

ИНФОРМАЦИОНЕН ЛИСТ ЗА УСЛУГАТА

Тестване за проникване

Ръчни тестове на приложения, API, инфраструктура и облачни среди. Доказваме как уязвимостите могат да бъдат използвани и свързани в атака, след което даваме конкретни мерки и проверяваме корекциите.

ПОДХОДЯЩО ЗА	Пускане на нови продукти, въпросници за сигурност от клиенти, доказателства за съответствие
ПОЛУЧАВАТЕ	Резюме за ръководството, технически доклад, писмо за повторен тест
ОБХВАЩА	Уеб, мобилни, API, мрежи, облак

Отвъд скенера

Автоматизираните инструменти откриват очевидното. Истинските нападатели свързват малки слабости в сериозна компрометация. Нашите тестери работят ръчно: картографират логиката на приложението, злоупотребяват с границите на доверие и комбинират констатациите, за да покажат действителния обхват на поражението, а не просто една оценка по CVSS.

Обхватът на всеки ангажимент се определя според вашите цели и риск, работата се извършва безопасно и се предава с ясни, възпроизводими доказателства, по които екипът ви може да действа незабавно.

Какво тестваме

- Уеб приложения и SaaS платформи
- Мобилни приложения за iOS и Android
- REST и GraphQL API-та
- Външни и вътрешни мрежи
- Облачни среди в AWS, Azure и GCP
- Thick-client и настолен софтуер

Как протича

- Обхват и правила — Целите, обектите и правилата на ангажимента се договарят предварително.
- Проучване и картографиране — Картографираме атакуваната повърхност и разбираме как системата работи в действителност.
- Ръчна експлоатация — Практическо тестване и безопасна експлоатация, за да докажем верижно, реално въздействие.
- Доклад и повторен тест — Приоритизирани констатации, среща за обсъждане на резултатите и безплатен повторен тест след отстраняването.

Какво получавате

- Резюме за ръководството — Бизнес рискът, представен ясно за ръководството и управителния съвет.
- Технически доклад — Всяка констатация със степен на критичност, доказателства и стъпки за възпроизвеждане.
- Приоритизирани корекции — Насоки за отстраняване, готови за разработчиците и подредени по реален риск.
- Писмо за повторен тест — Проверяваме вашите корекции и потвърждаваме писмено закриването им — включено стандартно.

Методологии и стандарти, на които се опираме

OWASP WSTG · OWASP MASVS · OWASP API Security Top 10 · PTES · NIST SP 800-115 · OSSTMM · CWE

Старши тестери. Доказателства за всяка констатация. Включен повторен тест. Минимум пет дни тестване. Обхват и примерни доклади — pxlsec.com/bg/services/penetration-testing.