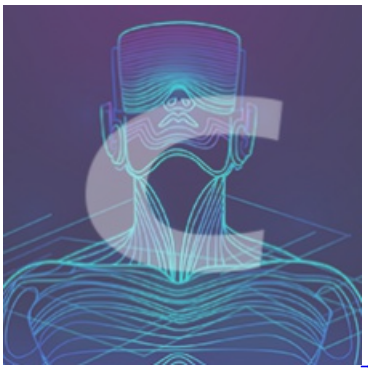
i春秋Web渗透测试工程师（初级）学习笔记（第一章）

原创

draper-crypto 于 2021-10-04 19:35:28 发布 531 收藏 2

文章标签： javascript 信息安全 渗透测试 安全

by draper-crypto



下期博文：

i春秋Web渗透测试工程师（初级）学习笔记（第二章）

第一章:你了解web吗？

1.1 Web的发展史

1.1.1 静态网页的诞生

1994年7月，HTML2规范发布。

1994年9月，因特网工程任务组（Internet Engineering Task Force）设立了HTML工作组。

1994年11月，Mosaic浏览器的开发人员创建了网景公司（Netscape Communications Corp.），并发布了Mosaic Netscape 1.0 beta浏览器，后改名为Navigator。

1.1.2 万维网的诞生

1994年底，由Tim牵头的万维网联盟（World Wide Web Consortium）成立，这标志着万维网的正式诞生。此时的网页以HTML为主，是纯静态的网页，网页是“只读”的，信息流只能通过服务器到客户端单向流通，由此世界进入了Web 1.0时代。

1.1.3 JavaScript的诞生

1996年，微软发布了VBScript和JScript。JScript是对JavaScript进行逆向工程的实现，并内置于Internet Explorer 3中。但是JavaScript与JScript两种语言的实现存在差别，这导致了程序员开发的网页不能同时兼容Navigator和Internet Explorer浏览器。Internet Explorer开始抢夺Netscape的市场份额.

1.1.4 动态页面的崛起

JavaScript诞生之后，可以用来更改前端DOM的样式，实现一些类似于时钟之类的小功能。那时候的JavaScript仅限于此，大部分的前端界面还很简单，显示的都是纯静态的文本和图片。这种静态页面不能读取后台数据库中的数据，为了使得Web更加充满活力，以PHP、JSP、ASP.NET为代表的动态页面技术相继诞生。
（1）PHP（PHP：Hypertext Preprocessor）最初是由Rasmus Lerdorf在1995年开始开发的，现在PHP的标准由PHP Group维护。PHP是一种开源的通用计算机脚本语言，尤其适用于网络开发并可嵌入HTML中使用。PHP的语法借鉴吸收C语言、Java和Perl等流行计算机语言的特点，易于一般程序员学习。PHP的主要目标是允许网络开发人员快速编写动态页面。
（2）JSP（JavaServer Pages）是由Sun公司倡导和许多公司参与共同创建的一种使软件开发者可以响应客户端请求，从而动态生成HTML、XML或其他格式文档的Web网页的技术标准。JSP技术是以Java语言为基础的。1999年，JSP1.2规范随着J2EE1.2发布。
（3）ASP（Active Server Pages）1.0 在1996年随着IIS 3.0 而发布。2002年，ASP.NET发布，用于替代ASP。

1.1.5 Node.js的爆发

早在1994年，Netspace就公布了其Netspace Enterprise Server中的一种服务器脚本实现，叫做LiveWire，是最早的服务器端JavaScript，甚至早于浏览器中的JavaScript。对于这门图灵完备的语言，Netspace很早就开始尝试将它用在后端。微软在1996年发布的IE 3.0中内嵌了自己的JScript语言，其兼容JavaScript语法。1997年年初，微软在它的服务器IIS 3.0中也包含了JScript，这就是我们在ASP中能使用的脚本语言。

1.2 web的常见术语

1.2.1 浏览器的刷新与转到的区别

刷新：
在现有网页的基础上检查网页是否有更新的内容。在检查时会保留之前的一些变量的值，因此有时可能会造成刷新后网页出现错误，或者无法打开的情况。与转到的区别是浏览器取网页的新内容来更新本机缓存，在更新的同时保留之前的一些变量。

转到：
相当于在地址栏中重新输入网页的URL访问，浏览器会尽量使用已经存于本机中的缓存。相对于刷新，转到是一种全新的访问，它会尽量使用本机中的缓存文件，但不保留之前的变量。

区别： 转到是一个全新的访问，不会使用本地缓存，而刷新则会使用本机的缓存，保留之前的变量。

1.2.2常见术语

（1）WWW(World Wide Web)

即万维网，遵循http协议，建立在internet上的一个网络服务。

优点：全球性，交互性，动态，多平台

（2）Web Browser

即浏览器，显示服务器提供的html文件，并且能和网站进行交互。主流浏览器有IE浏览器、Chrome浏览器、Firefox浏览器、Safari浏览器。

（3）C/S和B/S

C/S(Client-Server)：即**客户机/服务器**模式，软件系统的体系结构，例如：QQ，微博等。

B/S(Browser/Server)：即**浏览器/服务器**模式，WEB浏览器是客户端最主要的应用软件。这种模式统一了客户端，将系统功能实现的核心部分集中到服务器上，简化了系统的开发、维护和使用。客户机上只要安装一个浏览器，如Chrome、Safari、Microsoft Edge、Netscape Navigator等，服务器安装SQL Server、Oracle、MYSQL等数据库。浏览器通过Web Server 同数据库进行数据交互。

（4）HTML

HTML的全称为**超文本标记语言**，是一种**标记语言**。它包括一系列标签．通过这些标签可以将网络上的文档格式统一，使分散的Internet资源连接为一个逻辑整体。HTML命令可以说明文字，图形、动画、声音、表格、链接等。

（5）HTTP

超文本传输协议（Hyper Text Transfer Protocol，HTTP）是一个简单的请求-响应协议，它通常运行在TCP之上。它指定了客户端可能发送给服务器什么样的消息以及得到什么样的响应。

（6）XML

可扩展标记语言，标准通用标记语言的子集。是一种用于标记电子文件使其具有结构性的标记语言。

（7）Session

在计算机中，尤其是在网络应用中，称为“会话控制”。Session对象存储特定用户会话所需的属性及配置信息。这样，当用户在应用程序的Web页之间跳转时，存储在Session对象中的变量将不会丢失，而是在整个用户会话中一直存在下去。当用户请求来自应用程序的 Web页时，如果该用户还没有会话，则Web服务器将自动创建一个 Session对象。当会话过期或被放弃后，服务器将终止该会话。**通俗来说就是从打开网站直到完全关闭网站的这段时间，是一个特定的时间。**

（8）Web Server

即服务端，例如windows server 2008，redhat，centOS等等

（9）Cookie

类型为“小型文本文件”，是某些网站为了辨别用户身份，进行Session跟踪而储存在用户本地终端上的数据（通常经过加密），由用户客户端计算机暂时或永久保存的信息 。**（类似于身份证）**

（10）request

向服务器发送一个请求，然后服务器会返回一个结果给请求客户端，并附带一个response code。

（11）forward

是服务器内部重定向，程序收到请求后重新定向到另一个程序，而客户机并不知晓。客户端页面的url地址不会发生改变。

（12）redirect

是服务器收到请求后发送一个状态头给客户，客户将再次请求，就有两次网络通行的来往。并且对于客户来说url地址已经发生了变化。