Тестирование защищенности веб-приложений

Структура курса

1. Основные принципы компроментации
2. Уязвимости серверной части
3. Уязвимости клиентской части
4. SOAP API и JSON API. Общий чек-лист

Занятие 1

Основные принципы компроментации веб-приложений

План занятия

- Основы тестирования защищенности
  - Что тестируем?
  - Почему это проблема?
- Защищенность веб-приложени
- Протокол HTTP

ТЗ: Что тестируем?

ГОСТ Р ИСО/МЭК 9126-93

- Функциональность
- Надежность
- Практичность (удобство)
- Эффективность
- Сопровождаемость
- Мобильность

ГОСТ Р ИСО/МЭК 9126-93

- **Функциональность**
  - Пригодность для применения
  - Корректность (правильность, точность)
  - Способность к взаимодействию
  - **Защищенность**

Куда вставить частицу НЕ?

- качественная программа:
  - делает то, что должна делать

- **НЕ**качественная программа:
  - **НЕ** делает то, что должна делать
    - «традиционный» функциональный б
  - делает то, что **НЕ** должна делать
    - баг защищенности

Про это НЕ пишут в спецификации

- Пользователь с ролью “user” может менять свои личные данные
- Пользователь с ролью “admin” может менять данные любого пользователя

- Пользователь с ролью **НЕ** “user” и **НЕ** “admin” может менять чьи-то данные
- Пользователь с ролью “user” может менять **НЕ** свои данные

Более формальное определение

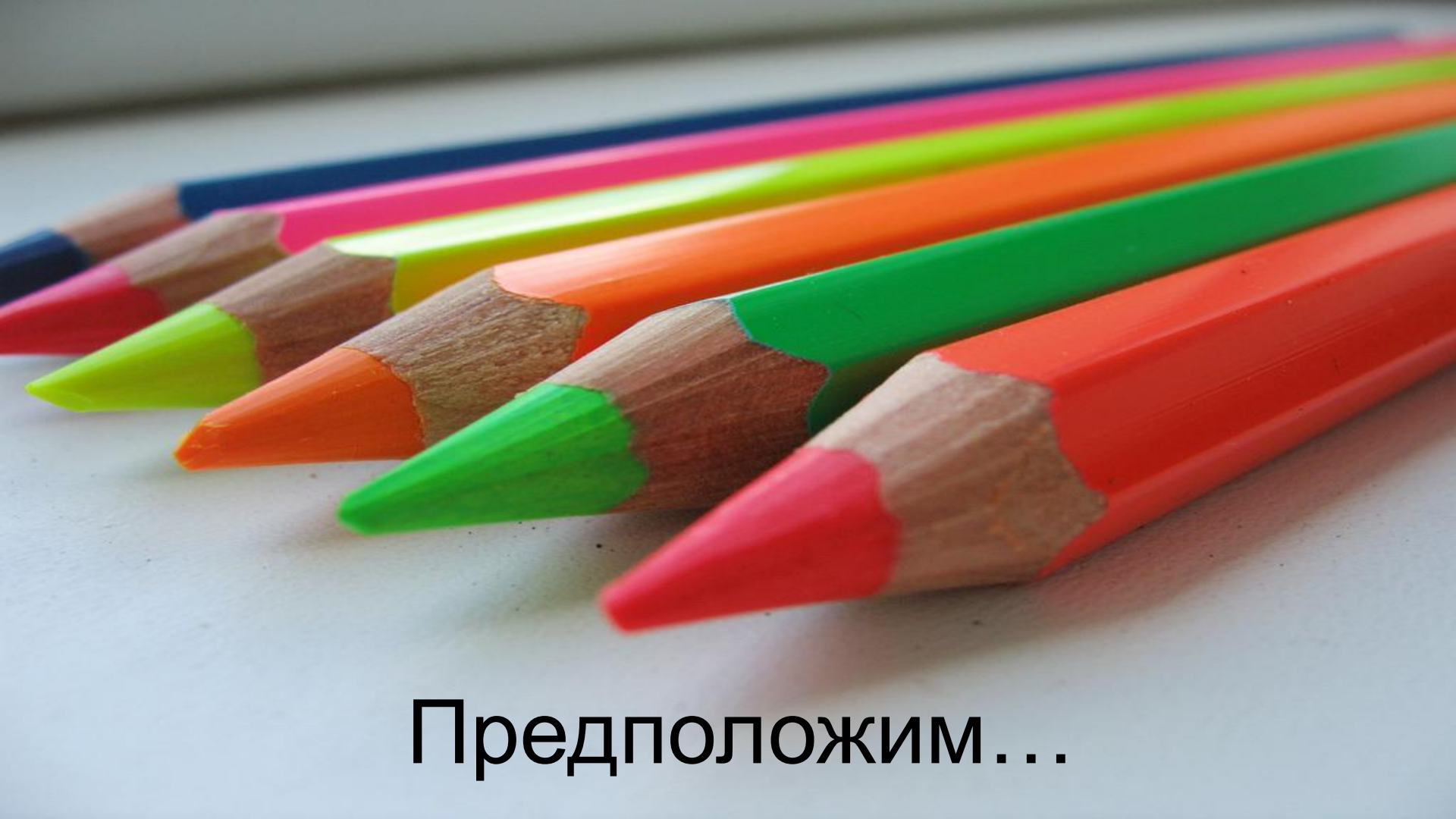
- Нарушение функциональности:
  - **НЕ**возможность получения **санкционированного** доступа к функциям и данным системы
- Нарушение защищенности:
  - возможность получения **НЕсанкционированного** доступа к данным и функциям

Почему это проблема?

Почему это проблема?

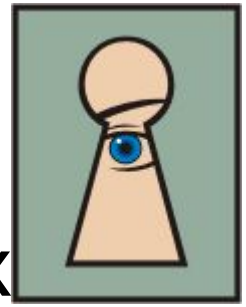
- Несанкционированный доступ к данным:
  - чтение данных
  - модификация данных
  - разрушение данных

- Несанкционированный доступ к функциям:
  - модификация данных или системы
  - разрушение данных или системы



Предположим…

Чтение данных



- Конкуренты узнали телефоны ваших клиентов, сделали им предложение, клиенты решили сменить поставщика

- Конкуренты получают информацию о том, как у вас идут дела, что чаще заказывают ваши клиенты, проводят ответные акции

Модификация данных

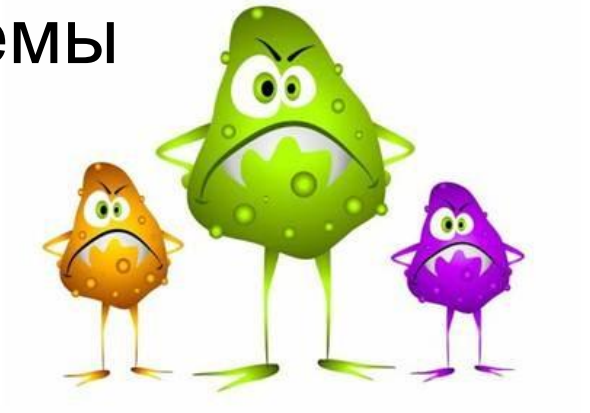
- Конкуренты меняют телефоны и адреса ваших клиентов, вы не можете с ними связаться
- Конкуренты «накручивают» цены в вашем прейскуранте, клиенты уходят
- Конкуренты портят ссылки, картинки в каталоге товаров, клиенты недовольны

Разрушение данных

Хорошо, если есть резервная копия…

Модификация системы

- Внедрение вирусов и «троянов»
- Создание помех в работе системы
  - функциональные неточности
  - снижение производительности
- Использование ресурсов системы
  - как части ботнета
  - для иных целей



Разрушение системы

Хорошо, если есть резервная копия…

Более формальное определение

- Нарушение функциональности:
  - **НЕ**возможность получения **санкционированного** доступа к функциям и данным системы
- Нарушение защищенности:
  - возможность получения **НЕсанкционированного** доступа к данным и функциям

Способы доступа к системе

- Предусмотренные спецификацией
  – зона функционального тестирования

- **НЕ** предусмотренные спецификацией
  – зона тестирования защищенности

Немного терминологии

- Уязвимость
  - непредусмотренный спецификацией способ доступа к функциям или данным системы
- Атака
  - действия, нацеленные на поиск узявимостей
  - действия, нацеленные на нанесение ущерба
- Вектор атаки
  - отдельное действие в процессе атаки (типа 1)

Тестировщик – не «хакер»!

- Нет злого умысла
- Достаточно найти **потенциальные** уязвимости, не требуется их эксплуатация

Статья 272 УК РФ

Статья 272. Неправомерный доступ к компьютерной информации

1. Неправомерный доступ к охраняемой законом компьютерной информации, то есть информации на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети, - наказывается штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо обязательными работами на срок от ста двадцати до ста восьмидесяти часов, либо исправительными работами на срок до одного года, либо лишением свободы на срок до двух лет.

Уязвимости веб-приложений

Способы доступа к системе

- Предусмотренные спецификацией
  – зона функционального тестирования

- **НЕ** предусмотренные спецификацией
  – зона тестирования защищенности

Как искать «непредусмотренное»?

Каталоги уязвимостей

- OWASP
  The Open Web Application Security Project
  https://www.owasp.org/

- CWE
  Common Weakness Enumeration
  http://cwe.mitre.org/

Каталоги уязвимостей

- OWASP Top 10

  https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

- CWE/SANS Top 25

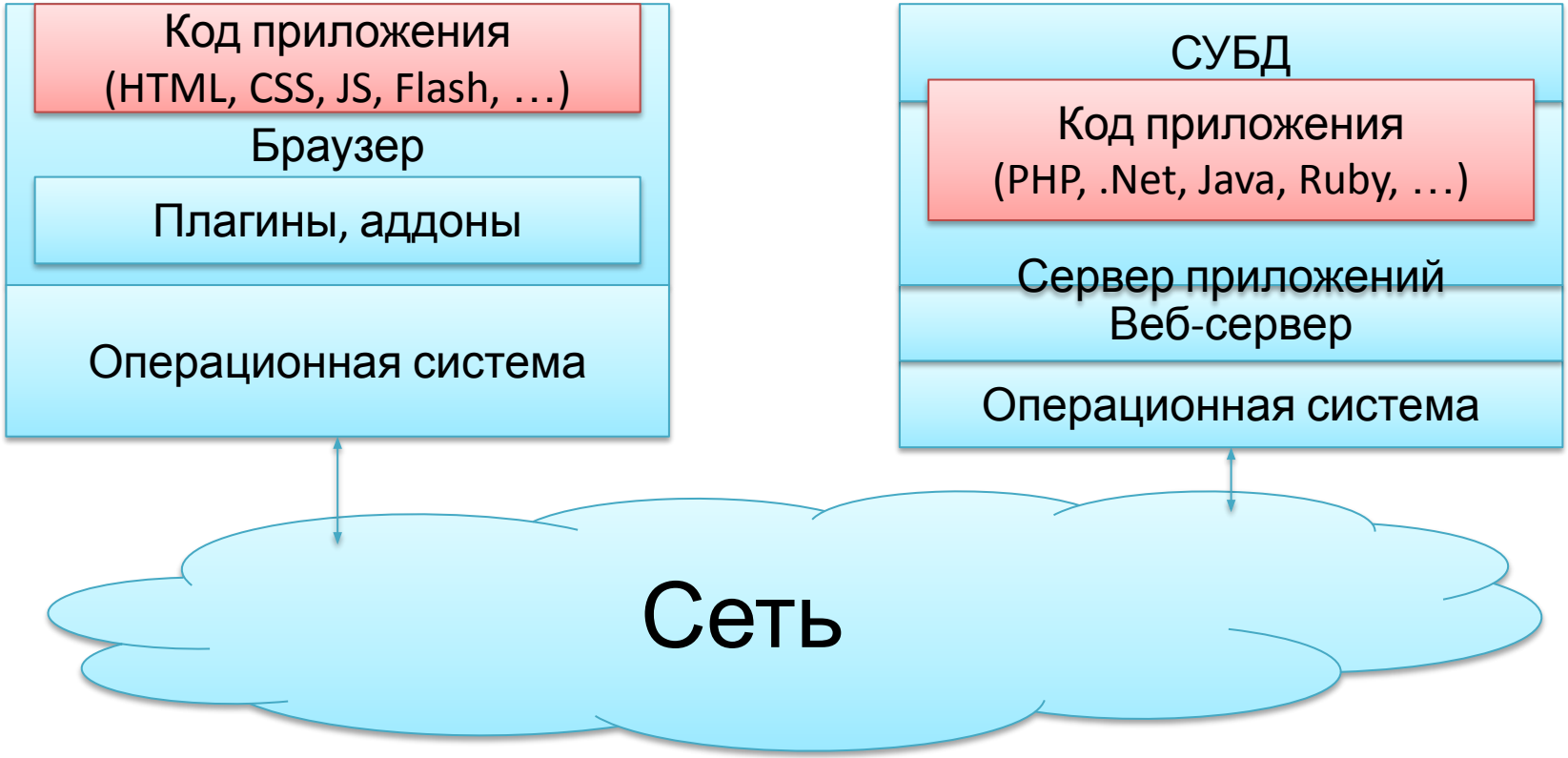
  http://cwe.mitre.org/top25/

Что можно атаковать?

Что должно быть защищено?

ВСЁ!!!

Что можно атаковать?



Что можно атаковать?

- **Клиент**
- **Сервер**

- Сеть
- Человек

Способы поиска

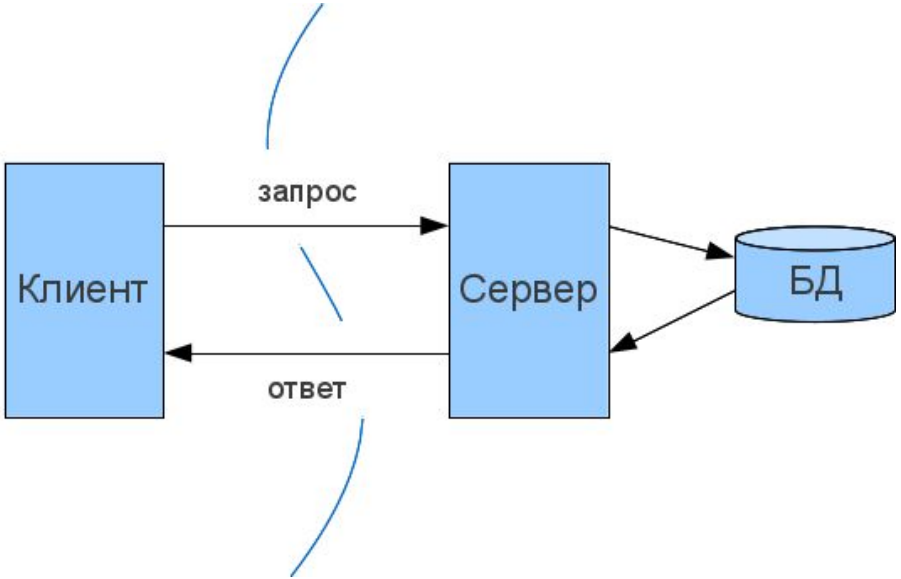
- Ищем признаки наличия уязвимости
  - основная работа тестировщика
- Ищем способ эксплуатации
  - необязательная часть для тестировщика
  - но иногда бывает необходимо сделать

Инструменты

- Сканеры уязвимостей, действующие по принципу «чёрного ящика»
- Сканеры кода, действующие по принципу «прозрачного ящика»
  - преимущество тестировщика в том, что у него есть доступ к коду, в отличие от взломщика
- Комбинация вышеперечисленных средств
- Ручной анализ кода и/или данных

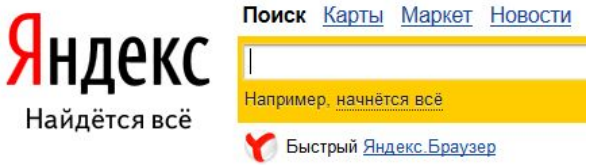
Протокол HTTP
(HyperText Transfer Protocol)

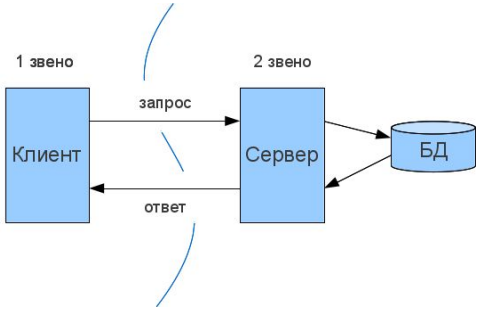
Клиент и Сервер



- Клиент
  - отправляет запросы
- Сервер
  - обрабатывает («обслуживает») запросы

Запрос-ответ






```
GET / HTTP/1.1
Host: www.yandex.ru
User-Agent: Mozilla/5.0 (Windows NT 6.0; WOW64; rv:20.0) Gecko/20100101 Firefox/20.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: ru,en-us;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
Cookie: yandexuid=257878398135832613 8; fuid01=4ddc07700003b01b.VTi0dpt_xNsyg0rjEctXKGjyhfXGwt
Connection: keep-alive
```

```
HTTP/1.1 200 Ok
Server: nginx
Date: Thu, 11 Apr 2013 14:15:50 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: close
Cache-Control: no-cache,no-store,max-age=0,must-revalidate
Expires: Thu, 11 Apr 2013 14:15:50 GMT
Last-Modified: Thu, 11 Apr 2013 14:15:50 GMT
P3P: policyref="/w3c/p3p.xml", CP="NON DSP ADM DEV PSD IVDo OUR IND STP PHY PRE NAV UNI"
Set-Cookie: t=p; Domain=.yandex.ru; Path=/
x-frame-options: DENY
X-XRDS-Location: http://openid.yandex.ru/server_xrds/
```

```
<!DOCTYPE html><html class="i-ua_js_no i-ua_css_standart i-ua_browser_firefox" lang="ru"><head><meta
 http-equiv="X-UA-Compatible" content="IE=EmulateIE7,IE=edge"><title>Яндекс</title><meta http-equiv=Content-Type
 content="text/html;charset=UTF-8"><link  rel="alternate" type="application/rss+xml" title="Новости
Яндекса" href="http://company.yandex.ru/news/news.rss"><link  rel="alternate" type="application/rss+xml"
 title="Блог Яндекса" href="http://company.yandex.ru/blog/index.rss"><link  rel="search" href="http:
//yandex.ru/opensearch.xml" title="Яндекс" type="application/opensearchdescription+xml"><link  rel="shortcut
 icon" href="http://yandex.st/morda-logo/i/favicon.ico"><meta  name="yamm" content="p"><style relates
="morda" type="text/css">html,body{height:100%}body,input{font:13px Arial,Helvetica,sans-serif}img{border
:0}.js .b-pseudo-link{cursor:pointer;text-decoration:none;border-bottom:1px dotted}ul,ol,li{padding:0
}.b-head-search{position:relative;margin-left:-4px}.b-head-search__wrap{padding:3px 4.1% 3px 4px}.b-head-search__arr
{position:absolute;top:-1px;right:0;bottom:-1px;overflow:hidden;width:7%}.b-head-search__arr-i{position
:absolute;right:0;top:50%;margin-top:-100px;border:solid #fff;border-width:100px 0 100px 50px;border-left-color
:transparent;-moz-border-end-style:dotted}body{font:.8em Arial,Helvetica,sans-serif;position:relative
;z-index:0;margin:0;padding:0 0 1em 0;color:#000;background:#fff}wbr{display:inline-block}:link:hover
,:visited:hover{color:#f00!important/*!head*/}::-ms-clear{display:none}.b-page{color:#000;position:relative
;width:100%;height:auto;min-height:100%;margin:0;padding:0;background-color:white;min-width:650px;font
:.8em Arial,Helvetica,sans-serif}.b-yabrowser-promo__wrap{text-align:right;margin-top:2px;height:18px
;overflow:visible}.b-yabrowser-promo__wrap_left{text-align:left}.b-yabrowser-promo{margin-right:18px
;white-space:nowrap}.b-yabrowser-promo__icon{display:inline-block;width:34px;height:33px;margin:0 2px
 0 5px;vertical-align:middle}.b-link:hover .b-yabrowser-promo__icon{background-position:0 -33px}.b-yabrowser-promo__wrap_left
 .b-yabrowser-promo__icon{margin-left:0}.b-yabrowser-promo .b-link{display:inline-block}.b-yabrowser-promo
```

Запрос-ответ

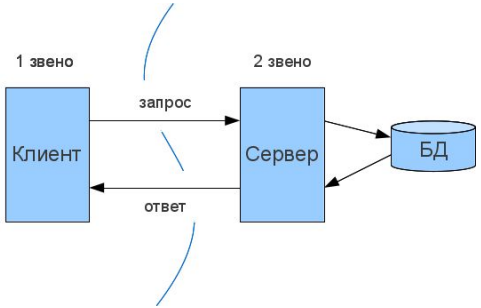
```
GET / HTTP/1.1
Host: www.yandex.ru
User-Agent: Mozilla/5.0 (Windows NT 6.0; WOW64; rv:20.0) Gecko/20100101 Firefox/20.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: ru,en-us;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
Cookie: yandexuid=2578783981358326138; fuid01=4ddc07700003b01b.VTi0dpt_xNsyg0rjEctXKGjyhfXGwt
Connection: keep-alive
```

```
HTTP/1.1 200 Ok
Server: nginx
Date: Thu, 11 Apr 2013 14:15:50 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: close
Cache-Control: no-cache,no-store,max-age=0,must-revalidate
Expires: Thu, 11 Apr 2013 14:15:50 GMT
Last-Modified: Thu, 11 Apr 2013 14:15:50 GMT
P3P: policyref="/w3c/p3p.xml", CP="NON DSP ADM DEV PSD IVDo OUR IND STP PHY PRE NAV UNI"
Set-Cookie: t=p; Domain=.yandex.ru; Path=/
x-frame-options: DENY
X-XRDS-Location: http://openid.yandex.ru/server_xrds/
```

Протокол HTTP

```
GET / HTTP/1.1
Host: www.yandex.ru
User-Agent: Mozilla/5.0 (Windows NT 6.0; WOW64; rv:20.0) Gecko/20100101 Firefox/20.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: ru,en-us;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
Cookie: yandexuid=2578783981358326138; fuid01=4ddc07700003b01b.VTi0dpt_xNsyg0rjEctXKGjyhfXGwt
Connection: keep-alive
```

```
HTTP/1.1 200 Ok
Server: nginx
Date: Thu, 11 Apr 2013 14:15:50 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: close
Cache-Control: no-cache,no-store,max-age=0,must-revalidate
Expires: Thu, 11 Apr 2013 14:15:50 GMT
Last-Modified: Thu, 11 Apr 2013 14:15:50 GMT
P3P: policyref="/w3c/p3p.xml", CP="NON DSP ADM DEV PSD IVDo OUR IND STP PHY PRE NAV UNI"
Set-Cookie: t=p; Domain=.yandex.ru; Path=/
x-frame-options: DENY
X-XRDS-Location: http://openid.yandex.ru/server_xrds/
```



- Текстовый
- Расширяемый
- Синхронный
- **Stateless**
- **Незащищенный**
  - HTTPS с шифрованием

Коды ответов

1** – информационный

2** – успех

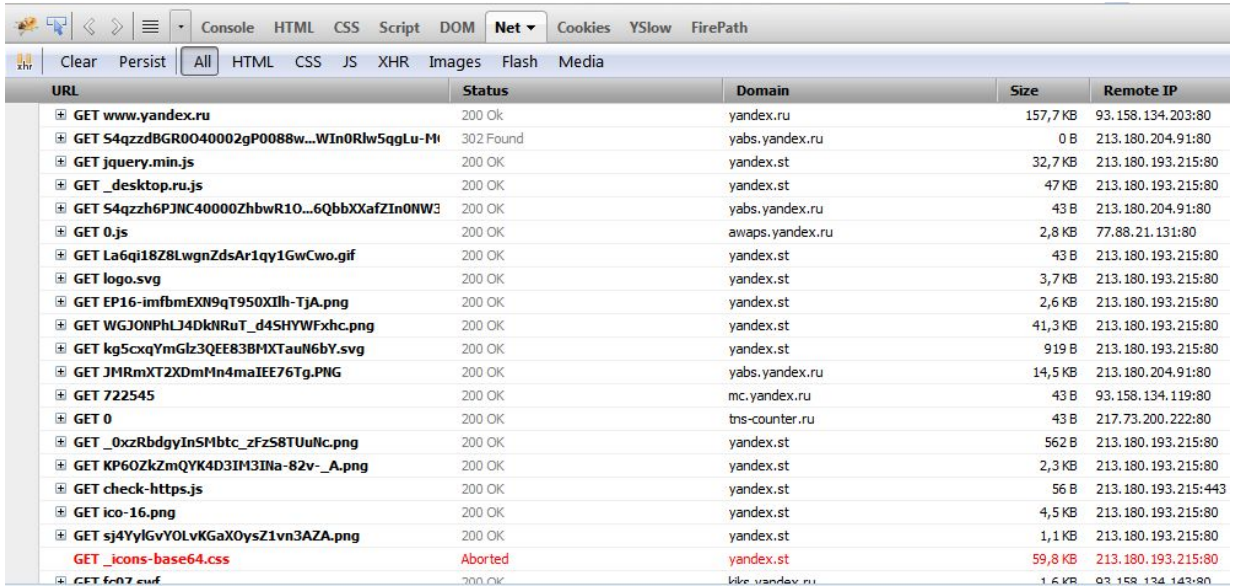
3** – перенаправление

4** – ошибка клиента

5** – ошибка сервера

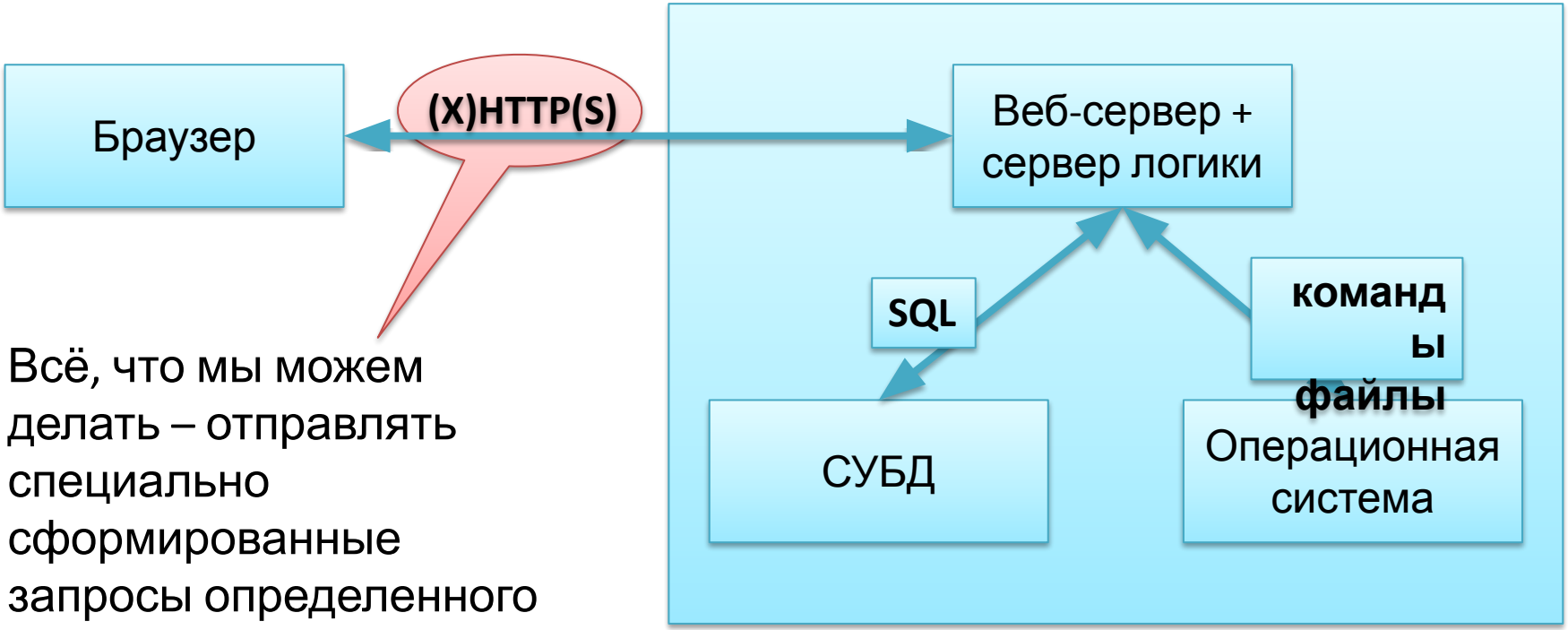
http://www.flickr.com/photos/girliemac/sets/72157628409467125/

Как это увидеть?



- Dev Tools
- Firebug
- Fiddler

Как это «сломать»?



Всё, что мы можем делать – отправлять специально сформированные запросы определенного вида

Виды запросов

- **GET – параметры в строке адреса**
- **POST – параметры в теле запроса**

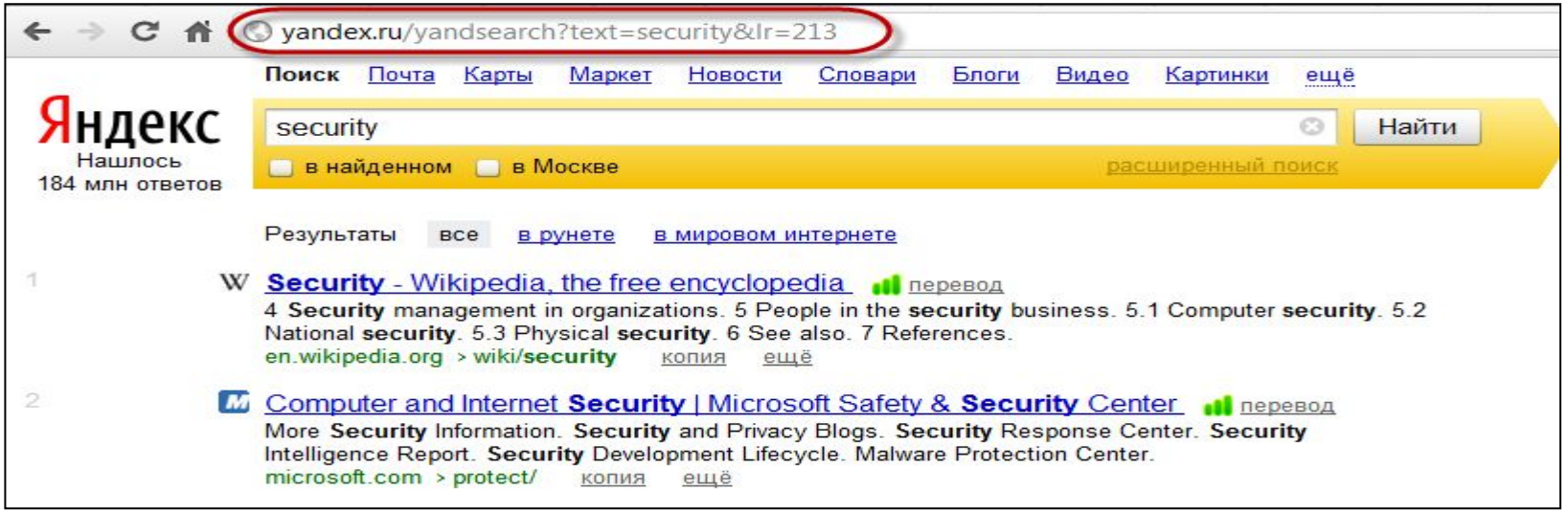
- HEAD
- TRACE
- DELETE
- OPTIONS
- CONNECT
- PUT, PATCH

GET-запрос

GET **http://yandex.ru/yandsearch?text=security&lr=213** HTTP/1.1
Host: yandex.ru
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 6.1) AppleWebKit/535.16 (KHTML, like Gecko) Chrome/18.0.1003.1 Safari/535.16
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://www.yandex.ru/
Accept-Encoding: gzip,deflate,sdch
Accept-Language: ru-RU,ru;q=0.8,en-US;q=0.6,en;q=0.4
Accept-Charset: UTF-8,*;q=0.5
Cookie: …

Как отправить GET-запрос?

Адресная строка браузера



POST-запрос

POST http://www.tarifer.ru/calculator HTTP/1.1
Host: www.tarifer.ru
Content-Length: 275
Origin: http://tarifer.ru
User-Agent: Mozilla/5.0 (Windows NT 6.1) AppleWebKit/535.16 (KHTML, like Gecko) Chrome/18.0.1003.1 Safari/535.16
Content-Type: application/x-www-form-urlencoded
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://tarifer.ru/calculator
Accept-Encoding: gzip,deflate,sdch
Accept-Language: ru-RU,ru;q=0.8,en-US;q=0.6,en;q=0.4
Accept-Charset: UTF-8,*;q=0.5
Cookie: …

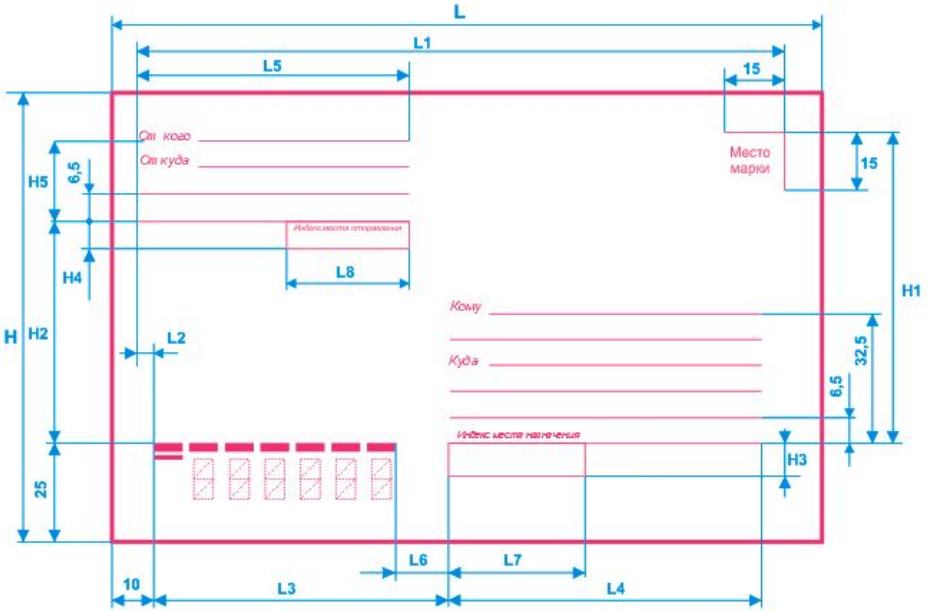
mode=simple&region=%D0%9C%D0%BE%D1%81%D0%BA%D0%B2%D0%B0&operator=&USE_SHORT_NUMBERS=&call_count=320&call_dur=90&city_pct=7.5&sms_count=4&mms_count=2&gprs_size=4&night_percent=4&simplesubmit=%D0%9F%D0%BE%D0%B4%D0%BE%D0%B1%D1%80%D0%B0%D1%82%D1%8C+%D1%82%D0%B0%D1%80%D0%B8%D1%84

Как отправить POST-запрос?

- Заполнить форму
  - валидаторы и модификаторы данных
- Преобразовать POST в GET
- Сделать макет формы

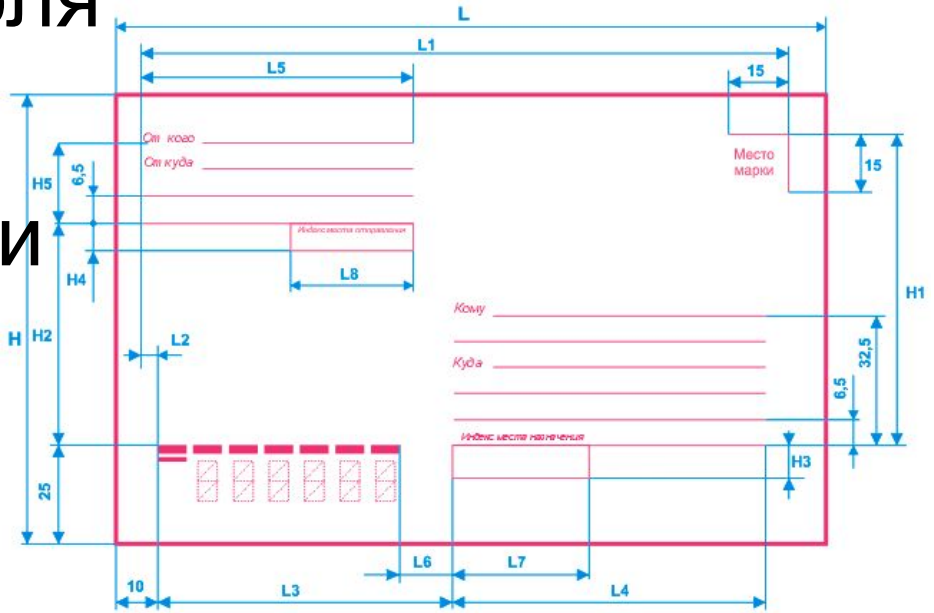
- Плагины – TamperData
- Инструменты – Fiddler

- Написать программу на ЯП



А ещё можно менять заголовок

- URL, его отдельные части
- Дополнительные поля
- Cookies
- Языковые настройки



Домашнее задание

- Научиться отправлять модифицированные запросы с помощью:
  - макета страницы
  - Tamper Data
  - Fiddler

- На этом пока всё

- «Домашка»
- Форум
- Скайп-чат