kali linux渗透测试

第28课 认识XSS跨站脚本攻击

什么是跨站脚本攻击?

XSS（Cross Site Scripting）攻击全称跨站脚本攻击，是为不和层叠样式表(Cascading Style Sheets, CSS)的缩写混淆，故将跨站脚本攻击缩写为XSS，XSS是一种经常出现在web应用中的计算机安全漏洞，它允许恶意web用户将代码植入到提供给其它用户使用的页面中。比如这些代码包括HTML代码和客户端脚本。

主要危害

1、盗取各类用户帐号，如机器登录帐号、用户网银帐号、各类管理员帐号

2、控制企业数据，包括读取、篡改、添加、删除企业敏感数据的能力

3、盗窃企业重要的具有商业价值的资料

4、非法转账

5、强制发送电子邮件

6、网站挂马

7、控制受害者机器向其它网站发起攻击

攻击方式

1、反射型

反射型XSS，也叫非持久型XSS，是指发生请求时，XSS代码出现在请求URL中，作为参数提交到服务器，服务器解析并响应。响应结果中包含XSS代码，最后浏览器解析并执行。从概念上可以看出，反射型XSS代码是首先出现在URL中的，然后需要服务端解析，最后需要浏览器解析之后XSS代码才能够攻击。

这类通常使用URL，具体流程：

1、Alice给Bob发送一个恶意构造了Web的URL。

2、Bob点击并查看了这个URL。

3、恶意页面中的JavaScript打开一个具有漏洞的HTML页面并将其安装在Bob电脑上。

4、具有漏洞的HTML页面包含了在Bob电脑本地域执行的JavaScript。

5、Alice的恶意脚本可以在Bob的电脑上执行Bob所持有的权限下的命令。

举个列子：

localhost:8080/helloController/search?name=<script>alert("hey!")</script>

localhost:8080/helloController/search?name=<img src='w.123' onerror='alert("hey!")'>

localhost:8080/helloController/search?name=点我

服务端代码片段，只做了一个简单的字符串连接就返回给客户端。

2、存储型

存储型XSS，也叫持久型XSS，主要是将XSS代码发送到服务器（不管是数据库、内存还是文件系统等。），然后在下次请求页面的时候就不用带上XSS代码了。最典型的就是留言板XSS。用户提交了一条包含XSS代码的留言到数据库。当目标用户查询留言时，那些留言的内容会从服务器解析之后加载出来。浏览器发现有XSS代码，就当做正常的HTML和JS解析执行。XSS攻击就发生了。

Beef框架

攻击手段：

1. 利用XSS漏洞
2. 诱使用户访问含有恶意脚本的伪造站点
3. 结合中间人攻击注入恶意脚本

常见用途

键盘记录器

网络扫描

浏览器信息收集

绑定shell

与Metasploit集成一起使用

谢谢观赏