Безопасность приложений

Хостинг статического контента

URL – основной концепт WWW

- http://server/path/program?query#fragment
- **server**
  - dns-имя (localhost, lvk.cs.msu.su, президент.рф)
    - как будет выглядеть президент.рф в HTTP-запросе?
  - IP-адрес (127.0.0.1, 2130706433 или bin или hex)
  - опционально – порт (service.nalog.ru:8080)
  - опционально – login & pwd
- **Превращается браузером в запрос:**

  GET /path/program?query HTTP/1.1

  Host: server

URL – основной концепт WWW

- http://server/path/program?query#fragment
  - секции program, query и fragment опциональны
  - path – путь (логический) к ресурсу
  - query – аргументы для динамического ресурса
  - fragment вообще не передается на сервер
- URL-кодирование
  - разрешенные символы: [A-Za-z0-9] и ‘.’, ‘-’, ‘~’, ‘_’
  - пробел кодируется +
  - все остальные символы кодируются %xx, где xx – код символа в кодировке UTF-8

Протокол HTTP

- Текстовый; версии: 0.9, 1.0 и 1.1
- HTTP-запрос
  - метод, URL ресурса, версия протокола
  - заголовки
  - (опционально) тело запроса
- HTTP-ответ
  - версия, код и статус ответа
  - заголовки
  - тело ответа

HTTP-запрос

POST /wp-includes/charts/flot-stats-data.php HTTP/1.1

User-Agent: Opera/9.80 (Macintosh; Intel Mac OS X 10.6.7; U; en)

Host: andrepetukhov.wordpress.com

Referer: http://andrepetukhov.wordpress.com/wp-admin/index.php

Cookie: wp-settings-time-13503864=1297961777

Content-Type: application/x-www-form-urlencoded

Content-Length: 139

height=260&page=estats&chart_type=stats-data&target=stat-chart&width=555&blog=13110337&unit=1&noheader=1&site=false&num=15&syn

HTTP-ответ

HTTP/1.1 200 OK
Last-Modified: Mon, 11 Oct 2010 10:20:16 GMT
ETag: "c135d73798bc4bc5aad6d1aa4a8aa073”
Accept-Ranges: bytes
Content-Type: application/xml
Content-Length: 78
Server: nginx/0.6.39
Date: Sun, 03 Apr 2011 15:59:11 GMT
Connection: keep-alive

<cross-domain-policy>
<allow-access-from domain="*"/>
</cross-domain-policy>

Коды ответов (1 из 2)

- 1xx – информационные
  - 100 Continue
    - В запросе должно быть Expect: 100-continue
- 2xx – успех
  - 200 Ok
- 3xx – перенаправление
  - 301 Moved Permanently
  - 302 Found
  - 303 See Other
  - 304 Not Modified
  - 307 Temporary Redirect

Коды ответов (2 из 2)

- 4xx - ошибка со стороны клиента
  - 400 Bad Request
  - 401 Unauthorized
    - В ответе должен быть проставлен WWW-Authenticate
  - 403 Forbidden
  - 404 Not Found
  - 405 Method Not Allowed
- 5xx – ошибка со стороны сервера
  - 500 Internal Server Error
  - 501 Not Implemented
  - 502 Bad Gateway
  - 503 Service Unavailable

Server side

- Какую логику можно придумать для приложения с сокетом на порту 80, который умел бы парсить HTTP?
  - выдача тела запрошенного пользователем файла
  - запуск запрошенного пользователем файла и выдача его output’а
  - маршрутизация запросов по произвольной логике
  - кеширование
  - терминирование SSL
  - аутентификация
  - фильтрация контента (AV, DLP, AUP, …)

Хостинг/постановка задачи

- Как сделать так, чтобы:
  - на узле было N сайтов разных владельцев
  - владелец одного сайта не мог вмешиваться в работу другого
  - владелец одного сайта не мог вмешиваться в работу хостинга
- Вопросы к программе, которая слушает сокет
  - как хранить файлы сайта?
  - как понимать по запросу, с какого сайта надо взять файл?
  - как понимать, надо отдать файл as-is или выполнить его?
  - как передать исполняемому файлу входные параметры и получить от него вывод?
- Хостинг и HTTPS

Вопросы?