تقييد الوصول إلى المعلومات)

TH-02 رسائل إعادة تعيين كلمة المرور قد تحمل رابطاً إلى موقع المهاجم

الخطر	**مرتفع**: الاحتمالية متوسطة، والأثر على الأعمال مرتفع (الملحق أ)
CVSS 3.1	8.1 (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:N)
الاحتمالية	متوسطة: لا تتطلب حساباً، لكنها تتطلب أن ينقر الضحية الرابط الوارد في الرسالة، وهي رسالة صادرة من عنوان البوابة نفسه.
الأثر على الأعمال	مرتفع: يمنح السيطرة على أي حساب ينقر صاحبه الرابط، ومنها حسابات الموظفين، وحساب موظف واحد يطّلع على طلبات جميع العملاء.
الأصل المتأثر	https://api.example.com/v1/auth/password-reset
التصنيف	OWASP Top 10 2025 A07: Authentication Failures، و OWASP API Security Top 10 2023 API2: Broken Authentication، و CWE-640
تاريخ الاكتشاف	14 سبتمبر 2026
جهد الإصلاح	منخفض
الحالة	**تمت المعالجة**

الوصف

عند طلب إعادة تعيين كلمة المرور، ترسل البوابة رابطاً إلى بريد صاحب الحساب. وهي تبني هذا الرابط من الترويسة `X-Forwarded-Host` الواردة في الطلب، لا من عنوانها الثابت. فيستطيع المهاجم الذي يطلب إعادة تعيين كلمة مرور حساب غيره أن يحدد الموقع الذي يشير إليه الرابط.

والرسالة حقيقية، فهي صادرة من البوابة، والرابط يحمل رمز إعادة التعيين الصحيح.

الأثر

إذا نقر صاحب الحساب الرابط وصل الرمز إلى موقع المهاجم، فيعيّن المهاجم كلمة مرور جديدة ويسيطر على الحساب.

وفي حساب العميل ينكشف ما له من طلبات وفواتير. وفي حساب الموظف تنكشف طلبات جميع العملاء وبيانات التواصل معهم، وهي بيانات شخصية بكميات كبيرة وفق نظام حماية البيانات الشخصية.

خطوات إعادة الاختبار

1. اطلبوا إعادة تعيين كلمة مرور العميل التجريبي (ب)، وأضيفوا إلى الطلب الترويسة `X-Forwarded-Host: attacker.example`.
2. افتحوا الرسالة التي تصل إلى بريد العميل التجريبي (ب)، وستجدون أن رابط إعادة التعيين يشير إلى `attacker.example`.
3. خذوا الرمز من ذلك الرابط وأرسلوه إلى `/v1/auth/password-reset/confirm` مع كلمة مرور جديدة، فتتغير كلمة مرور العميل التجريبي (ب).

الأدلة

```
POST /v1/auth/password-reset HTTP/1.1
Host: api.example.com
X-Forwarded-Host: attacker.example
Content-Type: application/json

{"email": "customer-b@example.com"}

HTTP/1.1 202 Accepted
```

الرابط الوارد في الرسالة التي تلقّاها العميل التجريبي (ب):

```
https://attacker.example/reset?token=(removed, ending 7d2e)
```

التوصية

ابنوا رابط إعادة التعيين من عنوان ثابت في إعدادات الخادم، لا من ترويسة في الطلب.

- ارفضوا كل طلب تحمل ترويسته `Host` أو `X-Forwarded-Host` اسماً ليس من أسماء البوابة المعتمدة.
- اجعلوا رموز إعادة التعيين قصيرة الصلاحية وصالحة للاستخدام مرة واحدة.
- أضيفوا اختباراً آلياً يرسل ترويسة `X-Forwarded-Host` مزوّرة ويتوقع أن يبقى الرابط على عنوان البوابة.

المراجع

- PortSwigger Web Security Academy, Password reset poisoning: https://portswigger.net/web-security/host-header/exploiting/password-reset-poisoning
- OWASP Forgot Password Cheat Sheet: https://cheatsheetseries.owasp.org/cheatsheets/Forgot_Password_Cheat_Sheet.html
- CWE-640: https://cwe.mitre.org/data/definitions/640.html

الربط بالأطر

- PDPL: المادة 19 (حماية البيانات الشخصية)
- NCA ECC: 2-2, 2-15 (إدارة هويات الدخول والصلاحيات، وحماية تطبيقات الويب)
- ISO 27001: A.8.5 (المصادقة الآمنة)

TH-03 تسجيل الدخول يقبل عدداً غير محدود من محاولات تخمين كلمة المرور

الخطر	**مرتفع**: الاحتمالية متوسطة، والأثر على الأعمال مرتفع (الملحق أ)
CVSS 3.1	7.4 (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N)
الاحتمالية	متوسطة: لا تتطلب حساباً، لكنها لا تنجح إلا مع الحسابات ذات كلمات المرور السهلة التخمين، وهو ما يسمح به الحد الأدنى البالغ ستة أحرف.
الأثر على الأعمال	مرتفع: يسجّل الموظفون دخولهم عبر النموذج نفسه، وحساب موظف واحد يطّلع على طلبات جميع العملاء وبيانات التواصل معهم.
الأصل المتأثر	https://api.example.com/v1/auth/login
التصنيف	OWASP Top 10 2025 A07: Authentication Failures، و OWASP API Security Top 10 2023 API2: Broken Authentication، و CWE-307
تاريخ الاكتشاف	13 سبتمبر 2026
جهد الإصلاح	متوسط
الحالة	**معالجة جزئية**

الوصف

تردّ واجهة تسجيل الدخول على كل محاولة فوراً مهما بلغ عدد المحاولات الفاشلة قبلها. فلا تأخير ولا إقفال مؤقت ولا تحقق إضافي بعد تكرار الفشل، لا على مستوى الحساب ولا على مستوى العنوان الذي تصدر منه المحاولات.

وتقبل البوابة كذلك كلمات مرور من ستة أحرف، ولا تقارنها بقوائم كلمات المرور الشائعة.

الأثر

يستطيع المهاجم تجربة آلاف كلمات المرور الشائعة على أي حساب. وقد أرسل الفريق 5,000 محاولة في أقل من أربع دقائق على حسابه التجريبي دون أي إبطاء، فوصل إلى كلمة المرور الضعيفة التي عُيّنت له لأغراض الاختبار.

وستسقط الحسابات ذات كلمات المرور الضعيفة، وحسابات الموظفين تستخدم النموذج نفسه. وإذا أضيفت إلى ذلك النتيجة TH-05، التي تمنح المهاجم عناوين بريد الموظفين، أصبح الطريق إلى حساب موظف مباشراً.

خطوات إعادة الاختبار

1. استخدموا عنوان بريد العميل التجريبي (أ)، وقد عُيّنت له في هذا الاختبار كلمة مرور شائعة من ستة أحرف.
2. أرسلوا 5,000 طلب تسجيل دخول إلى `/v1/auth/login`، كل منها بكلمة مرور مختلفة من قائمة منشورة.
3. تُعيد كل محاولة خاطئة الرد `401` خلال نحو 40 جزءاً من الألف من الثانية، ولا تُرفض أي محاولة ولا تُؤخَّر، وتُعيد كلمة المرور الصحيحة الرد `200`.

الأدلة

```
POST /v1/auth/login HTTP/1.1
Host: api.example.com
Content-Type: application/json

{"email": "customer-a@example.com", "password": "(guess 1 to 5,000)"}

Attempts sent           5,000 in 3 minutes 41 seconds
Answered 401            4,999
Answered 200            1 (attempt 3,112)
Answered 429 or locked  0
```

التوصية

حدّدوا عدد محاولات الدخول الفاشلة لكل حساب ولكل عنوان مصدر، كأن تُبطَّأ الردود بعد خمس محاولات فاشلة ويُقفل الحساب 15 دقيقة بعد عشر، مع إشعار صاحبه بالبريد الإلكتروني.

- طبّقوا الحد في واجهة برمجة التطبيقات نفسها، ليشمل كل تطبيق يسجّل الدخول عبرها.
- اشترطوا ألا تقل كلمة المرور عن 12 حرفاً، وارفضوا كلمات المرور الواردة في قوائم الكلمات الشائعة أو المسرّبة.
- أتيحوا التحقق بعامل ثانٍ للعملاء، واجعلوه إلزامياً للموظفين.
- تحقّقوا بتكرار الخطوات أعلاه وتوقّع إقفال الحساب.

المراجع

- OWASP Authentication Cheat Sheet: https://cheatsheetseries.owasp.org/cheatsheets/Authentication_Cheat_Sheet.html
- OWASP API Security Top 10 2023, API2 Broken Authentication: https://owasp.org/API-Security/editions/2023/en/0xa2-broken-authentication/
- CWE-307: https://cwe.mitre.org/data/definitions/307.html

الربط بالأطر

- PDPL: المادة 19 (حماية البيانات الشخصية)
- NCA ECC: 2-2, 2-15 (إدارة هويات الدخول والصلاحيات، وحماية تطبيقات الويب)
- ISO 27001: A.8.5 (المصادقة الآمنة)

TH-04 رابط مُعدّ يشغّل شيفرة المهاجم داخل البوابة

الخطر	**متوسط**: الاحتمالية متوسطة، والأثر على الأعمال متوسط (الملحق أ)
CVSS 3.1	6.1 (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N)
الاحتمالية	متوسطة: تتطلب أن يفتح عميل مسجّل الدخول رابطاً يرسله المهاجم.
الأثر على الأعمال	متوسط: تعمل الشيفرة بصفة ذلك العميل وحده، فتقرأ طلباته وفواتيره وتغيّر بياناته.
الأصل المتأثر	https://portal.example.com/orders?search=
التصنيف	OWASP Top 10 2025 A05: Injection، و CWE-79
تاريخ الاكتشاف	14 سبتمبر 2026
جهد الإصلاح	منخفض
الحالة	**تمت المعالجة**

الوصف

تعرض صفحة البحث في الطلبات نص البحث للمستخدم كما هو دون ترميزه. فإذا تضمّن النص وسوم HTML عُدّ جزءاً من الصفحة، واشتغلت الشيفرة الواردة فيه في متصفح الزائر بصلاحيات البوابة نفسها.

الأثر

يرسل المهاجم إلى أحد العملاء رابطاً إلى البوابة الحقيقية، يتضمن نص البحث فيه شيفرة. فإذا كان العميل مسجّلاً دخوله وفتح الرابط، استطاعت الشيفرة قراءة الرمز المميّز الذي تحفظه البوابة في المتصفح وإرساله إلى المهاجم. فيستخدم المهاجم الحساب إلى أن تنتهي صلاحية الرمز، ويطّلع على طلبات العميل وفواتيره ويغيّر بياناته.

وتزيد النتيجة TH-06 الأمر سوءاً، لأن تسجيل الخروج لا يُلغي الرمز. والصفحة موجودة في قسم العملاء فقط، فلا تنكشف حسابات الموظفين من خلالها.

خطوات إعادة الاختبار

1. سجّلوا الدخول بصفة العميل التجريبي (أ).
2. افتحوا العنوان `https://portal.example.com/orders?search=<img src=x onerror=alert(document.domain)>`.
3. تعرض الصفحة نافذة تنبيه فيها `portal.example.com`، أي أن الشيفرة اشتغلت داخل البوابة.

الأدلة

```
GET /orders?search=%3Cimg%20src%3Dx%20onerror%3Dalert(document.domain)%3E HTTP/1.1
Host: portal.example.com

HTTP/1.1 200 OK
Content-Type: text/html; charset=utf-8

<p class="results-title">Results for <img src=x onerror=alert(document.domain)></p>
```

التوصية

رمّزوا نص البحث ترميز HTML قبل كتابته في الصفحة، باستخدام الترميز التلقائي في محرك القوالب وإزالة الإخراج غير المرمَّز من هذه الصفحة.

- ابحثوا في الشيفرة عن مواضع أخرى تكتب قيماً واردة في الطلب دون ترميزها.
- أضيفوا سياسة Content Security Policy تمنع الشيفرة المضمّنة في الصفحة، لتكون طبقة حماية ثانية (TH-07).
- أضيفوا اختباراً آلياً يطلب الصفحة ونص البحث فيه `<script>` ويتوقع أن يعود مرمَّزاً.

المراجع

- OWASP Cross Site Scripting Prevention Cheat Sheet: https://cheatsheetseries.owasp.org/cheatsheets/Cross_Site_Scripting_Prevention_Cheat_Sheet.html
- CWE-79: https://cwe.mitre.org/data/definitions/79.html

الربط بالأطر

- PDPL: المادة 19 (حماية البيانات الشخصية)
- NCA ECC: 2-15 (حماية تطبيقات الويب)
- ISO 27001: A.8.28 (البرمجة الآمنة)

TH-05 يستطيع أي عميل الاطلاع على قائمة حسابات الموظفين بعناوين بريدهم وأدوارهم

الخطر	**متوسط**: الاحتمالية مرتفعة، والأثر على الأعمال منخفض (الملحق أ)
CVSS 3.1	4.3 (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N)
الاحتمالية	مرتفعة: لا تتطلب سوى حساب عميل يستطيع أي شخص إنشاءه، وطلب واحد.
الأثر على الأعمال	منخفض: يكشف أسماء الموظفين وعناوين بريد العمل وأدوارهم، دون بيانات العملاء، لكنه يدلّ المهاجم على من يستهدفهم.
الأصل المتأثر	https://api.example.com/v1/staff
التصنيف	OWASP Top 10 2025 A01: Broken Access Control، و OWASP API Security Top 10 2023 API5: Broken Function Level Authorization، و CWE-862
تاريخ الاكتشاف	14 سبتمبر 2026
جهد الإصلاح	منخفض
الحالة	**تمت المعالجة**

الوصف

واجهة دليل الموظفين مخصصة لقسم الموظفين، لكنها تردّ على أي حساب مسجّل الدخول. فالعميل الذي يطلبها يحصل على اسم كل موظف وعنوان بريد العمل ودوره.

الأثر

لا تتضمن القائمة بيانات عملاء، لكن قيمتها للمهاجم فيما تتيحه: فهي تسمّي الحسابات الجديرة بالاستهداف وتبيّن أيها حسابات مسؤولين.

وهي تجعل النتيجتين TH-03 وTH-02 قابلتين للتطبيق على الموظفين، وتساعد المهاجم على صياغة رسائل تصيّد مقنعة موجّهة إليهم.

خطوات إعادة الاختبار

1. سجّلوا الدخول بصفة العميل التجريبي (أ) وانسخوا الرمز المميِّز من أي طلب إلى واجهة برمجة التطبيقات.
2. اطلبوا `/v1/staff` بذلك الرمز.
3. تتضمن الاستجابة جميع حسابات الموظفين.

الأدلة

```
GET /v1/staff HTTP/1.1
Host: api.example.com
Authorization: Bearer (token of test customer A, ending 9f3c)

HTTP/1.1 200 OK
Content-Type: application/json

{"staff": [
  {"name": "(removed)", "email": "(removed)", "role": "admin"},
  {"name": "(removed)", "email": "(removed)", "role": "support"},
  (9 more accounts)
]}
```

التوصية

اشترطوا دور الموظف في `/v1/staff` وفي كل عنوان آخر من عناوين قسم الموظفين، وتحقّقوا منه في الخادم عند كل طلب.

- راجعوا عناوين واجهة برمجة التطبيقات مقابل الأدوار المسموح لها باستدعائها.
- أضيفوا اختباراً آلياً يستدعي كل عنوان خاص بالموظفين برمز عميل ويتوقع الرد `403` .

المراجع

- OWASP API Security Top 10 2023, API5 Broken Function Level Authorization: https://owasp.org/API-Security/editions/2023/en/0xa5-broken-function-level-authorization/
- CWE-862: https://cwe.mitre.org/data/definitions/862.html

الربط بالأطر

- PDPL: المادة 19 (حماية البيانات الشخصية)
- NCA ECC: 2-2 (إدارة هويات الدخول والصلاحيات)
- ISO 27001: A.8.3 (تقييد الوصول إلى المعلومات)

TH-06 تسجيل الخروج لا يُنهي الجلسة في الخادم

الخطر	**منخفض**: الاحتمالية منخفضة، والأثر على الأعمال متوسط (الملحق أ)
CVSS 3.1	4.8 (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N)
الاحتمالية	منخفضة: تتطلب أن يحصل المهاجم أولاً على الرمز المميِّز لأحد المستخدمين، عبر نقطة ضعف أخرى أو من جهاز المستخدم.
الأثر على الأعمال	متوسط: يتيح استخدام حساب واحد مدة تصل إلى 12 ساعة بعد تسجيل صاحبه الخروج.
الأصل المتأثر	https://api.example.com/v1/auth/logout
التصنيف	OWASP Top 10 2025 A07: Authentication Failures، و CWE-613
تاريخ الاكتشاف	15 سبتمبر 2026
جهد الإصلاح	متوسط
الحالة	**خطر مقبول**

الوصف

عند تسجيل الخروج يحذف تطبيق الويب الرمز المميِّز من المتصفح، لكن الخادم يواصل قبول ذلك الرمز إلى أن تنتهي صلاحيته بعد 12 ساعة من إصداره. وتغيير كلمة المرور لا يُلغي الرموز السابقة أيضاً.

الأثر

يبقى الرمز المنسوخ صالحاً بعد أن يسجّل صاحبه الخروج أو يغيّر كلمة مروره، فلا تمنع أي من الخطوتين المهاجم من مواصلة الدخول. ويمكن نسخ الرمز بشيفرة تعمل في الصفحة (TH-04)، أو من حاسوب مشترك، أو من سجلات خادم وسيط.

ولا تمنح هذه النتيجة وصولاً بمفردها، ولذلك صُنّفت احتماليتها منخفضة.

خطوات إعادة الاختبار

1. سجّلوا الدخول بصفة العميل التجريبي (أ) ودوّنوا الرمز المميِّز الوارد في الترويسة `Authorization`.
2. سجّلوا الخروج من تطبيق الويب.
3. أرسلوا الطلب `GET /v1/orders` بالرمز الذي دوّنتموه، فيردّ الخادم بالرد `200` مع طلبات العميل.

الأدلة

```
POST /v1/auth/logout HTTP/1.1
Host: api.example.com
Authorization: Bearer (token of test customer A, ending 9f3c)

HTTP/1.1 204 No Content


GET /v1/orders HTTP/1.1
Host: api.example.com
Authorization: Bearer (the same token, after signing out)

HTTP/1.1 200 OK
```

التوصية

احتفظوا في الخادم بسجل للرموز الملغاة أو للجلسة المرتبطة بكل رمز، وارفضوا الرمز فور تسجيل صاحبه الخروج أو تغيير كلمة مروره.

- قلّصوا مدة صلاحية الرمز إلى 30 دقيقة أو أقل، وجدّدوه برمز تجديد يستطيع الخادم إلغاءه.
- تحقّقوا بتكرار الخطوات الثلاث أعلاه وتوقّع الرد `401`.

المراجع

- OWASP Session Management Cheat Sheet: https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html
- CWE-613: https://cwe.mitre.org/data/definitions/613.html

الربط بالأطر

- NCA ECC: 2-15 (حماية تطبيقات الويب)
- ISO 27001: A.8.5 (المصادقة الآمنة)

TH-07 ترويسات الحماية الخاصة بالمتصفح غير مفعّلة

الخطر	**للعلم**: الاحتمالية منخفضة، والأثر على الأعمال منخفض (الملحق أ)
CVSS 3.1	0.0
الاحتمالية	منخفضة: تتطلب وجود نقطة ضعف أخرى أولاً، فغياب الترويسات لا يمكن استغلاله بمفرده.
الأثر على الأعمال	منخفض: لا ضرر مباشراً، لكن الترويسات تحدّ من أثر نقاط ضعف أخرى مثل TH-04.
الأصل المتأثر	https://portal.example.com
التصنيف	OWASP Top 10 2025 A02: Security Misconfiguration، و CWE-693
تاريخ الاكتشاف	13 سبتمبر 2026
جهد الإصلاح	منخفض
الحالة	**لم تُعالج**

الوصف

لا تتضمن ردود البوابة ثلاث ترويسات تطلب من المتصفحات تطبيق حماية إضافية، وهي `Content-Security-Policy` و`X-Content-Type-Options` و`Referrer-Policy`.

وترسل البوابة الترويسة `Strict-Transport-Security`، وهذا جيد.

الأثر

لا أثر مباشراً لذلك. لكن وجود سياسة Content Security Policy يجعل تحويل نقطة ضعف مثل TH-04 إلى هجوم فعلي أصعب كثيراً، فالترويسات طبقة حماية ثانية قليلة الكلفة.

خطوات إعادة الاختبار

1. اطلبوا `https://portal.example.com/` واقرؤوا ترويسات الاستجابة.
2. الترويسات `Content-Security-Policy` و`X-Content-Type-Options` و`Referrer-Policy` غير موجودة.

الأدلة

```
GET / HTTP/1.1
Host: portal.example.com

HTTP/1.1 200 OK
Content-Type: text/html; charset=utf-8
Strict-Transport-Security: max-age=31536000; includeSubDomains
Cache-Control: no-store
```

التوصية

أرسلوا الترويستين `X-Content-Type-Options: nosniff` و`Referrer-Policy: strict-origin-when-cross-origin` مع كل استجابة.

- ابدؤوا تطبيق سياسة Content Security Policy في وضع الإبلاغ فقط، وأزيلوا الشيفرة المضمّنة في الصفحات كلما كشفتها البلاغات، ثم فعّلوا السياسة.
- تحقّقوا بأدوات المطوّر في المتصفح من أن كل صفحة تحمل الترويسات الثلاث.

المراجع

- OWASP HTTP Security Response Headers Cheat Sheet: https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Headers_Cheat_Sheet.html
- OWASP Secure Headers Project: https://owasp.org/www-project-secure-headers/

الربط بالأطر

- NCA ECC: 2-15 (حماية تطبيقات الويب)
- ISO 27001: A.8.9 (إدارة الإعدادات)

5. خطة المعالجة

الأولوية	النتائج	المدة المقترحة	المسؤول
فوراً	TH-01	خلال 7 أيام	فريق التطوير
تالياً	TH-02، TH-03	خلال 30 يوماً	فريق التطوير
مُجدولة	TH-04، TH-05	خلال 90 يوماً	فريق التطوير
اعتيادية	TH-06، TH-07	دورة الإصدار القادمة	فريق التطوير، فريق البنية التحتية

6. ربط النتائج بالأطر

يوضح الجدول الضوابط التي تمسّها كل نتيجة في الأطر التي ترفعون تقاريركم وفقها، وهو دليل لفريق الامتثال لديكم، وليس رأياً تدقيقياً ولا شهادة.

النتيجة	PDPL	NCA ECC	ISO 27001
TH-01	المادة 19	2-15 ,2-2	A.8.3
TH-02	المادة 19	2-15 ,2-2	A.8.5
TH-03	المادة 19	2-15 ,2-2	A.8.5
TH-04	المادة 19	2-15	A.8.28
TH-05	المادة 19	2-2	A.8.3
TH-06	-	2-15	A.8.5
TH-07	-	2-15	A.8.9

7. نتائج إعادة الاختبار

الرقم	النتيجة	الحالة بعد إعادة الاختبار	تاريخ إعادة الاختبار	ملاحظات
TH-01	يستطيع أي عميل تنزيل فواتير جميع العملاء الآخرين	تمت المعالجة	25 أكتوبر 2026	تُعيد الواجهة الآن الرد `404` لفاتورة أي حساب آخر، وقد اختُبر ذلك بحسابَي الاختبار.
TH-02	رسائل إعادة تعيين كلمة المرور قد تحمل رابطاً إلى موقع المهاجم	تمت المعالجة	25 أكتوبر 2026	يحمل الرابط الآن عنوان البوابة دائماً، وتُهمَل الترويسة المزوّرة.
TH-03	تسجيل الدخول يقبل عدداً غير محدود من محاولات تخمين كلمة المرور	معالجة جزئية	25 أكتوبر 2026	يعمل الحد في `/v1/auth/login`، فقد أُقفل الحساب بعد عشر محاولات فاشلة. أما العنوان الأقدم `/v1/login`، الذي ما زال موقع الجوال يستخدمه، فقد قبل 1,000 محاولة دون أي حد.
TH-04	رابط مُعدّ يشغّل شيفرة المهاجم داخل البوابة	تمت المعالجة	25 أكتوبر 2026	يُرمَّز نص البحث الآن، وتظهر نصوص الاختبار نصاً عادياً.

الرقم	النتيجة	الحالة بعد إعادة الاختبار	تاريخ إعادة الاختبار	ملاحظات
TH-05	يستطيع أي عميل الاطلاع على قائمة حسابات الموظفين بعناوين بريدهم وأدوارهم	تمت المعالجة	25 أكتوبر 2026	تُعيد الواجهة الآن الرد `403` لحسابات العملاء.
TH-06	تسجيل الخروج لا يُنهي الجلسة في الخادم	خطر مقبول	25 أكتوبر 2026	قلّص العميل مدة صلاحية الرمز من 12 ساعة إلى 30 دقيقة، وقرر كتابةً بتاريخ 20 أكتوبر 2026 قبول الخطر المتبقي إلى أن يستبدل مكوّن تسجيل الدخول.
TH-07	ترويسات الحماية الخاصة بالمتصفح غير مفعّلة	لم تُعالج	25 أكتوبر 2026	ما زالت الترويسات الثلاث غائبة، ويعتزم العميل إضافتها في الإصدار القادم من واجهة المستخدم.

8. الخطوات التالية

- خطاب الإغلاق: يصدر مع هذا الإصدار من التقرير، ويوثّق حالة كل نتيجة في تاريخ إعادة الاختبار.
- ما زال قائماً: النتيجة TH-03 عولجت جزئياً، والنتيجة TH-07 لم تُعالج، وتوضح نتائج إعادة الاختبار ما تبقّى في كل منهما.
- بيانات المشروع: تُتلفها «صائد الثغرات» بعد 30 يوماً من إصدار خطاب الإغلاق، وتؤكد الإتلاف كتابةً.

الملحق (أ): تصنيف مستوى الخطر

يجمع مستوى الخطر لكل نتيجة بين احتمالية الاستغلال والأثر على أعمالكم، وفق منهجية OWASP لتقييم المخاطر، وتُذكر بجانبه الدرجة الأساسية وفق CVSS، بالإصدار المحدد في وثيقة نطاق العمل، مقياساً تقنياً معيارياً. وقد يختلف التصنيفان، لأن CVSS يقيس نقطة الضعف نفسها، بينما يعكس مستوى الخطر بياناتكم وأنظمتكم، ومستوى الخطر هو الذي يحدد ترتيب النتائج وأولويات خطة المعالجة.

الاحتمالية	المعنى
مرتفعة	يمكن استغلالها عن بُعد دون بيانات دخول، أو بحساب يستطيع أي شخص إنشاؤه، ولا تتطلب مهارة أو جهداً يُذكر.
متوسطة	تتطلب حساباً صالحاً، أو معرفة محددة، أو تفاعلاً من المستخدم، أو قدراً من الجهد.
منخفضة	تتطلب صلاحيات عالية أو وصولاً محلياً، أو ظروفاً غير معتادة، أو استغلال نقاط ضعف أخرى أولاً.

الأثر على الأعمال	المعنى
مرتفع	كشف بيانات حساسة أو بيانات شخصية بكميات كبيرة أو تعديلها، أو السيطرة على أنظمة حرجة أو حسابات المسؤولين، أو ضرر جسيم مالياً أو نظامياً أو في السمعة.
متوسط	كشف محدود لبيانات شخصية أو داخلية، أو السيطرة على حساب مستخدم عادي أو على جزء من نظام، أو تعطّل خدمة غير حرجة.
منخفض	كشف معلومات ثانوية، أو نقطة ضعف تسهّل هجمات أخرى دون ضرر مباشر.

الأثر / الاحتمالية	منخفضة	متوسطة	مرتفعة
مرتفع	متوسط	مرتفع	حرج
متوسط	منخفض	متوسط	مرتفع
منخفض	للعلم	منخفض	متوسط

الدرجة الأساسية وفق CVSS	التصنيف
من 9.0 إلى 10.0	حرج
من 7.0 إلى 8.9	مرتفع
من 4.0 إلى 6.9	متوسط
من 0.1 إلى 3.9	منخفض
0.0	لا يوجد

النتائج المصنفة «للعلم» ليس لها أثر أمني مباشر، مثل غياب أحد إجراءات تعزيز الحماية، ودرجتها وفق CVSS هي 0.0.

نُبلغ جهة التصعيد لديكم بالنتائج الحرجة خلال 24 ساعة من تأكيدها وقبل هذا التقرير. وتُعدّ النتيجة حرجة افتراضياً إذا صُنّف مستوى خطرها حرجاً أو بلغت درجتها الأساسية وفق CVSS القيمة 9.0 فأعلى، ما لم تحدد وثيقة نطاق العمل حداً آخر.

الملحق (ب): الجدول الزمني للاختبار

التاريخ	النشاط
10 سبتمبر 2026	اجتماع البدء
13 سبتمبر 2026	بدء الاختبار
13 سبتمبر 2026، 13:15	إبلاغ جهة التصعيد بالنتيجة الحرجة TH-01
15 سبتمبر 2026	انتهاء الاختبار
20 سبتمبر 2026	تسليم التقرير
22 سبتمبر 2026	جلسة العرض
25 أكتوبر 2026	إعادة الاختبار
27 أكتوبر 2026	تسليم الإصدار 1.1 من التقرير وخطاب الإغلاق

الملحق (ج): تغطية الاختبار

المجال (OWASP WSTG)	مُختبَر	النتائج
جمع المعلومات (WSTG-INFO)	نعم	لا يوجد
الإعدادات والنشر (WSTG-CONF)	نعم	TH-07
إدارة الهوية (WSTG-IDNT)	نعم	لا يوجد
المصادقة (WSTG-ATHN)	نعم	TH-02، TH-03
التفويض (WSTG-ATHZ)	نعم	TH-01، TH-05
إدارة الجلسات (WSTG-SESS)	نعم	TH-06
التحقق من المدخلات (WSTG-INPV)	نعم	TH-04
معالجة الأخطاء (WSTG-ERRH)	نعم	لا يوجد
التشفير (WSTG-CRYP)	نعم	لا يوجد
منطق الأعمال (WSTG-BUSL)	نعم	لا يوجد
جهة المستخدم (WSTG-CLNT)	نعم	TH-04
واجهات برمجة التطبيقات (WSTG-APIT)	نعم	لا يوجد