

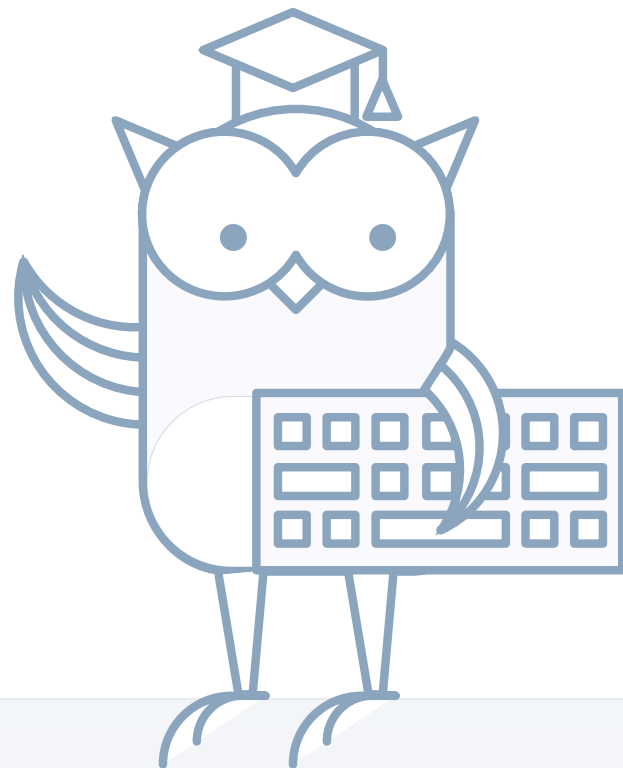


ОНЛАЙН-ОБРАЗОВАНИЕ

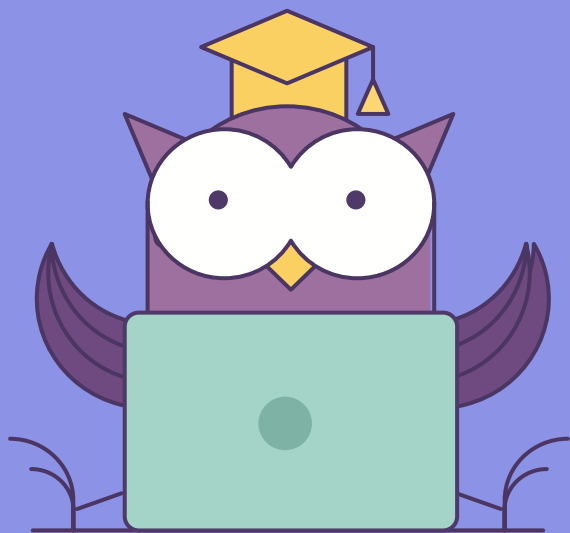


Разбор уязвимостей веб-приложений

Часть 1



Меня хорошо слышно && видно?



Напишите в чат, если есть проблемы!

Ставьте если все хорошо

- Практика:
 - Burp Suite
 - Уязвимости:
 - XSS
 - sqli

01

SQLi



- Возникает при неправильной обработке пользовательского ввода
- Возможна при:
 - Неверной конфигурации сервера бд
 - Наличии неверной процедуры формирования запроса в базу
- Присутствует как в обычных приложениях, так и в web



02

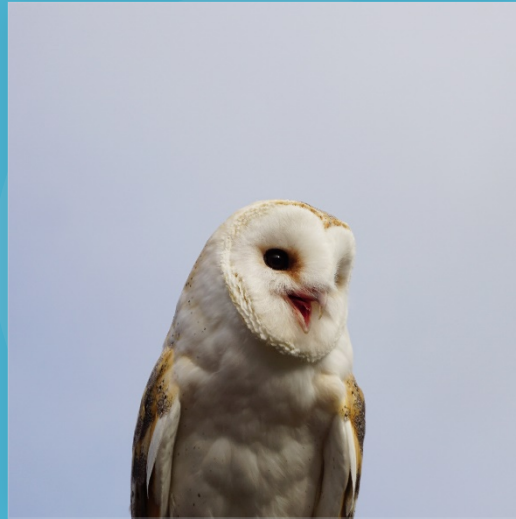
XXE



- Уязвимость, которая находится в парсеке формата файла
- Самые популярные уязвимости:
 - XXE
 - XPath
 - Billion of laughs
- Что можно сделать:
 - Прочитать файл
 - Вызвать команду

```
<?xml version="1.0" encoding="iso-8859-8" standalone="yes" ?>
<CURRENCIES>
  <LAST_UPDATE>2004-07-29</LAST_UPDATE>
  <CURRENCY>
    <NAME>dollar</NAME>
    <UNIT>1</UNIT>
    <CURRENCYCODE>USD</CURRENCYCODE>
    <COUNTRY>USA</COUNTRY>
    <RATE>4.527</RATE>
    <CHANGE>0.044</CHANGE>
  </CURRENCY>
  <CURRENCY>
    <NAME>euro</NAME>
    <UNIT>1</UNIT>
    <CURRENCYCODE>EUR</CURRENCYCODE>
    <COUNTRY>European Monetary Union</COUNTRY>
    <RATE>5.4417</RATE>
    <CHANGE>-0.013</CHANGE>
  </CURRENCY>
</CURRENCIES>
```

Тестирование сервисов



Колесников Александр

**Спасибо
за внимание!**

