# Web应用安全发展与介绍

# HTTP协议与会话管理

当我们访问一个网址的时候，这中间发生了什么？

输入网址

浏览器查找域名的IP地址

浏览器给Web服务器发送一个HTTP请求

服务端处理请求

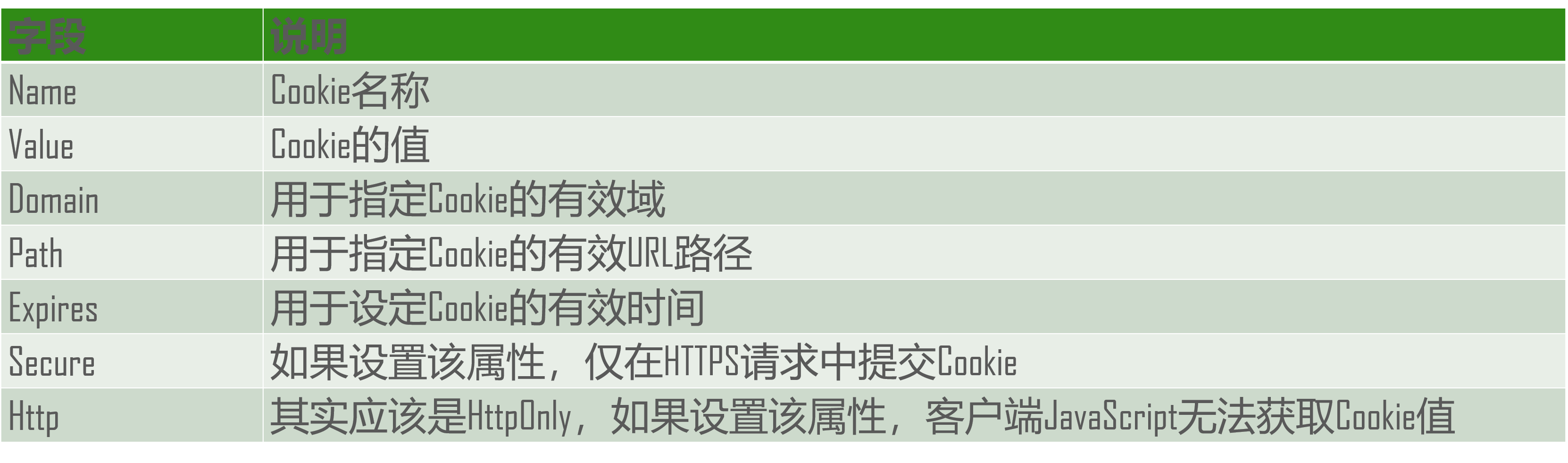
服务端发回一个HTTP响应

浏览器渲染显示HTML

让我们来看一个URL（统一资源定位器）

scheme://login:password@address:port/path/to/resource/?query\_string#fragment





# Web应用的组成与网页的渲染

## HTML

超文本标记语言

由标签（Tag）组成的层级结构，标签参数的格式为“名称=值”数据对，则文本节点（构成了文档实际内容）穿插其中。



## CSS（层叠样式表）

HTML页面引用示例：

<link href="css/style.css" rel="stylesheet">

或

<style>body {width}</style>

## 浏览器解析顺序



## 浏览器解码顺序



## DOM树

DOM，文档对象模型(Document Object Model)

JavaScript可以操作DOM树

这是一个网页的DOM结构：



这是一个通过JavaScript代码操作DOM树的示例代码：



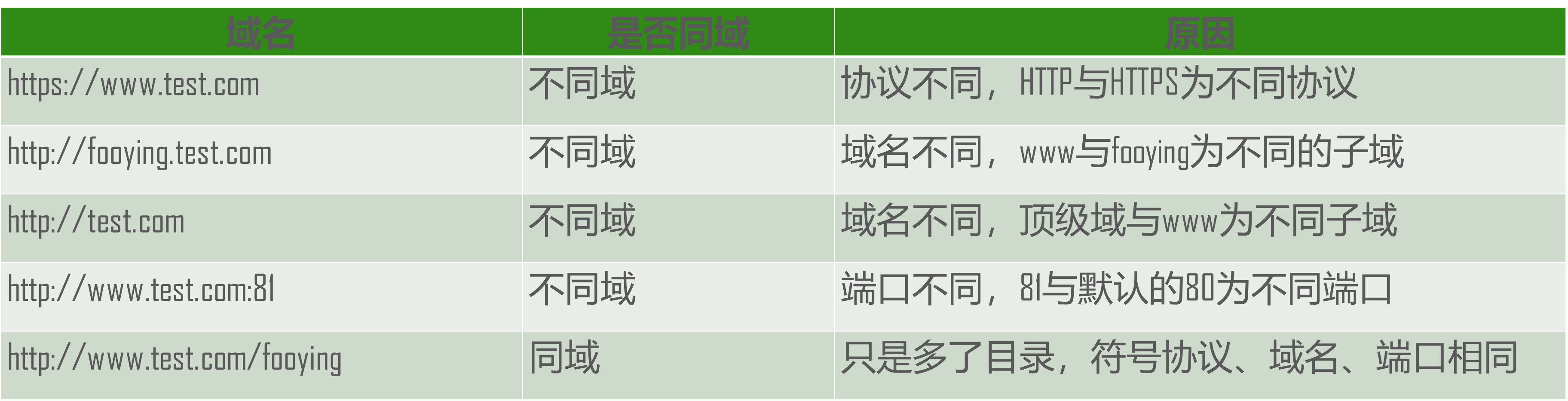
# 浏览器特性与安全策略

## 同源策略

同源策略规定：不同域的客户端脚本在没明确授权的情况下，不能读写对方的资源。

## 同域与不同域

以下为与www.test.com同域情况



## 授权

HTTP响应头返回

Access-Control-Allow-Origin:http://www.fooying.com

## 沙盒框架（Sandboxed frame）

是对常规<iframe>表现行为的扩展，它能让顶级页面对其嵌入的子页面及这些子页面的子资源设置一些额外的限制

通过设置<iframe>的参数实现限制

