ОНЛАЙН-ОБРАЗОВАНИЕ

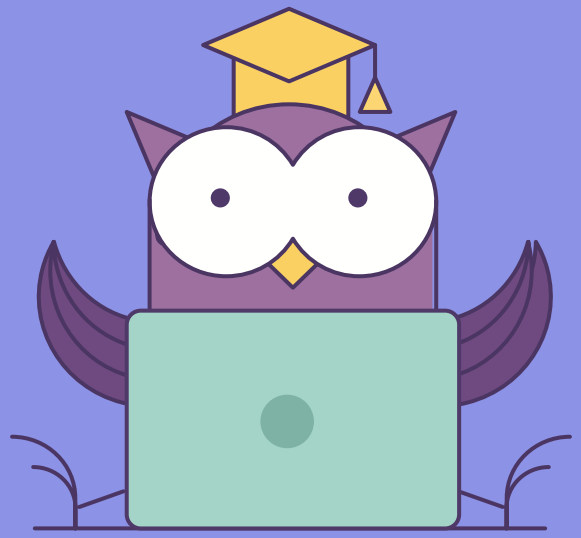
OTUS

Разбор уязвимостей веб-приложений

Часть 3

Колесников Александр Александрович

Меня хорошо слышно && видно?



Напишите в чат, если есть проблемы!

Ставьте + если все хорошо

Содержание

- WAF
- Практика и уязвимости:
    - Deserialization
        - Php
    - Template injection
        - JWT
    - SSRF

01

Template Injection

WAF

- Web Application Firewall
- Приложение, которое отслеживает атаки, которые проводятся на приложение
- Работает с 1 протоколом, чаще всего http
- Может детектировать отдельные payload отправляемые приложению
- Пример WAF: OWASP ModSecurity

Способы обхода

- Атака на FireWall:
  - RegExp Bomb
  - DDos
- Изменение payload:
  - Кодирование
  - Использование непопулярных команд
  - Замена разделителей

02

Template Injection

JWT

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

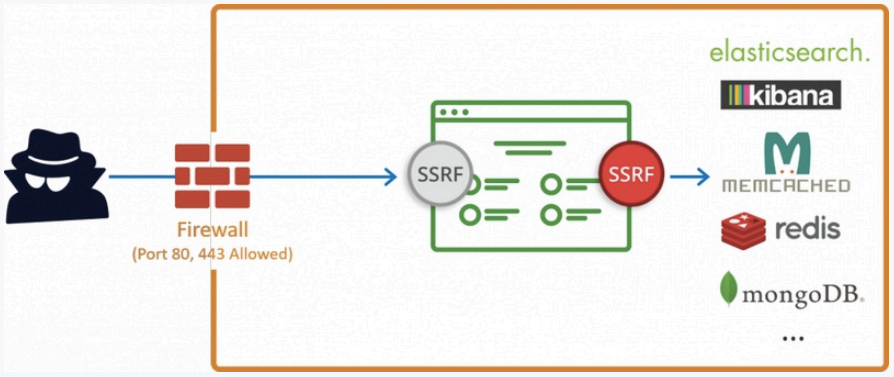
03

SSRF

SSRF

- Тип уязвимостей, который заставляет сервер выполнить запрос или действие

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

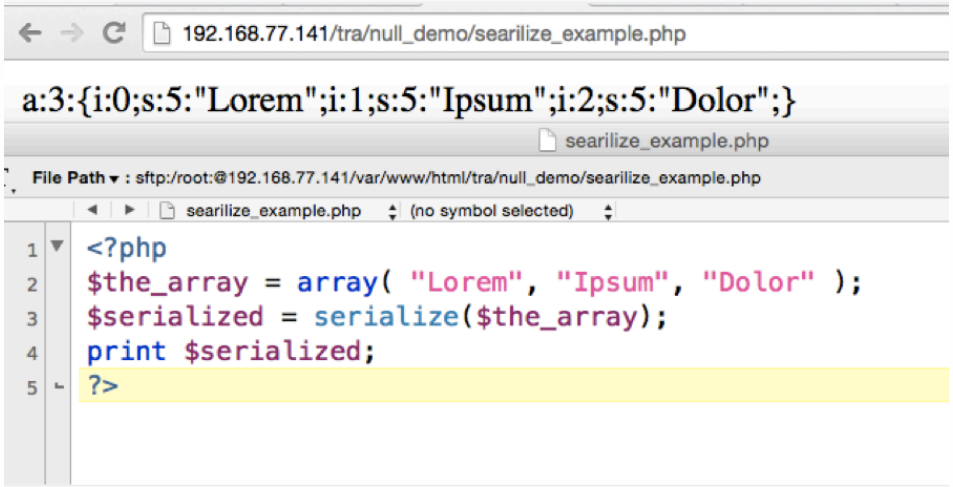


03

SSRF

Deserialization attack

- Уязвимость, которая появляется в следствии того, что приложение выполняет код на основании данных, которые предоставил пользователь
- Уязвимые языки:
  - Php
  - Java
  - .NET
  - Python
  - Ruby
- Может приводить к:
  - Выполнению кода
  - Патчингу логики приложения
  - Любому типу уязвимости



Тестирование сервисов

Колесников Александр

Спасибо
за внимание!