

# Решение СЗИ-9 Защити магазин от IDOR-читера

## Описание

"Читеры получили доступ к чужим покупкам и ключам. Почини просмотр заказа так, чтобы пользователи видели только свои заказы, а админы — могли смотреть все."

## Решение

### Анализ уязвимости

Открываем задание и видим функцию `get_order()`, которая возвращает заказ без проверки прав доступа:

```
def get_order(order_id: int, current_user_id: int, current_user_role: str) -> dict:
    order = None
    for o in ORDERS:
        if o.order_id == order_id:
            order = o
            break
    if not order:
        return None
    # БЛОК ДЛЯ РЕДАКТИРОВАНИЯ:

    # КОНЕЦ БЛОКА ДЛЯ РЕДАКТИРОВАНИЯ
    return {
        "order_id": order.order_id,
        "owner_id": order.owner_id,
        "owner_name": order.owner_name,
        "items": order.items,
        "total_diamonds": order.total_diamonds,
        "secret_key": SECRET_KEYS.get(order.order_id, "N/A")
    }
```

Проблема: любой пользователь может получить доступ к любому заказу, зная его ID.

## Решение

Добавляем проверку прав доступа после нахождения заказа:

```

def get_order(order_id: int, current_user_id: int, current_user_role: str) ->
dict:
    order = None
    for o in ORDERS:
        if o.order_id == order_id:
            order = o
            break
    if not order:
        return None
    # Проверяем, что пользователь является владельцем заказа
    if order.owner_id != current_user_id:
        return None
    return {
        "order_id": order.order_id,
        "owner_id": order.owner_id,
        "owner_name": order.owner_name,
        "items": order.items,
        "total_diamonds": order.total_diamonds,
        "secret_key": SECRET_KEYS.get(order.order_id, "N/A")
    }

```

## Получение флага

После отправки исправленного кода на проверку получаем флаг:

```
vsosh{1D0R_pr0t3ct10n_m1n3cr4ft_5h0p}
```