



ПРИМЕР ОТ ПРАКТИКАТА

24-часов токен на всички погрешни места

Здравеопазване · Тест на уеб приложение и API с предоставени акаунти

План за преработка на жизнения цикъл на токените

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

ПРИМЕР ОТ ПРАКТИКАТА

24-часов токен на всички погрешни места

Сектор	Здравеопазване
Ангажимент	Тест на уеб приложение и API с предоставени акаунти
Резултат	План за преработка на жизнения цикъл на токените

1	24 ч.	0
тип токени, разкрит по 3 начина	срок на валидност на токена	токени, отнети при изход

ПРЕДИЗВИКАТЕЛСТВОТО

Платформа за множество клиентски организации в регулиран сектор поиска тест на уеб приложението, API и OAuth удостоверяването с акаунти за няколко потребителски роли.

КАК СЕ РАЗВИ

1. Проверихме уеб приложението, API и OAuth удостоверяването с акаунти за няколко роли.
2. Открихме API токен с валидност 24 часа във фрагмента на URL адреса при SSO вход.
3. Същият тип токен беше достъпен в глобална JavaScript променлива на страницата.
4. Токен можеше да се получи и чрез включения поток resource owner password grant за публичен клиент, с дълготрайни токени за подновяване.
5. Потвърдихме, че изходът от приложението не отнема токените. Откраднат токен можеше да продължи да се използва до изтичането му.
6. Открихме GraphQL крайна точка, която разкриваше схемата въпреки ограничената си функционалност, и работен процес за поръчки, който приемаше статус и дати, зададени от клиента.

ОСНОВНИ КОНСТАТАЦИИ

High	Дълготраен токен за здравни данни, изложен чрез фрагмент в адреса и глобална променлива
High	Включен resource owner password grant върху публичен клиент
Medium	Токените не се отнемат при изход
Medium	Работният процес за клинични назначения се доверява на статус и дата, подадени от клиента

ВЪЗДЕЙСТВИЕ

Получаването на токен от клиентската част позволяваше достъп до свързаните записи в продължение на 24 часа.

РЕЗУЛТАТ

Решението обхваща жизнения цикъл на токените: authorization code с PKCE, кратка валидност, отнемане от сървъра и премахване на токените от адресите и глобалните променливи. Добавянето на сървърни проверки на работния процес прекъсна веригата от слабости.

ТЕХНИКИ

OAuth/OIDC · Изтичане на токени · Разкриване чрез GraphQL · Заобикаляне на бизнес логиката · BOLA/IDOR

УСЛУГИ

Тестване за проникване · Сигурна разработка

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