Уязвимости системы команды FURRY VIBES

# **Админ-панель**

**Атака: эскалация прав / IDOR**

* Вектор: прямой доступ к API типа /admin/orders/{id} без проверки ролей, небезопасные “isAdmin” флаги на фронте.
* Последствия: чтение/изменение заказов, управление движением «лифтов», отключение ограничений безопасности.

**Атака: CSRF на опасных действиях**

* Вектор: админ открывает вредоносную страницу → невидимый POST на “отправить/остановить лифт”.
* Последствия: нежелательные операции, нарушение SLA/безопасности.

**Атака: инъекции / небезопасные фильтры**

* Вектор: сырые SQL или динамические LINQ/фильтры без санитации.
* Последствия: чтение/порча БД, утечка персональных данных.

**Атака: DoS по “оперативным” эндпоинтам**

* Вектор: частые вызовы «старт/стоп/скорость».
* Последствия: деградация сервиса, блокировки.

# **Клиентское веб-приложение**

**Атака: подмена маршрутов (SPA) + небезопасный CORS**

* Вектор: злоумышленник хостит фишинговый SPA с таким же роутером; расслабленный Access-Control-Allow-Origin: \* для приватных API.
* Последствия: кража токенов/сессий, несанкционированные запросы.

**Атака: XSS через поля заказа/описание груза**

* Вектор: отображение непровалидированного HTML в кабинетах/админке.
* Последствия: кража JWT/сессий, скрытые действия от имени пользователя.

**Атака: манипуляция ценой/тарифом на фронте**

* Вектор: изменение скрытых полей/тарифа в SPA и повторная отправка.
* Последствия: занижение стоимости, фрод.

**Атака: отсутствие rate-limit на создание заказов**

* Вектор: ботнет создаёт тысячи заказов.
* Последствия: переполнение очереди, счета за инфраструктуру

# **API-шлюз (Nginx)**

**Атака: проброс внутренних хостов (SSRF через прокси/редиректы)**

* Вектор: эндпоинты загрузок/вебхуков разрешают URL-ы.
* Последствия: скан внутренней сети, доступ к метаданным.

# **Backend (ASP.NET Core)**

**Атака: уязвимые JWT/куки**

* Вектор: долгоживущие токены без aud/iss, отсутствие HttpOnly/SameSite, слабые ключи.
* Последствия: угон сессий, доступ к API.

**Атака: небезопасная сериализация / загрузки файлов**

* Вектор: обработка пользовательских файлов/форматов без проверки.
* Последствия: RCE в обработчиках, переполнение диска.
* Защита: разрешённые типы/размеры, антивирус/сканеры, хранение вне webroot, фоновые очереди.

**Атака: гонки состояний (двойная отгрузка/списание)**

* Вектор: параллельные запросы «подтвердить заказ».
* Последствия: дубликаты, нарушения инвентаря.

# **База данных (MySQL)**

**Атака: утечка резервных копий / дампов**

* Вектор: бэкапы в общедоступном бакете/сервере.
* Последствия: полная компрометация данных.

**Атака: слабые роли БД**

* Вектор: аккаунт приложения с SUPER/GRANT.
* Последствия: изменение схемы, скрытые пользователи.

# **Telegram-бот (склад)**

**Атака: компрометация токена бота**

* Вектор: токен в репозитории/логах.
* Последствия: полный контроль: выдача/приём грузов “от бота”.

**Атака: подмена пользователя / доверие к username**

* Вектор: логика авторизации завязана на ник/отправителя без привязки к БД/ролям.
* Последствия: «принять/отгрузить» груз от лица сотрудника.

**Атака: инъекции в callback-data / команды**

* Вектор: длинные callback\_data, спецсимволы.
* Последствия: обход проверок, ошибки логики.

**Атака: фрод через deep-links**

* Вектор: ссылки вида t.me/bot?start=... с подставленным грузом/заказом.
* Последствия: подбор заказов, несанкционированная отметка.