



SECURITY REPORT PLAYBOOK

01

قالب تقرير أمني

اختبار واضح ودليل يقدر غيرك يعيده

قالب كتابة ومراجعة املأ الأقسام بأدلة اختبارك الفعلي واحذف أي قسم غير مناسب المثال أدناه تعليمي وليس تقريراً عن ثغرة في خدمة حقيقية

03

اكتب

خلي غيرك يقدر يعيد النتيجة

02

اثبت

اربط كل خطوة بدليل من الاختبار

01

افهم

حدد المتوقع والفرق اللي لاحظته



اكتب تقرير يقدر غيرك يراجعه

رتب السلوك والخطوات والأثر وراجع دليلك قبل الإرسال

01 عنوان يصف السلوك والأثر

اكتب نوع الخلل + الوظيفة المتأثرة + الأثر المثبت

مثال للصياغة غياب فحص ملكية الطلب يسمح لحساب اختباري بعرض طلب حساب اختباري آخر

02 ملخص

اذكر السلوك الطبيعي والسلوك الذي لاحظته والشروط اللازمة وضح هل يتطلب حساباً أو دوراً معيناً

03 النطاق وبيئة الاختبار

- حدد الأصل والمسار والطريقة HTTP method والدور الذي استخدمته
- سجل وقت الاختبار ونسخة التطبيق إن كانت معروفة
- استخدم أسماء مثل Account A و Account B للحسابات التي تملكها
- احذف Cookies و Tokens والبيانات الشخصية من النسخة المعدة للمشاركة

04 خطوات إعادة الاختبار

- 1 جهز الحسابات والموارد المطلوبة داخل النطاق المصرح به
- 2 نفذ العملية الطبيعية من صاحب المورد وسجل الطلب المرجعي Baseline
- 3 غير متغيراً واحداً من جلسة الحساب الآخر مع توضيح المورد المطلوب
- 4 قارن النتيجة المتوقعة بالنتيجة الفعلية
- 5 تحقق من البيانات أو الحالة المحفوظة على السيرفر HTTP 200 وحده لا يثبت الخلل



الدليل والأثر والمراجعة

رتب السلوك والخطوات والأثر وراجع دليلك قبل الإرسال

05 الأدلة

لكل خطوة الطلب المهم الجزء الدال من الاستجابة والحساب المستخدم وضح الربط بين معرف المورد وصاحبه استخدم صورا واضحة ومقطعا قصيرا عند الحاجة ولا تجعل الفيديو بديلا للخطوات المكتوبة

06 الأثر وحدود الاستنتاج

اذكر ما أثبته تحديدا قراءة تعديل تنفيذ إجراء أو تغيير حالة فرق بين الدليل والاحتمال لا تستنتج الوصول لكل المستخدمين من تجربة محدودة ولا تضع رقم خسائر بلا دليل

07 توصية معالجة

اربط التوصية بسبب الخلل في مثال ملكية الطلب تحقق على السيرفر من صلاحية المستخدم على المورد عند كل عملية حساسة مع اختبارات تمنع الرجوع للخلل

08 مراجعة قبل الإرسال

- الهدف والاختبار داخل النطاق
- الخطوات قابلة للتكرار من شخص آخر
- النتيجة المتوقعة والفعلية واضحتان
- الأسرار والبيانات الخاصة محذوفة من النسخة المشتركة
- الأثر مرتبط بالأدلة والتقييم لا يتجاوز ما أثبته
- العنوان والملخص لا يكرران نصا عاما لا يصف الحالة



من الاختبار لمسودة قابلة للإرسال

رتب السلوك والخطوات والأثر وراجع دليلك قبل الإرسال

الحسابات والموارد

Account A / Account B / Owner

الأصل والمسار

العنوان والملخص

الخلل + الوظيفة + الأثر المثبت + الشروط

خطوات إعادة الاختبار

التجهيز ثم Baseline ثم التغيير ثم النتيجة

الأثر وحدود الدليل

المتوقع والفعلي

الأدلة وتوصية المعالجة

اربط المرفقات بالخطوات وحدد سبب الخلل

مراجعة أخيرة

شخص تاني يقدر يعيد الاختبار؟ الأسرار محذوفة؟ الأثر على قد الي أثبتته؟ HTTP 200 لوحده مش دليل على ثغرة