

# Безопасность приложений

---

## Введение

# ТТХ

---

## □ Где и когда

- понедельник в 18:00 в П8-а

## □ Кто

- Андрей Петухов (petand@seclab.cs.msu.su)
  - Иван Новиков (aka Владимир @d0znpp Воронцов, [oxod@onsec.ru](mailto:oxod@onsec.ru))
  - Денис Гамаюнов (gamajun@cs.msu.su)
-

# О чем этот курс

---

- ❑ О том, из каких технологий состоят современные приложения
  - ❑ О том, как эти технологии используются криво
  - ❑ О том, как этим воспользоваться
  - ❑ О том, как это исправить
  - ❑ Что за технологии?
    - HTTP, DNS, клиентские (HTML/CSS/DOM/JS), веб-сервера, сервера приложений, СУБД, технологии уровня ОС
-

# Workflow курса

---

- Тенденции развития технологий и ИБ
  - Хостинг статического контента в Интернет
  - Хостинг динамического контента в Интернет
  - Многопользовательские приложения
  - Многозвенные приложения
-

# Краткая история технологий

---

- Технологии: сетевые, системные, прикладные
  - DNS и клиент-серверные приложения
  - HTTP, HTML и браузерные войны
  - Повышение интерактивности клиентов
  - Повышение уровней абстракции на сервере
    - облачные и мобильные технологии на системном и сетевом уровнях
    - сервис-ориентированный подход на прикладном
    - веб-технологии: от CGI-программ до CMS и сервисов
  - Концепция: «все, что надо – только браузер»
-

# Субъекты и типы недостатков

---

- Субъекты технологического взаимодействия
    - Разработчики
    - Администраторы
    - Пользователи
  - Все могут «косячить»!
  - Недостатки:
    - Проектирования
    - Кодирования
    - Внедрения и настройки
    - Эксплуатации
-

# Application security vs Network & System security

---

- Сетевое и системное ПО – стандартное
    - недостатки внедрения, настройки и эксплуатации
    - проблема 0day
  - Прикладное ПО – кастомное
    - добавляются недостатки проектирования и кодирования
  - Проблемы AppSec
    - колоссальная сложность технологий
    - отсутствие коробочных решений
    - развитие технологий опережает процесс стандартизации
-

# Вопросы?

---

---