



НАРЪЧНИК ЗА КУПУВАЧА

Контролен списък при избор на тест за проникване

Не всички „тестове за проникване“ са еднакви. Много от тях са сканиране за уязвимости с титулна страница. Използвайте този контролен списък, когато избирате доставчик — отговорите отличават истинското тестване от изхода на скенер.

PXLSecurity LTD. · София, България · pxlsec.com · Офанзивна сигурност от 2014 г.



НАРЪЧНИК ЗА КУПУВАЧА

Контролен списък при избор на тест за проникване

Не всички „тестове за проникване“ са еднакви. Много от тях са сканиране за уязвимости с титулна страница. Използвайте този контролен списък, когато избирате доставчик — отговорите отличават истинското тестване от изхода на скенер.

Преди да купите — попитайте доставчика

- ✓ Кой извършва тестването и какви практически сертификати притежава?
- ✓ Може ли да видя анонимизиран примерен отчет?
- ✓ Ще откриете ли дефекти в бизнес логиката и контрола на достъпа, а не само известни CVE?
- ✓ Колко дни ръчно тестване са включени?
- ✓ Включен ли е повторен тест след отстраняване, без допълнително заплащане?
- ✓ Как определяте обхвата и фиксирана ли е цената, преди работата да започне?
- ✓ Как се съобщават критичните констатации по време на теста?
- ✓ Можете ли да съотнесете констатациите към нашата рамка (ISO 27001, SOC 2, PCI DSS, DORA, NIS2)?

Тревожни признаци

- Оферта, базирана само на броя IP или URL адреси, без разговор за целите.
- Няма посочен тестер — работата е „възложена на екипа“.
- Отчет, който е таблица с критичност, без стъпки за възпроизвеждане или бизнес въздействие.
- Няма повторен тест или той се продава като скъпа добавка.
- Неясни отговори за тестването на бизнес логика или контрол на достъпа.

Добри признаци

- ✓ Старши тестери, посочени по име, с практически сертификати (OSCP, OSWE, CRT0, CREST...).
- ✓ Примерен отчет с навързани констатации, доказателства и конкретни поправки.
- ✓ Фиксиран обхват и цена, договорени писмено, с включен повторен тест.

-
- ✓ Ясни правила на ангажимента и съобщаване на критичните проблеми в същия ден.

Този контролен списък е на PXLSec — независима фирма за офанзивна сигурност, която тества от 2014 г. Въпроси? Пишете на hello@pxlsec.com или вижте pxlsec.com/bg/methodology.

Работете с PXLSec

Независимо офанзивно тестване на сигурността от 2014 г. — тестване за проникване, red teaming и сигурна разработка, с доказателство за всяка констатация и повторен тест, който потвърждава поправката.

Заявете предложение: pxlsec.com/bg/contact · hello@pxlsec.com

PXLSecurity LTD. · бул. „Васил Левски“ 12, 1142 София, България · VAT BG203239331