## 跨站脚本攻击

**\*\*\*以下实例内容均可以在合天网安实验室进行\*\*\*\***

**\*\*\*\*** [**www.hetianlab.com**](http://www.hetianlab.com) **\*\*\*\***

## 基础：

1）跨站脚本攻击(Cross Site Scripting)，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。

**2）XSS工作原理**

恶意web用户将代码植入到提供给其它用户使用的页面中，如果程序没有经过过滤或者过滤敏感字符不严密就直接输出或者写入数据库。合法用户在访问这些页面的时候，程序将数据库里面的信息输出，这些恶意代码就会被执行。

**3）XSS漏洞的分类**

1.本地利用漏洞，这种漏洞存在于页面中客户端脚本自身；

2.反射式漏洞，这种漏洞和类型A有些类似，不同的是Web客户端使用Server端脚本生成页面为用户提供数据时，如果未经验证的用户数据被包含在页面中而未经HTML实体编码，客户端代码便能够注入到动态页面中；

3.存储式漏洞，该类型是应用最为广泛而且有可能影响到Web服务器自身安全的漏洞，攻击者将攻击脚本上传到Web服务器上，使得所有访问该页面的用户都面临信息泄漏的可能，其中也包括了Web服务器的管理员。

**4）XSS攻击的危害**

1.盗取用户cookie；

2.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；

3.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；

4.盗窃企业重要的具有商业价值的资料；

5.强制发送电子邮件；

6.网站挂马；

**存储式跨站脚本漏洞检测**：

一般留言系统可能存在该漏洞：

在留言框中输入：<script>alert(“xss test”)</script>

刷新留言板，若有JS脚本弹框，则说明存在该漏洞。

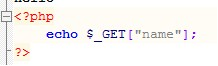
<iframe src="http://www.xxxx.com"></iframe>//将恶意网址插入到留言系统中

<iframe src="http://www.xxxx.com" width=”0” height=”0”></iframe>// 将而已网址隐藏起来

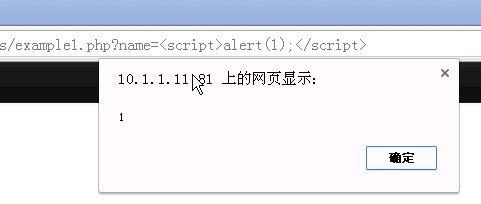
<script>document.write(document.cookie)</script>//利用存储式漏洞盗取用户cookie

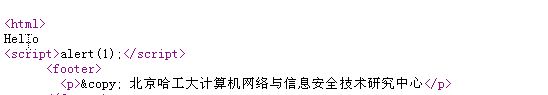
## 进阶（一）

### 实例一



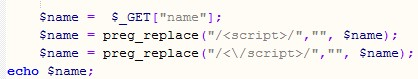
**此php代码并没有对输入的name进行任何的过滤。**可以直接利用





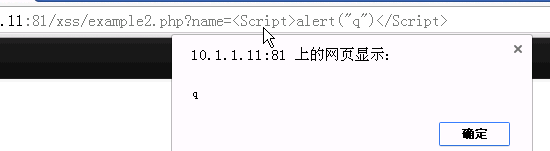
查看源代码会知道，我们的输入已经被认作是js代码，进行执行

### 实例二



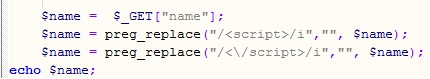
如图php引用preg\_replace();方法对<script>进行过滤，匹配到<script>和</script>时，替换为空。

所以这个可以利用大写来绕过

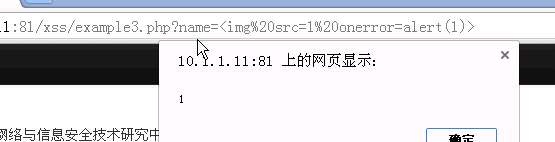


当然，不是只有首字母大写，任何一个字母大写都可以绕过。

### 实例三



由源代码可以知道，方法参数中用i进行大写匹配，所以现在使用大写是没有办法绕过的。可以用其他的JS标签绕过。如<img>标签



<img src=1 onerror=alert(1)>

其中src指向一个不存在的资源，也就是这个图片不可能加载出来，进而才会执行onerror。

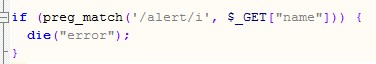
## 进阶（二）

### **实例四**

http://www.hetianlab.com/image1/GB218.76.35.752013122014274800001/63dc32e6-6d02-4bb2-aca4-f45821130178.png

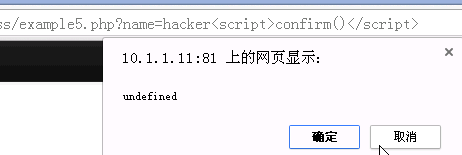
与实例三相同，用<img>即可绕过

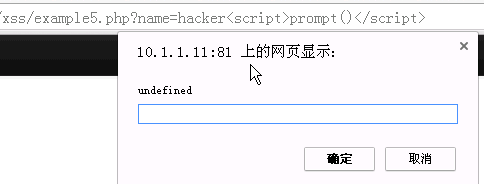
### 实例五



源代码过滤了alert关键字，在JS中，alert关键字用于弹窗，此处被过滤，可以用其他的关键字进行弹窗：

http://www.cnblogs.com/asd-sun/p/6560195.html





当然还有很多种语句构造可以实现，需要自己进行多次实验.

### 实例六

http://www.hetianlab.com/image1/GB218.76.35.752013122014274800001/200b341f-c65c-4742-afc9-12a3cdf31a3a.png

源代码可以理解为：

从地址栏输入的name=之后的所有字符，都处于<script>与</script>之间，

且第一对引号之内的字符均赋值给变量a，所以需要先用引号和分号闭合赋值语句，再进行弹窗。

可以这样实现：a”;alert($a);$a=”



最后的$a=”也是用来闭合源代码后面的引号。