ОНЛАЙН-ОБРАЗОВАНИЕ

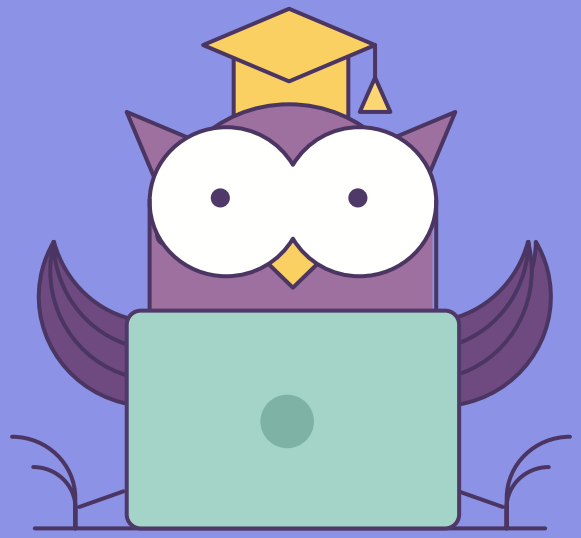
OTUS

Разбор уязвимостей веб-приложений

Часть 5

Колесников Александр Александрович

Меня хорошо слышно && видно?



Напишите в чат, если есть проблемы!

Ставьте + если все хорошо

- NoSQL injection
- Code Review
- PHP wrappers
- Итоги модуля

- Практика и уязвимости:
  - NoSQli
  - PHP Wrappers
  - Code review

01

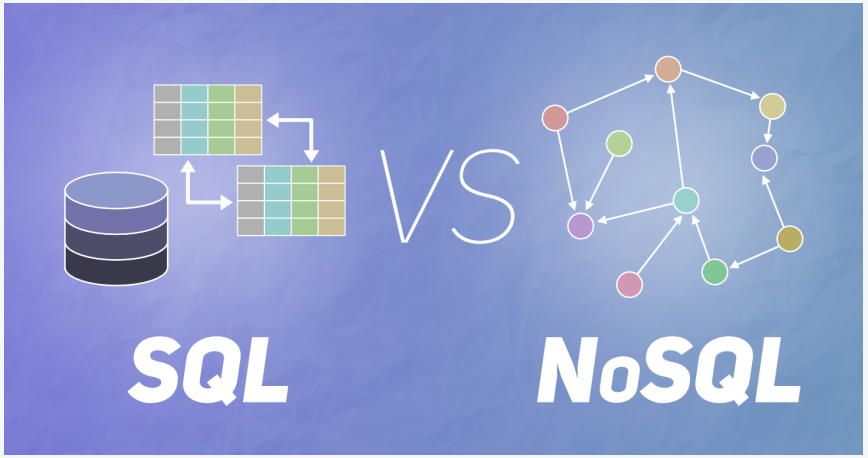
NoSQL injection

No SQL

- Базы данных, в которых нет SQL запросов

- **Какие бывают:**
  - MongoDB
  - CouchDB
  - MemCached

- **Какие особенности есть:**
  - Хранение больших объемов данных
  - Нет стандартного механизма аутентификации
  - Нет общего механизма работы с базами

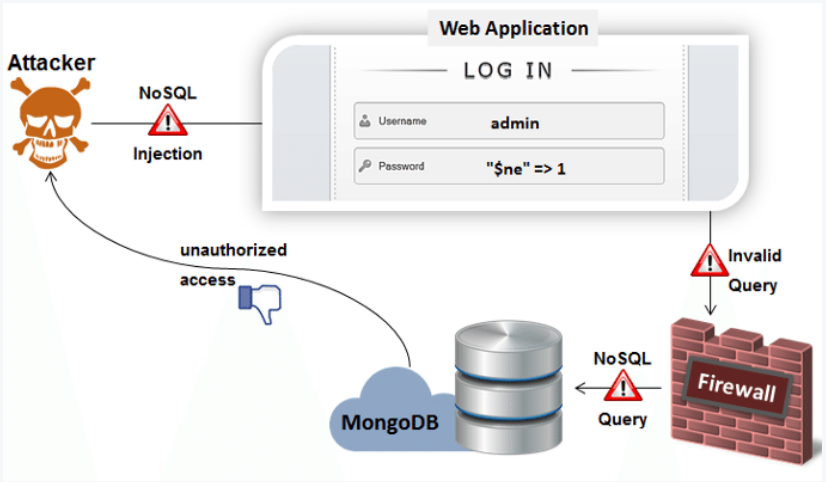


No SQL Injection

- Максимально тривиальная атака

- **Стандартные запросы:**
  - $gt
  - $ne
  - $regex
  - $where

- **Какие особенности есть:**
  - Запросы надо форматировать в JSON

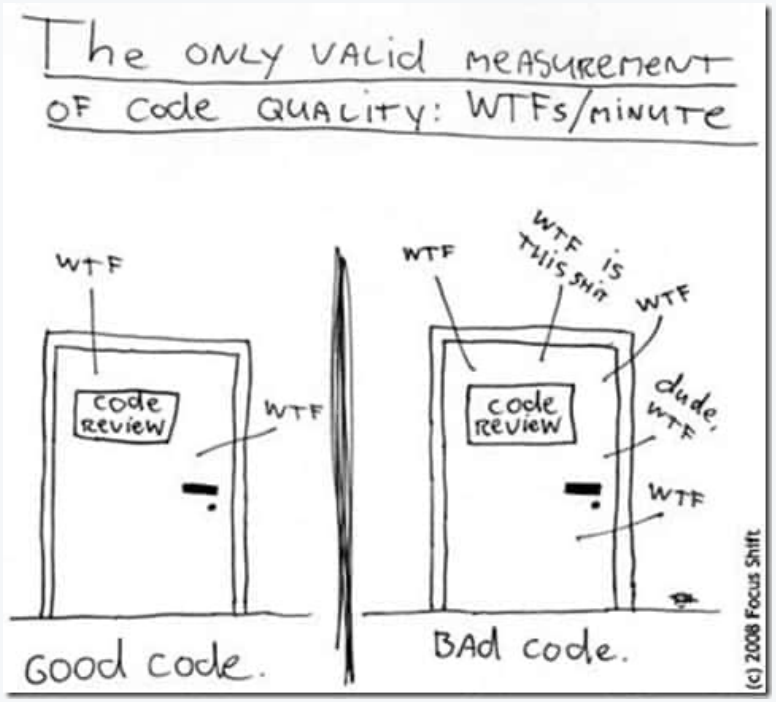


02

Code Review

Тестирование приложений с исходным кодом

- **Определить уязвимые точки:**
  - Работа с файлами
  - Работа с парсерами
  - Работа с компиляторами
- **Сформировать тест-кейс:**
  - Отправить запрос
  - Сформировать файл
  - Подменить шаблон



03

PHP Wrappers

PHP Wrappers

- Механизм, который позволяет представлять данные в различном формате и кодировке.
- **Какие существуют:**
- file:// — Доступ к локальной файловой системе
- http:// — Доступ к URL-адресам по протоколу HTTP(s)
- ftp:// — Доступ к URL-адресам по протоколу FTP(s)
- php:// — Доступ к различным потокам ввода-вывода
- zlib:// — Сжатые потоки
- data:// — Схема Data (RFC 2397)
- glob:// — Нахождение путей, соответствующих шаблону
- phar:// — PHP-архив
- ssh2:// — Secure Shell 2
- rar:// — RAR
- ogg:// — Аудиопотоки
- expect:// — Потоки для взаимодействия с процессами

04

Итоги

Какие темы были изучены

- Какие уязвимости были рассмотрены:
  - SSRF
  - SQLi
  - NoSQLi
  - XSS
  - XXE
  - Command Injection
  - Web Cache Poison
- Что изучить и где найти еще задания:
  - Pentesterlab
  - Hack the box

Тестирование сервисов

Колесников Александр

Спасибо
за внимание!