

前记

大年 30，北神开始在群里吆喝着，要分享思路，出于对漏洞挖掘的渴望，放下手中的趺突泉啤酒，带上一根烟溜到外边去听课。

当时讲的是某文库，并发点：点赞，以及领取金币等一次性的奖励，通过并发同一时间对服务器发送多个数据包，就会对服务器造成欺骗，从而多个请求包会相应成功。（原理不明白的可以看北神发的企业逻辑漏洞）。




正文：

北神讲完以，我就想着怎么去找别人不想的不太全的漏洞点测试，碰巧当时想洗澡，思考了一下，当时我正好挖掘的短信轰炸比较多，短信验证码就是一次性的东西，在一定的时间内只能获取一次，所以就引发了下面的 xx 存在并发短信轰炸

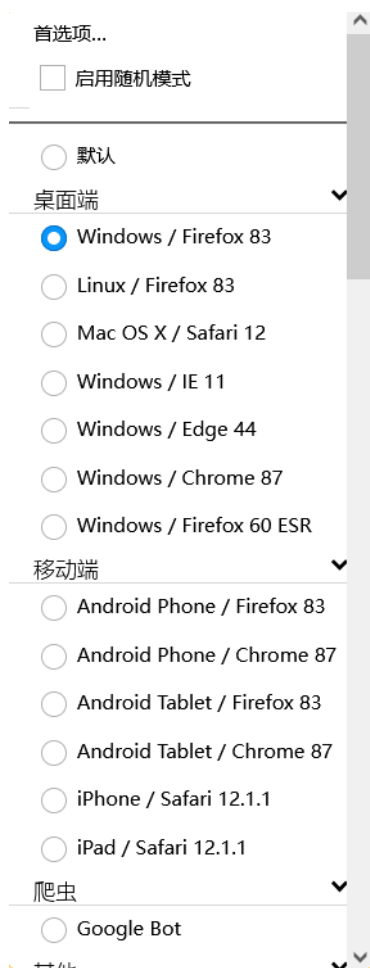
1. 电脑端打开时没有获取验证码选项的

扫码登录

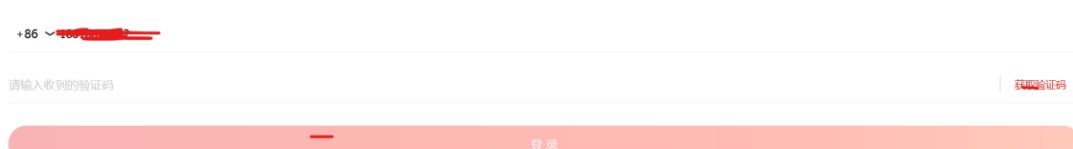
账户登录

A screenshot of a web login page. At the top, there are two tabs: '扫码登录' (Scan QR Code Login) and '账户登录' (Account Login). Below the tabs, there are two input fields. The first input field is for a phone number, with a redacted value '1000...' and a red line drawn over it. The second input field is for a password, with a redacted value '密码' and a red line drawn over it.A screenshot of a web login page. At the top, there are two tabs: '扫码登录' (Scan QR Code Login) and '账户登录' (Account Login). Below the tabs, there are two input fields. The first input field is for a phone number, with a redacted value '1000...' and a red line drawn over it. The second input field is for a password, with a redacted value '密码' and a red line drawn over it.

2. 更改 user-agent 为移动端（或者在域名前加 m.xx.com），
重新访问，这里推荐 火狐：User-Agent Switcher

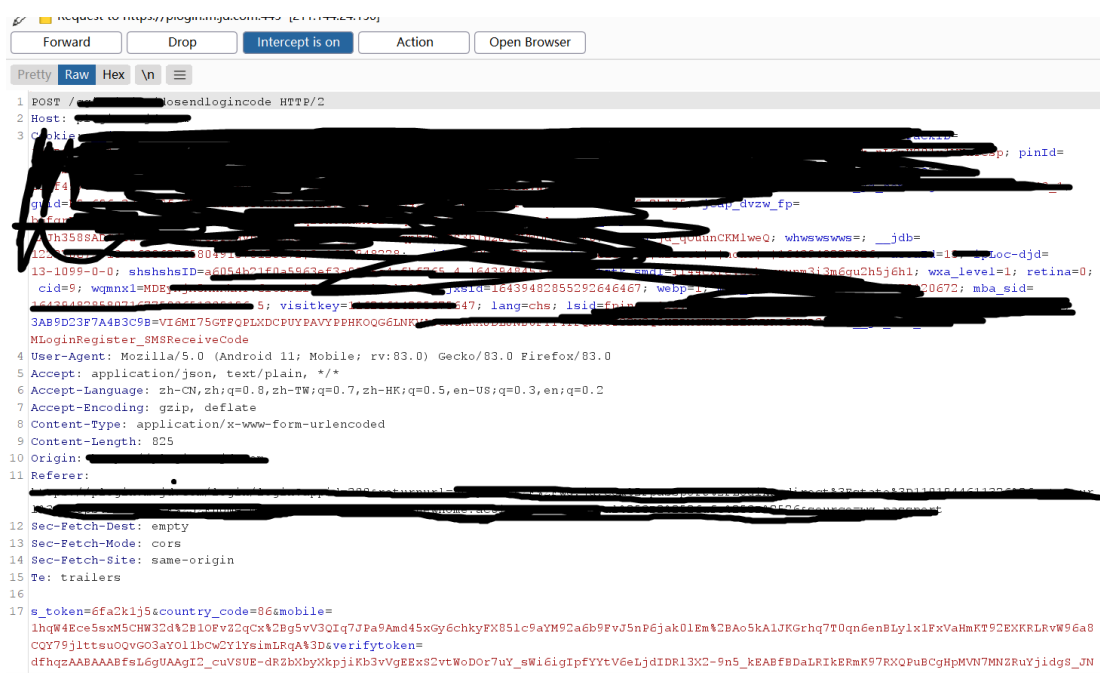


3. 刷新如下：



这就可以获取验证码了，

4. 输入手机号，点击获取验证码抓包，找到这个发送验证码的数据包，利用并发，同一时间多次对服务器发该数据包，从让服务器发送给手机多个验证码，造成短信轰炸



5. 并发成功截图：这里我只是同时发送了 30 个请求包，成功 8-9 个，如果请求包增多的话，对用户会造成很大的影响。

Turbo Intruder - piogn.mjg.com - done

Row	Payload	Status	Words	Length	Time	Label
1		200	128	409	57	
6		200	128	409	50	
7		200	128	409	49	
8		200	128	409	49	
9		200	128	409	47	
10		200	128	409	47	
11		200	128	409	47	
12		200	128	409	47	
13		200	128	409	47	
16		200	128	409	46	
17		200	128	409	45	
18		200	128	409	43	
0		200	156	486	32	
19		200	156	486	43	
20		200	156	486	35	
21		200	156	486	37	
22		200	156	486	35	

1 POST /sendlogincode HTTP/1.1

2 Host: [REDACTED]

3 Cookie: [REDACTED]

4 Content-Type: text/html; charset=utf-8

5 Connection: close

6 Set-Cookie: isld=[REDACTED] Path=/; Expires=Fri, 02-Jan-1970 00:00:00 GMT

7 Set-Cookie: guild=[REDACTED] Path=/; Expires=Fri, 02-Jan-1970 00:00:00 GMT

8 Server: jfe

9 Strict-Transport-Security: max-age=7776000

10

11 {"err_code":0,"err_msg":"","errcode":0,"message":""}

12

🔍 搜索通知信息



短信登录验证码: 599234。...



短信登录验证码: 476428。...



短信登录验证码: 841791。...



短信登录验证码: 189463。...



短信登录验证码: 807098。...



短信登录验证码: 040330。



短信登录验证码: 893084。



短信登录验证码: 942766



短信登录验证码: 573315



短信登录验证码: 255817



短信登录验证码: 720317



18分钟



50100420021 中午11:30

96130 中午11:2



6.经过对我自己一顿轰炸，也赢来了胜利的曙光

WEB漏洞—其它

自评等级
低危核定等级
中危原始积分
0活动倍数
1翻倍后积分
80报告加分
0共获得积分
80兑换方式
积分兑换

我的现金

已发放

所有

项目名称	奖励对象	奖励类型	金额	预计完成时间	实际完成时间	状态
██████████	0	0	400.00	2022-02-22 12:43:19	0000-00-00 00:00:00	已发放

总结：

通过这一次测试，我发现万物皆可并发，所以师傅们有事没事的时候试试并发。

完事以后，我又思考了起来，有点不切实际，可看可不看

既然我们可以同时获取多个验证码，是不是这几个验证码都可以同时登录进去。

如果这样的话，我们在登录处先并发一下，然后我们再用 burp 爆破 6 位验证码，实现任意用户登录。

这样我们爆破成功的几率得到了提升，加入：通过并发，获取到 10 个验证码，burp 爆破 6 位是

100w 种可能，通过并发，这样一来我们成功的几率就降到了 10w 种。

以上只是思考，不切实际，希望和师傅们成为朋友，共同进步。

师傅们慢点喷，同时感谢北神和十二师傅的指导。