ОНЛАЙН-ОБРАЗОВАНИЕ

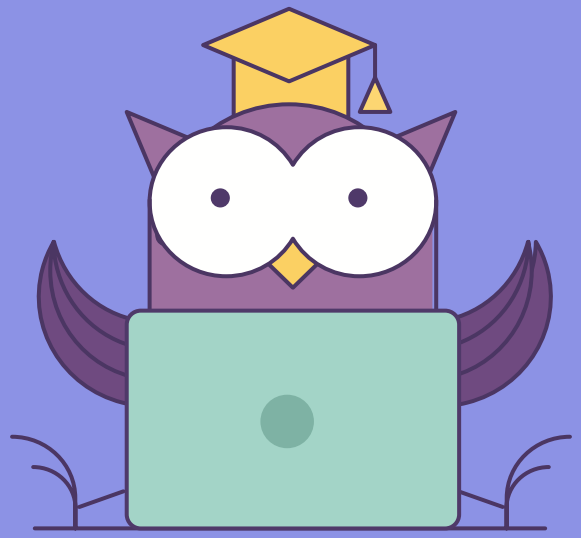
OTUS

Разбор уязвимостей веб-приложений

Часть 2

Колесников Александр Александрович

Меня хорошо слышно && видно?



Напишите в чат, если есть проблемы!

Ставьте + если все хорошо

- Практика и уязвимости:
  - XSS:
    - CSP
  - XML:
    - Encoding
  - Template injection
    - JWT
    - Jinja
  - SSRF

01

XSS

Что такое CSP

- Стандарт, который был разработан для предотвращения XSS, clickjacking и code injection

- Технологии, которые попадают под влияние:
  - JavaScript
  - CSS
  - HTML frames
  - web workers
  - images, Java applets
  - HTML5
  - Video files
  - …
- Имеет несколько версий - крайняя 3.

02

Template Injection

JWT

- JSON Web Tokens - метод аутентификации пользователя на веб ресурсе
- Описаны в RFC 7519
- Составные части JWT:
  - Header
  - Payload
  - Signature

03

Template Injection

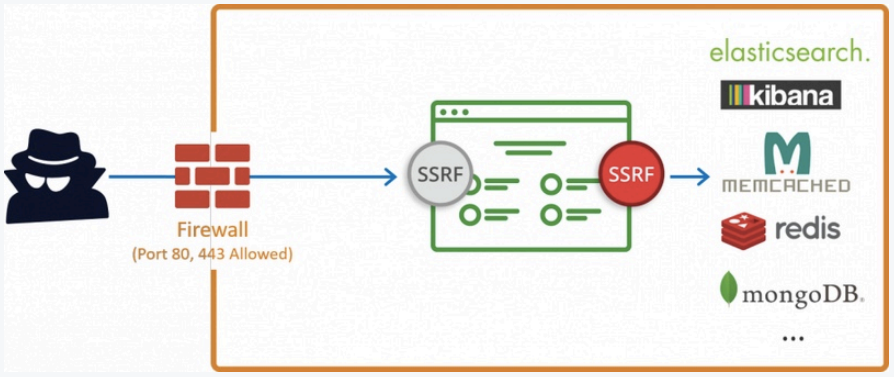
04

SSRF

SSRF

- Тип уязвимостей, который заставляет сервер выполнить запрос или действие

- Может приводить к:
  - Утечке информации
  - Любому типу уязвимости



Тестирование сервисов

Колесников Александр

Спасибо
за внимание!