

Подсказки для bash

JULIA EVANS
@b0rk

назначение переменных

MYVAR=2

низя ставить пробелы!!!

каждой переменной
по кавычкам

if [\$X = \$Y] ← **ПЛОХО**

♥ if ["\$X" = "\$Y"] ← **верно**

предохраняйтесь:
set -eu

- e : выход при ошибке
- u : выход, если переменная не объявлена
- x : вывод каждой команды (полезно для отладки)
- o pipefail: выход, при любой ошибки в конвейере

≡ **попробуйте shellcheck** ≡

Опупенный статический
анализатор шелл скриптов:
shellcheck.net

3 типа переменных

переменные окружения

export MYVAR=2

глобальные

MYVAR=2

локальные

local MYVAR=2

используйте [[, а не [

if [[2 = 3]]

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

&& против ;

штука 1; штука 2;

штука 2 выполнится в любом случае.

штука1 && штука2;

штука 2 выполнится только если штука 1 отработает без ошибок.

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:



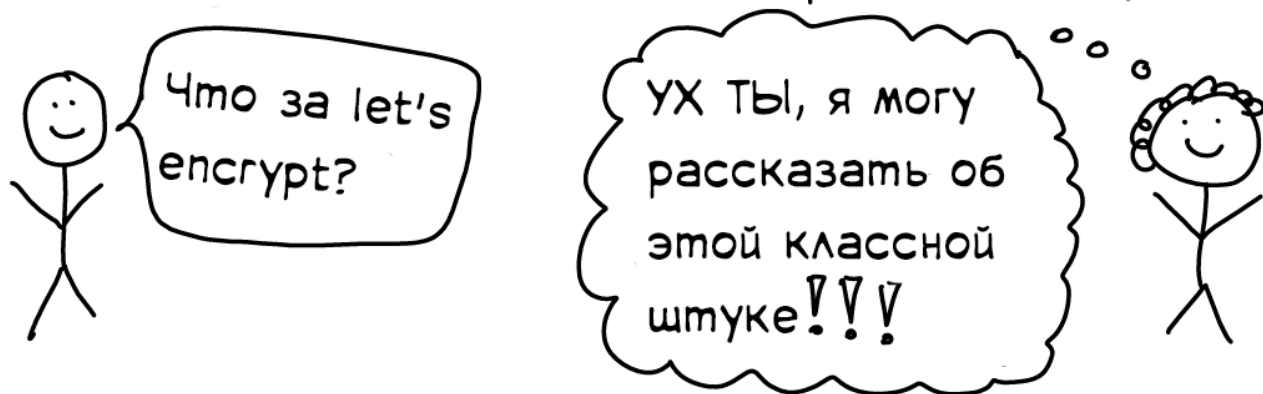
Есть классный и простой прием!

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! ☺☺☺

Двухфакторная аутентификация ("2FA")



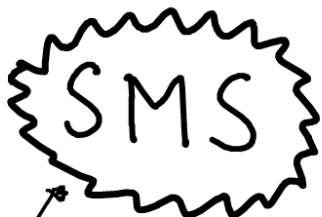
У меня очень
безопасный пароль
от почты!

Датышо?

Зашибись! Но знаешь,
даже если хакер узнает
мой пароль, то все равно
не сможет получить
доступ =)



Есть три основных способа использования 2FA:



нормально !



Хочу
войти!

Отправил тебе
SMS с кодом.
Введи код и
сможешь войти.



Проблемы:

→ Номер телефона могут украсть

→ Иногда SMS не доходят

(все это происходит
в жизни !!!)



очень хорошо!

или TOTP



Хочу
войти!

12345

телефон

Введи-ка код
из того этого
приложения на
телефоне!



Проблемы: Все-таки, эти коды фишатся.



самый
простой
и безопасный!

он же
U2F



Хочу
войти!

* тапаеть YubiKey *
≡ готово ≡

Это ПРЕКРАСНО
работает для gmail'a!



Просто втыкаешь
в USB порт!

Проблемы: • Нужно купить

• Не каждый сайт поддерживает

CORS

Использование ресурсов из перекрестных источников

У браузеров есть не менее
5 базиллионов функций
безопасности.



я защитю вас
от зло.рф!

Загружать картинки с
другого вебсайта МОЖНО.



зло.рф

Вот картиночка
этого профиля
одноклассников!

Но запросы AJAX
ЗАПРЕЩЕНЫ.



зло.рф

Хочу прочитать
все личные
сообщения!

А ВОТ ФИГУШКИ!

Поэтому браузеры
применяют "Политику единого
происхождения".



site.com

Хочу послать
AJAX-запрос
для google.com.



браузер

НЕТУШКИ!

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



Эй, вообще-то вот эту
штуку может
использовать каждый!

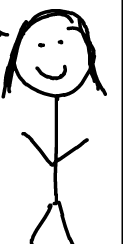
google.com/
что-то-публичное



это и
называется
CORS!

Как рассказать браузеру,
что меня может
использовать любой?

Используй заголовок
Access-Control-
Allow-Origin! =)

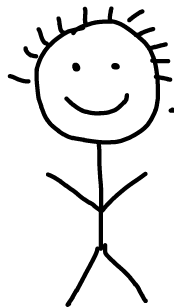




libc



JULIA EVANS
@bork



Что это за
файл такой
libc.so.6 на моем
компьютере?

Чтобы использовать
системные вызовы к ядру
Линукса, вам нужно:

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



Я не особо хочу
ассемблировать
просто, чтобы
открыть файл!

glibc позволит тебе
вызвать C функцию,
что намного проще!



Когда вы открываете
файл в Питоне:



Питон

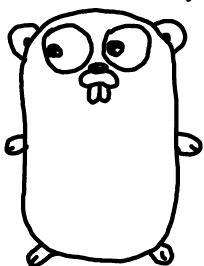
вызывает open
C функцию

libc

Linux

делает
open syscall

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



Мне не нужен libc!
Я вызываю syscall'ы
самостоятельно!

libc: больше, чем системные
вызовы!

и glibc есть

потоки

случайные
числа

математика

сокет

да и вообще куча разного.

Фильтры BPF

(самый маленький гайд)

JULIA EVANS
@bork

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

host 192.168.3.2

проверяет, является ли исходящий или входящий IP 192.168.3.2

src host 1.2.3.4

dest host 1.2.3.4

host 11.22.33.44

and port 80

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

udp[17] & 0xf == 3

можно использовать битовые вычисления на содержимом пакета.

Это, например, проверяет на ответ DNS "NXDOMAIN"!

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

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

≧ 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 С?

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")



системные вызовы



Какие файлы ты там сейчас открываешь?

≡ сетевые запросы ≡



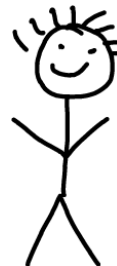
Эй, какие HTTP заголовки ты там отправляешь?

♥♥♥♥♥♥♥♥ вызовы функций ♥



С какими конкретно аргументами была вызвана эта функция?

? ? ? запросы к базе данных ? ?

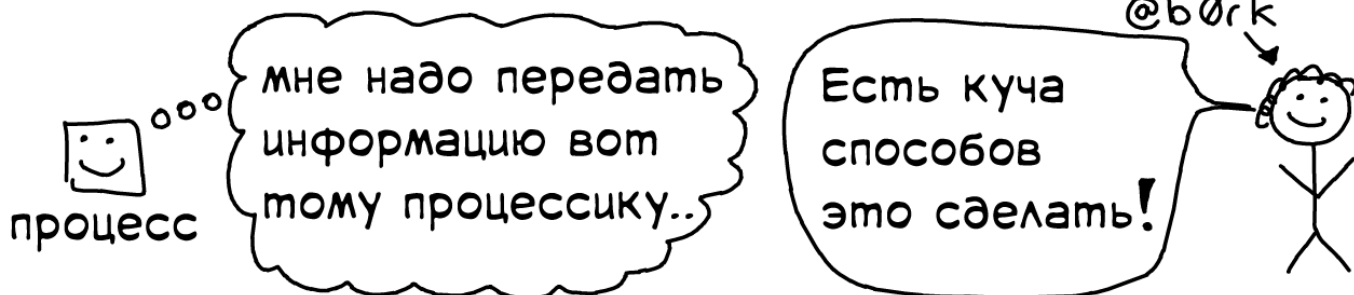


Кто-нибудь вообще обращается сейчас к этой таблице?

Межпроцессное взаимодействие

(на Линуксе)

by Julia Evans
@b0rk



в произвольном порядке:

① записать в файл

② отправить по локальной сети

③ конвейер!

(HTTP запросом или как-нибудь так)

'program 1 | program 2'

крутома: у вас будет автоматическая буферизация.

крутома: можно легко разнести программы на разные машины.

④ общая память

процессы тоже могут совместно использовать память!

смотри **shm_open**

крутома: очень быстро/мощно (а еще пугающе ☹)

⑤ юниксовые сокеты

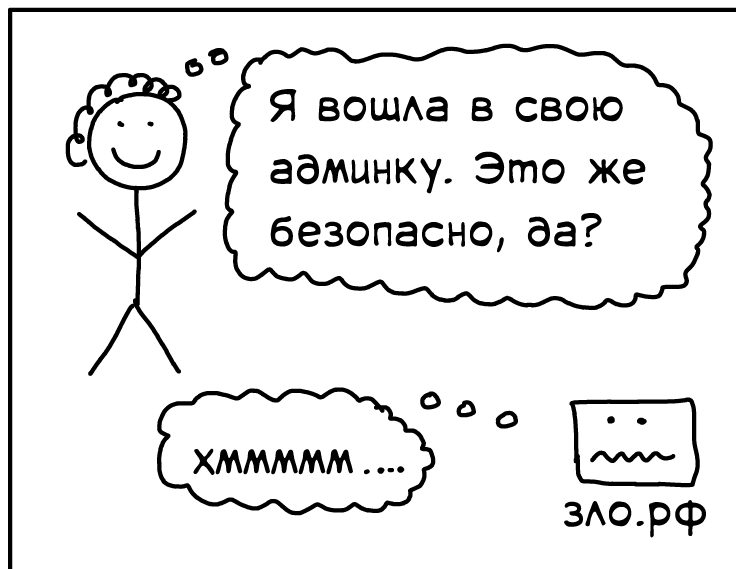
Еще один способ передать данные.

крутома: через сокеты можно передавать файловые дескрипторы.

CSRF

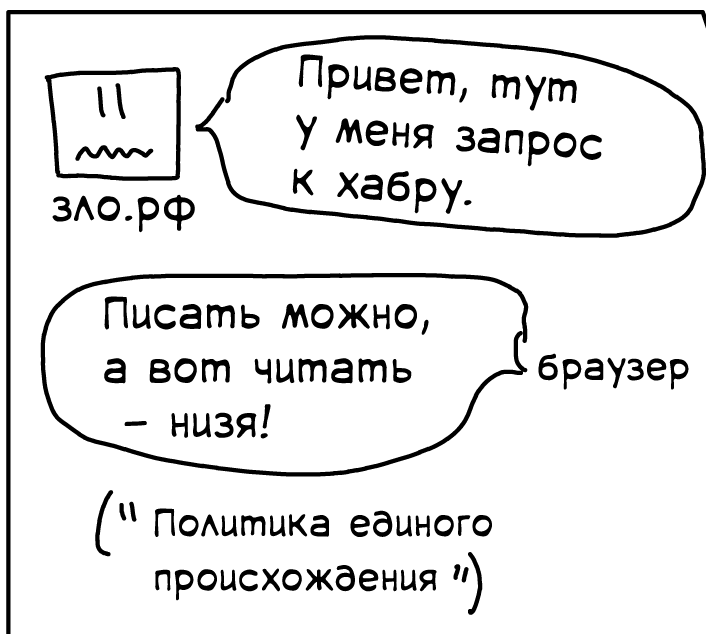
JULIA EVANS
@b0rk

Подделка запросов между сайтами ☹️



Вы открываете множество скрытых сайтов.

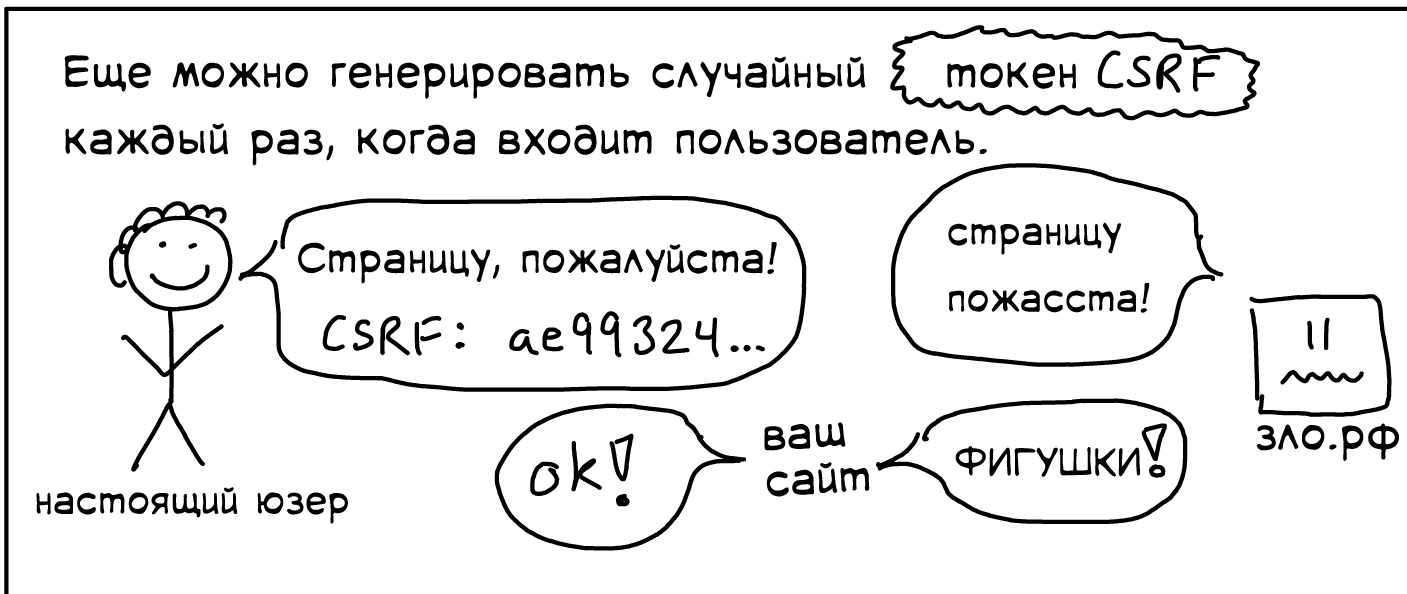
Всякие злыдни ОЧЕНЬ ХОТЯТ что-нибудь подменить в вашей админке.



Хорошим решением будет обезопасить себя от кросс-сайтовых запросов

Origin: xp--glaij.xp--plai

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



Перевела Команда FirstVDS.ru