



ОНЛАЙН-ОБРАЗОВАНИЕ

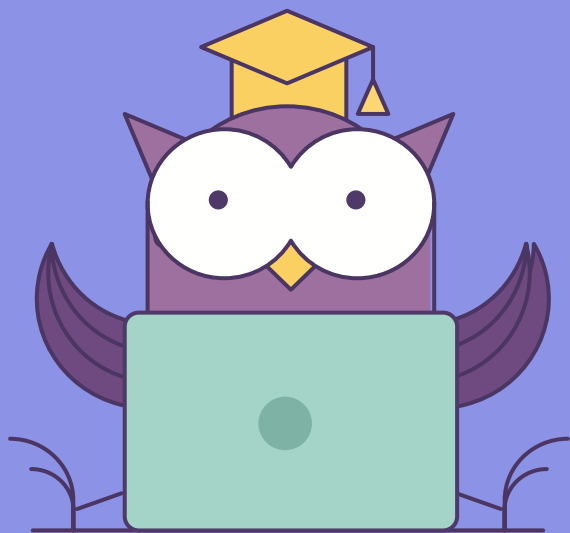


# Разбор уязвимостей веб-приложений

Часть 2



# 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**



- 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

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

```
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6IkpvaG4gRG91IiwiaWF0IjoxNTE2MjM5MDIyfQ.SflKxwRJSMeKKF2QT4fwpMeJf36P0k6yJV_adQssw5c
```

HEADER: ALGORITHM & TOKEN TYPE

```
{  
  "alg": "HS256",  
  "typ": "JWT"  
}
```

PAYLOAD: DATA

```
{  
  "sub": "1234567890",  
  "name": "John Doe",  
  "iat": 1516239022  
}
```

VERIFY SIGNATURE

```
HMACSHA256(  
  base64UrlEncode(header) + "." +  
  base64UrlEncode(payload),  
  your-256-bit-secret  
)  
 secret base64 encoded
```

03

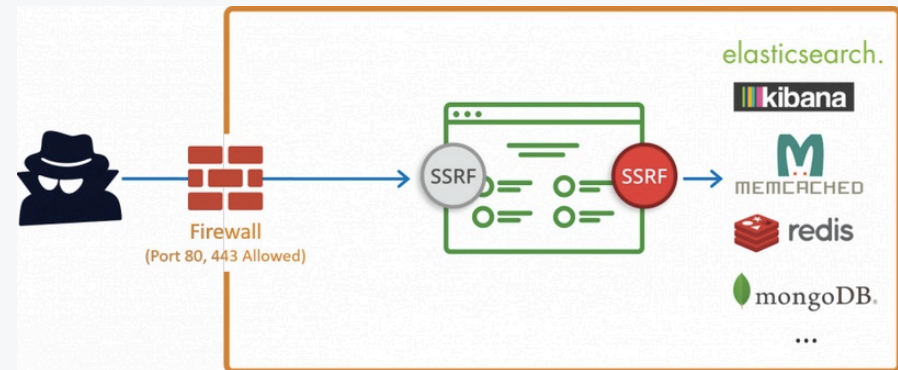
# Template Injection

04

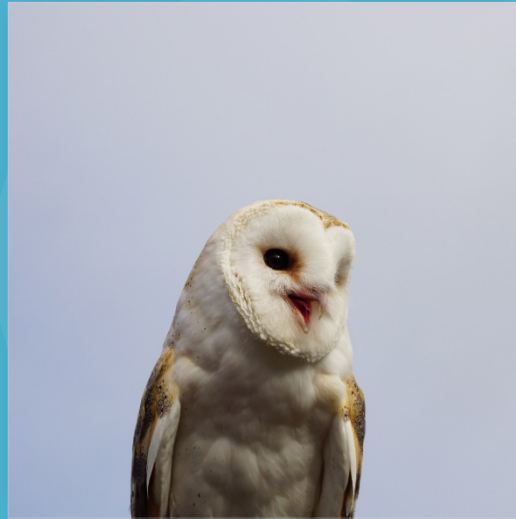
**SSRF**



- Тип уязвимостей, который заставляет сервер выполнить запрос или действие
- Может приводить к:
  - Утечке информации
  - Любому типу уязвимости



# Тестирование сервисов



**Колесников Александр**

**Спасибо  
за внимание!**

