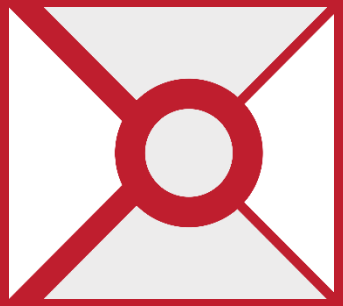


PENTESTIT

Сафонов Лука, Pentestit
luka@pentestit.ru

DevConf

http://www.devconf.ru

Методы защиты веб-приложения от хакерских атак

Комплексный подход при оказании услуг позволяет избавить наших клиентов от всех вопросов, связанных с информационной безопасностью. Среди наших клиентов – крупнейшие компании из ИТ, телекоммуникационной, банковской, финансовой сфер, а также компании, специализирующиеся в области электронной коммерции.

Наши специалисты имеют опыт нахождения уязвимостей на самых защищенных ресурсах. **8 из 10 аудитов заканчивается обнаружением уязвимостей со статусом «Критичный».**

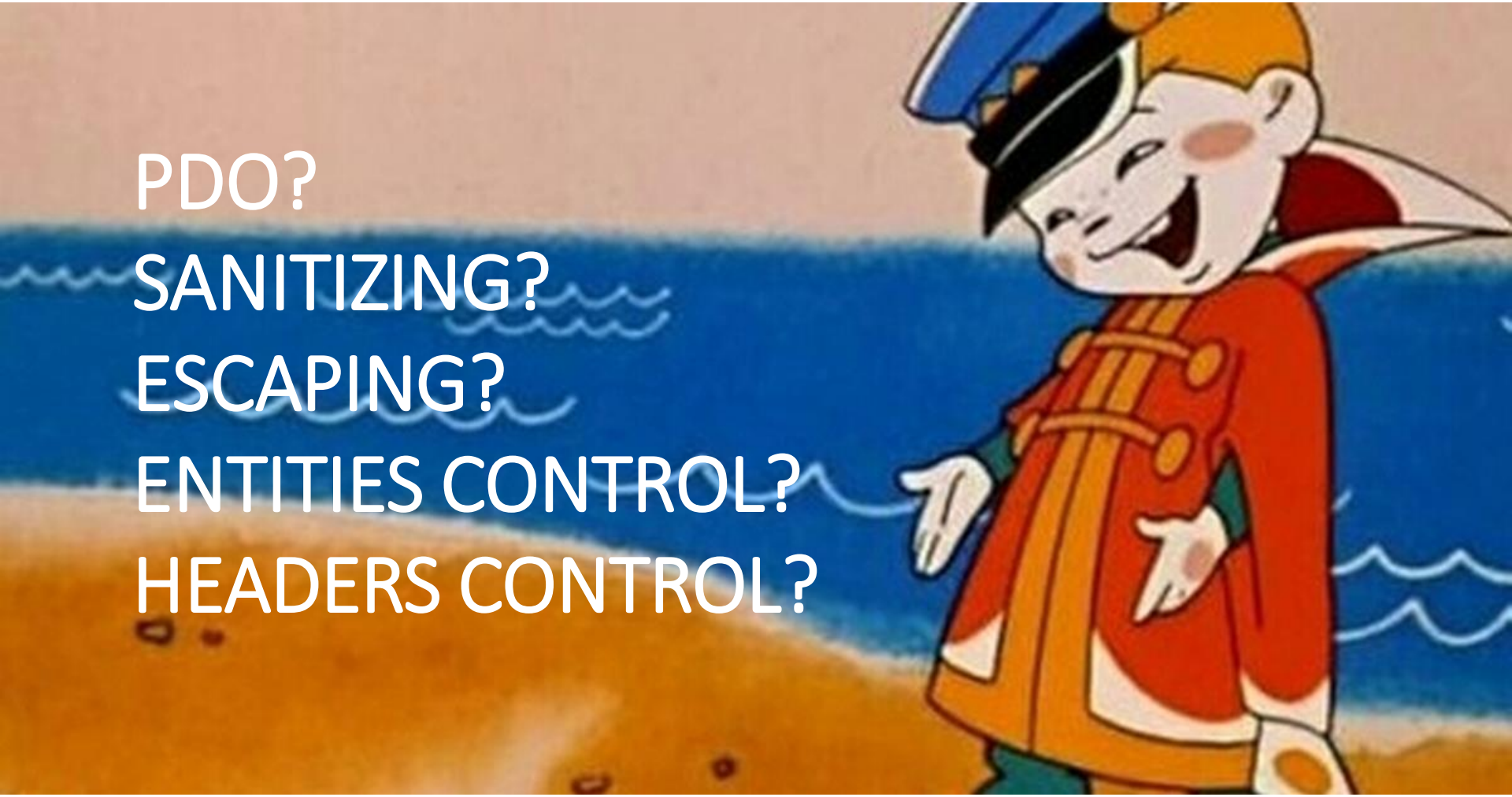
Разработка и поддержка **lab.pentestit.ru** – хакерские лаборатории, имитирующие сеть настоящих компаний: только актуальные уязвимости, более 15.000 участников со всего мира.

Defcon.ru – сообщество специалистов в области практической информационной безопасности.

Почему возможны атаки на веб-приложения?

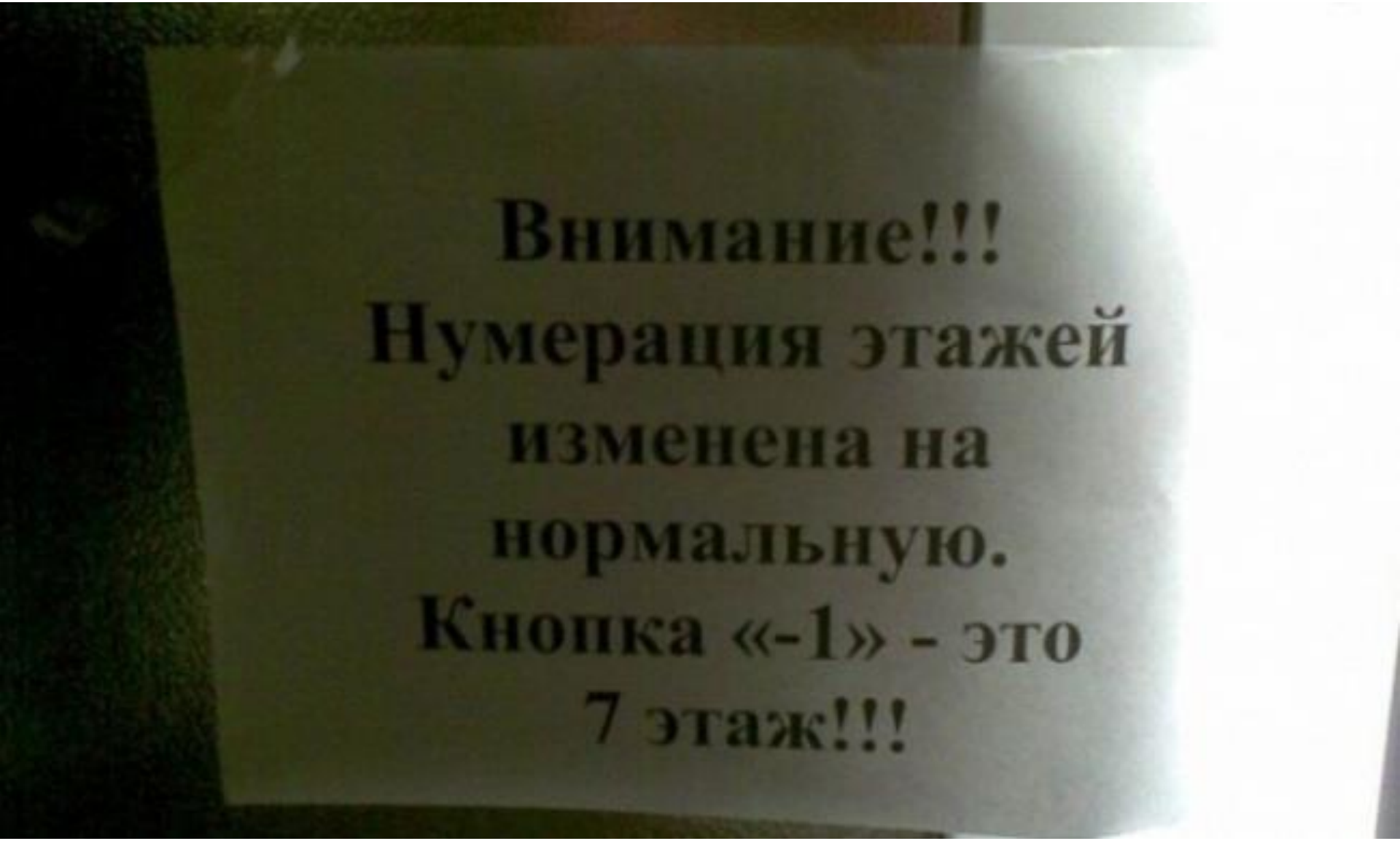
Because hack you, that’s why:

- OWASP TOP 10 – все слышали, но воз и ныне там;
- контроль на этапе разработки – у нас все ок;
- тестирование –может быть, потом, в следующем релизе;
- архитектура – код нормальный, а сервера это не нам;
- full stack senior devops – мне 20 лет и я бородат.


PDO?
SANITIZING?
ESCAPING?
ENTITIES CONTROL?
HEADERS CONTROL?

Все допускают ашибки

- накатим патч;
- даже на сложный продакшн;
- при патч-менеджменте других ошибок не будет;
- точно ошибок не будет, ну или наверно;
- вроде все ок.


Внимание!!!
Нумерация этажей
изменена на
нормальную.
Кнопка «-1» - это
7 этаж!!!

Шутки кончились. За время вступления было отражено %count% атак:

- из них сложных атак:
- ботов:
- сканеров и краулеров:

Самые распространенные атаки:

- попытки выявления критичных файлов и доступа к служебным скриптам;
- попытки выявления уязвимых плагинов/модулей;
- попытки эксплуатации «нашумевших» уязвимостей;
- попытки доступа к критичным зонам;
- использование autopwn-систем и ботов.

Методы защиты:

- на этапе разработке;
- на этапе внедрения;
- на продакшене.

Методы защиты:

Web Application Firewall — защитный экран уровня приложений, предназначенный для выявления и блокирования современных атак на веб-приложения, в том числе и с использованием уязвимостей нулевого дня.

Выявление атак: сигнатурный анализ

Выявление атак: машинное обучение – прецеденты или база знаний

Выявление атак: машинное обучение - закономерности

Выявление атак: математические модели

Выявление атак: репутация

Лучшая защита: комплексные меры

Демо-стенд:
vulns.pentestit.ru

luka@pentestit.ru
telegram: @lukasafonov

2017.pentestit.ru