قواعد الاشتباك: اختبار الاختراق وتقييم الأمان

أخصائي أمن المعلومات

2025-12-21

نظرة عامة

تحدد هذه الوثيقة قواعد الاشتباك لإجراء اختبار الاختراق وتقييم أمان أنظمة المعلومات. تضع الوثيقة إطار عمل للتعاون بين العميل وفريق الاختبار، مما يضمن الأمان والشرعية وفعالية العملية.

أهداف الوثيقة

الهدف الأساسي — ضمان اختبار محكوم ومصرح به مع أدنى المخاطر على الأنظمة الإنتاجية

تضمن قواعد الاشتباك: - **أمان** الأنظمة الإنتاجية - **الامتثال** للمتطلبات القانونية - **التواصل الشفاف** بين جميع الأطراف - **الاختبار المحكوم** والمصرح به

.

معلومات الاتصال

المؤسسة العميلة

الدور	تفاصيل الاتصال
جهة الاتصال الأساسية	
المنصب	_____
الهاتف المحمول	_____
البريد الإلكتروني	_____
جهة الاتصال الاحتياطية	
المنصب	_____
الهاتف المحمول	_____
البريد الإلكتروني	_____

فريق الاختبار

الدور	تفاصيل الاتصال
قائد الفريق	
الهاتف المحمول	_____
البريد الإلكتروني	_____
جهة الاتصال الاحتياطية	
الهاتف المحمول	_____
البريد الإلكتروني	_____
جهة الاتصال الطارئة 24/7	
الهاتف المحمول	_____

الدور	تفاصيل الاتصال
البريد الإلكتروني	_____

.

نطاق الاختبار

الأصول المشمولة في الاختبار

البنية التحتية للشبكة: - النطاقات: _____ - النطاقات الفرعية: _____
الموارد السحابية: - _____ نطاقات IP: - _____
_____

التطبيقات والخدمات: - تطبيقات الويب: _____ - واجهات API:
الأنظمة الداخلية: _____ - _____

الأصول المستبعدة من الاختبار

⚠ **القيود الحرجة:**

- الأنظمة غير المملوكة للمؤسسة
- خدمات الطرف الثالث بدون تصريح مكتوب
- قواعد البيانات الإنتاجية (ما لم يُسمح صراحة)
- الهندسة الاجتماعية (ما لم تُوافق عليها)
- أنظمة البنية التحتية الحرجة

.

قواعد وإجراءات الاختبار

الأنشطة المصرح بها

طرق الاختبار المعتمدة:

- فحص الثغرات الأمنية
- اختبار الاختراق اليدوي
- اختبار تطبيقات الويب
- اختبار واجهات API
- تحليل تكوين السحابة
- اختبار أمان الشبكة
- التحقق من سياسات كلمات المرور

الأنشطة المحظورة

× **الإجراءات المحظورة بشدة:**

- هجمات رفض الخدمة (DoS/DDoS)
- التسلل الفيزيائي
- الهندسة الاجتماعية بدون تصريح صريح
- هجمات القوة الغاشمة بدون تحديد المعدل
- الإجراءات التي قد تسبب فساد البيانات
- الوصول غير المصرح به للبيانات الشخصية

.

قيود الحمولة

القيود التقنية للأنظمة الإنتاجية

حدود الحمولة الحرجة: ⚡

المعامل	القيد	الملاحظات
الحد الأقصى للطلبات في الثانية	_____	لمنع التحميل الزائد
الاتصالات المتزامنة	_____	حد الاتصالات المتوازية
حجم الحمولة	_____	الحد الأقصى لحجم البيانات
مهلة الاتصال	_____	وقت انتظار الاستجابة

القيود الزمنية

جدولة الاختبار المكثف: 🕐

- **الفحص الشامل**: خارج ساعات العمل فقط
- **اختبار Fuzzing**: _____ (تحديد النوافذ الزمنية)
- **اختبار الحمولة**: إشعار مسبق مطلوب
- **الماسحات الآلية**: تحديد المعدل خلال ساعات العمل

مراقبة الحمولة

التحكم في تأثير النظام: - مراقبة المعالج والذاكرة للأنظمة المستهدفة - تتبع وقت استجابة التطبيق - التحكم في عرض النطاق الترددي للشبكة - التوقف الفوري عند تجاوز الحدود 📊

.

الأساس القانوني

الأساس القانوني للاختبار

المبرر القانوني: ⚖

> جميع أنشطة اختبار الاختراق تُنفذ حصرياً بناءً على تصريح مكتوب من ممثل مخول للمؤسسة العميلة

الأسس الوثائقية: - اتفاقية خدمة موقعة - قواعد الاشتباك هذه - المواصفات التقنية التي تصف نطاق الاختبار - اتفاقيات إضافية (عند الضرورة)

تحديد المسؤولية

إعفاء من المسؤولية: 🛡

فريق الاختبار معفى من المسؤولية عن: - عدم توفر النظام المؤقت نتيجة للاختبار المصرح به - اكتشاف الثغرات الموجودة قبل بدء الاختبار - الإجراءات المنفذة بدقة ضمن نطاق الاختبار المتفق عليه - الخسائر غير المباشرة المتعلقة بتحديد مشاكل الأمان

الامتثال القانوني

الامتثال التنظيمي: - الالتزام بتشريعات حماية البيانات الشخصية - الامتثال لمعايير الأمان 🏷 الصناعية - التوافق مع الممارسات الدولية لاختبار الاختراق - توثيق جميع الإجراءات لأغراض التدقيق

.

مصفوفة خطورة الثغرات

تصنيف مستوى المخاطر

نظام التقييم المعياري:

المستوى	الوصف	أمثلة الثغرات	وقت المعالجة
P0 - حرج	تهديد أمني فوري	RCE, SQL Injection, Authentication Bypass	24-48 ساعة
P1 - عالي	انتهاك أمني خطير	XSS, LFI, Privilege Escalation	1-2 أسبوع
P2 - متوسط	مخاطر معتدلة	Security Misconfiguration, CSRF	شهر واحد
P3 - منخفض	مخاطر دنيا	Information Disclosure, Weak Ciphers	3 أشهر
P4 - إعلامي	توصيات للتحسين	Best Practices, Hardening	حسب الإمكان

معايير التقييم

عوامل تحديد الخطورة: - **التأثير**: الضرر المحتمل من الاستغلال - **الاحتمالية**: سهولة 📈 استغلال الثغرة - **النطاق**: عدد الأنظمة المتأثرة - **إمكانية الوصول**: متطلبات الوصول للاستغلال

إجراء التصعيد

الاستجابة الطارئة للنتائج الحرجة: ⚡ 1. **P0-P1**: إشعار فوري بالهاتف + البريد الإلكتروني 2. **P2**: إشعار خلال يوم العمل 3. **P3-P4**: إدراج في التقارير المنتظمة

.

أدوات الاختبار المصرح بها

مجموعة الأدوات الأساسية

الأدوات الأساسية:

الفئة	الأداة	الغرض	الإصدار
ماسحات الثغرات	Nessus	الفحص الآلي	_____
	OpenVAS	فحص الشبكة والتطبيقات	_____
	Qualys VMDR	الفحص السحابي	_____

الفئة	الأداة	الغرض	الإصدار
اختبار الويب	Burp Suite Professional	اختبار تطبيقات الويب	_____
	OWASP ZAP	تحليل أمان تطبيقات الويب	_____
	Nikto	فحص خوادم الويب	_____
اختبار الشبكة	Nmap	فحص المنافذ والخدمات	_____
	Masscan	الفحص عالي السرعة	_____
الاستغلال	Metasploit Framework	اختبار الاستغلال	_____
	Cobalt Strike	محاكاة الهجمات ((بالاتفاق	_____

الأدوات الإضافية

البرامج المتخصصة (بالاتفاق): - **الهندسة الاجتماعية** 🛠: SET, Gophish ((بإذن صريح فقط) - **الشبكات اللاسلكية**: Aircrack-ng, Kismet - **تطبيقات الهاتف المحمول**: MobSF, Frida - **أمان السحابة**: ScoutSuite, Prowler

قيود الأدوات

الأدوات المحظورة أو المقيدة: - الماسحات غير المصرح بها DDoS - ⚠ أدوات هجمات بإعدادات عدوانية - أدوات كسر كلمات المرور بدون حدود معدل - أي برنامج غير متفق عليه مع العميل

.

تحديد هوية فريق الاختبار

القوائم البيضاء لأنظمة الدفاع

🔍 أمر بالغ الأهمية لمنع حجب الاختبار المصرح به:

معامل التحديد	القيمة	الغرض
عناوين IP المصدر	_____	عناوين IP ثابتة للقائمة البيضاء WAF/IPS
نطاقات الشبكات الفرعية	_____	شرائح شبكة الفريق الإضافية
سلاسل User-Agent	_____	معرفات محددة لماسحات الويب
مفاتيح SSH	_____	المفاتيح العامة للوصول المصرح به

المعرفات الخاصة

🏷 علامات للتسجيل والمراقبة:

- **بادئة طلبات الاختبار**: _____
- **خاصة**: _____ **رؤوس HTTP**
- **معرفات الجلسة**: _____
- **علامات في الحمولة**: _____

التنسيق مع الفريق الأزرق

التفاعل مع فريق الدفاع: - إشعار مسبق ببدء الاختبار - قائمة جهات اتصال مركز عمليات الأمان (SOC) - إجراء تأكيد شرعية النشاط - بروتوكول إيقاف الاختبار الطارئ

.

تعريف الاختبارات عالية المخاطر

تصنيف العمليات المحفوفة بالمخاطر

⚠ **اختبارات عالية المخاطر تتطلب اهتماماً خاصاً:**

فئة الاختبار	الوصف	نافذة التنفيذ	التدابير الإضافية
هجمات القوة الغاشمة	تخمين كلمات المرور/أرقام PIN	خارج ساعات العمل فقط	تحديد المعدل، مراقبة الحجب
التطبيقات Fuzzing	إرسال بيانات غير صحيحة	_____	التحكم في استقرار النظام
استغلال الثغرات	تنفيذ إثبات المفهوم	بالاتفاق	إشعار فوري عند النجاح
اختبار DoS	التحقق من مقاومة الحمولة	بيئة الاختبار فقط	اتفاق مسبق مطلوب

نوافذ خدمة الاختبارات الحرجة

🕐 **فترات زمنية خاصة:**

- **النافذة الأساسية للاختبارات المحفوفة بالمخاطر**: _____
- **النافذة الاحتياطية**: _____
- **النافذة الطارئة (بالاتفاق)**: _____
- **الفترات المحظورة**: _____

اختبار جانب العميل

حماية المستخدمين النهائيين:

- **محاكاة التصيد**: موافقة مكتوبة من الموارد البشرية فقط
- **اختبار المتصفحات**: أجهزة اختبار معزولة
- **الهندسة الاجتماعية**: نطاق محدود بدقة
- **حماية البيانات الشخصية**: تجنب الوصول للمعلومات الشخصية

.

المنهجية التقنية

المعايير والتصنيفات

📊 المعايير الدولية المستخدمة:

المعيار	الإصدار	التطبيق
CVSS	v3.1/4.0	تقييم خطورة الثغرات
OWASP Top 10	2021	تطبيقات الويب
NIST إطار عمل الأمن السيبراني	v1.1	المنهجية العامة
OSSTMM	v3	منهجية الاختبار
PTES	v1.0	معيار اختبار الاختراق

نموذج الاختبار

🔍 مستوى الوصول للمعلومات:

- ☐ **الصندوق الأسود** - بدون معرفة مسبقة بالنظام
- ☐ **الصندوق الرمادي** - وصول جزئي للوثائق/البنية
- ☐ **الصندوق الأبيض** - وصول كامل للكود والبنية

النموذج المختار: _____

تقييم CVSS

📈 معايير تقييم الثغرات:

- **المقاييس الأساسية**: متجه الهجوم، التعقيد، الامتيازات، تفاعل المستخدم
- **المقاييس الزمنية**: توفر الاستغلال، مستوى الإصلاح
- **المقاييس البيئية**: التأثير على بيئة العميل المحددة
- **القيم العتبة**: P0 (9.0-10.0), P1 (7.0-8.9), P2 (4.0-6.9), P3 (0.1-3.9)

.

الجوانب القانونية الإضافية

نقل البيانات عبر الحدود

🌍 الامتثال الدولي:

وأنظمة حماية CCPAو GDPR عند العمل مع فرق اختبار دولية، يتم ضمان الامتثال لـ البيانات الأخرى المطبقة

المتطلبات القضائية: - **بلد قاعدة الفريق**: _____ - **التشريع المطبق**: قرار الكفاية - / (SCC) **آليات نقل البيانات**: البنود التعاقدية المعيارية - _____ **توطين البيانات**: _____

الامتثال للمعايير الدولية

الامتثال التنظيمي: ◇

المعيار/التنظيم	حالة الامتثال	الملاحظات
GDPR (الاتحاد الأوروبي)	_____	حماية البيانات الشخصية
ISO 27001	_____	نظام إدارة أمن المعلومات
SOC 2 Type II	_____	ضوابط الأمان
PCI DSS	_____	أنظمة الدفع

حقوق التدقيق

التحكم في عمليات معالجة البيانات: 🔍

للعميل الحق في: - التحقق من إجراءات حذف البيانات بعد إكمال المشروع - طلب تأكيد تدمير المعلومات السرية - تدقيق تدابير أمان فريق الاختبار - الحصول على شهادات الامتثال للمعايير المطبقة

.

عملية الاستجابة للحالات الحرجة

خوارزمية الاستجابة الطارئة

إجراء خطوة بخطوة للحوادث الحرجة:

1. اكتشاف الحالة الحرجة
   ↓
2. إيقاف الاختبار فوراً
   ↓
3. إشعار العميل (خلال 15 دقيقة)
   ↓
4. تقييم التأثير والضرر
   ↓
5. اتخاذ قرار المتابعة
   ↓
6. توثيق الحادث
   ↓
7. تحليل الأسباب الجذرية والتدابير التصحيحية

مصفوفة التصعيد

جهات الاتصال حسب مستويات الخطورة:

المستوى	وقت الاستجابة	طريقة التواصل	المسؤول
P0 - حرج	15 دقيقة	هاتف + رسالة نصية + بريد إلكتروني	_____ _____
P1 - عالي	ساعة واحدة	هاتف + بريد إلكتروني	_____

المستوى	وقت الاستجابة	طريقة التواصل	المسؤول
			_____
P2 - متوسط	4 ساعات	بريد إلكتروني + Slack/Teams	_____ _____
P3 - منخفض	24 ساعة	بريد إلكتروني	_____ _____

معايير إيقاف الاختبار

محفزات إيقاف العمل التلقائية:

- عدم توفر الخدمات الحرجة لأكثر من 5 دقائق
- اكتشاف استغلال نشط للثغرات من قبل أطراف ثالثة
- تجاوز حدود الحمولة المتفق عليها
- طلب الإيقاف من أي ممثل مخول

.

التعامل مع الأدلة والتنظيف

بروتوكول التعامل مع الأدلة

التعامل مع الأدلة - متطلبات أمنية صارمة: 🔒

المرحلة	المتطلبات	المسؤول
الجمع	التشفير، التجميع، الطوابع الزمنية	المختبر
التخزين	تخزين معزول، التحكم في الوصول	مدير المشروع
النقل	قنوات آمنة، تأكيد الاستلام	كلا الطرفين
التدمير	حذف لا رجعة فيه، شهادة التدمير	فريق الاختبار

خطة التنظيف بعد الاختبار

تنظيف ما بعد الاختبار - إجراءات إلزامية:

إزالة الكائنات المُنشأة: - [ ] حسابات المستخدمين التجريبية - [ ] الملفات والنصوص المرفوعة - [ ] التكوينات المؤقتة - [ ] قواعد البيانات والجداول التجريبية

استعادة الحالة الأصلية: - [ ] التراجع عن تغييرات التكوين - [ ] إزالة الشهادات التجريبية - [ ] تنظيف سجلات الاختبار (بالاتفاق) - [ ] استعادة النسخ الاحتياطية (عند الضرورة)

شهادة تدمير البيانات

التأكيد الوثائقي:

عند إكمال المشروع، يقدم فريق الاختبار: - شهادة الحذف اللارجعي لجميع بيانات العميل - تقرير عن إجراءات التنظيف المنفذة - تأكيد الامتثال لمعايير تدمير البيانات (DoD 5220.22-M أو ما يعادلها)

.

جدولة الاختبار

الإطار الزمني

المعامل	القيمة
تاريخ البدء	_____
تاريخ الانتهاء	_____
نافذة الاختبار	_____
المنطقة الزمنية	_____
الإحاطة اليومية	_____

بروتوكول التواصل

التحديثات المنتظمة: - تقارير الحالة اليومية - ملخصات التقدم الأسبوعية - إشعارات طارئة للنتائج الحرجة

.

التعامل مع الحوادث

إجراء الاستجابة للحوادث

في حالة عدم استقرار النظام أثناء الاختبار:

1. **الإيقاف الفوري** للاختبار من قبل الفريق
2. **إشعار** المؤسسة العميلة
3. **اتخاذ القرار** من قبل جهة الاتصال الطارئة بشأن المتابعة
4. **توثيق الحادث**

معايير إيقاف الاختبار

شروط وقف العمل: - اكتشاف ثغرات حرجة - عدم استقرار الأنظمة الإنتاجية - تجاوز نطاق الاختبار المتفق عليه - طلب من العميل 🔍

.

التعامل مع البيانات والسرية

مبادئ التعامل مع البيانات

السرية — الأولوية رقم واحد عند معالجة أي معلومات

التزامات فريق الاختبار: - البيانات الحساسة لا تُحفظ إلا عند الضرورة - جميع البيانات المجمعة مشفرة - البيانات تُحذف بعد تسليم التقرير - تجنب الوصول للبيانات الشخصية

اتفاقية عدم الإفشاء

جميع المشاركين في الاختبار يلتزمون بـ: - الحفاظ على سرية المعلومات المحصلة - عدم إفشاء النتائج لأطراف ثالثة - استخدام البيانات حصرياً لأغراض الاختبار

.

متطلبات التقارير

هيكل التقارير

التقارير المؤقتة: - تحديثات يومية أو أسبوعية - حالة إنجاز المهام - النتائج الأولية

التقارير النهائية: - **التقرير التقني** — وصف مفصل للثغرات - **تقرير الإدارة** — توصيات للقيادة - **الملخص التنفيذي** — نظرة عامة موجزة للإدارة العليا

تنسيق عرض النتائج

الهيكل المعياري: - تصنيف الثغرات حسب الخطورة - توصيات المعالجة - الأطر الزمنية 📊 للإصلاح - مقاييس الأمان

.

قبول المخاطر

تأكيد المؤسسة العميلة

المؤسسة العميلة تؤكد فهمها أن:

- الاختبار قد يكشف ثغرات حرجة
- بعض الاختبارات قد تسبب انخفاضاً مؤقتاً في الأداء
- جميع الإجراءات مصرح بها ومتفق عليها
- النتائج ستُستخدم لتحسين الأمان

.

قائمة فحص الجاهزية للاختبار

الأنشطة التحضيرية

- ☐ تحديد نطاق الاختبار
- ☐ تعيين جهات الاتصال المسؤولة
- ☐ الاتفاق على جدول العمل
- ☐ توقيع جميع الوثائق الضرورية
- ☐ إعداد قنوات التواصل
- ☐ تحضير بيئة الاختبار (عند الضرورة)
- ☐ إجراء إحاطة لفريق الاختبار

نقاط التحكم أثناء الاختبار

- ☐ اجتماعات الحالة اليومية
- ☐ مراقبة الأنظمة الإنتاجية
- ☐ توثيق جميع الإجراءات
- ☐ الالتزام بالجدول الزمني
- ☐ التواصل المنتظم مع العميل

.

التوقيعات والموافقات

ممثل المؤسسة العميلة

الحقل	القيمة
الاسم والمنصب	_____
التوقيع	_____
التاريخ	_____

قائد فريق الاختبار

الحقل	القيمة
الاسم والمنصب	_____
التوقيع	_____
التاريخ	_____

.

نموذج الاتصال الطارئ

معلومات الاستجابة السريعة

المعامل	تفاصيل الاتصال
جهة الاتصال الأساسية للعميل	_____
جهة الاتصال الثانوية للعميل	_____
قائد الاختبار	_____
الخط الطارئ 24/7	_____

إجراء الاتصال الطارئ

1. الممثل الأساسي للعميل — **الاتصال الأولي**
2. جهة الاتصال الثانوية — **عند عدم التوفر**
3. الخط الطارئ 24/7 — **الحالات الحرجة**
4. جميع الاتصالات **توثيق**

.

هذه الوثيقة هي اتفاقية ملزمة قانونياً بين الأطراف ويجب أن توقع من قبل جميع المشاركين في عملية اختبار الاختراق.