ОНЛАЙН-ОБРАЗОВАНИЕ

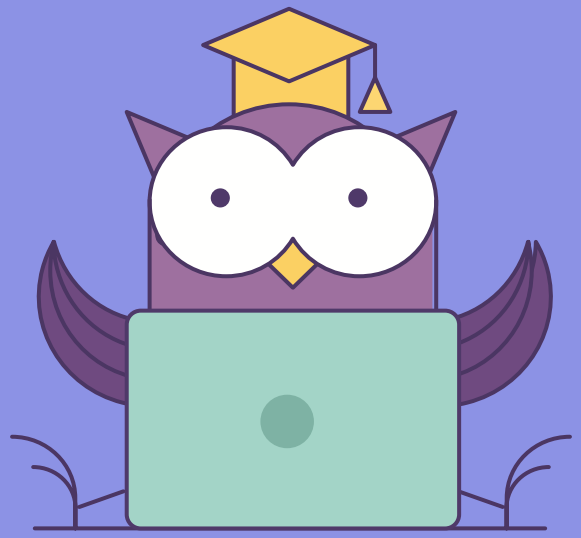
OTUS

Классификация уязвимостей веб-приложений.

Способы эксплуатации. Часть 2

Колесников Александр Александрович

Меня хорошо слышно && видно?



Напишите в чат, если есть проблемы!

Ставьте + если все хорошо

Содержание

- Burp Suite - основные команды
- Эксплуатация и поиск:
  - Sqli
  - XXE
  - NoSQL
  - SSTi

00

Burp Suite

Основной инструмент

- Основной инструмент при тестировании web-приложений
- Включает в себя:
  - Proxy
  - Intruder
  - Repeater
  - Sequencer
  - Инструменты для декодирования и сравнения запросов
  - Есть возможность расширения функционала
- Документация

01

SQli

Насколько опасны данные?

- 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

Безобидный XML

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

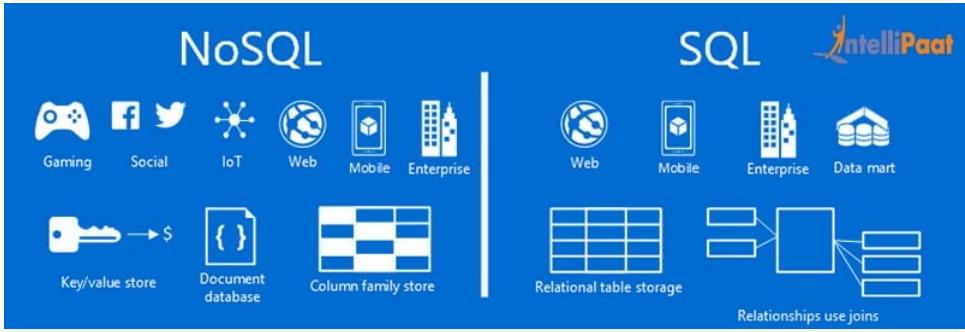
```
<?xml version="1.0" encoding="iso-8859-8" standalone="yes" ?>
<CURRENCIES>
  <LAST_UPDATE>2004-07-29</LAST_UPDATE>
  <CURRENCY>
    <NAME>dollar</NAME>
    <UNIT>1</UNIT>
    <CURRENCYCODE>USD</CURRENCYCODE>
    <COUNTRY>USA</COUNTRY>
    <RATE>4.527</RATE>
    <CHANGE>0.044</CHANGE>
  </CURRENCY>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

03

NoSQL

Снова данные

- NOSql отличная от реляционной архитектуры баз
- Так же включает в себя специальный порядок выполнения команд
- Практически всегда выдает доступ без авторизации =)

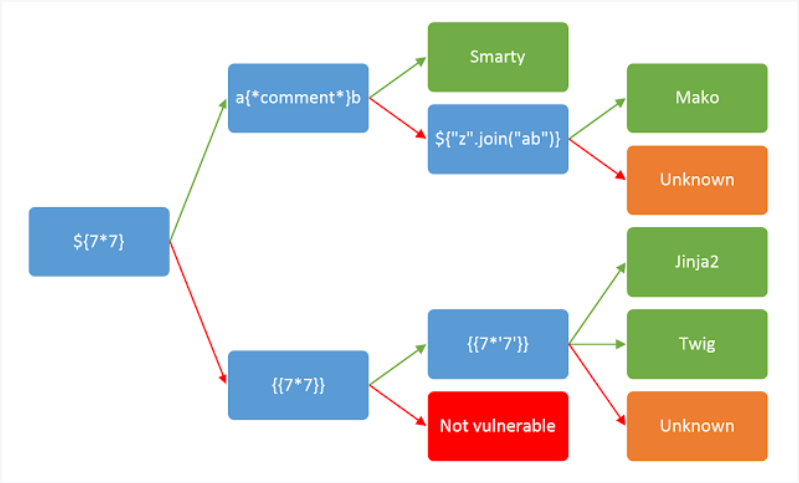


03

SSTi

Сервер не знает что делать

- Уязвимость, которая возникает в «песочницах пользовательского интерфейса»
- Инжект специальный символов может привести к RCE
- Подвержены все языки, на которых пишутся FrameWork` и для создания динамического пользовательского интерфейса



Тестирование сервисов

Колесников Александр

Спасибо
за внимание!