## **Broken Access Control**

## Неправильная проверка авторизации - когда система доверяет, что пользователь может делать то, что он хочет, но не проверяет, кем он является и какиеправа у него есть. Это опасно - когда злоумышленник может получить доступ к чужим данным, украсть личную информацию, использовать систему для дальнейших атак, нанести финансовый, репутационный ущерб и особенно болезненно, когда речь идёт о персональных данных, документах.

## **Реальные примеры**

## **1. Optus (Австралия), 2022**

* Пострадавших - ~ 10 миллионов клиентов.
* Что утекло: имена, даты рождения, адреса, номера телефонов, в некоторых случаях - номера водительских удостоверений и паспортов.
* Как произошло: один из факторов - API, доступный без адекватной авторизации/аутентификации. То есть API, через который можно было запрашивать данные клиентов, допускал, что любой пользователь может сделать запрос чужой информации.
* Последствия: широкая утечка PII (лично идентифицируемой информации), серьёзные риски для жертв (идентичность, мошенничество), судебные иски, крупные штрафы, серьезный удар по репутации компании. Федеральный регулятор подал иск. В бюджете Optus на борьбу с последствиями утечки было зарезервировано 140 миллионов австралийских долларов.

### **2. Snapchat, 2014**

* Утечка - ~ 4,6 миллионов аккаунтов.
* Что было нарушено: API-функция «Find Friends» позволяла сопоставлять номера телефонов с аккаунтами пользователей - злоумышленники могли перебирать/сканировать контакт-листы и выяснять, кто из контактов активно пользуется Snapchat, и связывать это с пользовательскими именами.
* Последствия: утекла персональная информация, снижен уровень доверия к сервису, негатив в медиа. Snapchatобязался улучшить меры безопасности, изменить политику конфиденциальности.

### **3. USPS (США), 2018**

* Пострадавших: до 60 млн пользователей
* Что было нарушено: залогиненный пользователь мог подменой параметров запросов просматривать чужие профили и в ряде случаев менять их данные.
* Что утекало: имена, адреса, email/телефон, идентификаторы аккаунтов.
* Последствия. Риск смены контактных данных/настроек, репутационные потери. Данный пример вошёл в подборки крупнейших гос-утечек за последние годы.

## **Анализ причин и ошибок**

Из данных примеров видно, что часто причиной Broken Access Control становятся:

1. **Пропущенные проверки на стороне сервера**Часто разработчики полагаются на клиентскую проверку, скрытие элементов интерфейса, или просто “скрытые” ссылки. Но если сервер не проверяет - злоумышленник может просто отправить запрос напрямую.
2. **Недостаточно строгие спецификации API / публичные API с чувствительными данными**Когда API сделаны “доступными” без должной авторизации.
3. **Использование предсказуемых идентификаторов, слабое управление ресурсами**Простые порядковые идентификаторы, URL - параметры с ID объекта и т.п.
4. **Ошибки в логике ролей / привилегий**Когда разработчики неправильно понимают, как должны работать роли или доступы “пробрасываются” через параметры, которые клиент может изменить.
5. **Отсутствие мониторинга и тестирования**Когда баги известны (например, Snapchat был предупреждён), но не исправлены вовремя. Или когда не ведутся логи доступа, не анализируются необычные запросы.

## **Предотвращение ошибок**

1. Всегда проверять авторизацию на сервере, не доверять интерфейсу клиента, URL, параметрам, кнопкам.
2. Принцип минимальной привилегии - пользователю давать ровно те права, что нужны, и ничего больше.
3. Использовать надежную модель ролей или политик доступа.
4. Не допускать публичных API, которые возвращают или позволяют изменять чувствительные данные без авторизации.
5. Шифровать и защищать персональные данные, особенно документы, удостоверения личности.
6. Регулярно проводить автоматизированные и ручные тестирования, целевые проверки Broken Access Control.
7. Логи + мониторинг: выявление необычного поведения, попытки доступа к чужим объектам.

## **Вывод**

Broken Access Control - не “теоретическая” угроза, а реальная, и её последствия приводят к крупным утечкам личной информации, финансовым и репутационным потерям. Часто ущерб мог быть значительно уменьшен, если бы были встроены базовые меры безопасности.