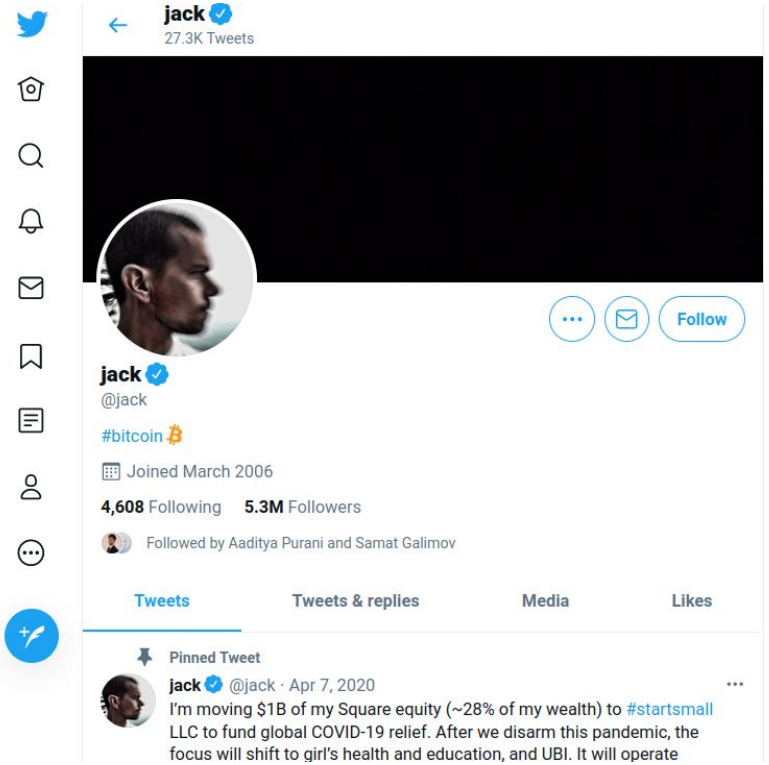
SSTI


Elon Musk
13.7K Tweets
Follow
Elon Musk
@elonmusk
Joined June 2009
103 Following 48.6M Followers
Followed by Ramazan, Black Turtle, and 16 others you follow
Tweets
Tweets & replies
Media
Likes
Elon Musk @elonmusk · 7h
Starbase, Texas


jack
27.3K Tweets
Follow
jack
@jack
#bitcoin
Joined March 2006
4,608 Following 5.3M Followers
Followed by Aaditya Purani and Samat Galimov
Tweets
Tweets & replies
Media
Likes
Pinned Tweet
jack @jack · Apr 7, 2020
I'm moving $1B of my Square equity (~28% of my wealth) to #startsmall LLC to fund global COVID-19 relief. After we disarm this pandemic, the focus will shift to girl's health and education, and UBI. It will operate

- Model — модель объекта
- View — представление
- Controller — связывает модели и представления

```
<html>
    <head>
        <title> Home page of {owner.name} </title>
    </head>
    <body>
            Hello, {user.name}!
     </body>
</html>
```

```
Welcome, %username%!
```

```
printf("Hello, %s!", name);
```

- Специальный синтаксис для инструкций
- Есть множество доступных объектов
- Можно брать их свойства
- Можно дергать некоторые методы
- Есть встроенные функции

```
SELECT * FROM users where name = "$name"
```

```
system("cat files/$name.txt")
```

```
render_template($user_input);
```

Атакуем SSTI

- Поиск инъекции
- Идентификация движка
- Эксплуатация уязвимости

Поиск уязвимости

- Детектим странное поведение
- Для этого подставляем инструкции
- Нужно угадать синтаксис

Типичный синтаксис

- `{varname}`
- `{{varname}}`
- `${varname}`
- `$varname`
- `<%= varname %>`

Атакуем SSTI

- `{{varname}}` вырезается
- `{{varname}}` приводит к ошибке
- `{{2*2}}` выводит 4

Пробуем для каждого варианта синтаксиса

Легко пропустить

```
render("Value is {{"+inp+"}}")
```

- Тестируем `name}}sometext`
- Расследуем, если выдало `sometext`

Определяем движок

- Пытаемся угадать язык бекенда
- Гуглим движки
- Ищем синтаксические особенности

Определяем движок

- Вычисляет арифметику?
- Строки приводятся к числам?
- Какие свойства есть у объектов?

Движок придётся угадать :(

Эксплуатация

- Читаем документацию движка
- Смотрим, что можно сделать

Эксплуатация

```
{php}echo `id`;{/php}
```

Самый лучший метод эксплуатации — нагуглить пейлоад и исправить его.

Эксплуатация

- Доступен ряд объектов
- Можно брать свойства и методы
- Надо дотянуться до “хороших” функций

Эксплуатация

```
$class.inspect("java.lang.Runtime").type.getRuntime().exec("id")
```

Эксплуатация

- Python — ищем `__import__`
- Java — ищем `Runtime`
- Node — ищем `require`
- PHP — ищем `include`

Перерыв 5 минут

http://jinja-ssti.sh.je/

- Есть `requst` типа `flask.Request`
- У методов есть `__func__`
- У функций есть`__globals__`
- Внутри `__globals__` есть модуль `__builtins__`

http://ejs-ssti.sh.je/

- Есть объект `process`
- `Object` тоже доступен
- Вам нужно добраться до `require('child_process')`

http://secret-ssti.sh.je/

- Название движка вам не дано
- Нужно угадать синтаксис команд

${fin}