Подсказки для bash

Julia Evans
@b0rk

назначение переменных

```
MYVAR=2
```

низя ставить пробелы!!!

3 типа переменных

перменные окружения

```
export MYVAR=2
```

глобальные	локальные
`MYVAR=2`	`local MYVAR=2`

каждой переменной по кавычкам

```
if [ $X = $Y ]
```
← плохо

♥
```
if ["$X" = "$Y"]
```
← верно

используйте [[, а не [

```
if [[ 2 = 3 ]]
```

так лучше! /usr/bin/ [вообще программа, [[встроенная команда + с ней меньше проблем.

предохраняйтесь: set -eu

-e : выход при ошибке

-u : выход, если перменная не объявлена

-x : вывод каждой команды (полезно для отладки)

-o pipefail: выход, при любой ошибки в конвейере

&& против ;

```
штука 1; штука 2
```

штука 2 выполнится в любом случае.

```
штука 1 && штука 2
```

штука 2 выполнится только если штука 1 отработает без ошибок.

попробуйте shellcheck

Опупенный статический анализатор шелл скриптов: shellcheck.net

помните: bash – это язык программирования

Он странноват, но знать основы точно поможет

"Не выдавайте удивление"

Моё ♥ любимое ♥ правило общения из

 Центра рекрутинга 

Такое случается очень часто:

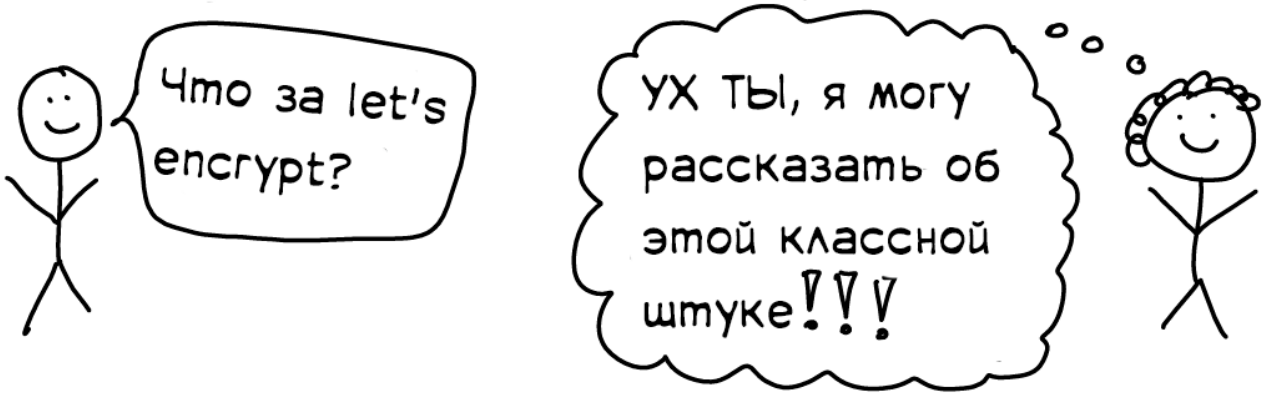
Есть классный и простой прием!

Не выдавайте удивление, когда кто-то чего-то не знает, а вы думали наоборот.

(Даже если вы и правда удивлены.)

Это совсем не помогает.

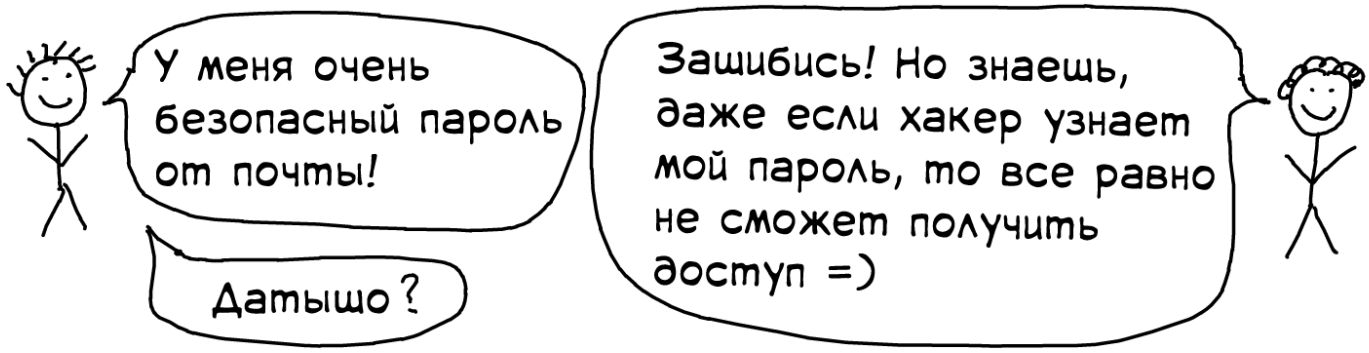
Тогда вы сможете отлично проводить время:



Практикуйтесь и станет легче! 

Julia Evans / @b0rk

Двухфакторная аутенфикация ("2FA")

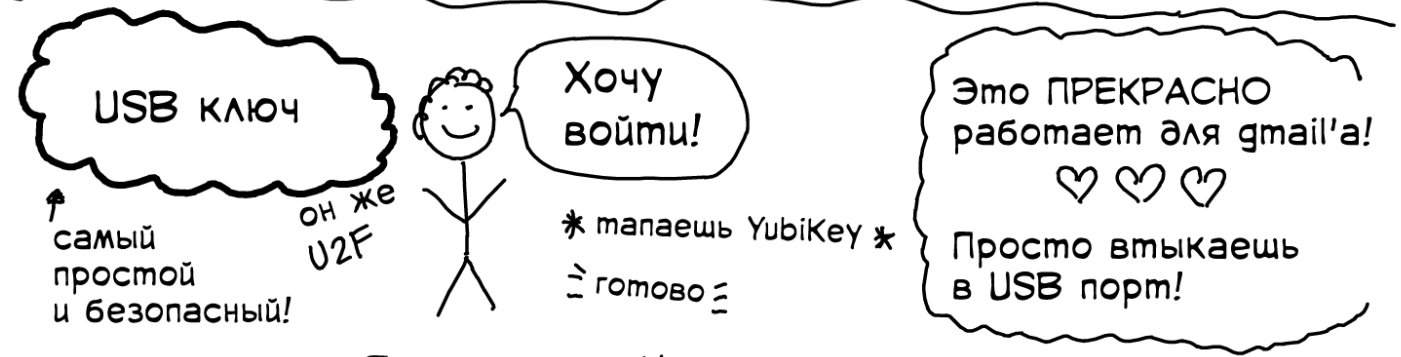


Есть три основных способа использования 2FA:

Проблемы:
- Номер телефона могут украсть
- Иногда SMS не доходят

(все это происходит в жизни !! !!)

Проблемы: Все-таки, эти коды фишатся.



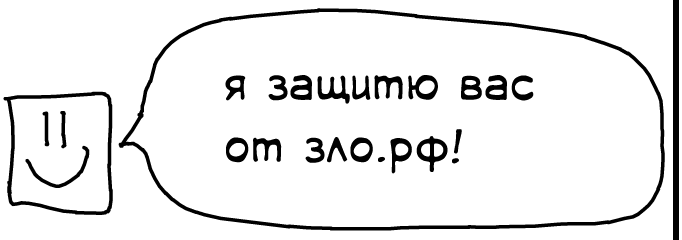
Проблемы:
- Нужно купить
- Не каждый сайт поддерживает

Julia Evans
@b0rk

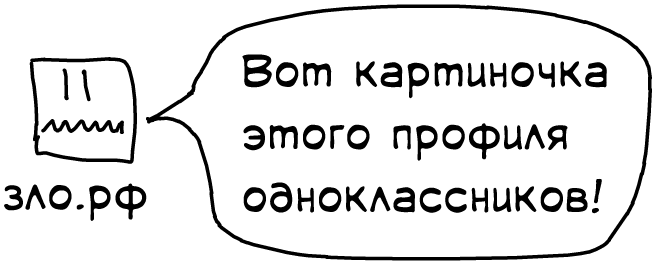
CORS

Использование ресурсов из перекрестных источников

У браузеров есть не менее 5 базиллионов функций безопасности.



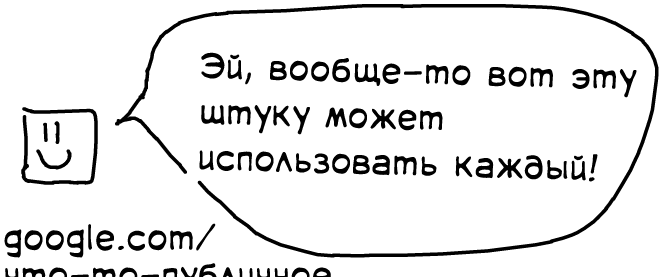
Загружать картинки с другого вебсайта МОЖНО.



Но запросы AJAX ЗАПРЕЩЕНЫ.

Поэтому браузеры применяют "Политику единого происхождения".

Но... если ХОЧЕТСЯ, можно разрешить другим сайтам отправлять AJAX-запросы себе.

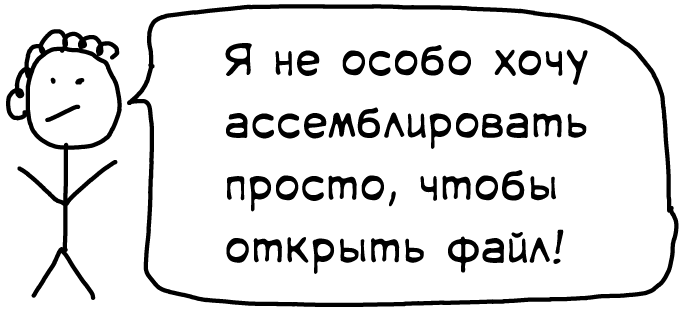


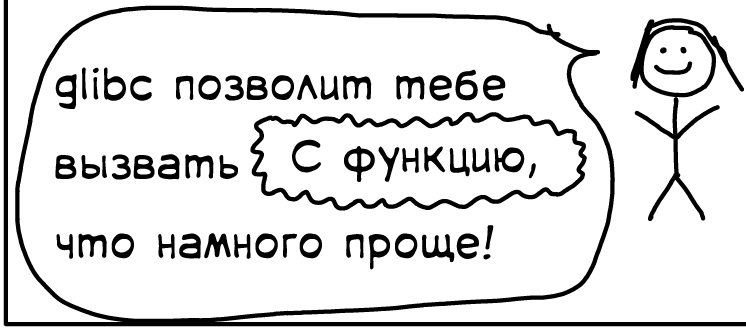
♥ libc ♥

Julia Evans
@b0rk

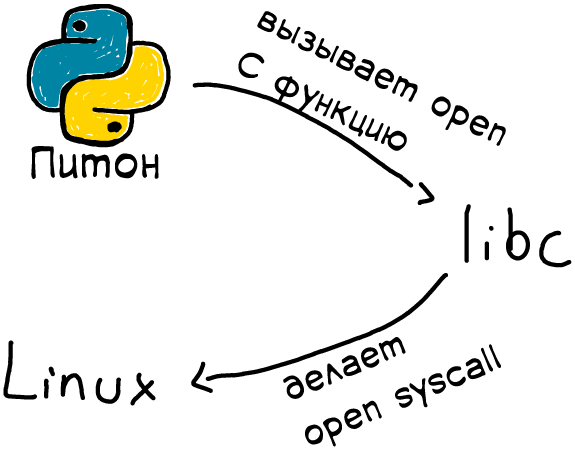
Чтобы использовать системные вызовы к ядру Линукса, вам нужно:

- задать кое-какие регистры
- использовать инструкцию ассемблера syscall.

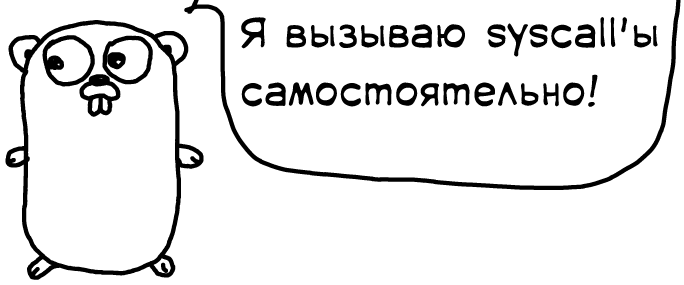




Когда вы открываете файл в Питоне:



Почти каждая программа использует libc. Но не программы на Go!



libc: больше, чем системные вызовы!

да и вообще куча разного.

Фильтры BPF
(самый маленький гайд)

Julia Evans
@b0rk

В tcpdump используется маленький язык под названием BPF, чтобы мы могли фильтровать пакеты.

port 53

проверяет, является ли исходящий ИЛИ входящий порт 53м. Соответствует TCP порту 53 и UDP порту 53.

→ src port 80
→ dest port 80
→ tcp port 80

это именно то, чем кажется :)

также как и

src host 1.2.3.4
dest host 1.2.3.4

host 192.168.3.2

проверяет, является ли исходящий или входящий IP 192.168.3.2

udp[11] & 0xf == 3

можно использовать битовые вычисления на содержимом пакета. Это, например, проверяет на ответ DNS "NXDOMAIN"!

(пришлось погуглить, чтобы найти, но оно работает!)

host 11.22.33.44 and port 80

можно использовать 'and' (и), 'or' (или) и 'not' (не).

Это не все, но до сих пор мне было этого достаточно!

Julia Evans @b0rk

Компьютеры ★ быстрые ★

Что я могу сделать за 1 секунду на своем лэптопе?

Посмотрите подробности на computers-are-fast.github.io

Сколько циклических итераций на Питоне?

50 миллионов!

Сколько циклических итераций на C?

500 миллионов!

Сколько запросов к проиндексированной таблице базы данных, 1 миллион строк?

50,000 запросов!

Сколько байт посчитает md5sum?

500 МБ!

Сколько раз я смогу распарсить 64к JSON'а?

500! (на Питоне)

Сколько байт могу записать на диск?

300 МБ!

Сколько байт может просмотреть 'grep'?

2 гигабайта!

Сколько файлов может вывести 'find'?

300,000 файлов!

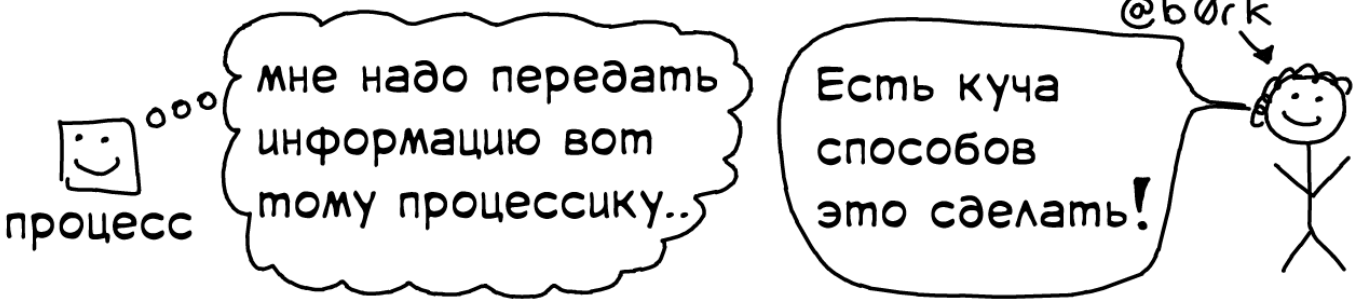
Классные интерфейсы для мониторинга

(читать "слежки")

Межпроцессное взаимодействие

(на Линуксе)

by Julia Evans
@b0rk



в произвольном порядке:

① записать в файл

② отправить по локальной сети

(HTTP запросом или как-нибудь так)

крутота: можно легко разнести программы на разные машины.

③ конвейер!

`program1 | program2`

крутота: у вас будет автоматическая буферизация.

④ общая память

процессы тоже могут совместно использовать память!

смотри `shm_open`

крутота: очень быстро/мощно (а еще пугающе 😬)

⑤ юниксовые сокеты

Еще один способ передать данные.

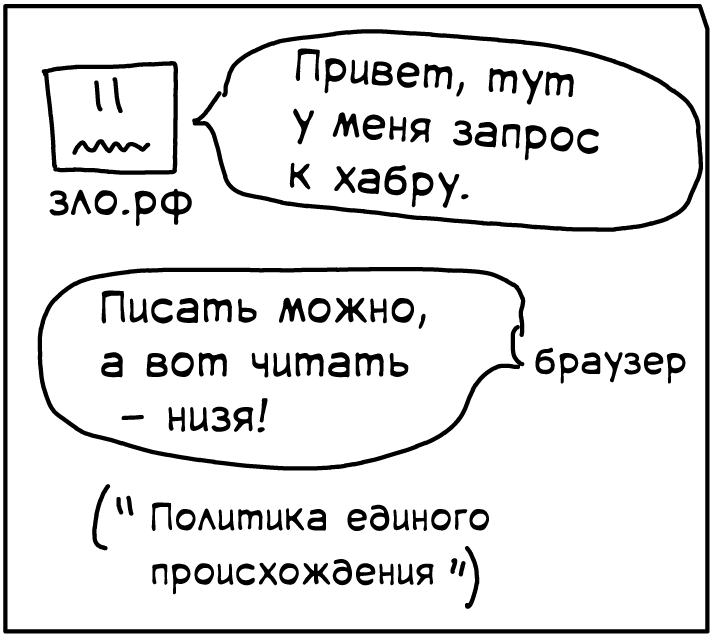
крутота: через сокеты можно передавать файловые дескрипторы.

CSRF

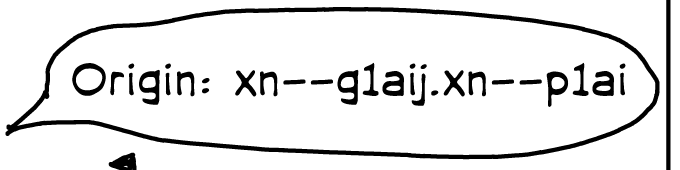
Julia Evans
@b0rk

Подделка запросов между сайтами !!

Вы открываете множество скрытых сайтов.
Всякие злыдни ОЧЕНЬ ХОТЯТ что-нибудь подменить в вашей админке.

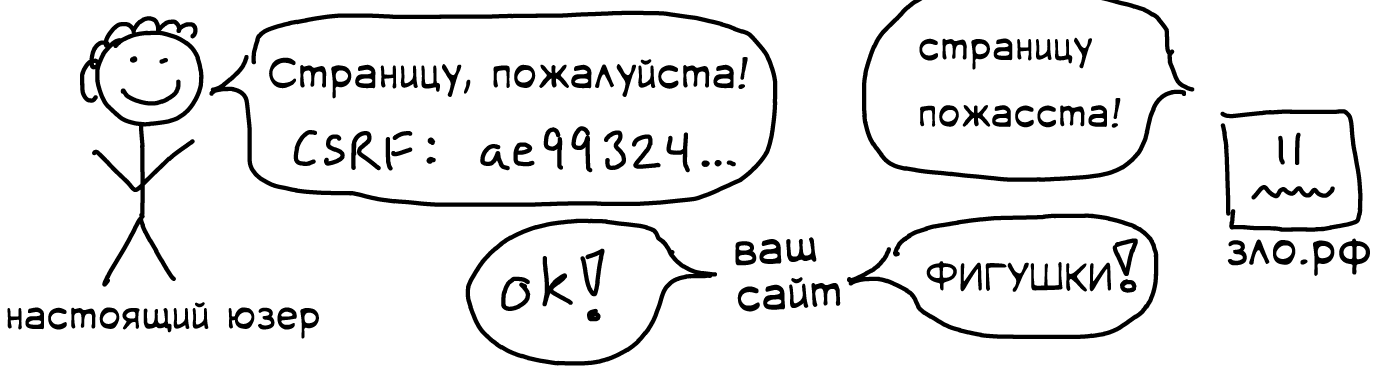


Хорошим решением будет обезопасить себя от кросс-сайтовых запросов



Заголовок Origin сообщает откуда пришел запрос. Неизвестные источники можно заблокировать.

Еще можно генерировать случайный токен CSRF каждый раз, когда входит пользователь.



Перевела Команда FirstVDS.ru