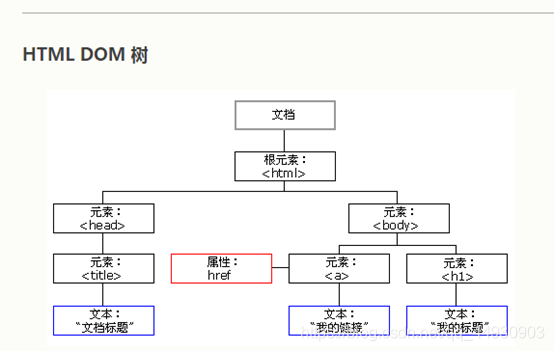
# 25 WEB漏洞-XSS跨站之原理分类及攻击手法



#XSS跨站漏洞产生原理，危害，特点？

本质，产生层面，函数类，漏洞操作对应层，危害影响，浏览器内核版本等

#XSS跨站漏洞分类：反射，存储，DOM

反射型：发包 x= xss => x.xss => 回包

存储型：发包 x=xss => x.xss =>写到数据库某个表 => x,ss => 回显

dom型：发包 x=xss => 本地浏览器静态前端代码 =x.xss

从产生层面，具体区别，危害等级等讲解

#’ οnclick=“alert(2)”>

#XSS常规攻击手法：平台，工具，结合其他等

#cookie session

用户凭据：通过凭据可以判断对方身份信息

cookie 存储本地 存活时间较长 小中型

session 会话 存储服务器 存活时间较短 大型

演示案例：

✧ 本地环境XSS漏洞原理讲解

<BODY onlaod="alert('XSS')">

1

✧ XSS漏洞各个分类差异讲解

✧ XSS漏洞代码绕过靶场使用

✧ XSS平台及工具简要演示测试

涉及资源：

https://xss8.cc/xss.php?do=login

https://xsshs.cn/xss.php?do=login

https://github.com/do0dl3/xss-labs

http://down.chinaz.com/soft/37581.htm