



НАРЪЧНИК ЗА КУПУВАЧА

Как да четете отчет от тест за проникване

Добрият отчет е написан, за да се действа по него. Ето какво означава всяка част, как да приоритизирате и какви въпроси да зададете на разговора по резултатите.

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



НАРЪЧНИК ЗА КУПУВАЧА

Как да четете отчет от тест за проникване

Добрият отчет е написан, за да се действа по него. Ето какво означава всяка част, как да приоритизирате и какви въпроси да зададете на разговора по резултатите.

Разделите, които ще видите

- Резюме за ръководството — общият риск и основните теми, за ръководството. Две страници, без жаргон.
- Обхват и методология — какво е тествано, как, и какво не е.
- Констатации — всяка с критичност, засегнат компонент, доказателство, стъпки за възпроизвеждане и поправка.
- План за отстраняване — констатациите, подредени по действителен риск, а не само по суров резултат по CVSS.
- Резултати от повторния тест — писмено потвърждение какво е отстранено.

Как да приоритизирате

Критичността е отправна точка, не отговор. „Средна“ в процеса на плащане може да е по-важна от „висока“ във вътрешен инструмент. Съчетайте критичността на констатацията със стойността на това, което излага, и с това колко лесно е достижима.

- ✓ Първо отстранете всичко, което води до компрометиране на акаунт или данни.
- ✓ Групирайте констатациите по първопричина — една поправка често затваря няколко.
- ✓ Следете отстраняването и планирайте повторния тест.
- ✓ Запазете отчета; одиторът и клиентите ви може да го поискат.

Въпроси за разговора по резултатите

- Кое е най-важното нещо за отстраняване тази седмица?
- Кой констатации са навързани — и прекъсва ли веригата отстраняването на една от тях?
- Какво би предотвратило повтарянето на тези проблеми, а не само този конкретен случай?
- Какво не успяхте да тествате и трябва да включим в следващия обхват?

От PXLSec. Всеки отчет, който предаваме, включва разговор по резултатите и безплатен повторен тест. Вижте примерен отчет на pxlsec.com/bg/get-the-report.

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