

simple_date_birth_brute

原地址：GZCTF-challenges/simple_date_birth_brute

访问容器网页，如下内容

学校统一登录平台

身份选择

学生

用户名

密码

登录

[录取名单查询](#)

[学生学籍信息查询](#)

点击 [录取名单查询](#)，获取 excel 文件，如下内容

	A	B	C	D	E
1	序号	姓名	专业	身份证号码	
2	1	高松灯	WEB	530428*****2843	
3	2	安若	MISC	441201*****7142	
4	3	苏幽璃	REVERSE	140211*****1321	
5	4	黎曦	PWN	130102*****9846	
6	5	姚乐奈	CRYPTO	140423*****9525	
7					
8					
9					
10					
11					
12					

可以看见其中的出生年月日信息被抹除了，接下来先看下 [学生学籍信息查询](#)

学生学籍信息查询

姓名

身份证号码

查询

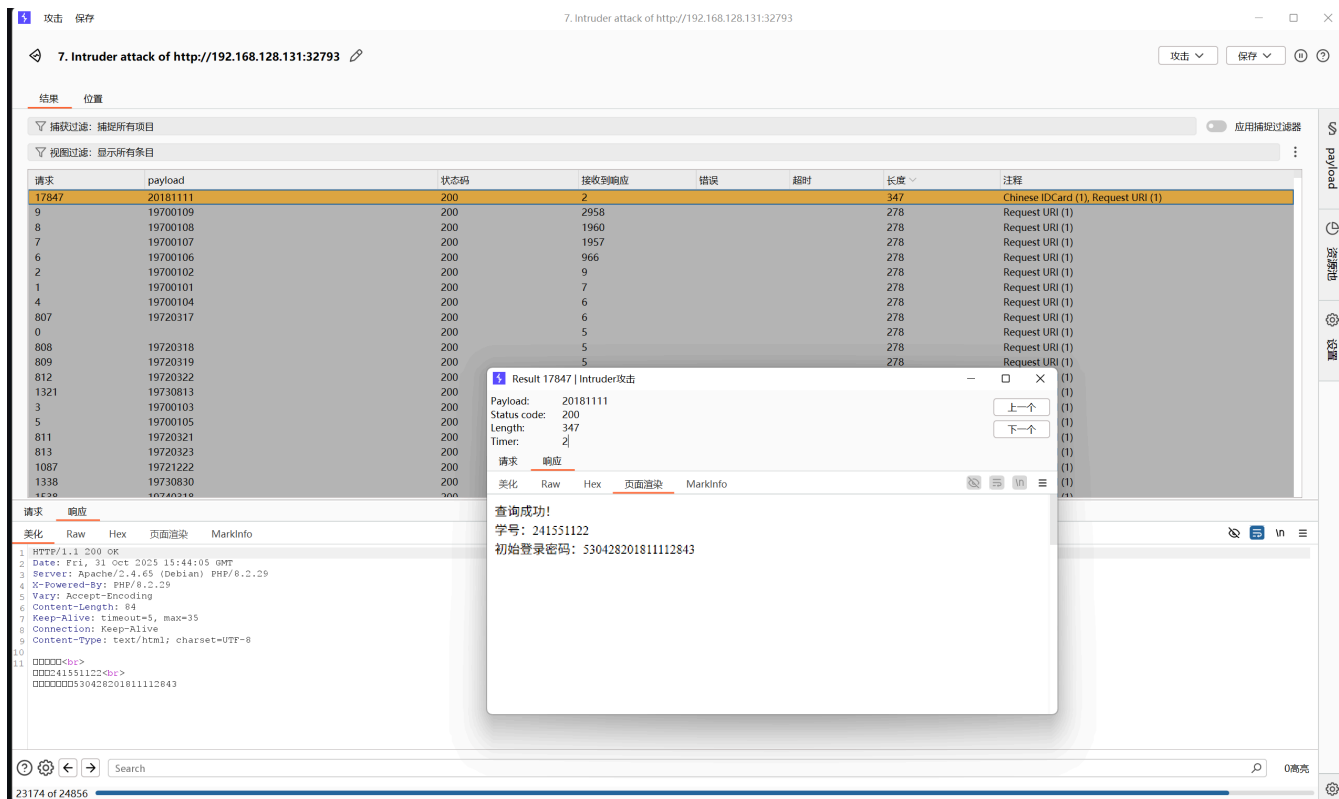
查询信息需要姓名和身份证号，我们通过爆破来爆破出完整的身份信息，先使用 bp 捕获一个请求包

```
1 POST /student_info_query.php HTTP/1.1
```

```
2 Host: IP:PORT
3 Content-Length: 59
4 Cache-Control: max-age=0
5 Accept-Language: zh-CN,zh;q=0.9
6 Origin: http://IP:PORT
7 Content-Type: application/x-www-form-urlencoded
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/137.0.0.0 Safari/537.36
10 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/w
ebp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
11 Referer: http://IP:PORT/student_info.php
12 Accept-Encoding: gzip, deflate, br
13 Connection: keep-alive
14
15 name=%E9%AB%98%E6%9D%BE%E7%81%AF&id_card=530428*****2843
```

接下来爆破（因为知道后端生成范围为 1970-01-01 至 2038-01-19，所以直接用这个范围）

The screenshot displays the Burp Suite Professional interface. The main window shows a list of HTTP requests, with the selected request being a POST to /student_info_query.php. The request body is a form-urlencoded string containing a name and an id_card. The right-hand pane is the 'payload' tab, which is used for configuring the attack. It includes fields for 'Payload位置' (Payload location), 'Payload类型' (Payload type), 'Payload数量' (Payload count), and '请求数量' (Request count). The 'payload配置' (Payload configuration) section allows for generating payloads based on a date range, with options for '从' (From), '到' (To), '间隔' (Interval), and '格式' (Format). The 'Payload处理' (Payload processing) section provides options for adding, editing, deleting, and moving rules. The 'Payload编码' (Payload encoding) section includes a checkbox for 'URL编码字符' (URL encoding characters) and a text field for the encoding pattern.



爆破出完整信息（学号、密码），接下来登录

学校统一登录平台

身份选择

学生

用户名

241551122

密码

530428201811112843

登录

[录取名单查询](#)

[学生学籍信息查询](#)

← → ↻ 🏠 ⚠ 不安全 192.168.128.131:32793/login.php

登录成功! Flag: flag{GZCTF_dynamic_flag_test}

得到 flag