



ПРИМЕР ОТ ПРАКТИКАТА

Административният слой на AI без проверка за администраторски права

Доставчик на корпоративен софтуер · Тест за проникване в AI / LLM
(удостоверен, без административни права)

1 висока, 2 средни, 4 ниски — една първопричина

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



ПРИМЕР ОТ ПРАКТИКАТА

Административният слой на AI без проверка за администраторски права

Сектор	Доставчик на корпоративен софтуер
Ангажимент	Тест за проникване в AI / LLM (удостоверен, без административни права)
Резултат	1 висока, 2 средни, 4 ниски — една първопричина

1Н / 2М / 4Л	1	0
в рамките на седем констатации	липсваща проверка на правата в основата на всички констатации	пренасочени или извлечени реални данни

ПРЕДИЗВИКАТЕЛСТВОТО

Софтуерен доставчик беше добавил генеративни AI функции към платформата си. Тестът трябваше да провери какво може да направи служител на клиентска организация с обикновен бизнес акаунт и без административни права.

КАК СЕ РАЗВИ

1. През целия тест използвахме обикновен бизнес акаунт със сесиен токен без административна роля.
2. Административният интерфейс скриваше AI екраните само от страна на клиента. Услугите зад тях оставаха достъпни и приемаха промени въз основа на общи разрешения на ниво услуга.
3. Променихме конфигурацията за достъп до обектното хранилище на AI — крайна точка, регион, контейнер, ключ за достъп и тайна. След това я прочетохме обратно; тайните бяха само частично маскирани.
4. Със същия обикновен токен променихме конфигурацията на промптите за генеративния AI и отделното хранилище за идентификационни данни на бизнес системи.
5. Задействахме задачата за въвеждане на данни в AI и проверихме целия жизнен цикъл на модел: създаване, обучение и изтриване.
6. Потвърдихме, че липсващата проверка е пропуск: услугата за идентичност на същата платформа изискваше администраторски права и отказваше аналогична операция на същия потребител.

ОСНОВНИ КОНСТАТАЦИИ

High	Потребител без административни права може да променя и чете конфигурацията за достъп до AI хранилището
Medium	Потребител без административни права може да променя конфигурацията на промптите
Medium	Сесията остава валидна след изход
Low	Разкриване на клиентска тайна при OIDC пренасочване
Low	Крайна точка за генериране с AI без ограничение на честотата на заявките
Low	API допуска произволни източници чрез CORS
Positive	Услугата за идентичност правилно изисква администраторски права

ВЪЗДЕЙСТВИЕ

Обикновен бизнес потребител можеше да променя къде се записват данните за обучение и генериране на резултати, да пренаписва промптите за генерираното съдържание и да изтрива продукционни модели. За тези операции не се изискваше административна роля.

РЕЗУЛТАТ

Предадохме седем констатации — една висока, две средни и четири ниски — и посочихме общата първопричина. Необходима беше единна проверка за администраторски права при всяка операция, която променя състоянието в административния слой на AI. Платформата вече прилагаше такава проверка на други места. Записаните при теста стойности бяха безвредни тестови маркери, описани за премахване при предаването.

ТЕХНИКИ

Нарушен контрол на достъпа · Оторизация само от страна на клиента · Злоупотреба с AI пайплайна · Разкриване на тайни · Злоупотреба с жизнения цикъл на моделите

УСЛУГИ

Тестване за проникване в AI / LLM · Тестване за проникване

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