CLASS 10

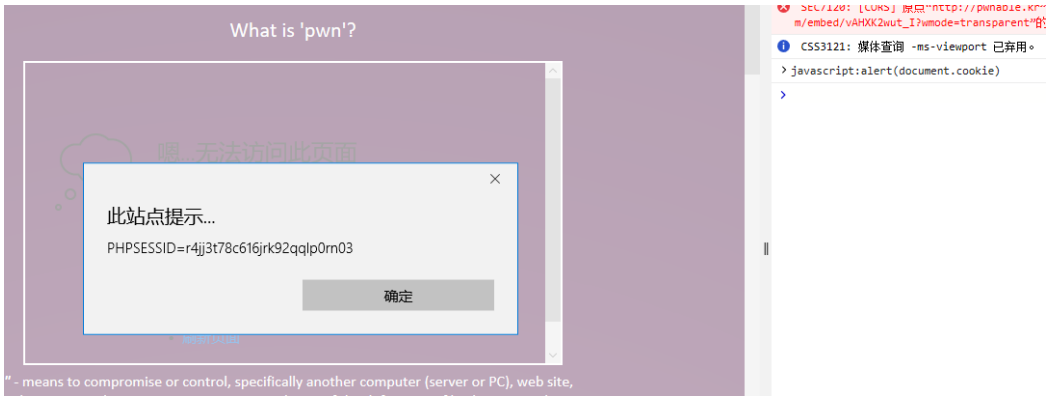
Attacks on TCP IP

吴瑞欣-E41614059

1、用 IE 访问某些网站的时候，输入

javascript:alert(document.cookie)

会有什么反应，并解释原因。



会产生它的 PHPSESSID，原因，输出它的缓存信息

2、阅读下面两篇文章或者阅读一本书

<<JavaScript DOM 编程艺术>>：

Javascript Tutorial

https://www.evl.uic.edu/luc/bvis546/Essential_Javascript_--_A_Javascript_Tutorial.pdf

XMLHttpRequest

http://www.w3school.com.cn/ajax/

http://www.hunlock.com/blogs/AJAX_for_n00bs

已了解

3、了解 FireFox 的两个插件 LiveHttpHeaders 和 Firebug 的基本使用方法。

LiveHTTPHeaders 可以抓取 http，https 的数据链接，包括 get 和 post。安装好插件后，重启 FireFox，打开下载页面，运行 LiveHTTPHeaders 抓包（工具->Live HTTP Headers)，然后再点击下载，

Firebug 是 firefox 下的一个扩展,能够调试所有网站语言，如 Html,Css 等， FireBug 最强大的是 javascript 调试功能，使用起来非常方便，而且在各种浏览器下都能使用（IE,Firefox,Opera, Safari)。除此之外，其他功能还很强大，比如 html,css,dom 的查看与调试，网站整体分析等等。是一整套完整而强大的 WEB 开发工具。

4、阅读下面这篇文章：

跨站脚本攻击实例解析

http://bbs.pediy.com/showthread.php?t=124209

跨站攻击，即 Cross Site Script Execution(通常简写为 XSS，因为 CSS 与层叠样式表同名，故改为 XSS) 是指攻击者利用网站程序对用户输入过滤不足，输入可以显示在页面上对其他用户造成影响的 HTML 代码，从而盗取用户资料、利用用户身份进行某种动作或者对访问者进行病毒侵害的一种攻击方式

5、阅读下面这两篇文章：

DOM Based Cross Site Scripting or XSS of the Third Kind

http://www.webappsec.org/projects/articles/071105.html

XSS (Cross Site Scripting) Cheat Sheet Esp: for filter evasion

http://80x86.io/post/xsscrosssitescriptingcheatsheetespforfilterevasion

Cross Site Scripting（XSS）其中一个人发送恶意数据（通常是带有 Javascript 代码的 HTML 内容），然后由应用程序在某种 HTML 上下文中回显，并且 Javascript 代码被执行。

文章 DOM Based Cross Site Scripting or XSS of the Third Kind 讲述了基于 DOM 的 XSS。XSS 通常分为“非持久性”和“持久性”。“非持久性”意味着服务器在立即响应来自受害者的 HTTP 请求时回应恶意（Javascript）有效负载。“持久”意味着有效载荷由系统存储，并且稍后可以由易受攻击的系统嵌入提供给受害者的 HTML 页面中。

6、XSS 漏洞的触发条件有哪些？应该如何防范？

通过构造标记代码，形成 XSS 攻击，如下：

"><script>alert('XSS');</script><"

可以通过过滤输入和转义输出进行防范，具体的执行方式如下：

第一、在输入方面对所有用户提交内容进行可靠的输入验证，提交内容包括 URL、查询关键字、http 头、post 数据等

第二、在输出方面，在用户输内容中使用<XMP>标签。标签内的内容不会解释，直接显示。

第三、严格执行字符输入字数控制。

四、在脚本执行区中，应绝无用户输入。