



ПРИМЕР ОТ ПРАКТИКАТА

Защитено, но недовършено: приложение за транзакции с висока стойност

Банкиране · Тест на уеб приложение с предоставени потребителски акаунти

16 констатации и план за разделение на отговорностите

Анонимизиран съгласно NDA. Клиентът и идентифициращите детайли са премахнати. PXLSecurity LTD. · София, България · pxlsec.com



ПРИМЕР ОТ ПРАКТИКАТА

Защитено, но недовършено: приложение за транзакции с висока стойност

Сектор	Банкиране
Ангажимент	Тест на уеб приложение с предоставени потребителски акаунти
Резултат	16 констатации и план за разделение на отговорностите

16	1	0
констатации	оператор можеше сам да пренасочи плащания	дефекти при инжектиране и оторизация

ПРЕДИЗВИКАТЕЛСТВОТО

Банка поиска тест от тип „сива кутия“ на уеб приложение за платежни операции от гледната точка на най-високата му стандартна административна роля.

КАК СЕ РАЗВИ

1. Тествахме с предоставен акаунт с най-високата стандартна административна роля.
2. Потвърдихме ефективността на основните защиты срещу инжектиране и на проверките за достъп до обекти.
3. Открихме поле от потребителския профил, чиято стойност се експортираше като формула и се изпълняваше при отваряне на електронната таблица.
4. Открихме роля, описана като „самообслужване на профила“, която всъщност позволяваше пълно управление на потребители и роли.
5. Операции с високо въздействие - промяна на дата, повторно изпращане, спиране, маршрутизиране и стартиране на плащания - не изискваха независимо одобрение от второ лице.

ОСНОВНИ КОНСТАТАЦИИ

High	Липса на разделение на отговорностите при операции с високо въздействие
High	Подвеждащ етикет на роля дава скрито пълно администриране
Medium	Съхранено инжектиране на формула за електронна таблица в експорта на данни
Positive	Контролите срещу инжектиране и за оторизация на ниво обект издържаха тестовете

ВЪЗДЕЙСТВИЕ

Пропуски в разделението на отговорностите можеха да позволят на един оператор да извършва или спира платежни операции без независимо одобрение. Рискът оставаше въпреки силните технически защиты на приложението.

РЕЗУЛТАТ

Докладвахме 16 констатации, свързани с разделението на отговорностите, описанията на ролите и безопасния експорт. Предоставихме конкретен план за одобрение от второ лице и преработка на ролите според принципа на минималните права.

ТЕХНИКИ

Бизнес логика · Разделение на отговорностите · Инжектиране на формули в CSV ·
Картографиране на правата по роли

УСЛУГИ

Тестване за проникване · Тестове за проникване за одитни и регулаторни изисквания

Работете с PXLSec

Независимо офанзивно тестване на сигурността от 2014 г. — тестване за проникване, red teaming и сигурна разработка, изпълнявани от старши инженери, 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