

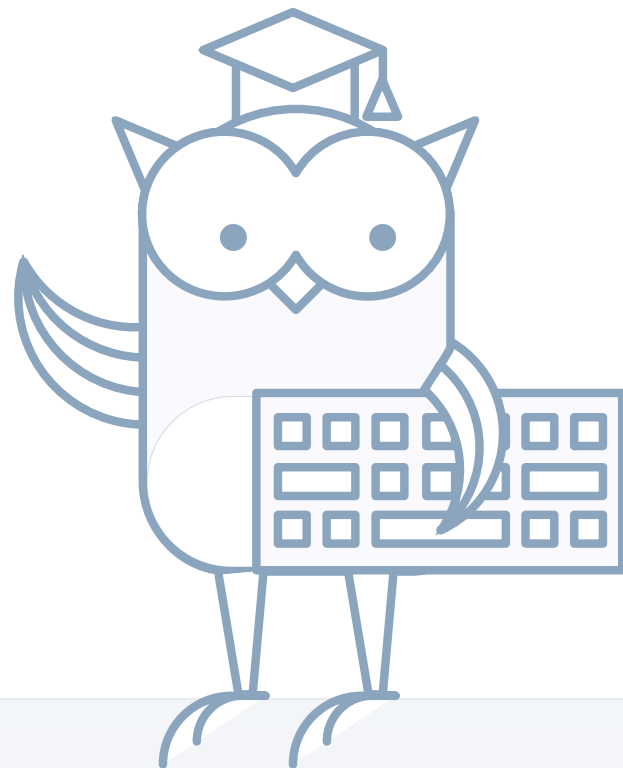


ОНЛАЙН-ОБРАЗОВАНИЕ

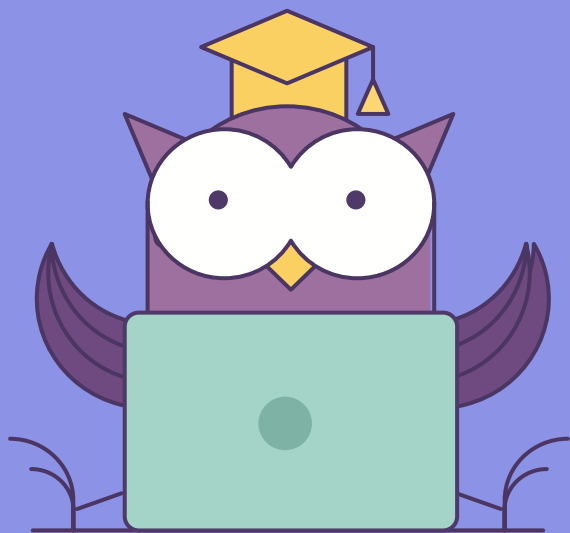


Разбор уязвимостей веб-приложений

Часть 3



Меня хорошо слышно && видно?



Напишите в чат, если есть проблемы!

Ставьте если все хорошо

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

01

Template Injection

- 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



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



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

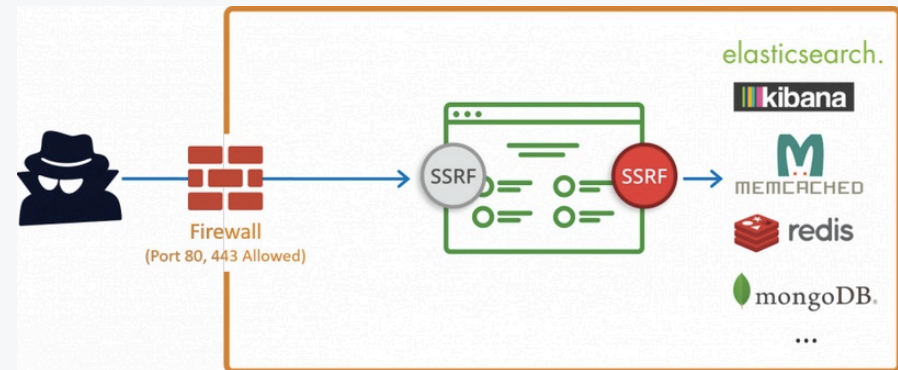
```
HMACSHA256(  
  base64UrlEncode(header) + "." +  
  base64UrlEncode(payload),  
  your-256-bit-secret  
)  
 secret base64 encoded
```

03

SSRF



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



03

SSRF

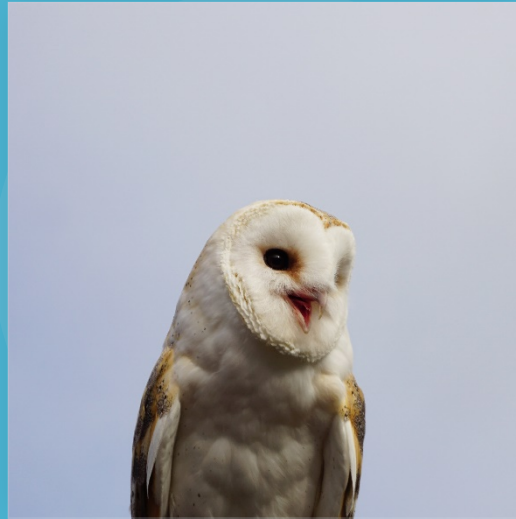


- Уязвимость, которая появляется в следствии того, что приложение выполняет код на основании данных, которые предоставил пользователь
- Уязвимые языки:
 - Php
 - Java
 - .NET
 - Python
 - Ruby
- Может приводить к:
 - Выполнению кода
 - Патчингу логики приложения
 - Любому типу уязвимости



```
<?php
1
2 $the_array = array( "Lorem", "Ipsum", "Dolor" );
3 $serialized = serialize($the_array);
4 print $serialized;
5 ?>
```

Тестирование сервисов



Колесников Александр

**Спасибо
за внимание!**

