Веб уязвимости

Подготовил: Муковкин Дмитрий

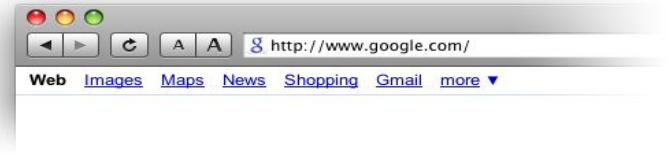
Содержание курса

1. Протоколы
2. Технологии
3. XSS, CSRF
4. SQL-injection
5. Pentest
6. Стандарты

Содержание

В этой лекции будут рассмотрены основные моменты работы веб приложений.

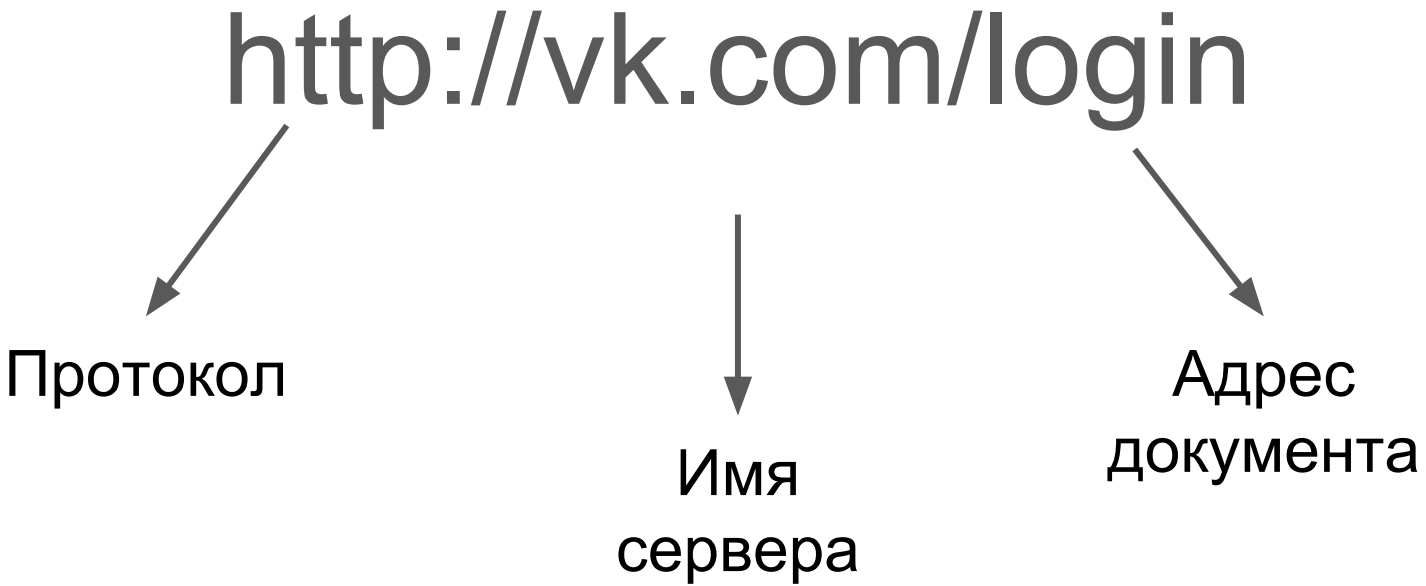
Мы набираем адрес в строке...



Браузер отсылает запрос
сервер и ожидает ответа

Сервер получает запрос,
обрабатывает его
и возвращает ответ

Что делает браузер



Имя сервера

vk.com  87.240.180.136

DNS

DNS

Распределённая система для получения информации о доменах

Появился в 1983 году.

Интернет появился в 70-ых годах. Как жили до DNS?

DNS 1970-ого года

Файл hosts

(/etc/hosts, C:/Windows/System32/drivers/etc/hosts)

127.0.0.1 localhost

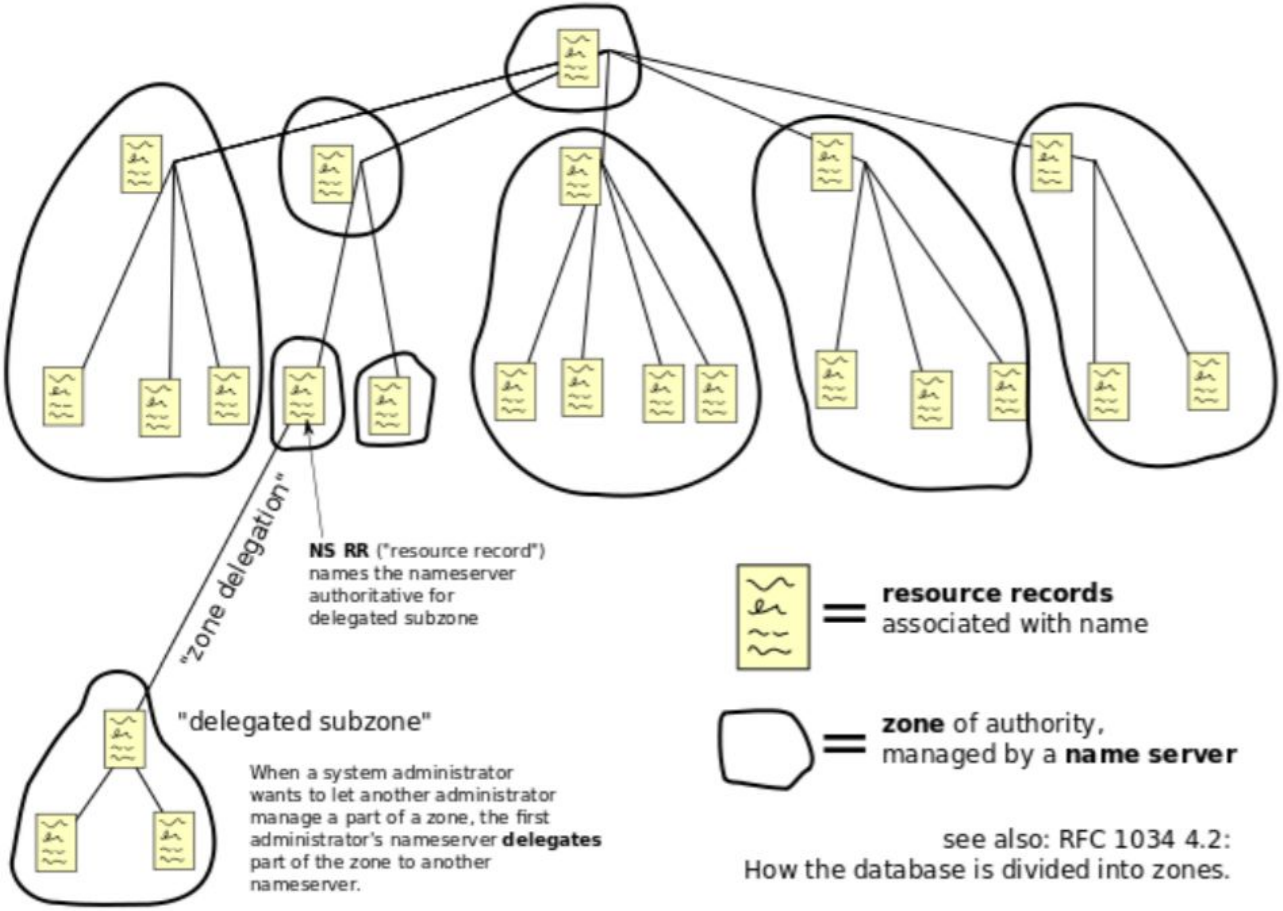
www.ru.

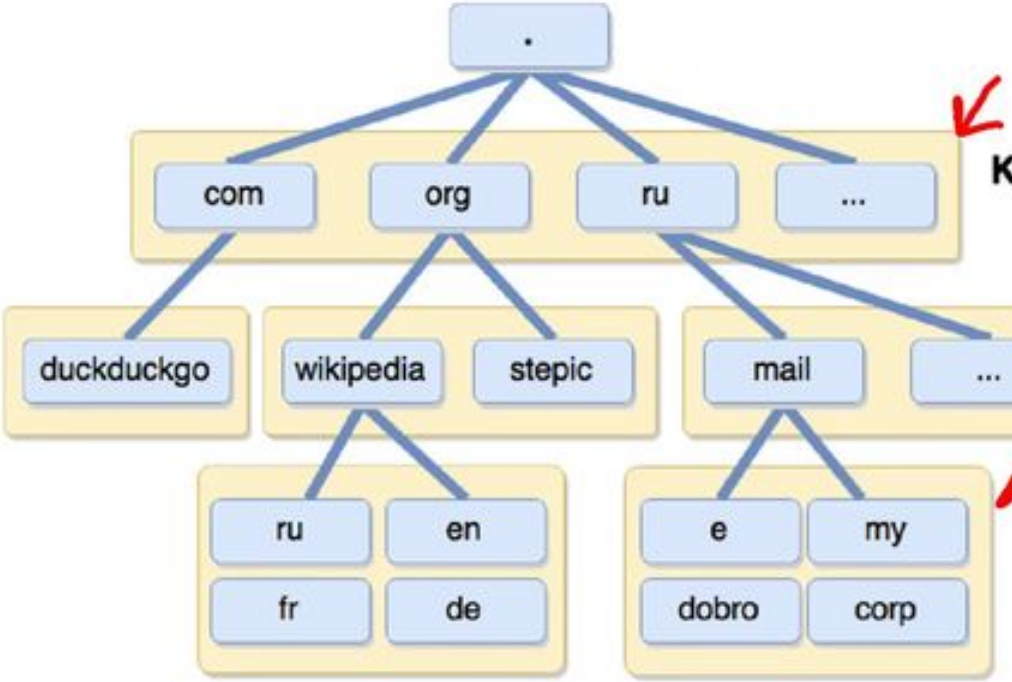
www.com.

Иерархия имен DNS

- com
- net
- org
- gov
- mil
- ru
- arpa
- рф - как он кодируется?

Domain Name Space

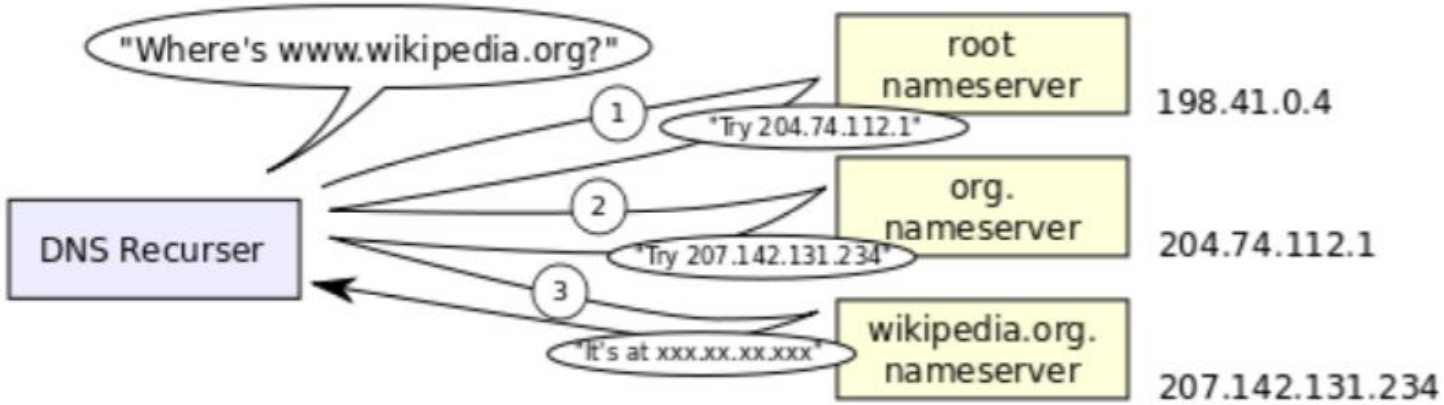




Корневые DNS сервера

DNS рунета

DNS mail.ru



Этап 0 - просмотр кэша

Сколько в мире корневых серверов DNS?

Корневые DNS

13 корневых серверов

Linux:

```
host -a .
```


Satellite
Photos
Greenland
Iceland
Norway
Russia
Canada
United States
Mexico
Kazakhstan
Mongolia
China
South Korea
Ukraine
Italy
Spain
Algeria
Libya
Egypt
Iraq
Saudi Arabia
Mali
Niger
Chad
Sudan
Nigeria
Kenya
DR Congo
Tanzania
Angola
Namibia
Botswana
Madagascar
South Africa
Venezuela
Colombia
Peru
Brazil
Bolivia
Argentina
Indonesia
Papua New Guinea
Australia
New Zealand
North Atlantic Ocean
North Pacific Ocean
South Pacific Ocean
South Atlantic Ocean
Indian Ocean
Southern
2000 mi
2000 km

DNS

Двоичные запросы

- рекурсивные
- итеративные (нерекурсивные)

Ответы

- Авторитарные
- Кешированные

Протоколы

Основные использующиеся протоколы в вебе:

1. HTTP
2. HTTPS

HTTP

Протокол прикладного уровня передачи данных.

Использует 80 порт.

Состоит из:

- Стартовая строка
- Заголовок
- Тело сообщения

Стартовая строка клиента

```
GET /wiki/HTTP
HTTP/1.0
Host: ru.wikipedia.org
```

Стартовая строка сервера

```
HTTP/1.0 200 OK
```

HTTP (стартовая строка)

Стартовая строка клиента

```
GET /wiki/HTTP
HTTP/1.0
```

Стартовая строка сервера

```
HTTP/1.0 200 OK
```

Методы HTTP

- GET
- POST
- PUT
- DELETE
- OPTIONS
- HEAD
- TRACE
- CONNECT
- PATCH

HTTP (заголовок)

Клиент

Host: vk.com
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (X11; Linux x86_64)
AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/47.0.2526.73 YaBrowser/16.2.0.1818 (beta)
Safari/537.36
Content-Type: text/plain;charset=UTF-8
Accept: */*
DNT: 1
Accept-Encoding: gzip, deflate
Accept-Language: ru,en;q=0.8,it;q=0.6
Cookie: _ym_uid=1448901273605329984;

Сервер

Server: nginx
Date: Tue, 16 Feb 2016 12:45:12 GMT
Content-Type: text/html; charset=Windows-1251
Content-Length: 0
Connection: keep-alive
X-Powered-By: PHP/5.2.5
Content-Language: ru

HTTP (Тело сообщения)

Клиент

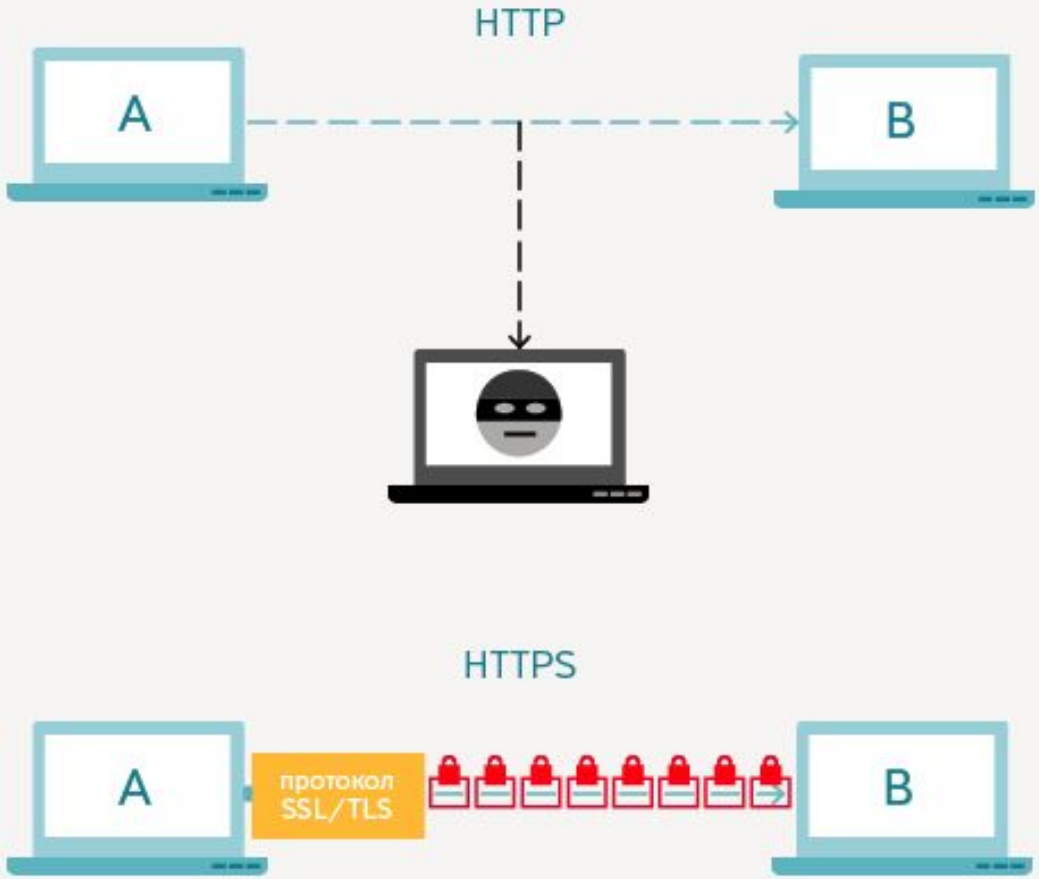
```
--Asrf456BGe4h
Content-Disposition: form-data;
name="DestAddress"
(пустая строка)
brutal-vasya@example.com
--Asrf456BGe4h
Content-Disposition: form-data;
name="MessageTitle"
(пустая строка)
Test message
```

Сервер

```
<!DOCTYPE HTML>
<html lang='ru'>
<head>
<meta charset='UTF-8'>
…..
```

Либо

```
<Двоичное содержимое>
```


HTTP
A
B
HTTPS
A
протокол
SSL/TLS
B

HTTPS

1.

2.

3.

4.

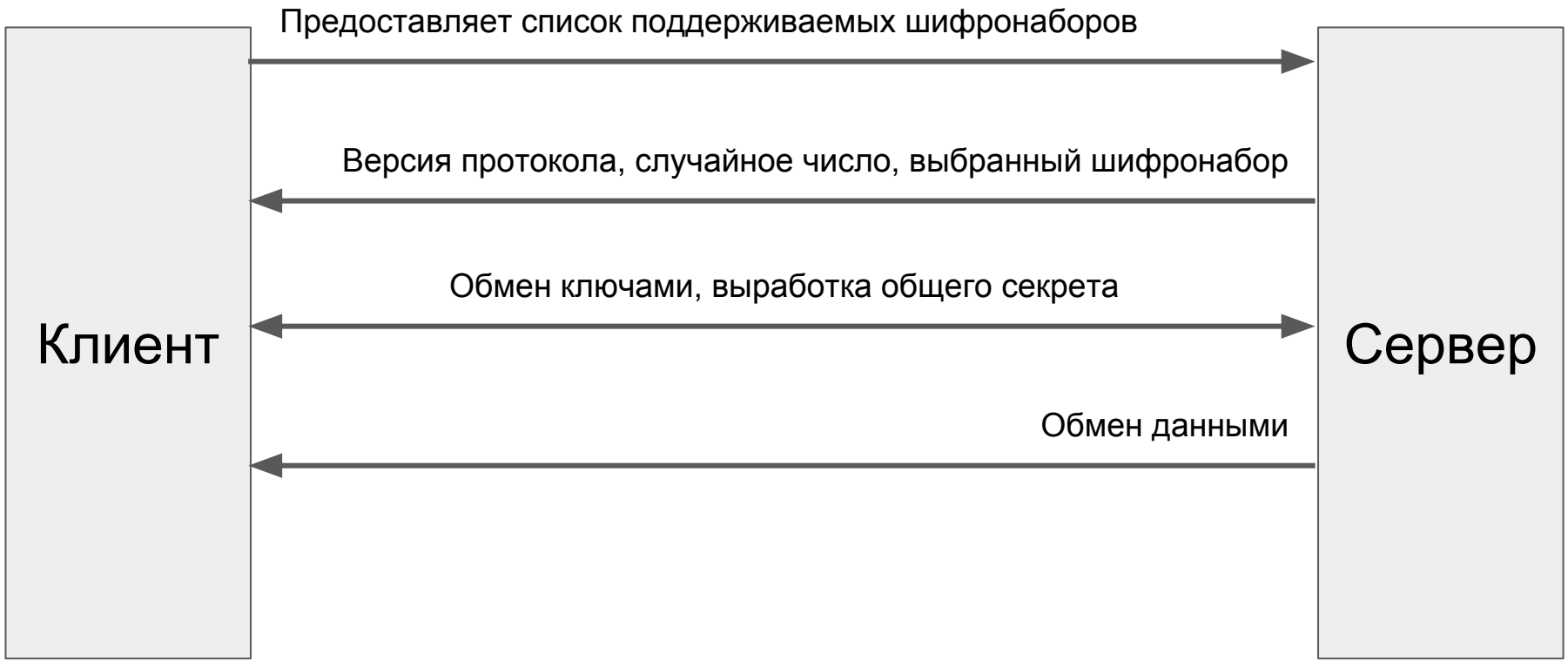
HTTPS

Расширение протокола HTTP, поддерживающее шифрование.

Данные, передаваемые по протоколу HTTPS, «упаковываются» в криптографический протокол SSL или TLS.

В отличие от HTTP, для HTTPS по умолчанию используется TCP-порт 443.

HTTPS и TLS


Предоставляет список поддерживаемых шифронаборов
Версия протокола, случайное число, выбранный шифронабор
Обмен ключами, выработка общего секрета
Обмен данными
Клиент
Сервер

На этом, кажется, все

Вопросы?

Всем спасибо за внимание

Следующая тема лекции - Технологии.