Web 基础

紫丁香 CTF 俱乐部

November 2020

在此之前

本 Slide 初始由紫丁香 CTF 俱乐部阮行止制作，于 2021-04-10 由 Billchenchina 以 LaTeX 重制。

intro

我是紫丁香 CTF 俱乐部的主席
您可以叫我，阮行止
曾经是 Oier & ACMer，从 19 年开始打 CTF
主攻 crypto 和 web

本系列讲座是……

- 开放的
- 面向零基础初学者的
- 实践的
- 尽量易于理解的
- 需要自学的

本系列讲座不是……

- 覆盖所有知识的
- 完全严谨的

Table of Contents

Table of Contents

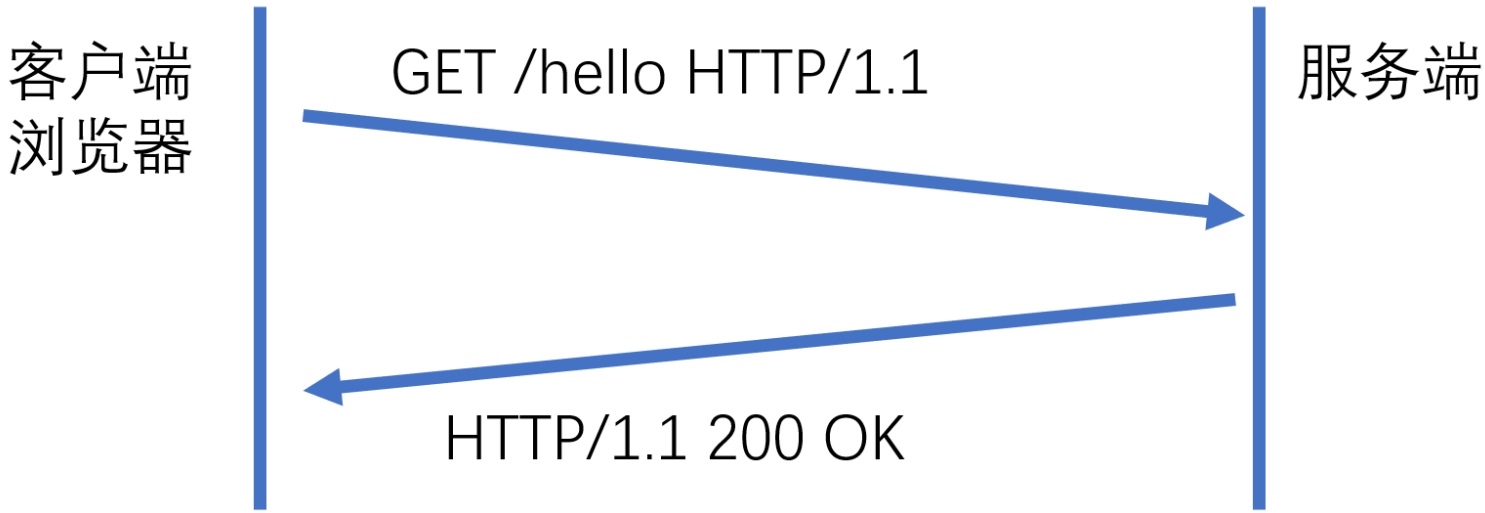
浏览器

浏览器是我们访问网站的工具

- Google chrome
- Mozilla firefox

浏览器负责发送请求、渲染页面、etc.

浏览器与服务器的交互



C/S 结构

web 服务器是典型的 client/server 结构。
有一台总是在线的服务器
客户端向服务器发起请求 (request)
服务器接受请求，并发回响应 (response)

服务器

web 中谈起服务器，往往指的是服务端程序

- nginx
- apache
- 其他，例如 python3 -m http.server

演示：搭建服务器

我将为各位演示搭建一个服务器的过程
客户端访问 index.html 时，返回一句 hello

URL

HTTP 请求的“地址”，称为 URL

- http://www.baidu.com/index.html
- http://127.0.0.1/nana.php?id=3
- http://lilac.run:12345/

主机和端口

主机可以用域名或者 IP 地址来指定。
端口号：0 65535 之间的一个数

主机类似于一栋楼，端口号类似于房间号
楼栋 + 房间号才能唯一定位到一个商户

备注：域名

我们注意到，记忆 IP 地址是困难的。
经常采用域名来代替冗长的 IP 地址。

域名可以指向一个 IP 地址。
详情请自学：DNS

备注：端口

1000 以下的端口号为周知端口号，我们约定

- 80 端口用于 HTTP 服务
- 443 端口用于 HTTPS 服务
- 22 端口用于 ssh 服务
- etc.

浏览器如何渲染页面？

请打开 https://ruanx.net ， 然后按 F12

请查阅：

- html
- javascript
- css

静态网站

静态网站类似于文件服务器
请求一个路径，返回对应的文件
无论谁访问，都会返回一样的文件

静态网站

静态网站能不能实现一个简单的博客？
https://merrg1n.github.io/
静态网站能不能实现电子邮箱？
静态网站能不能实现淘宝？

动态网站

静态网站无法为用户提供个性化的服务。

动态网站：由服务器上的程序计算出页面

演示：动态网站

我将演示一个 PHP 服务器。
访问 hello.php?username=nana
将会返回 hello, nana!

服务器后端程序

- PHP
- Python(flask, django)
- nodejs(express)
- C/C++ CGI
- etc.

动态页面实现

以 apache+php 为例

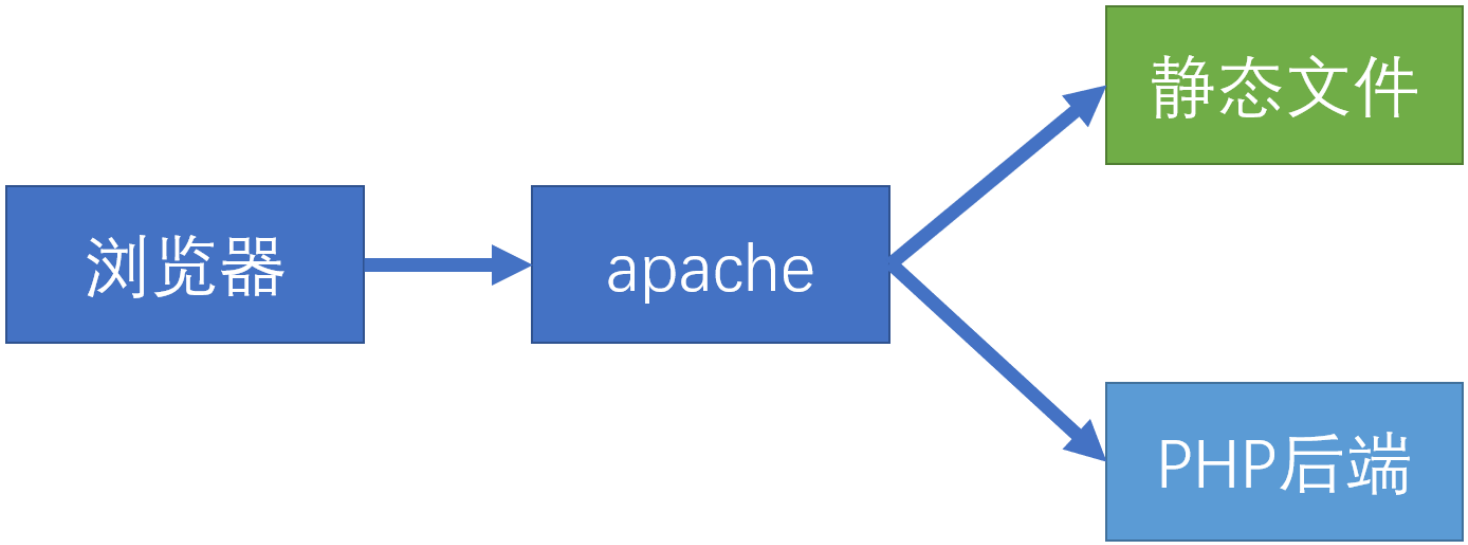


Table of Contents

实践：抓包

让我们看一看：

- 浏览器往服务器发送了什么内容
- 服务器返回了什么内容

工具：burp suite + SwitchyOmega
另，开发者工具 (F12) 也可以完成简易的抓包

HTTP 协议

参阅：

- 《图解 HTTP》（推荐）
- 《计算机网络：自顶向下方法》的 HTTP 部分

HTTP 请求实例

```
GET /somedir/page.html HTTP/1.1
Host: www.someschool.edu
Connection: close
User-agent: Mozilla/5.0
Accept-language: fr
```

请求格式

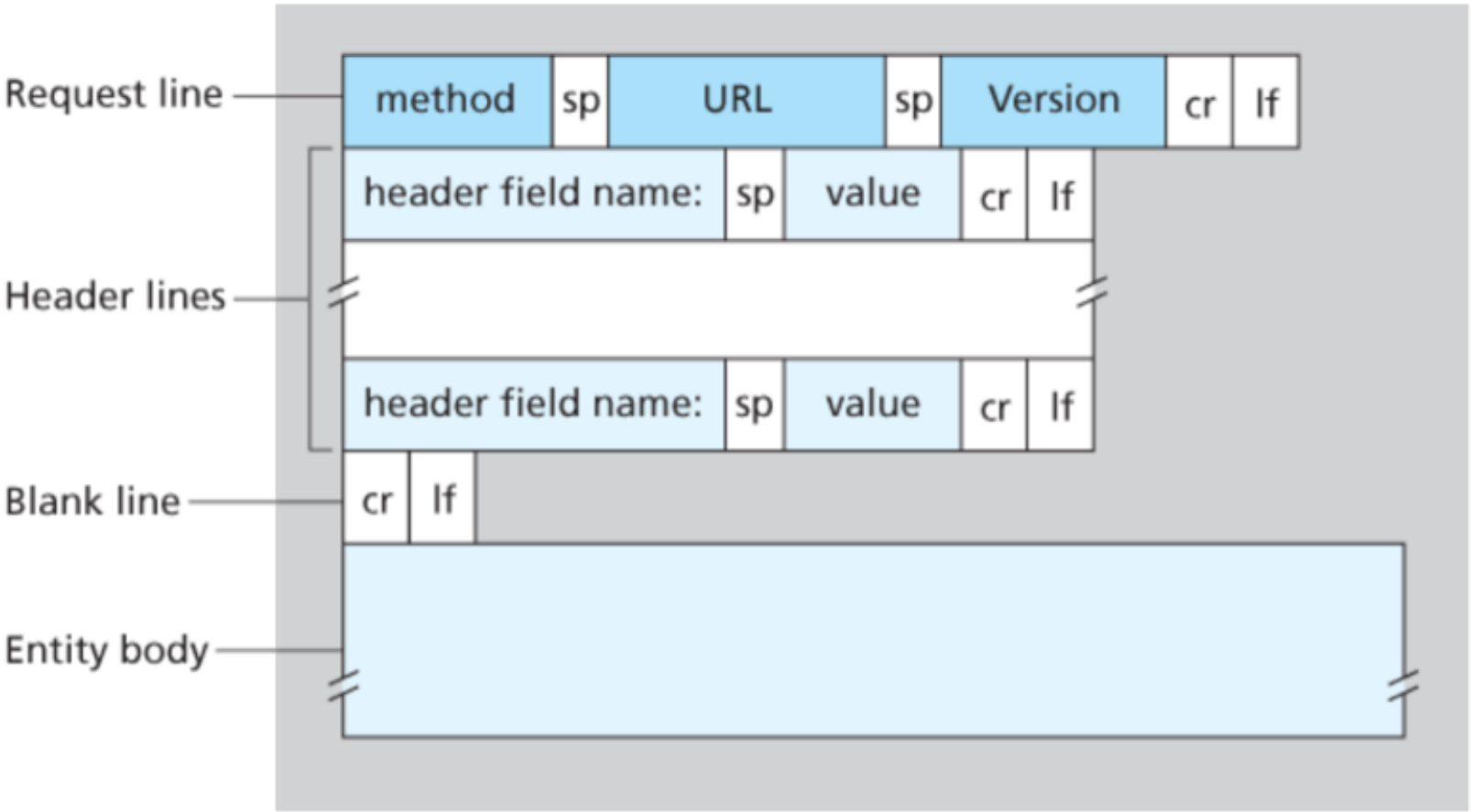


Figure 2.8 General format of an HTTP request message

HTTP 响应实例

```
HTTP/1.1 200 OK
Connection: close
Date: Tue, 18 Aug 2015 15:44:04 GMT
Server: Apache/2.2.3 (CentOS)
Last-Modified: Tue, 18 Aug 2015 15:11:03 GMT
Content-Length: 6821
Content-Type: text/html

Hello, world!
```

响应格式

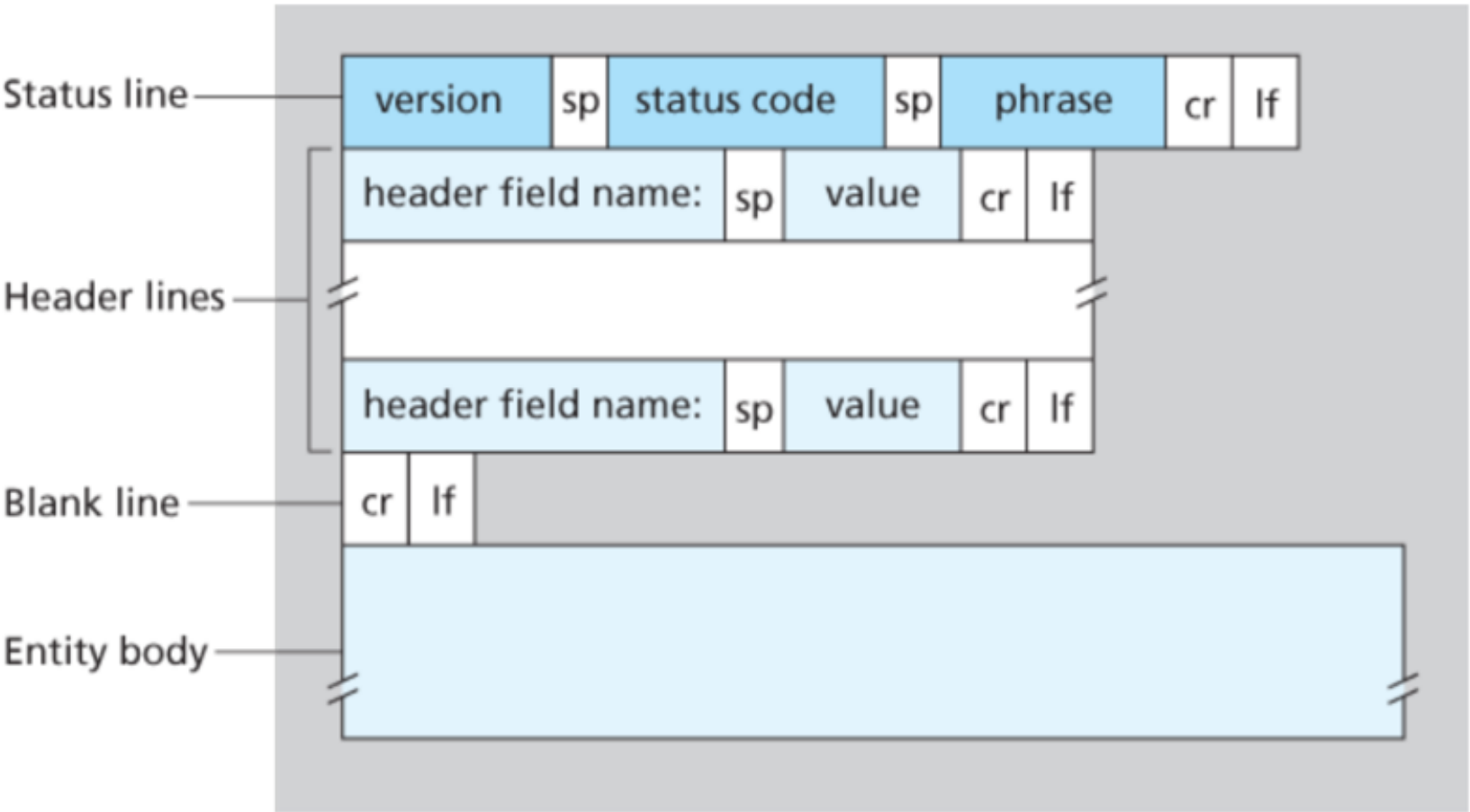


Figure 2.9 General format of an HTTP response message

注释：HTTP 请求方法

GET：一般用于不带参数或明文带参数的请求
POST：在 GET 的基础上，可以传输更大的参数，且 POST 上去的参数不显示在 URL

在论坛中请求特定 tag 的帖子，用哪种请求？
传输文件，用哪种请求？
登录时传输用户名和密码，用哪种请求？

演示：参数爆破

攻防世界 ics-06
提示：报表中心，1 5000 以内的某个 id 是特殊的

注释：HTTP 版本

总而言之，越高的版本越先进
有兴趣的同学可参阅 MDN 文档
https://developer.mozilla.org/zh-CN/docs/Web/HTTP/Basics_of_HTTP/Evolution_of_HTTP

注释：响应状态码

状态码 (status code) 指示请求的结果

- 200 请求成功，一切正常
- 404 页面找不到
- 403 没有权限访问
- 503 服务器炸了
- 502/504 网关无效、网关超时（常见于 proxy 服务器）

Table of Contents

请求头

请求头 (headers) 用于提供一些的信息。
CTF 简单 web 题经常考察请求头相关的知识。

可以通过 Hackbar 插件修改请求头。

记录源 IP 的 header

请求头中，可以有一些 header 指示源 IP

- X-Forwarded-For
- X-Real-IP

实践：伪造源 IP

Lilac Web Train 平台：web.lilac.run
用多种方式实现利用：

- Hackbar 插件
- burp
- python requests

HTTP 无状态性

HTTP 是一个无状态协议。
服务端程序不维护客户状态。
每次请求，服务端仅能得到 HTTP 请求数据。

如何实现一个购物车？

Cookie

Cookie 可以理解为由浏览器维护的一个记事本。
对相同的网站进行访问时：

- 客户端浏览器每次请求都把自己维护的 Cookie 写进请求头
- 服务器可以通过 Set-Cookie 响应头，要求客户浏览器设置 Cookie

注释：Cookie 的更多信息

详细信息请参阅 MDN 文档

`https://developer.mozilla.org/zh-CN/docs/Web/HTTP/Cookies`

Cookie 带来了隐私性问题

注释：Cookie 的安全性

若网站开发者希望使用 Cookie，但不想让用户知道 Cookie 里面的具体细节，有多种方式：

- 乞灵于密码学（先加密，再发给浏览器存储）
- Cookie 中只存放这个用户的 id，而由服务器后端来维护每个 id 对应的信息（PHP SESSION 采取的方式）

实践：篡改 Cookie

我们将通过篡改 Cookie，把自己伪装成管理员。
Lilac Web Train 平台
多种实现：

- Chrome 浏览器原生 cookie 管理
- burp, Hackbar, python requests

应对：防止用户篡改 Cookie

借助 SESSION ID，由后端维护用户状态 (PHP)
Cookie 存放密文数据
Cookie 存放明文数据 + 签名 (Flask)

演示：PYWebsite

BUUOJ PYWebsite

- 前端验证
- 请求头伪造

Table of Contents

web 后端

国内赛事，多数题目是 PHP 后端
有向 python、nodejs、java 转移的趋势
越来越少考察 PHP 的奇技淫巧
转而考察 web 与其他方向的综合

web 常见漏洞

SQL 注入：拼接数据库操作字符串产生漏洞
RCE：因某些不当原因，攻击者可以任意执行代码
反序列化：将字符串解析成对象时的漏洞
文件上传：一般是上传 PHP webshell

web 常见漏洞

SSTI：服务端用模板引擎渲染攻击者提供的字符串
XXE：XML 解析漏洞
XSS：向页面中注入恶意 js 代码，受害者浏览器访问页面
etc.

学习路线建议

- Python(所有方向必须)
- PHP(web 必须)
- HTML, js, css(了解即可)
- SQL(web 必须)
- nodejs,java(可选)

本周学习推荐

在自己的 PC 上搭建 PHP 环境
初步学习 PHP 语法（可考虑菜鸟教程）
学习 python3 （建议搭建 anaconda 环境）廖雪峰 Python3

Table of Contents

结语

吾生也有涯，而知也无涯
自学能力是 CTF 所有方向最重要的技能
以有涯随无涯殆已，学习要有取舍
共同努力，共同进步，请多与俱乐部会员交流