渗透课程里面：

01. 网站安全渗透技术介绍

02. 网站服务通讯原理介绍 -HTTP协议 cookie

03. 网站攻防环境搭建过程 -xss pikachu

04. 网站漏洞扫描工具使用 SQL XSS

05. 网站SQL注入攻击

06. php脚本编写概念

xss跨站脚本攻击

01. 跨站脚本攻击概念介绍

02. 跨站脚本攻击产生原因

03. 跨站脚本攻击造成危害

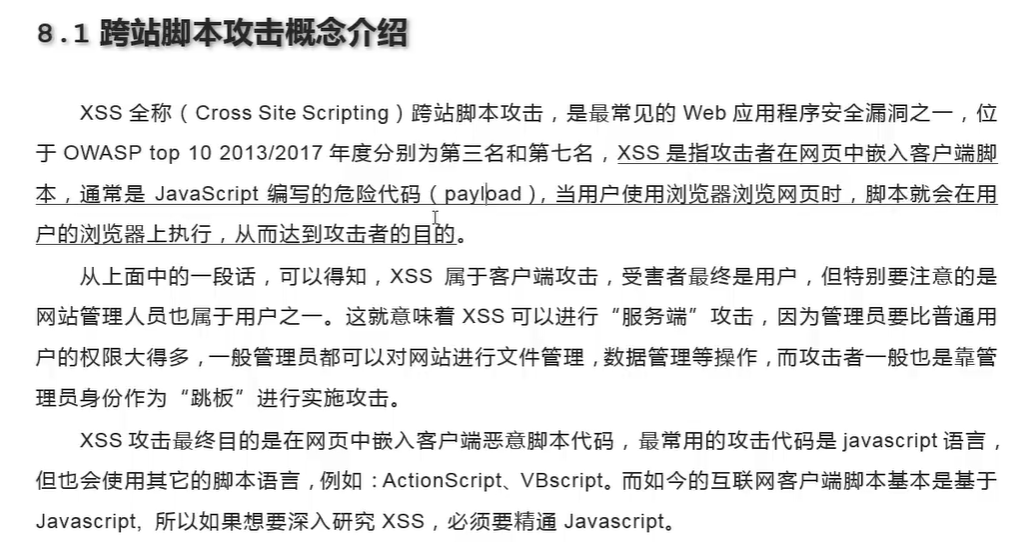
04. 跨站脚本攻击分类介绍（重点）

05. 跨站脚本攻击存在地方（了解）

06. 跨站脚本攻击测试方法（了解）

07. 跨站脚本攻击实战演示

01. 跨站脚本攻击概念介绍 xss



客户端攻击：客户端执行javascript恶意的脚本代码，从而影响客户端使用

服务端攻击：服务端管理员加载管理页面也可能受到攻击

HTTP方式进行访问

钓鱼网站

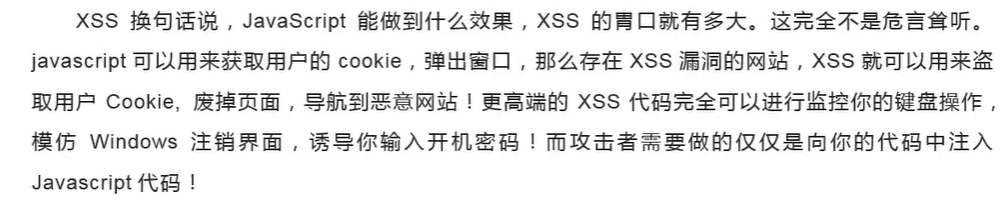
游戏--游戏币--QQ上游戏好友发送信息--免费赠送游戏币

[www.qq.cn](http://www.qq.cn) --- 页面信息 -- 登录信息 --- 发送到邮箱

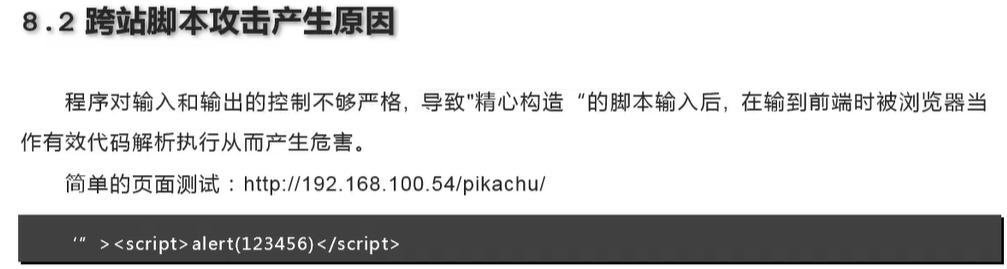
HTTPS方式进行访问

[www.qq.com](http://www.qq.com) -xss- [www.qq.com/test.php?javascripts恶意代码](http://www.qq.com/test.php?javascripts恶意代码)

-- 登录界面/截取你的cookie -- 保留下来 --- 替换掉攻击者访问网站cookie



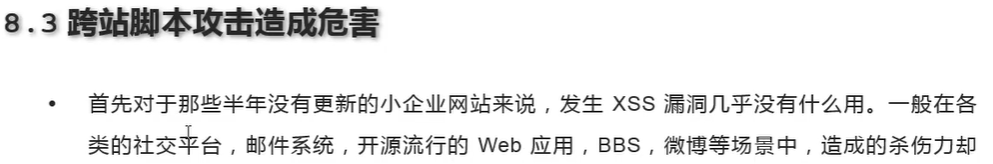
02. 跨站脚本攻击产生原因

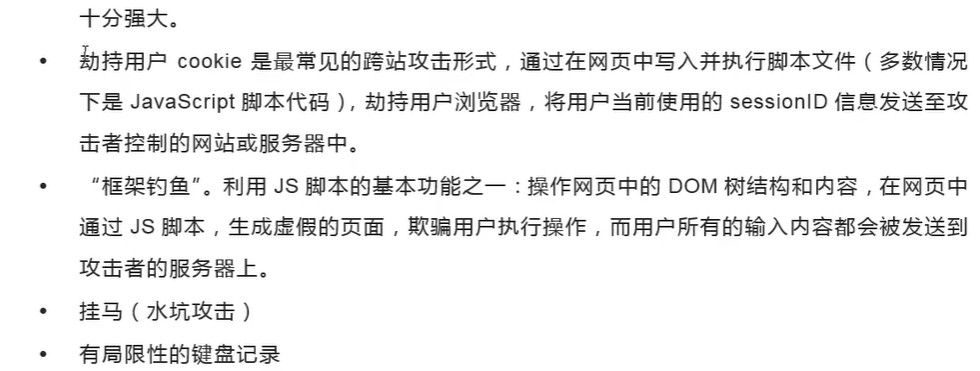


在网站页面上没有对输入输出的信息进行严格控制 可以加载恶意代码信息

从而对客户端用户造成威胁

03. 跨站脚本攻击造成危害

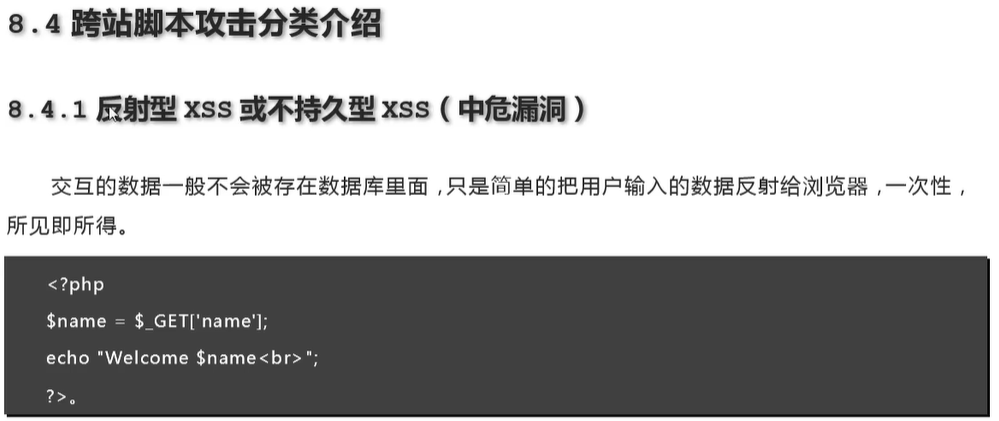




1. 会获取用户cookie信息
2. 会让用户数据信息泄露
3. 会获取用户登录信息
4. 会让用户电脑加载木马程序
5. 会记录用户键盘操作行为

04. 跨站脚本攻击分类介绍

1）反射型XSS或不持久型XSS

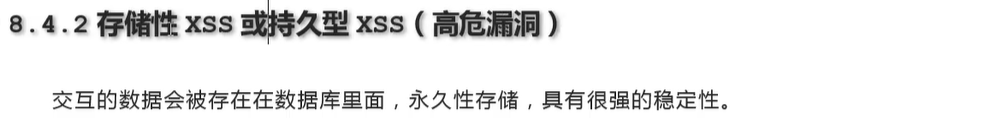


攻击过程必须让用户访问指定url才能生效，并且访问过程产生的数据不会对服务端 造成影响

1. 存储型XSS或持久型XSS

交互的数据会被存储在数据库里面，永久性存储，具有很强的稳定性。

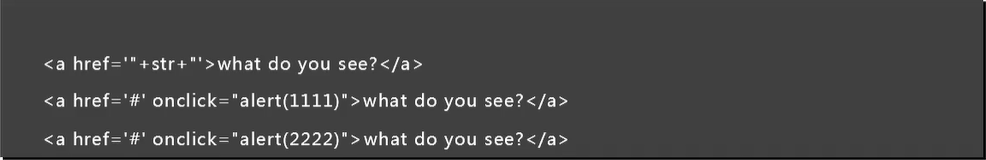
会对访问网站相应页面所有用户造成影响



1. DOM XSS (低危漏洞/中危漏洞)

会在网站页面生成超链接信息，超链接信息中会自动加载恶意代码，影响客户端





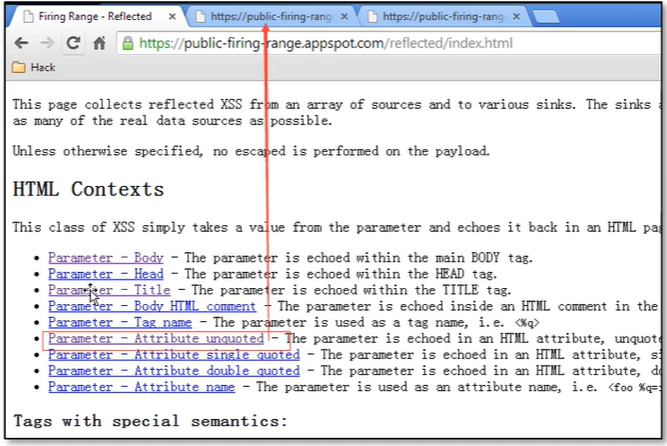
05. 跨站脚本攻击存在地方

1）HTML context 会出现javascript恶意代码



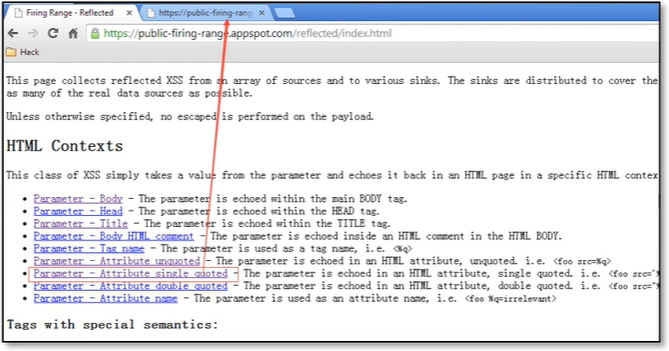
2）Attribute Context













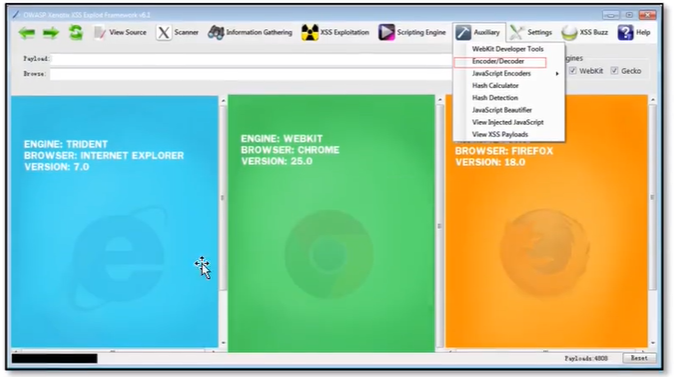


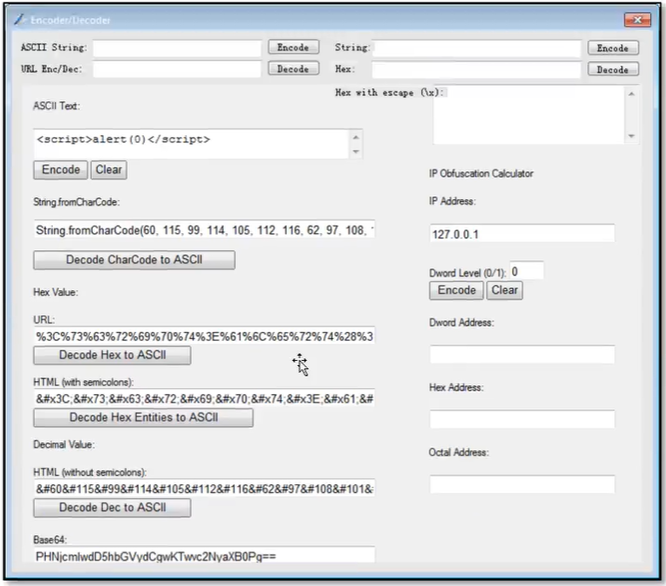
3）URL Context

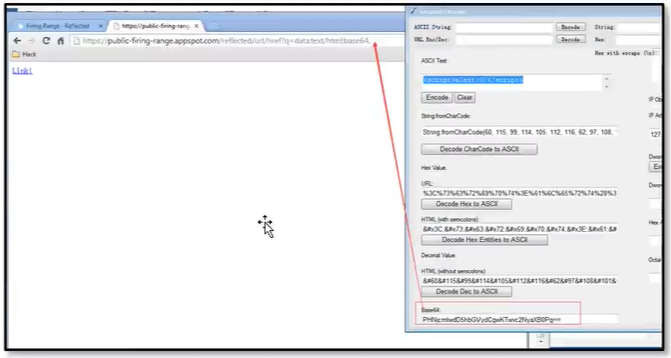


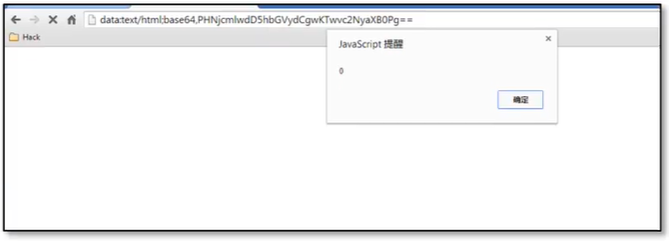




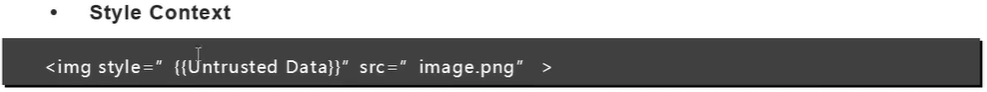




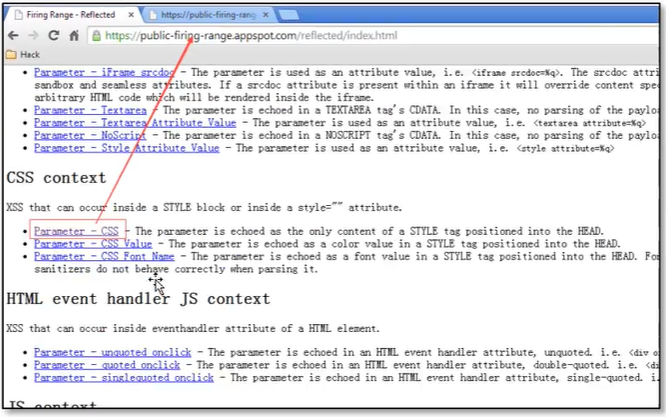




4）Style Context

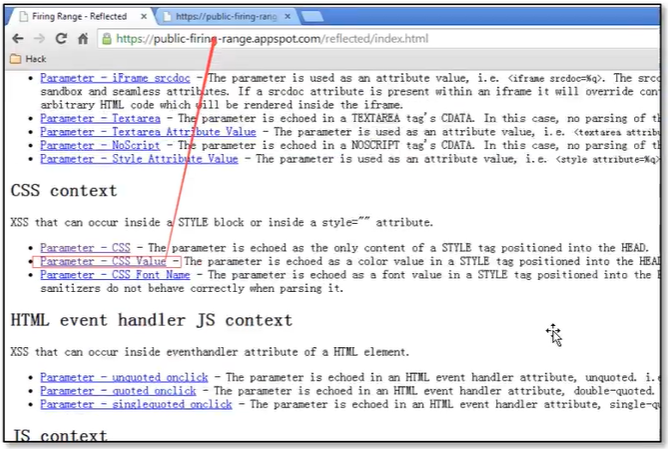








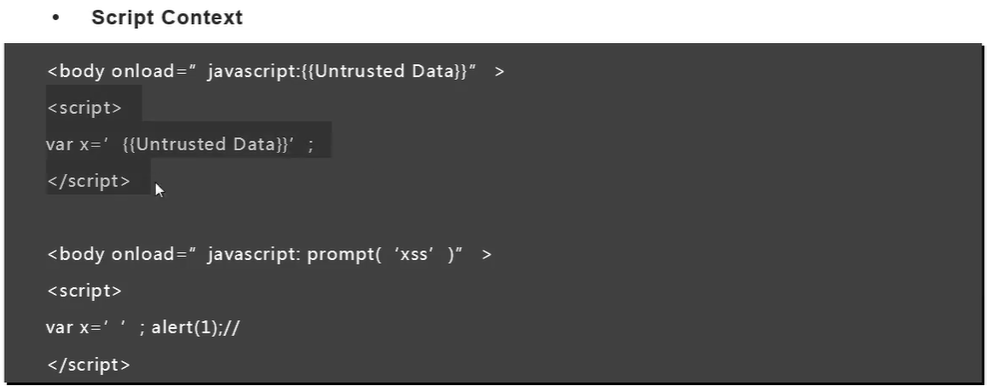


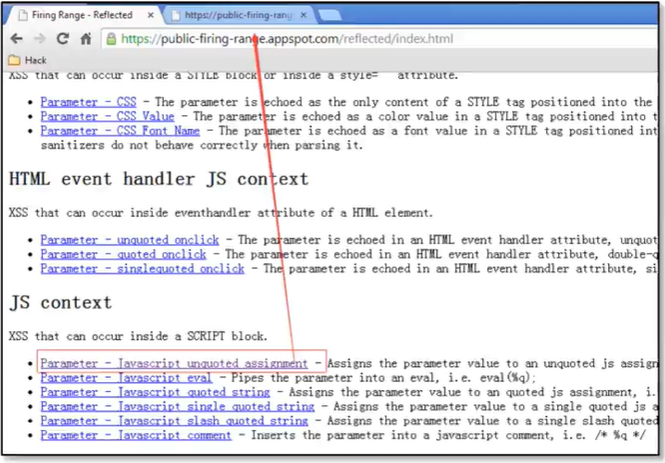




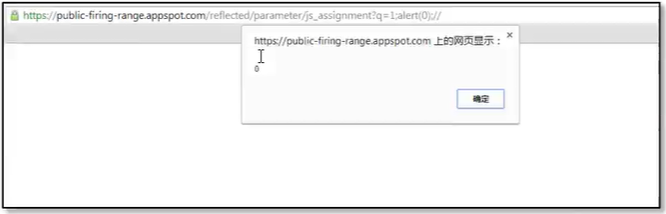


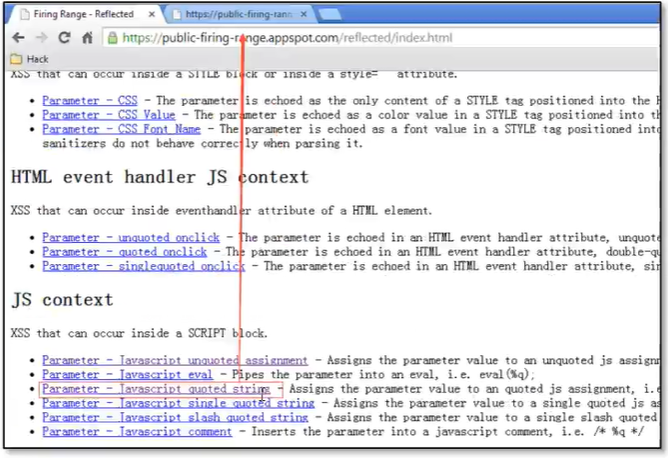
5）Script Context













、

06. 跨站脚本攻击测试方法

·工具扫描：APPscan、AWVS

