

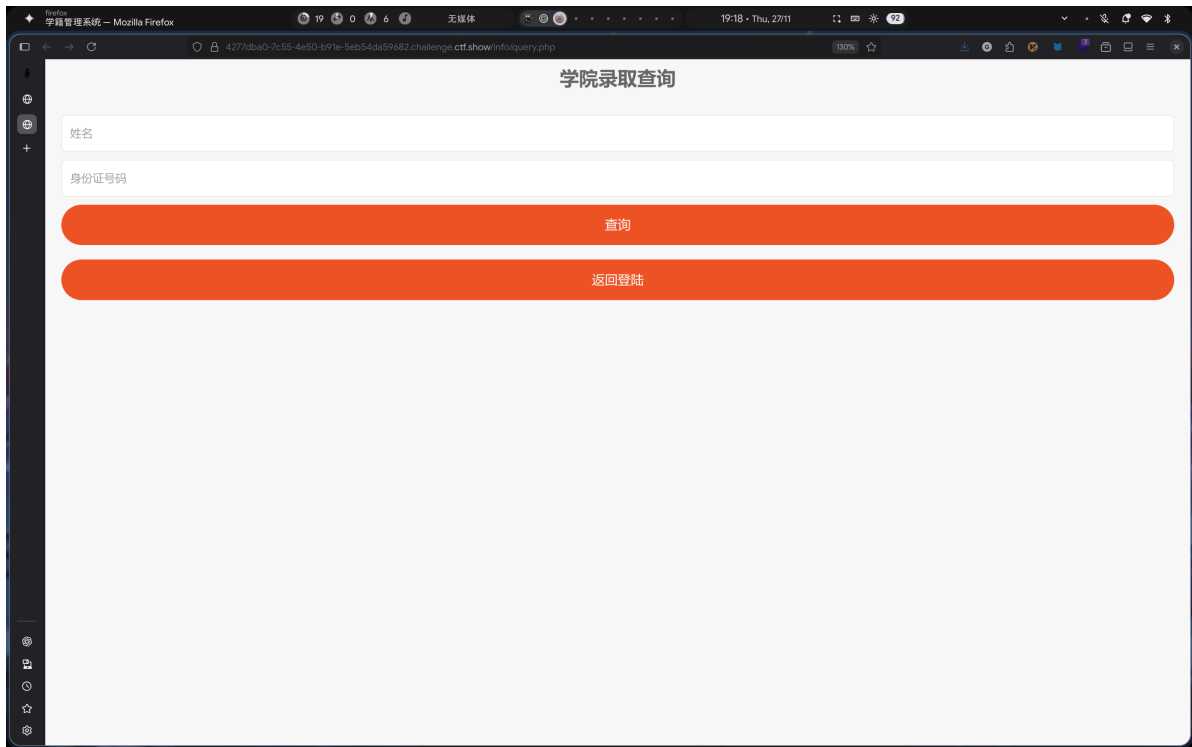
1.打开靶场是一个教务管理系统



2.点击下面的“录取名单”，下载了一个.xlsx文件，打开是一个学生数据库

CTFshow菜鸡学院录取名单				
序号	姓名	专业	身份证号码	备注
1	高先伊	WEB	621022*****5237	
2	嵇开梦	MISC	360730*****7653	党员
3	郎康焕	RE	522601*****8092	
4	元羿淳	PWN	451023*****3419	生源地贷款
5	祁落兴	CRYPTO	410927*****5570	

3.回到主界面点击下面的“学生学籍信息查询系统”，根据主界面推断这是用来查找学号的



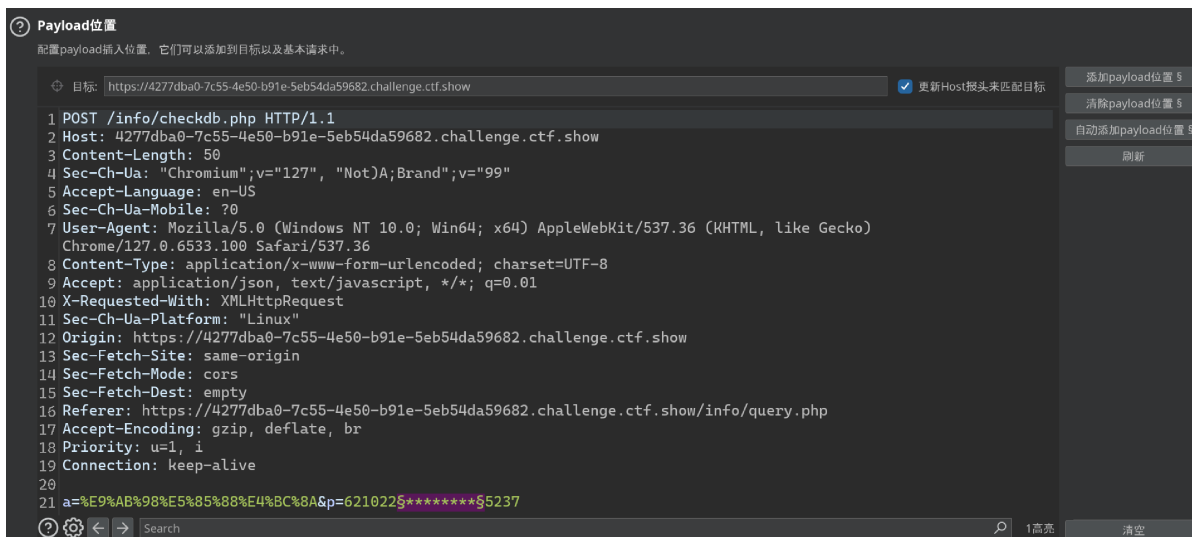
4.查看数据库发现刚好是8位数生日被隐藏了，要爆破出身份证号码，决定爆破“高先伊”身份证号码

1	高先伊	WEB	621022*****5237
---	-----	-----	-----------------

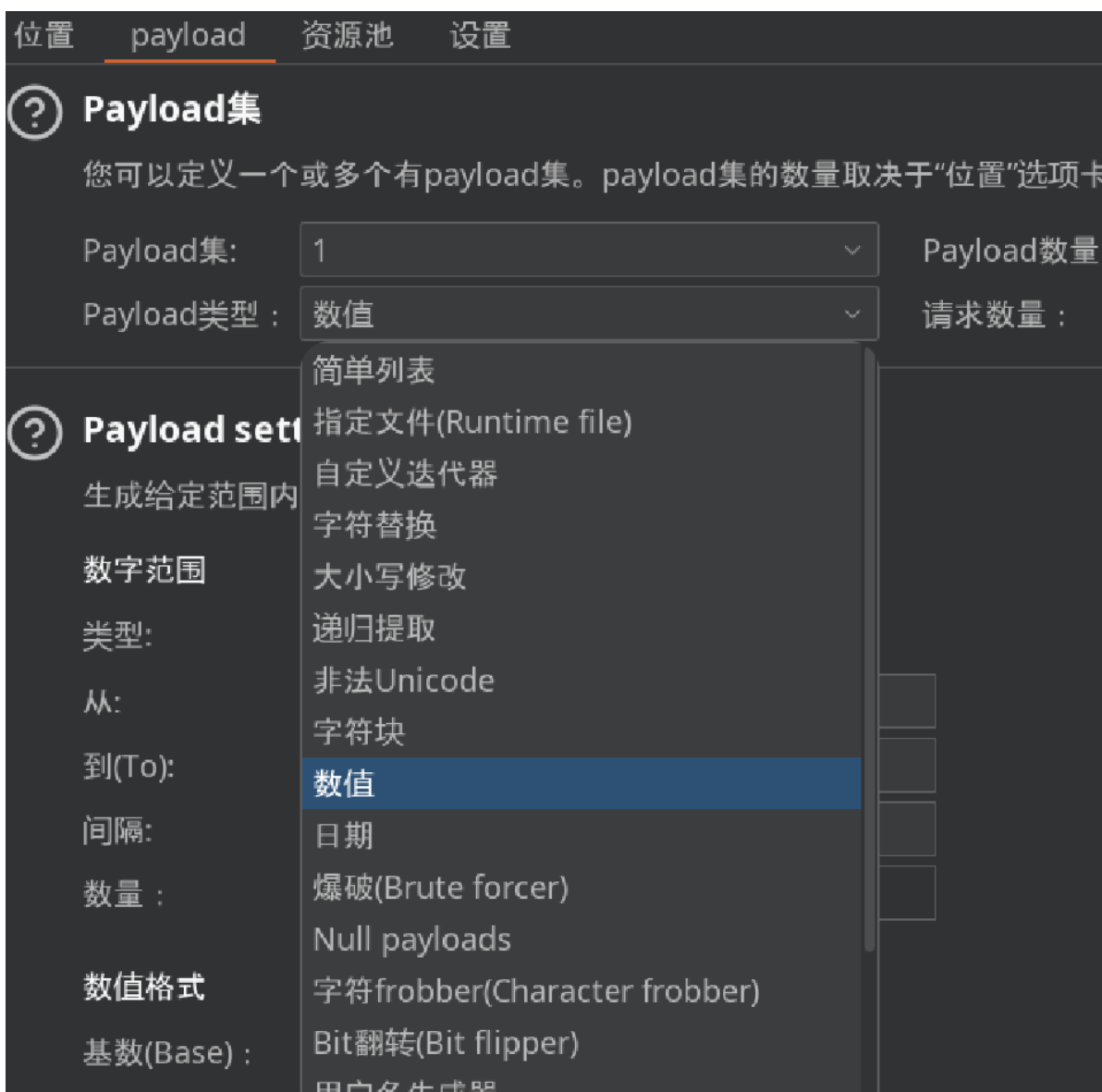
5.进入“学院录取查询”，输入姓名和部分正确身份证号码



6.点击查询用bp抓包，发送到Intruder，给引号“添加payload位置”



7. 进入“payload”模块，设置Payload类型为“数值”



8. 设置数字范围

? Payload settings [Numbers]

生成给定范围内指定格式的有效数值内容。

数字范围

类型: 顺序 随机

从:

到(To):

间隔:

数量:

数值格式

基数(Base): 十进制 Hex

整数最小位数:

9.0~99999999太久了，我们可以看到在主界面下面有1999-2017的时间,猜测他们被录取时有十几岁了，所以那数值范围可以设置为19800000~20180000



高先伊

621022199002015237

查询

返回登陆

13.抓包->发送到重发器->发送（也可以直接查询，我这麻烦了）

请求

```

coted; charset=UTF-8
9 Accept: application/json,
text/javascript, */*; q=0.01
0 X-Requested-With:
XMLHttpRequest
1 Sec-Ch-Ua-Platform: "Linux"
2 Origin:
https://631cb478-160f-4e5f-b
d02-7d7c01617d3c.challenge.c
tf.show
3 Sec-Fetch-Site: same-origin
4 Sec-Fetch-Mode: cors
5 Sec-Fetch-Dest: empty
6 Referer:
https://631cb478-160f-4e5f-b
d02-7d7c01617d3c.challenge.c
tf.show/info/query.php?
7 Accept-Encoding: gzip,
deflate, br
8 Priority: u=1, i
9 Connection: keep-alive
0
1 a=
%E9%AB%98%E5%85%88%E4%BC%8A&
p=621022199002015237

```

响应

```

s:
Content-Type, Cookies, Aaa, Dat
e, Server, Content-Length, Conn
ection
10 Access-Control-Allow-Headers
:
DNT, X-CustomHeader, Keep-Aliv
e, User-Agent, X-Requested-Wit
h, If-Modified-Since, Cache-Co
ntrol, Content-Type, Authoriza
tion, x-auth-token, Cookies, Aa
a, Date, Server, Content-Length
, Connection
11 Access-Control-Max-Age:
1728000
12 Content-Length: 195
13
14 {"0": "success", "msg": "\u606d
\u559c\u60a8\u597d\u60a8\u5d
f2\u88ab\u6211\u6821\u5f55\u
53d6\u597d\u4f60\u7684\u5b66
\u53f7\u4e3a02015237
\u521d\u59cb\u5b66\u7801\u4e
3a\u8eab\u4efd\u8bc1\u53f7\u
7801"}

```

14.解码得到学号，默认密码是身份证号码

Unicode与中文 编码/解码

```
\u606d\u559c\u60a8\u54c7\u60a8\u5df2\u88ab\u6211\u6821\u5f55\u53d6\u54c7\u4f60\u7684\u5b66\u53f7\u4e3a02015237  
\u521d\u59cb\u5bc6\u7801\u4e3a\u8eab\u4efd\u8bc1\u53f7\u7801
```

171

模式: Unicode 默认模式 \u[0-9a-f]{4}

编码忽略 Ascii 字符

编码成 Unicode

解码成 中文

↑ 交换

清空

02015237 初始密码为身份证号码

恭喜您, 您已被我校录取, 你的学号为020

15. 进行登录, 得到flag

用户登录 / LOGIN

 学号 : 02015237

 密码 :

部门 教师 学生 访客

[录取名单](#)
[学生学籍信息查询系统](#)

⊕ 631cb478-160f-4e5f-bd02-7d7c01617d3c.challenge.ctf.show

恭喜您，登陆成功!ctfshow{4677418a-518b-4a53-b6c2-d576ac50d832}

确定