КОД
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

25 октября 2018 г.
г. Казань

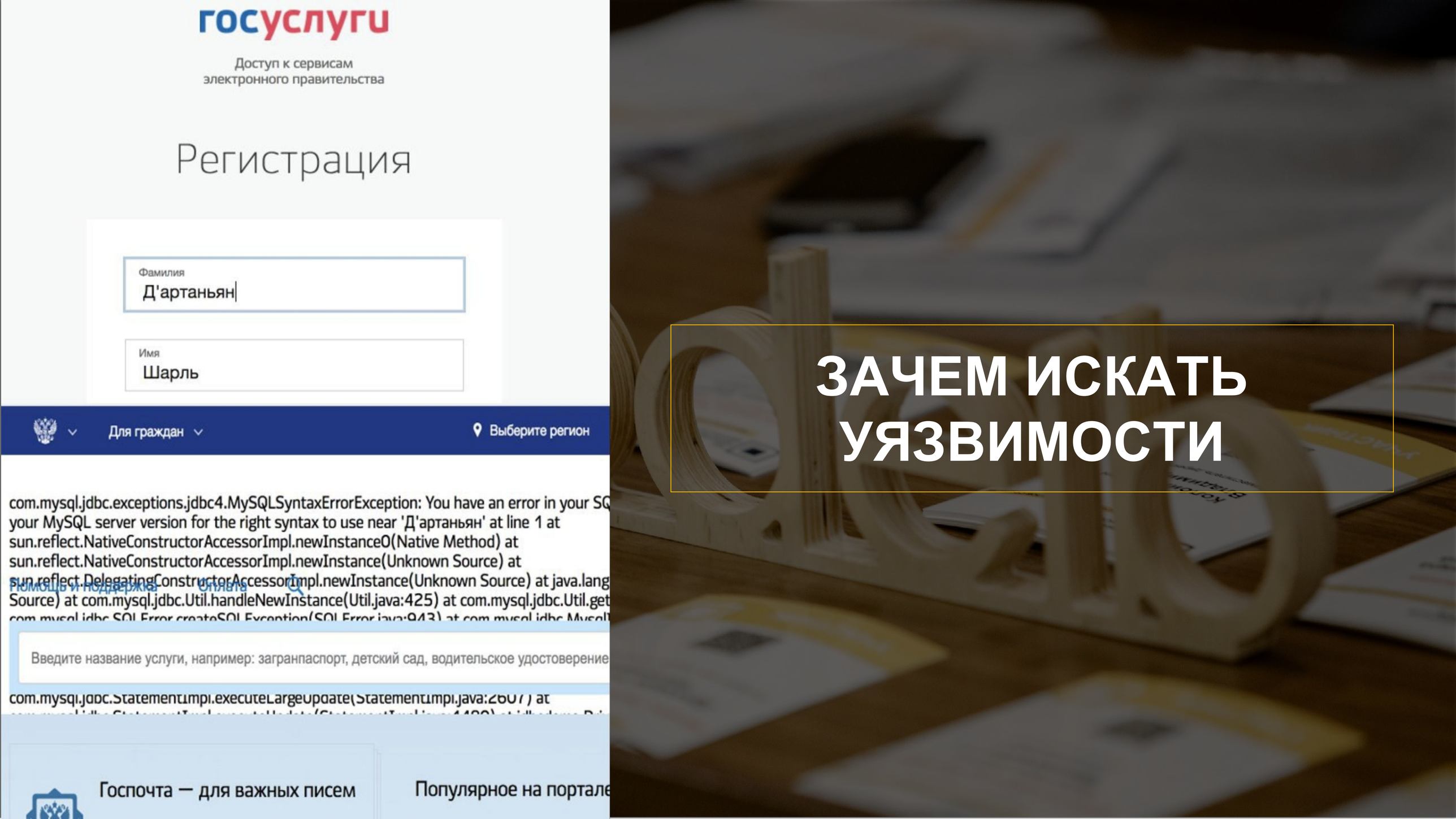
#CODEIB

Почему сканеры уязвимостей больше не работают*

*в зрелых веб-приложениях

Докладчик
АЙДАР САБИРОВ,
КОМПАНИЯ SORAMITSU

Telegram: @baydarich



ЗАЧЕМ ИСКАТЬ УЯЗВИМОСТИ

госуслуги

Доступ к сервисам
электронного правительства

Регистрация

Фамилия
Д'артаньян

Имя
Шарль

Для граждан

Выберите регион

com.mysql.jdbc.exceptions.jdbc4.MySQLSyntaxErrorException: You have an error in your SQ
your MySQL server version for the right syntax to use near 'Д'артаньян' at line 1 at
sun.reflect.NativeConstructorAccessorImpl.newInstance0(Native Method) at
sun.reflect.NativeConstructorAccessorImpl.newInstance(Unknown Source) at
sun.reflect.DelegatingConstructorAccessorImpl.newInstance(Unknown Source) at java.lang
Source) at com.mysql.jdbc.Util.handleNewInstance(Util.java:425) at com.mysql.jdbc.Util.get
com.mysql.jdbc.SQLError.createSQLException(SQLError.java:943) at com.mysql.jdbc.MysqlI

Помощь и поддержка Оплата

Введите название услуги, например: загранпаспорт, детский сад, водительское удостоверение

com.mysql.jdbc.StatementImpl.executeLargeUpdate(StatementImpl.java:2607) at

Госпочта — для важных писем

Популярное на портале

Existing users?

Mailbox name

Итак, вы купили сканер

КАК РАБОТАЮТ СКАНЕРЫ (1)

```
GET /getfile.php?=myfile HTTP/1.1
Host: example.com
User-Agent: code ib kazan 2018
```

КАК РАБОТАЮТ СКАНЕРЫ (1)

```
GET /getfile.php?=myfile HTTP/1.1
Host: example.com
User-Agent: code ib kazan 2018

GET /getfile.php?=§myfile§ HTTP/1.1
Host: example.com
```

КАК РАБОТАЮТ СКАНЕРЫ (1)

```
GET /getfile.php?=myfile HTTP/1.1
Host: example.com
User-Agent: code ib kazan 2018

GET /getfile.php?=§myfile§ HTTP/1.1
Host: example.com

GET /getfile.php?=../../../../../../etc/passwd HTTP/1.1
Host: example.com
```

КАК РАБОТАЮТ СКАНЕРЫ (2)

```
HTTP/1.1 200 OK
Content-Type: text/plain
Content-Length: 162
Connection: close

nobody:*:-2:-2:Unprivileged User:/var/empty:/usr/bin/false
root:*:0:0:System Administrator:/var/root:/bin/sh
daemon:*:1:1:System Services:/var/root:/usr/bin/false
...
```


КЕЙСЫ
#CODEIB

1. НЕПОНИМАНИЕ КОНТЕКСТА

```
POST /buy HTTP/1.1
Host: example.com
[...]
{"ItemId":123, "ItemPrice":-1337}
```

```
HTTP/1.1 200 OK
Content-Type: application/json
[...]
{
    "variants":[
        {
            "answer":2,
            "isCorrect":false
        },
        {
            "answer":3,
            "isCorrect":true
        }
    ]
}
```

2. ПРОБЛЕМЫ БИЗНЕС-ЛОГИКИ

уязвимость xss знатоки есть ?

Наташа Фролова Ученик (108), Вопрос открыт 14 часов назад

Нравится | Подписаться | Ответить | ⊘ | ★

2 ОТВЕТА

инштейн Профи (553) 14 часов назад

это такой вид отеки на сайт

Нравится | Комментировать | Пожаловаться

3. МНОГОХОДОВОЧКА

ЗАЙТИ В ЛИЧНЫЙ КАТАЛОГ → ЗАГРУЗИТЬ XSS ВЕКТОР ЧЕРЕЗ XML → ПРОИЗВЕСТИ ПОИСК ТОВАРА

```
<![CDATA[<script>confirm(document.domain)</script>]]>
```

4. ВЗАИМОДЕЙСТВИЕ СИСТЕМ

```
POST /login HTTP/1.1
Host: example.com
User-Agent: Mozilla/5.0 "><img src=x onerror=alert(1)>
[...]
```

5. ВРЕМЕННОЙ ИНТЕРВАЛ

```
GET / HTTP/1.1
Host: example.com
Referer: evil.com
```

6. ИНТУИЦИЯ

```
GET / HTTP/1.1
Host: evil.com
```

```
GET / HTTP/1.1
Host: example.com.evil.com
```

7. ДРУГИЕ ПРОБЛЕМЫ

1. ошибка - хорошо или плохо
2. разные запросы - один компонент
3. кодировка и интерпретация
4. атака прошла или нет
5. список далеко не полный

SDLC И DEVSECOPS СПЕШАТ НА ПОМОЩЬ

#CODEIB

SDLC


TRAINING
CORE SECURITY TRAINING
REQUIREMENTS
ESTABLISH SECURITY REQUIREMENTS
CREATE QUALITY GATES/ BUG BARS
SECURITY & PRIVACY RISK ASSESSMENT
DESIGN
ESTABLISH DESIGN REQUIREMENTS
ANALYSE ATTACKS SURFACE
THREAT MODELING
IMPLEMENTATION
USE APPROVED TOOLS
DEPRECATE UNSAFE FUNTIONS
STATIC ANALYSIS
VERIFICATION
DYNAMIC ANALYSIS
FUZZ TESTING
ATTACK SURFACE REVIEW
RELEASE
INCIDENT RESPONSE PLANS
FINAL SECURITY REVIEW
RELEASE ARCHIVE
RESPONSE
EXECUTE INCIDENT RESPONSE PLAN

ДРУГИЕ МЕРЫ

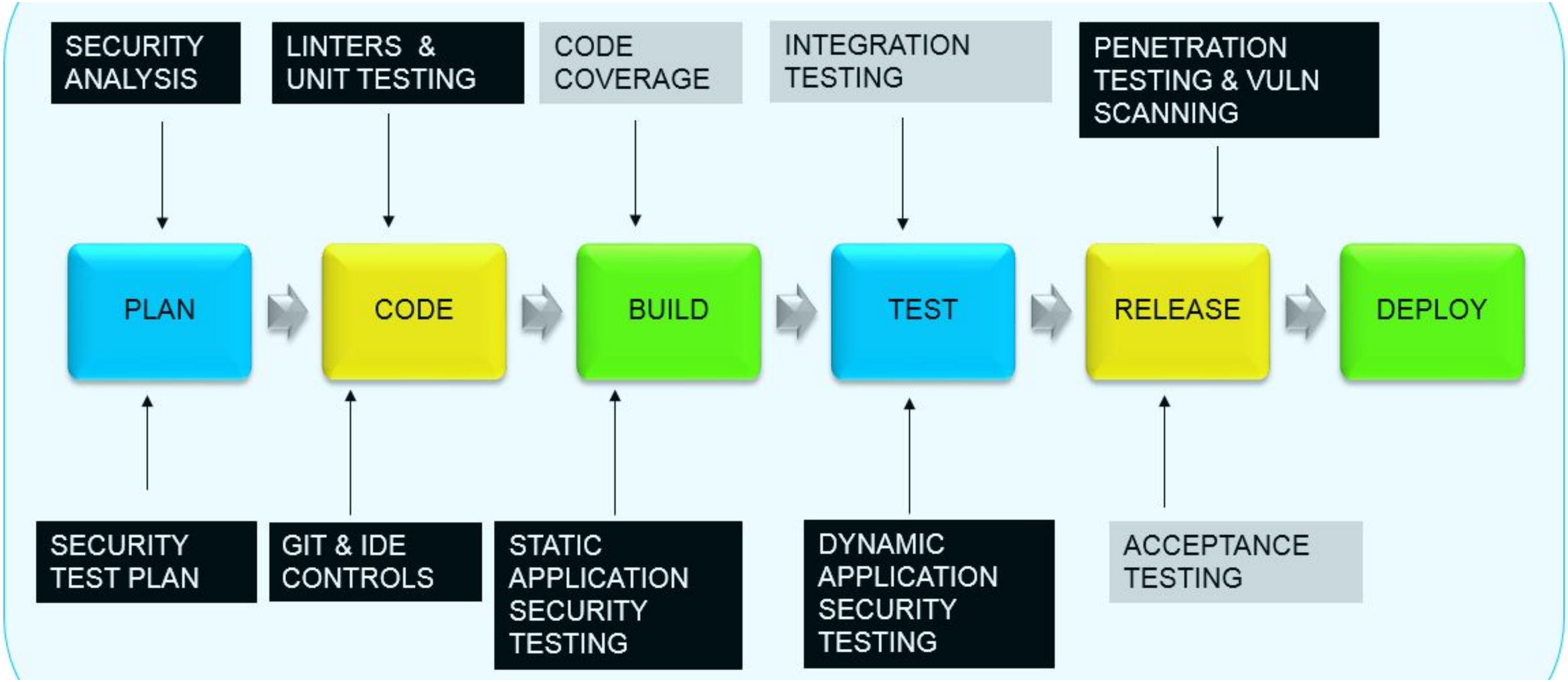
1 общие безопасные компоненты

2 унификация

4 bug bounty

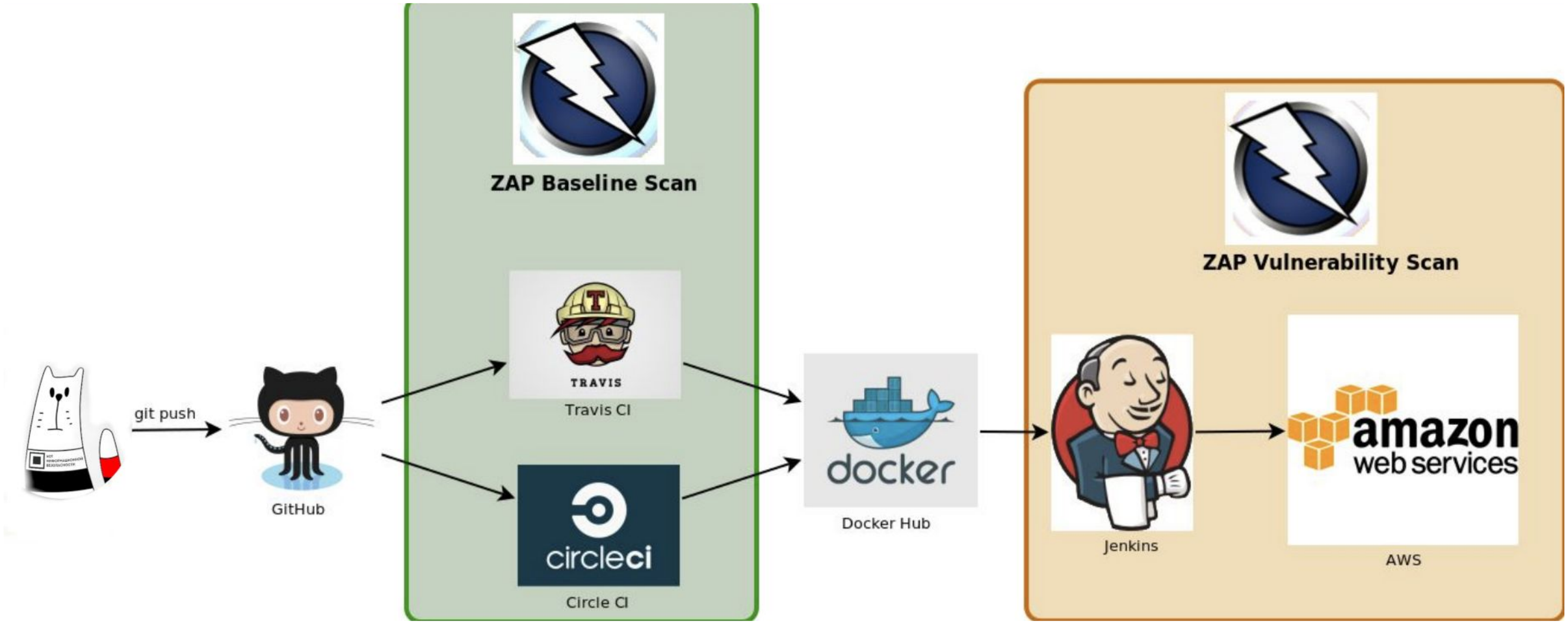
3 patch management

DevSecOps



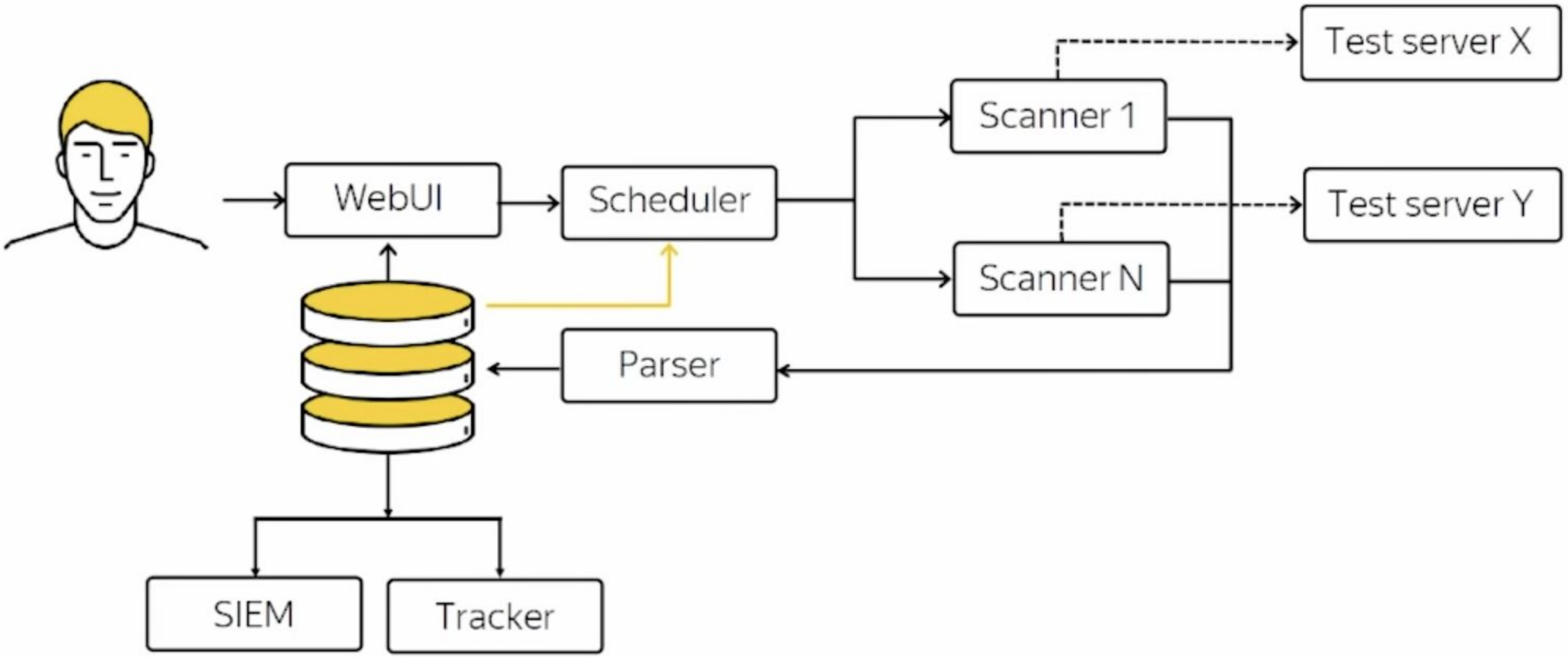
https://dzone.com/articles/shifting-left-devsecops

DevSecOps: DAST в Mozilla



https://www.usenix.org/sites/default/files/conference/protected-files/enigma17_slides_vehent.pdf

DevSecOps: пример Яндекса



https://www.youtube.com/watch?v=rSp2cpAI4Tc

ВМЕСТО ЗАКЛЮЧЕНИЯ

СПАСИБО ЗА ВНИМАНИЕ!

КОД
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

25 октября 2018 г.
г. Казань

#CODEIB

Докладчик

АЙДАР САБИРОВ,
КОМПАНИЯ SORAMITSU

Telegram: @baydarich

Группа CTF: https://t.me/kaiCTF