Безопасность приложений

Хостинг динамического контента

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

Хостинг динамического контента

- Как понимать, надо отдать файл as-is или выполнить его?
  - AddType application/x-httpd-php .php
  - <FilesMatch "\.ph(p[2-6]?|tml)$">
    SetHandler application/x-httpd-php
    </FilesMatch>
- Задается либо в конфигурации виртуального хоста, либо в .htaccess
- Можно выполнить .html как php
- Can you spot the weakness?
- http://blog.dynom.nl/archives/Be-careful-with-double-extensions_20081024_25.html

Хостинг динамического контента

- Как передать исполняемому файлу входные параметры и получить от него вывод?
- Приложение на том же узле, что и сервер
  - приложение на том же языке, что и сервер
  - приложение на другом языке
- Приложение на другом узле
  - передача по сети через HTTP, далее – см. п.1
  - передача по сети через свой протокол

App и сервер на одном языке

- Приложение реализуется с учетом соглашений об именах (API сервера)
- Веб-сервер воспринимает приложение как часть себя и вызывает функции, определенные в приложении
- Примеры
  - Java-контейнеры (Tomcat)
  - lightweight-веб-сервера на скриптовых языках (Python)
  - модули веб-сервера (например, Apache)

Пример сервлета

```
import java.io.*;
import javax.servlet.*;
import javax.servlet.http.*;

public class HelloWorld extends HttpServlet {
  public void doGet(HttpServletRequest request,
                    HttpServletResponse response)
      throws ServletException, IOException {
    PrintWriter out = response.getWriter();
    out.println("Hello World");
  }
}
```

Пример приложения на Python

```
import time
import BaseHTTPServer

class MyHandler(BaseHTTPServer.BaseHTTPRequestHandler):
    def do_GET(s):
        s.send_response(200)
        s.send_header("Content-type", "text/html")
        s.end_headers()
        s.wfile.write("<html><body>This is a test.</body></html>")

httpd = BaseHTTPServer.HTTPServer(('localhost', 80), MyHandler)
httpd.serve_forever()
```

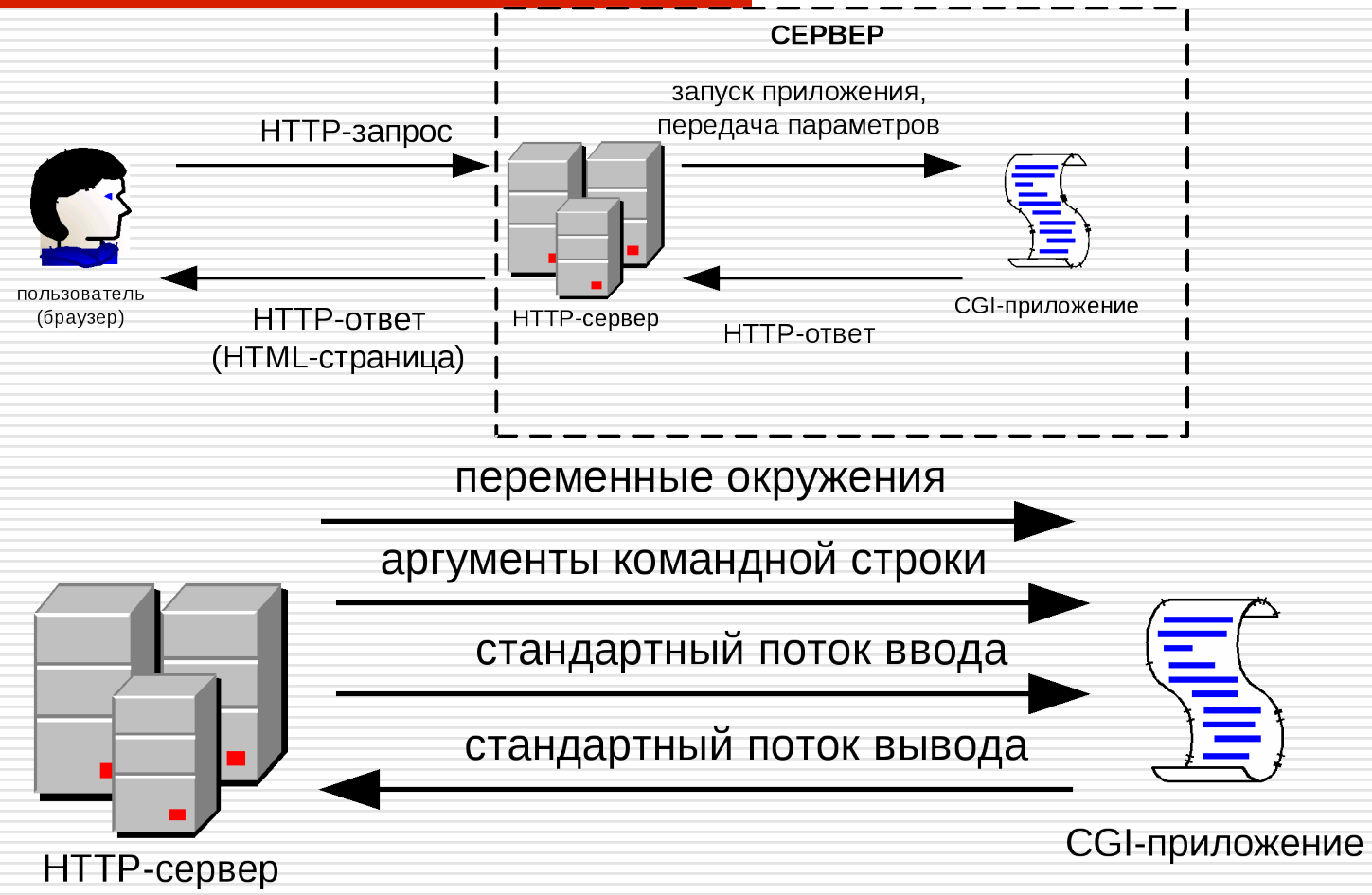
Модуль для сервера Apache

- Apache: я умею импортировать функции из других бинарников динамически
  - dlopen, dlsymb
  - http://www.ibm.com/developerworks/ru/library/l-dynamic-libraries/
- Программист модуля: Apache, дай мне соглашения о вызовах
  - http://httpd.apache.org/docs/current/developer/modguide.html
- Пример модуля, который легко читается – mod_python
  - нагуглите исходники и ознакомьтесь

Приложение на другом языке

- Частный случай
  - веб-сервер, интерпретируемый язык, один хост
  - как подружить?
    - у каждого интерпретатора есть библиотека с API типа libpython2.7
    - пример – mod_python; интегрирует API apache и libpython
- Общий случай
  - CGI как пример

Common Gateway Interface



http://www.cgi101.com/book/ch3/text.html

Приложения на другом узле

- Передавать запрос по HTTP, далее задача сводится к решенной (т.н. reverse proxy)
- Передавать по сети через свой протокол удаленного вызова программ
  - FastCGI
  - AJP
  - SCGI

Безопасная загрузка файлов

- Построить веб-приложение для организации со статической адресацией узлов
- Веб-приложение при первом посещении клиента выдает ему UUID и создает каталог
- Веб-приложение при первом посещении клиента выдает ему UUID и создает каталог
- В каталог пользователь может поместить любые файлы и создавать директории
- Чужие файлы нельзя ни просматривать ни изменять (сделано проверку IP-адреса и UUID)
- Какой бы файл пользователь ни загрузил, он не должен исполняться на сервере!

Простейший код

```
<?php
$uploaddir = ’/';
$uploadfile = $uploaddir . basename($_FILES['userfile']
['name']);
if (move_uploaded_file($_FILES['userfile']['tmp_name'],
$uploadfile)) {
    echo "File is valid, and was successfully uploaded.
\n";
} else {
    echo "File uploading failed.\n";
//can you spot the problem?
} ?>
```

Вопросы

- Как сделать проверку типа файла?
  - по расширению? по заголовку? по содержимому?
- Под какими именами можно загружать файлы, а под какими – нет?
- Как настроить каталог веб-сервера, в который будут загружаться файлы?
- С какого хоста (hostname) должны сервироваться файлы?
  - тот же? поддомен? другой домен?

Вопросы?