Основные принципы безопасности

- Безопасность всегда многоуровневая
- Безопасность критически важна
- Протестировать все возможные вектора атаки - невозможно
- Следовательно, "ни одна система не является безопасной"

Стандартные вектора атаки

- SQL injenction
- XSS
- Bruteforce
- Cookie stealing
- Clickjacking
- Social Engineering

SQL Injection

- Позволяет вставить SQL запрос в некие параметры, которые мы считает надежными

- Все современные фреймворки (и адаптеры для бд) предоставляют встроенную защиту от такого рода атак

- Не все ей пользуются

XSS

- Позволяет выполнить чужой код (чаще всего JS) на вашей странице
- Является инъекцией кода на страницу
- Чаще всего через параметры

Content Security Policy

- HTTP заголовок, который предотвращает выполнение загрузку определенных скриптов/стилей

- CSS опасен: http://i8jesus.com/2008/01/05/htmlcss-injections-primitive-malicious-code-or-whats-the-worst-that-could-happen/

Clickjacking

- Ворует нажатие пользователя

- https://learn.javascript.ru/clickjacking

Security in Django

- https://docs.djangoproject.com/es/1.9/topics/security/
- https://docs.djangoproject.com/en/1.9/ref/middleware/#module-django.middleware.security
- https://github.com/sdelements/django-security
- https://github.com/mozilla/django-csp
- ORM, template XSS escaping, CSRF, XFrameOptionsMiddleware,

Популярные в прошлом атаки на Django

- https://www.upguard.com/articles/top-10-django-security-vulnerabilities-and-how-to-fix-them

Уровни безопасности

- Не имеет значения, насколько хорош ваш код, если к базе можно подключиться и вставить/изменить/скачать данные

- Не имеет значения, насколько хорош ваш код, если к серверу можно подключиться по ssh постороннему человеку

- http://www.moscowpython.ru/meetup/31/pravila-bezopasnosti/

Атаки 0-дня

- Все может вас подвести
- Примеры: HTTPS Heartblead, http://www.networkworld.com/article/2168888/network-security/5-examples-of-zero-day-attacks.html

Ситуация не становится лучше

- https://habrahabr.ru/company/pt/blog/268779/