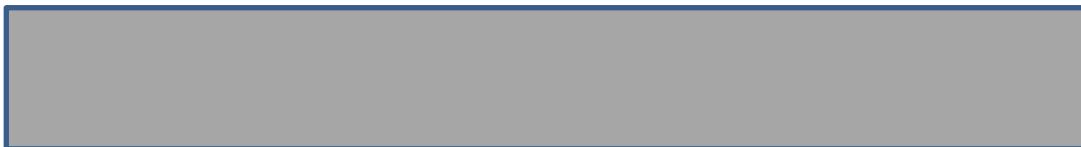


## 进阶实验

1. 通过 Google 或者 Shodan 引擎寻找使用有漏洞的 Discuz 论坛系统的站点
2. 在实验平台 <https://www.youwei.site/uv/discuz> 注册一个账号，尝试以下几个已披露的漏洞的利用。



## 漏洞证明

1. 漏洞需要开启后台四方格功能



2. 发表新帖子,在帖子标题中设置为payload

```
&#x003c;img src=1 onerror=alert(1)&#x003e;
```

3. 然后在首页鼠标放在帖子准备点击我们刚才的发表的帖子时，触发onmouseover事件，执行我们的代码。



## 漏洞分析

鼠标放在帖子上准备点击时，触发onmouseover事件。onmouseover事件中调用的showTip函数最终调用到了\_showTip函数



\_showTip函数中使用getAttribute取了tip属性值，然后又放入innerHTML。

重点是getAttribute函数获取属性值时会自动解码实体编码后的值，这样 `&#x003c;img src=1 onerror=alert(1)&#x003e;` 就变成 `<img src=1 onerror=alert(1)>`。

```
932 function _showTip(ctrlobj) {
933     if(!ctrlobj.id) {
934         ctrlobj.id = 'tip_' + Math.random();
935     }
936     menuid = ctrlobj.id + '_menu';
937     if(!$menuid) {
938         var div = document.createElement('div');
939         div.id = ctrlobj.id + '_menu';
940         div.className = 'tip tip_4';
941         div.style.display = 'none';
942         div.innerHTML = '<div class="tip_horn"></div><div class="tip_c">' + ctrlobj.getAttribute('tip') + '</div>';
943         $('append_parent').appendChild(div);
944     }
945     $(ctrlobj.id).onmouseout = function () { hideMenu('', 'prompt'); };
946     showMenu({'mtype': 'prompt', 'ctrlid': ctrlobj.id, 'pos': '12!', 'duration': 2, 'zindex': JSMENU['zIndex']['prompt']});
947 }
```



另外此漏洞中的payload只能用

`&#x003c;img src=1 onerror=alert(1)&#x003e;`

而不能

`&#x3c;img src=1 onerror=alert(1)&#x3e;`

这是由于Discuz中dhtmlspecialchars函数实现问题。

```
function dhtmlspecialchars($string, $flags = null) {
    if(is_array($string)) {
        foreach($string as $key => $val) {
            $string[$key] = dhtmlspecialchars($val, $flags);
        }
    } else {
        if($flags === null) {
            $string = str_replace(array('&', '"', '<', '>'), array('&amp;', '&quot;', '&lt;', '&gt;'), $string);
            if(strpos($string, '&#') !== false) {
                $string = preg_replace('/&#((\d{3,5}|x[a-zA-F0-9]{4}))/','&#x0001', $string);
            } //在这一行又将 & 解码成 &, 导致 dhtmlspecialchars 和 php 中的 htmlspecialchars 函数差异
        } else {
            if(PHP_VERSION < '5.4.0') {
                $string = htmlspecialchars($string, $flags);
            } else {
                if(strtolower(CHARSET) == 'utf-8') $charset = 'UTF-8';
                else $charset = 'ISO-8859-1';
                $string = htmlspecialchars($string, $flags, $charset);
            }
        }
    }
    return $string;
}
```

这个差异可以这么解释

```
1 htmlspecialchars(htmlspecialchars("&#x003c;")); 值是"&amp;amp;#x003c;";
2 dhtmlspecialchars(dhtmlspecialchars("&#x003c;")); 值是"&#x003c;";
```

而上面tip属性值就是两次dhtmlspecialchars了标题的值,输入存到数据库一次, 输出时一次。

```
1 tip=dhtmlspecialchars(dhtmlspecialchars(标题));
```

## 漏洞总结

1. dhtmlspecialchars函数和实际的htmlspecialchars函数有差异
2. getAttribute函数会将属性值解码



## 漏洞证明

2017.9月份在3.3,3.4最新版测试通过

前提条件:

1. 用户组允许使用media标签
2. 非PC端用户(程序会判断UA)

复现步骤:

0x1. 可以使用media标签的用户发表一篇文章

文章内容为

```
[media=mp3,200,300]http://www.tudou.com/programs/view/a'      onload=alert(1)
onerror=alert(1)[/media]
```

0x2. 使用手机, 或者使用UA修改工具, 修改成移动端头部

0x3. 浏览刚发过的帖子, 视频加载完毕后, 执行onload事件, 会弹窗.



## 漏洞分析

```
<span id="flv_dWh"></span><script type="text/javascript"
reload="1">$('flv_dWh').innerHTML=(mobileplayer() ? "<iframe height='300'
width='200'
src='http://www.tudou.com/programs/view/html5embed.action?code=a\\\'
onload=alert(1) onerror=alert(1)' frameborder=0 allowfullscreen></iframe>" :
AC_FL_RunContent('width', '200', 'height', '300', 'allowNetworking',
'internal', 'allowScriptAccess', 'never', 'src',
'http://www.tudou.com/v/a\\\' onload=alert(1) onerror=alert(1)', 'quality',
'high', 'bgcolor', '#ffffff', 'wmode', 'transparent', 'allowfullscreen',
'true'));</script></td></tr></table>
```

前端页面中有这么一段代码，非PC时，mobileplayer()=true。

简化下上面的代码，如下：

```
$('flv_dWh').innerHTML="<iframe
src='http://www.tudou.com/programs/view/html5embed.action?code=a\\\'
onload=alert(1)'"
```

其中虽然src属性单引号看似没有闭合，但是实际上浏览器解析时已经闭合了，于是就引入了一个onload属性。

至于后端的代码，在 `source/function/function_discuzcode.php` 文件的 `parseflv` 函数中下断点可以调试漏洞，这里就不详细说明。

## 漏洞总结

```
src='<?php addslashes("可控内容")?>'
```

这样是不能防XSS的,用下面这样的代码是可以弹框的。

```
<img src='x\' onerror=alert(1)//'>
```

漏洞编号：CVE-2018-10297

漏洞名称：Discuz!跨站脚本攻击

漏洞描述：Discuz! <= X3.4版本存在存储型跨站脚本漏洞，允许远程攻击者注入恶意脚本或HTML代码，从而获取敏感信息或劫持用户会话。

危险等级：中级

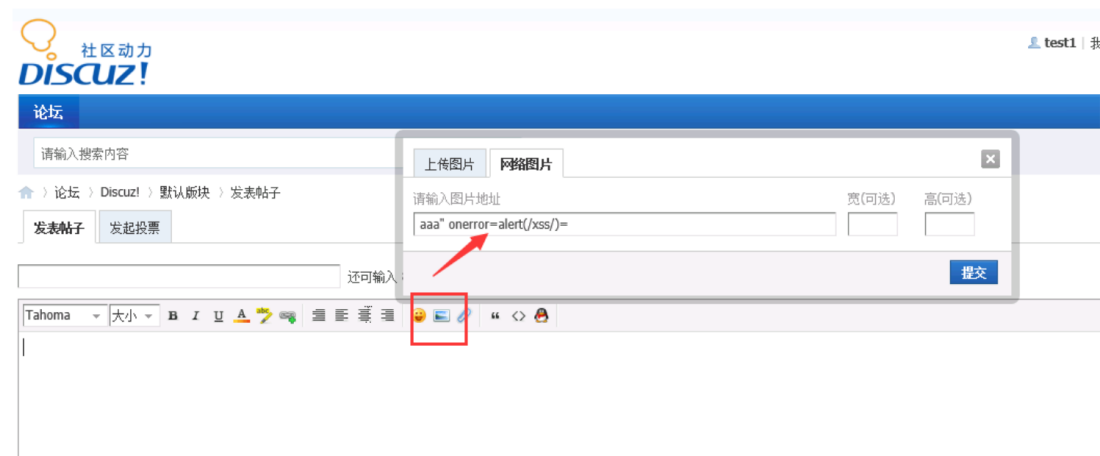
# 漏洞利用

## 反射型XSS

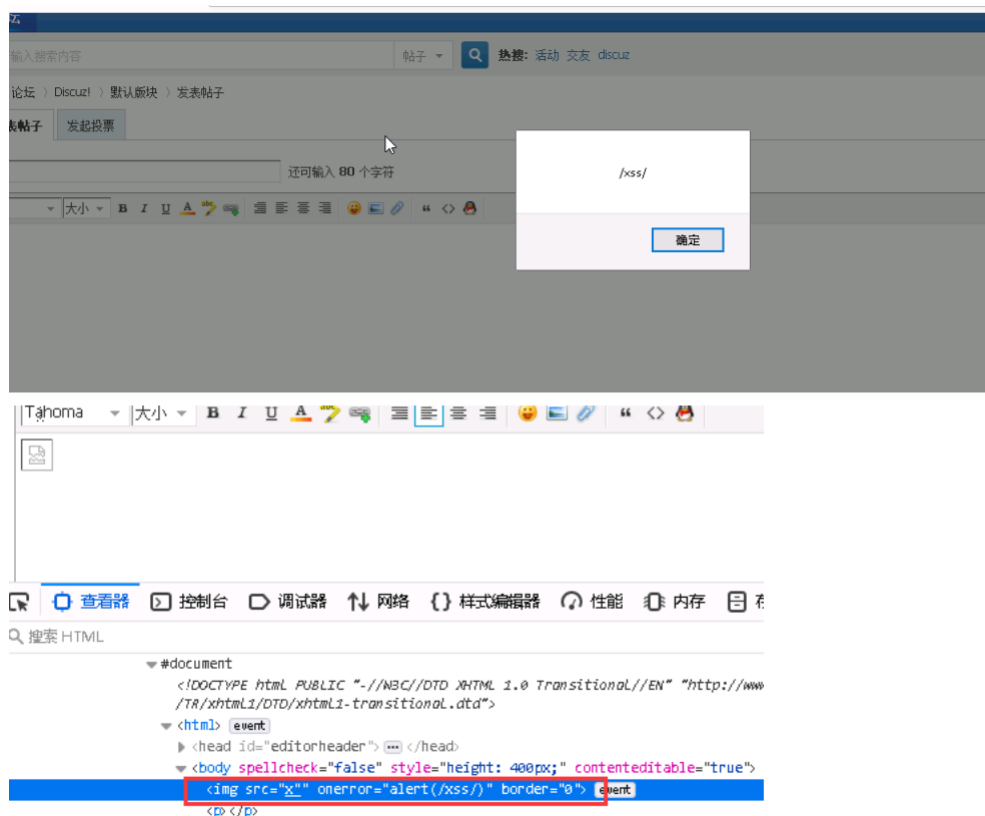
先注册一个用户test1

在用户发帖处,插入图片,选择网络图片

地址处填写payload `x" onerror=alert(/xss/)`



点击提交



## 储存型XSS

存储型XSS利用前提：目标网站开启门户功能，且所在用户组有发表文章的权限

以管理员身份,开启门户



添加频道



添加文章

