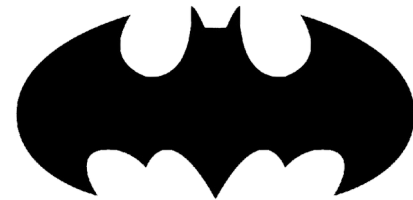


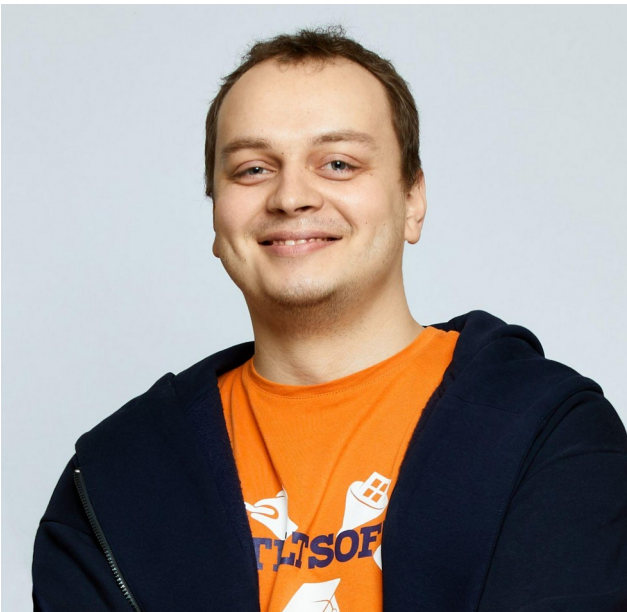
Поиск и устранение security- уязвимостей

в веб-приложениях на реальных

История о работе,
которую видят не все,
но делать её необходимо

STILTSOFT





Меня зовут Андрей, я разработчик в Stiltsoft

- Занимаюсь разработкой 4.5 года
- Люблю ходить пешком
- Пишу в open source
- Ненавижу корпоративы
- Мечтал быть детективом

STILTsoft

Компания Stiltsoft

Делаем приложения для продуктов Atlassian: Confluence, Jira, Bitbucket

- 2 офиса
- 12 лет
- 35 человек
- 25+ приложений
- 12 000+ B2B
КЛИЕНТОВ



Platinum
Top Vendor

STILTSOFT

resume@stiltsoft.co
m

Warning

1. Разработчики тоже
люди

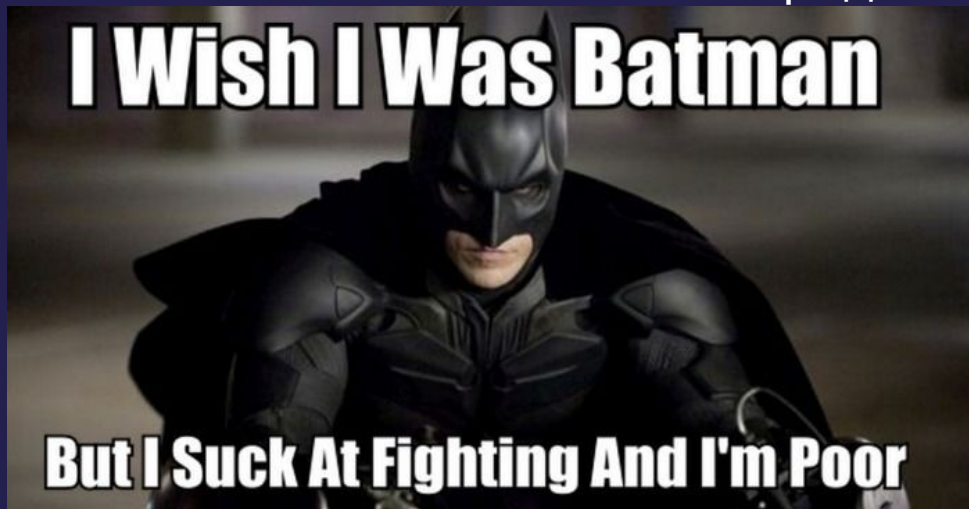


STILTSoft

Warning

1. Разработчики тоже
люди

2. Без научных
определений



STILTSoft

Agenda

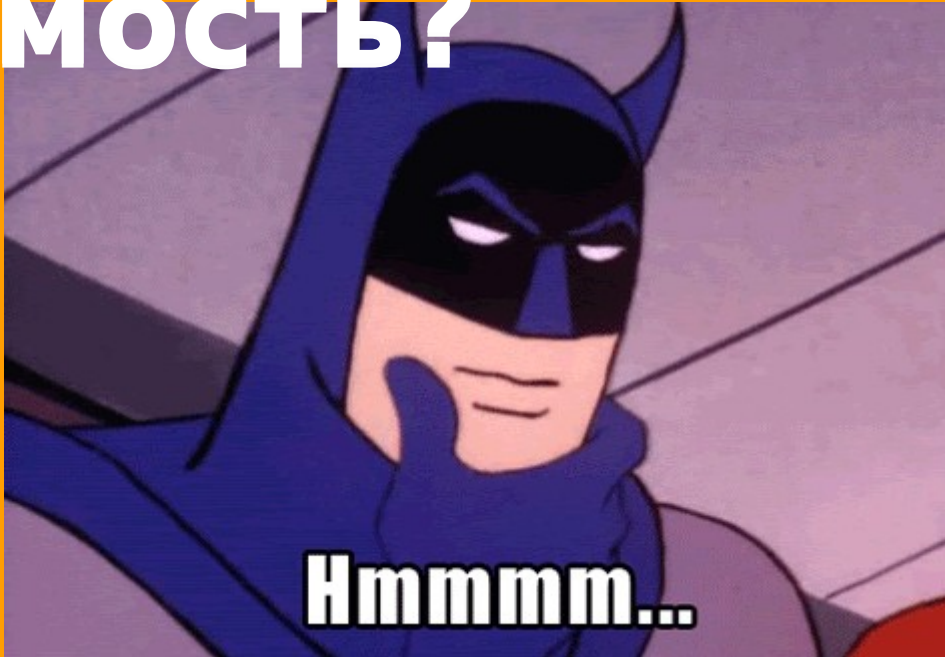
1. XSS с санитизацией и эскейпингом
2. Проблемы авторизации/аутентификации
3. Проблема кросстенантного доступа к данным
4. Поиск уязвимостей и договорные матчи

STILTSOFT



Что такое

уязвимость?



STILTSoft

Security-уязвимость

способ украсть или сломать
данные, к которым нет доступа
легальным способом.

Cross-site scripting (also known as **XSS**) is a web security vulnerability that allows an attacker to compromise the interactions that users have with a vulnerable application.

Cross-site scripting (also known as **XSS**) внедрение вредоносных скриптов на страницу.

XSS в Stiltsoft

Пример уязвимости



Как исправлять

STILTSOFT
XSS!

1. Использовать фреймворки (но аккуратно :))



React JS

STILTSoft



2. Экранировать “особо опасные” символы (проверенными библиотеками)

<	-	<
>	-	>
&	-	&



3. Удалять опасный контент (санитизация)

``

+

DOMPurify

=

``



Бонусный вариант исправления XSS

CSP (Content Security Policy) - это HTTP-заголовок (или метатег), который строго определяет, что и где может присутствовать на web-странице

Пример CSP

```
script-src = nonce- report-sample unsafe-eval self https://connect-cdn.atl-  
paas.net  
style-src = report-sample unsafe-inline self  
connect-src = self  
font-src = https://my-fonts.com  
img-src = self data: https:  
media-src = self
```



CSP не спасет от старых фреймворков



STILTSOFT

Проблемы аутентификации и авторизации



Аутентификация
Кто прислал запрос



Авторизация
Имеет ли он права



STILTSOFT

Почему мы с вами говорим об этом?

Ключ	Тема	Создан	Статус
AWEGRAPHS-635	Пользователь без прав на просмотр PR может получить информацию о нем через REST	июн 19, 2020	DONE
AWEGRAPHS-634	Пользователь без аутентификации может видеть данные (имя, email, email alias) всех пользователей Bitbucket	июн 19, 2020	DONE
AWEGRAPHS-633	Пользователь через REST видит метаданные активностей приватного (недоступного для него) репозитория / проекта	июн 19, 2020	DONE

Проблемы аутентификации и авторизации в Stiltsoft

Пример уязвимости



Как исправлять?

STILTsoft

1. Признание проблемы - первый шаг






STILTSoft

2. Проверьте параметры с клиента

```
public CompletionStage<Result> deleteMailbox(  
    Request request,  
    Long mailboxId  
)
```



Кросстенантность

	 id ▾	 name ▾	 ac_host_id ▾	 type ▾
1	50	IdeaForum	50	1
2	100	SupportForum	50	2
3	150	FirstForum	100	2

Подробности по Bugcrowd
<https://bugcrowd.com/stiltsoft>

STILTsoft



**Как решить проблемы
с кросстенантностью?**

STILTSOFT

Есть 2 варианта

1. Всегда следить за тем, чтобы у вас генерировались правильные SQL запросы с учетом тенанта.

STILTSOFT



Есть 2 варианта

1. Всегда следить за тем, чтобы у вас генерировались правильные SQL запросы с учетом тенанта.

Но это ненадежно, долго и не очень круто (разработчики бывают весьма забывчивы)).

STILTSOFT



Есть 2 варианта

1. Всегда следить за тем, чтобы у вас генерировались правильные SQL запросы с учетом тенанта.

Но это ненадежно, долго и не очень круто (разработчики бывают весьма забывчивы)).

STILTSOFT

2. Настроить расшаренный ресурс таким способом, чтобы он сам обеспечивал изоляцию данных всех клиентов.



Настройка RLS на уровне БД

```
ALTER TABLE forum ENABLE ROW LEVEL  
SECURITY;
```

```
CREATE POLICY forum_isolation_policy ON  
forum USING (tenant_id =  
current_setting('app.current_tenant_id')::U  
UID);
```



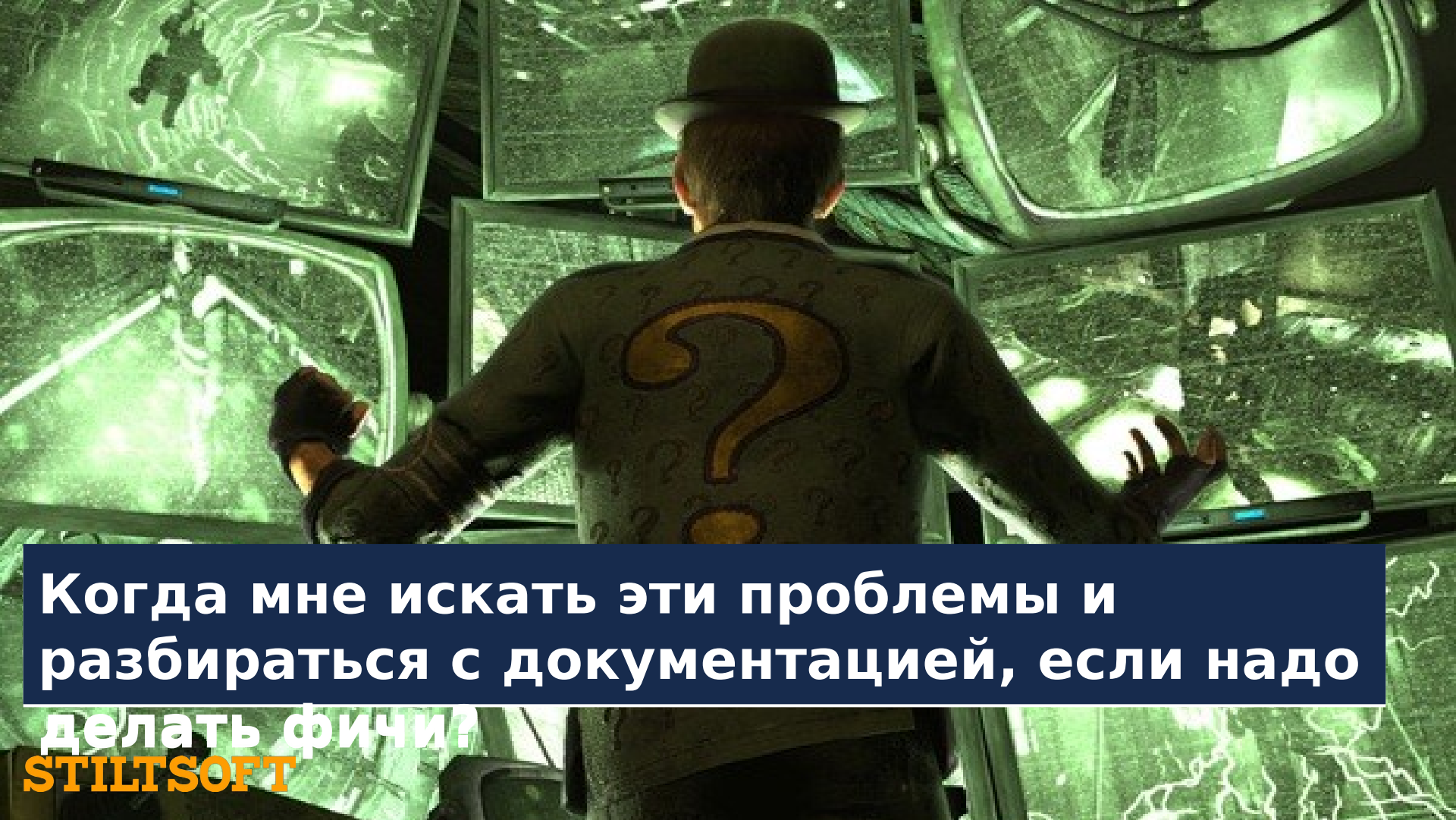
Имплементация RLS в Java

```
public static void setLocalTenantId(ACHost acHost, Connection connection) {  
    executeQuery(sql: "SET LOCAL app.current_tenant_id = '"  
        + acHost.getTenantId() + "'", connection);  
}
```

Пример работы RLS

```
DELETE FROM orders WHERE id = 567  
AND tenant_id = {UUID};
```





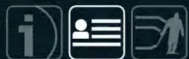
**Когда мне искать эти проблемы и
разбираться с документацией, если надо
делать фичи?**

STILTSOFT

1. Выделяйте время (Security Friday)

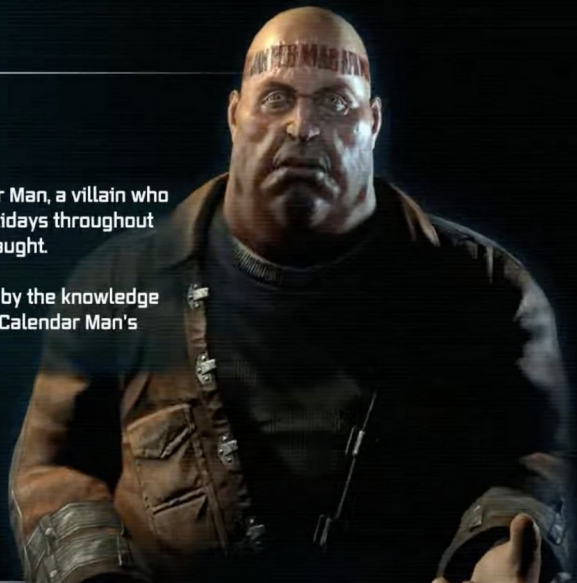
Calendar Man

BIO



Fixated on the calendar, Julian Day became Calendar Man, a villain who timed and tied his crimes thematically to certain holidays throughout the year, often leaving clues by which he could be caught.

Gotham City's hopes for a day off are often clouded by the knowledge that any holiday of note is likely to be shadowed by Calendar Man's presence.



2. Заранее определите направления поиска

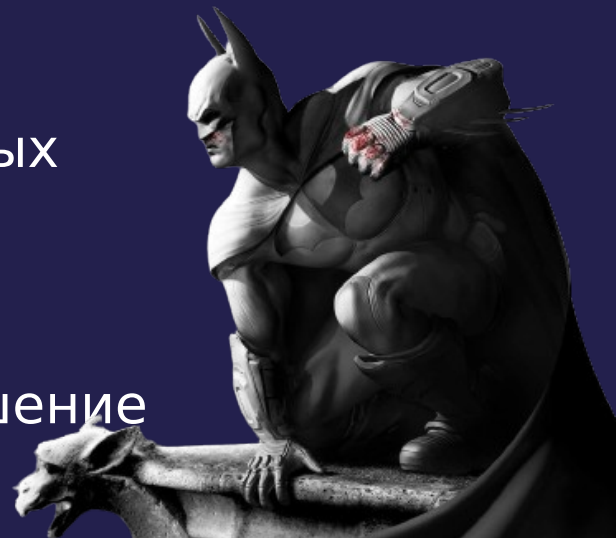


3. Попробуйте договорные матчи



4. Используйте STRIDE

- **S**poofing (представиться другим пользователем)
- **T**ampering (user input меняет логику приложения)
- **R**epudiation (неотказуемость выполненных действий)
- **I**nformation disclosure (утечка данных)
- **D**enial of service (отказ обслуживания)
- **E**levation of privilege (нелегальное повышение



Полезные ссылки

- С чего начать, если у вас веб-приложение
<https://owasp.org/www-project-top-ten/>
- По поводу STRIDE
<https://martinfowler.com/articles/agile-threat-modelling.html>
- RLS
<https://aws.amazon.com/ru/blogs/database/multi-tenant-data-isolation-with-postgresql-row-level-security/>
- Полезное видео “XSS on Google Search - Sanitizing HTML in The Client?”
<https://youtu.be/IG7U3fuNw3A>

**Андрей
Орлов**

[GitHub - Captain1653](#)

<https://t.me/stiltsoft>

resume@stiltsoft.co
m

STILT**SOFT**



ВАШ ФИДБЕК

Вопросы?



STILTSOFT