web入门 爆破

原创

sec0nd_ 已于 2022-03-13 16:25:50 修改 3913 收藏 7

分类专栏： ctfshow 从0开始学web 文章标签： 安全 web安全 系统安全

于 2022-03-12 16:55:15 首次发布

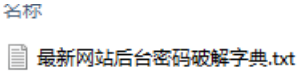
本文链接：https://blog.csdn.net/weixin_52444045/article/details/123445489

文章目录

web21

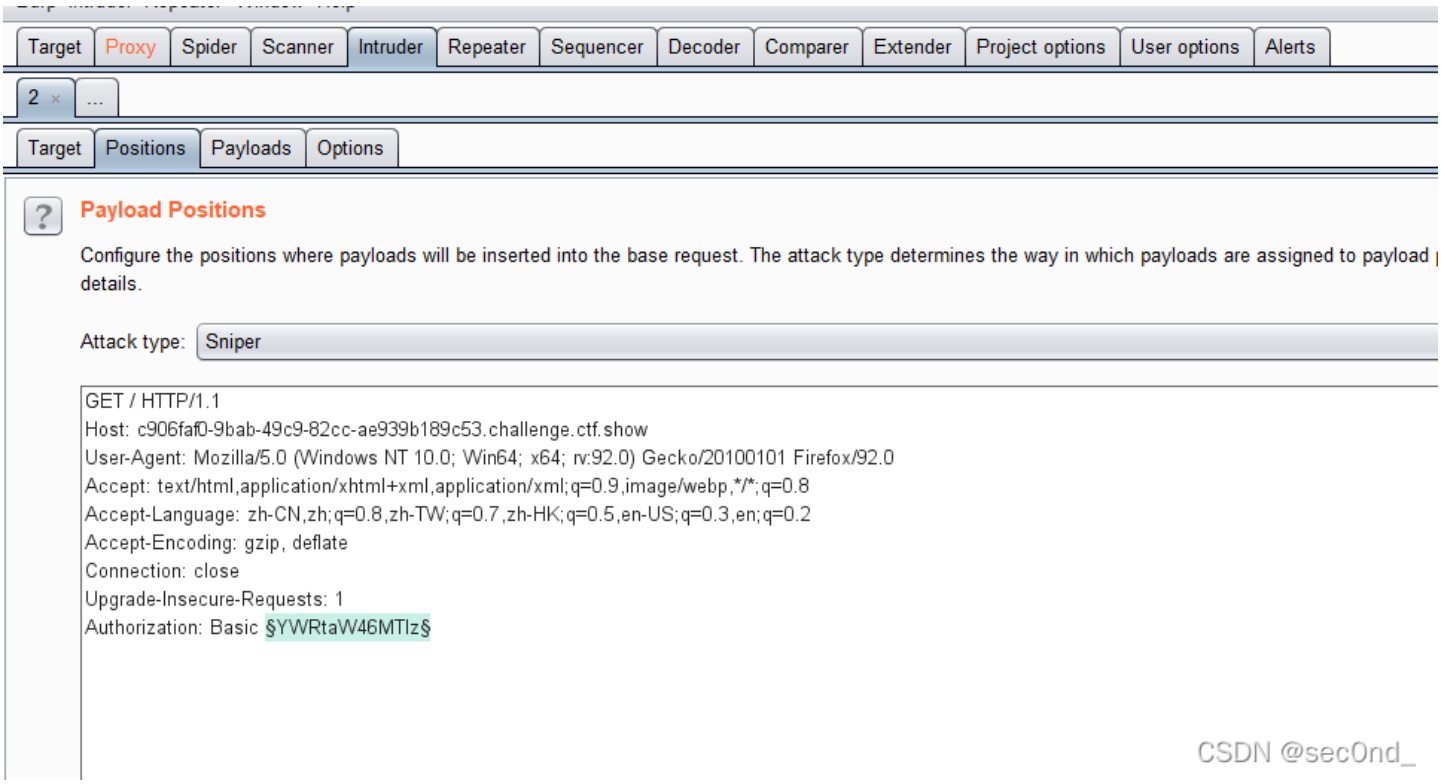
题目是个登录框

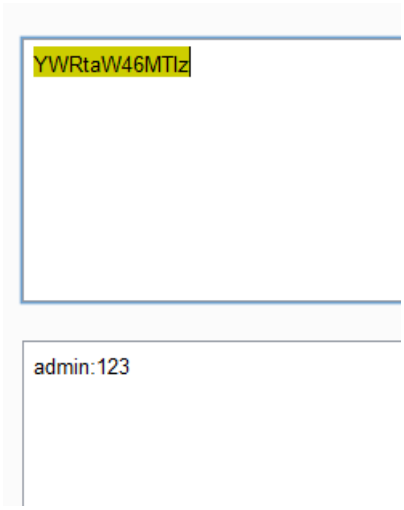
附件里面有一个爆破密码



应该是就用这个爆破了

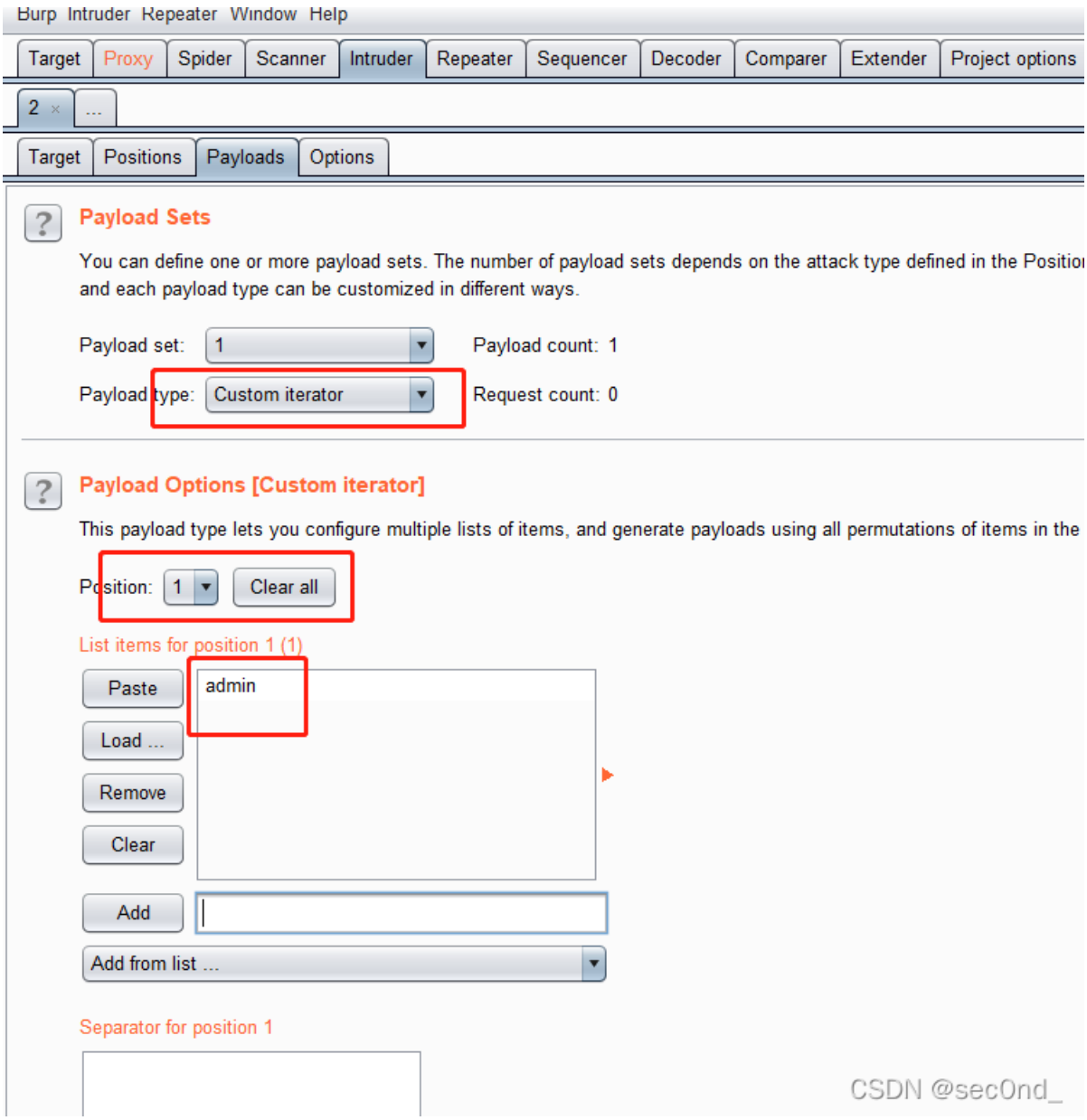
抓个数据包先



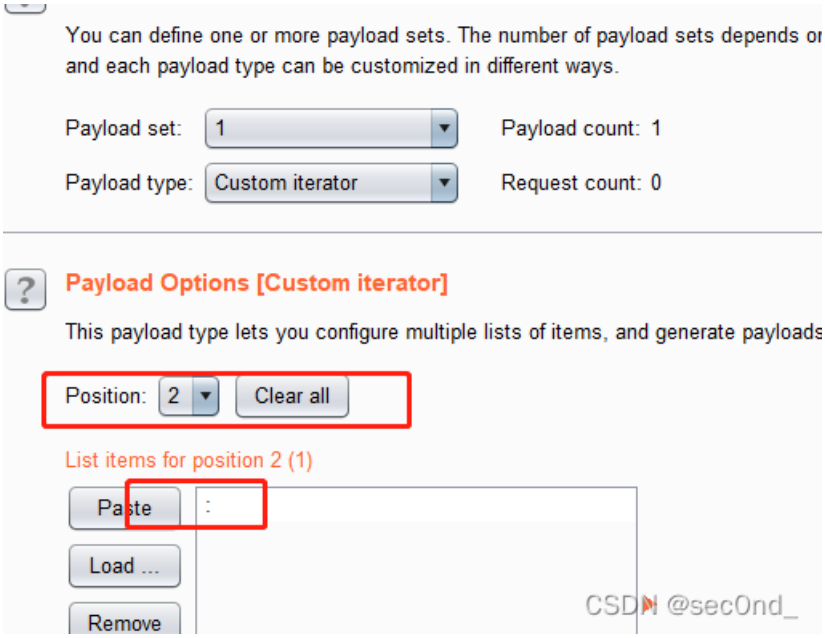


这里的用户名和密码是通过：连接，然后base64加密的

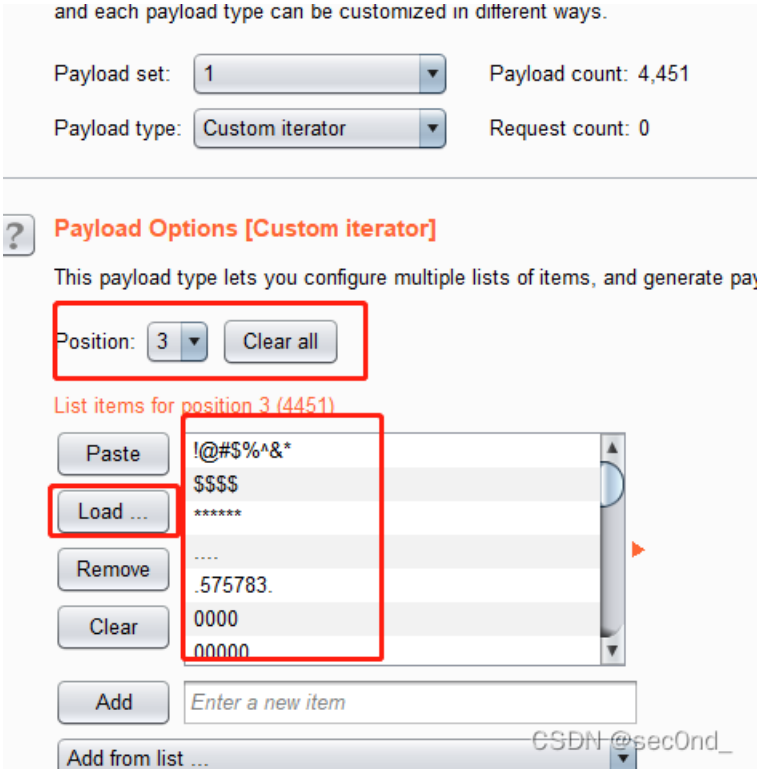
第一个放admin


Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options
2 ...
Target Positions Payloads Options
Payload Sets
You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positio
and each payload type can be customized in different ways.
Payload set: 1 Payload count: 1
Payload type: Custom iterator Request count: 0
Payload Options [Custom iterator]
This payload type lets you configure multiple lists of items, and generate payloads using all permutations of items in the
Position: 1 Clear all
List items for position 1 (1)
Paste
admin
Load ...
Remove
Clear
Add
Add from list ...
Separator for position 1
CSDN @secOnd_

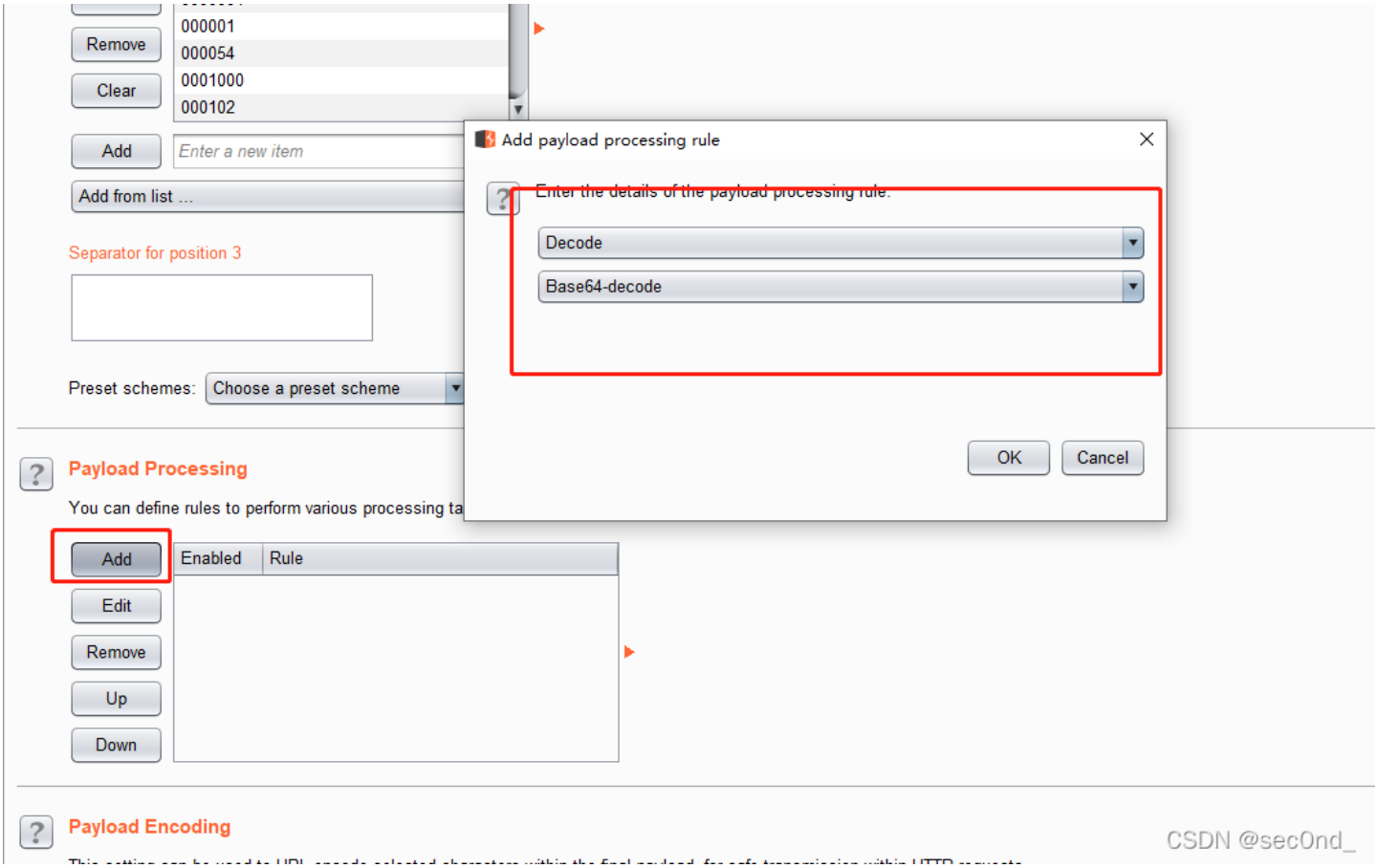
第二个放:

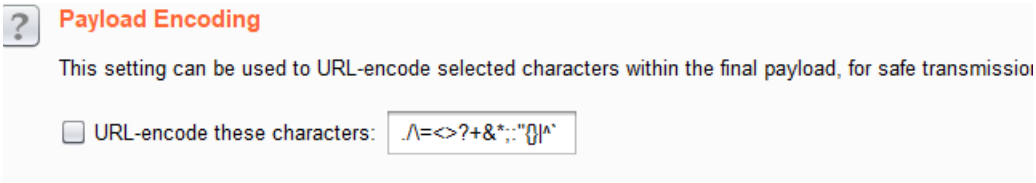


第三个放下载的密码包



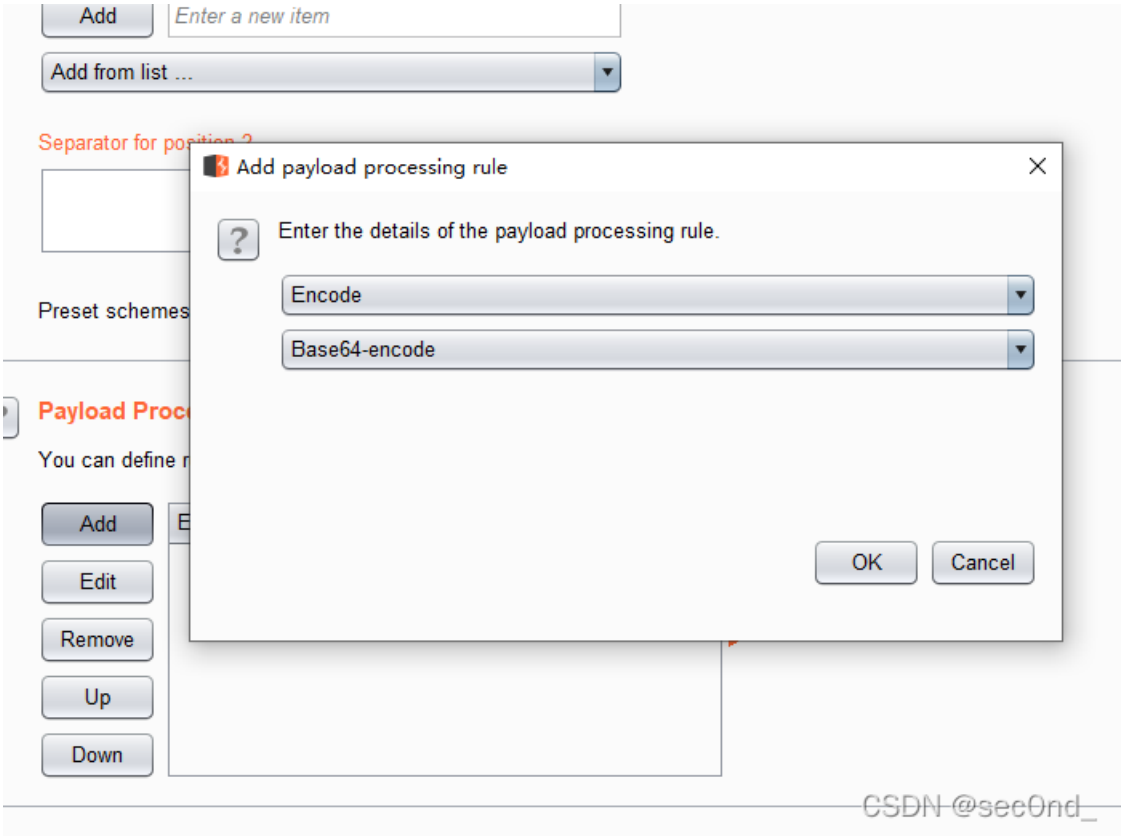
然后还需要进行加密



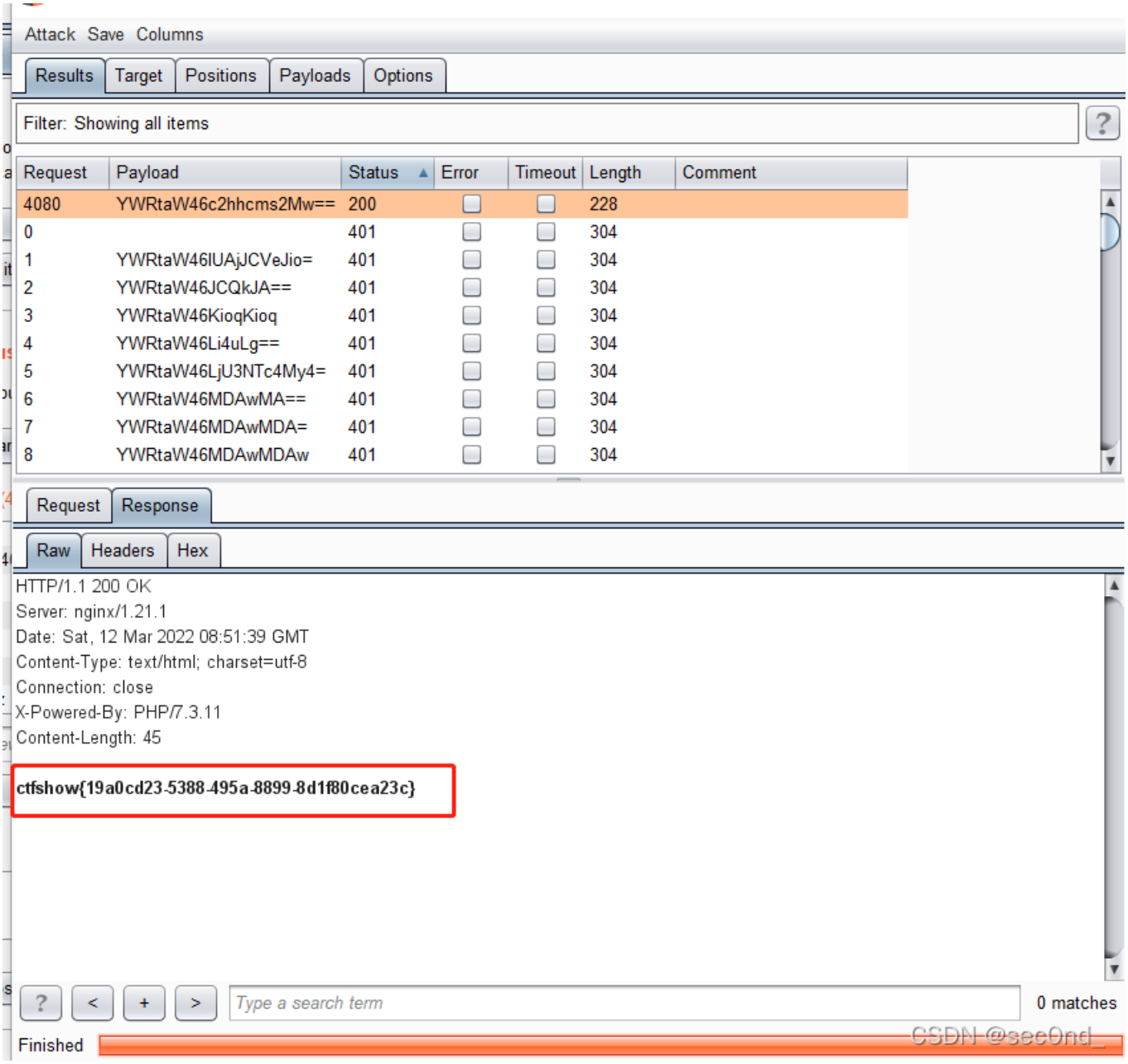


开始爆破，得到成功登录的信息

哦，设置错了……，应该是encode


Add
Enter a new item
Add from list ...
Separator for position 2
Preset schemes
Payload Proc
You can define r
Add
Edit
Remove
Up
Down
Add payload processing rule
Enter the details of the payload processing rule.
Encode
Base64-encode
OK
Cancel
CSDN @secOnd_

……经过了漫长的等待，谁知道竟然把密码放在最后面几百个里面



web22

“域名也可以爆破的，试试爆破这个ctf.show的子域名”

找工具爆破了半个小时，啥也没出来，看了下hint气死

果然这个子域名失效了……

web23

```php
<?php
error_reporting(0);

include('flag.php');
if(isset($_GET['token'])){
    $token = md5($_GET['token']);
    if(substr($token, 1,1)===substr($token, 14,1) && substr($token, 14,1) ===substr($token, 17,1)){
        if((intval(substr($token, 1,1))+intval(substr($token, 14,1))+substr($token, 17,1))/substr($token, 1,1)==
=intval(substr($token, 31,1))){
            echo $flag;
        }
    }
}else{
    highlight_file(__FILE__);

}
?>
```

intval — 获取变量的整数值
substr — 返回字符串的子串

应该是要求token的md5值的，第二位、第十五位和第十八位相等。还限制，三者的和除以第二位的值，等于第三十二位的值。

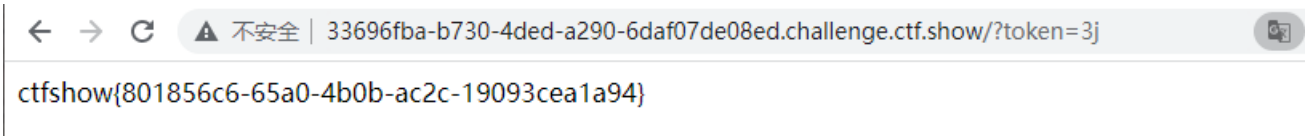
三者的和除以第二位，三者相等，等于任何一位的值，除以任一位的商应为3，即第三十二位的整数值应该是3

需要求一个md5值，当作token传值过去

```python
import hashlib
a = "0123456789qwertyuiopasdfghjklzxcvbnm"
for i in a:
    for j in a:
        b = (str(i) + str(j)).encode("utf-8")
        m = hashlib.md5(b).hexdigest()
        if(m[1:2] == m[14:15] and m[14:15] == m[17:18]):
            if ((int(m[1:2]) + int(m[14:15]) + int(m[17:18])) / int(m[1:2])) == int(m[31:32]):
                print('原字符串为:',b)
                print('加密后字符串为:',m)
```

跑出来的结果为，3j
加密后的值为，f12882fc7cde8e1ba1cadec10e3e9393

满足题目限制



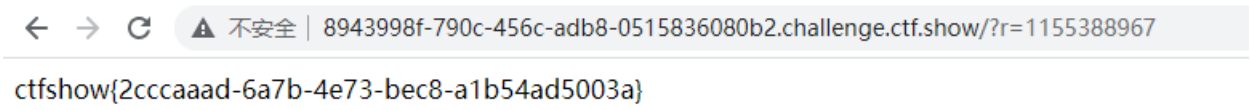
web24

```php
<?php

error_reporting(0);
include("flag.php");
if(isset($_GET['r'])){
    $r = $_GET['r'];
    mt_srand(372619038);
    if(intval($r)===intval(mt_rand())){
        echo $flag;
    }
}else{
    highlight_file(__FILE__);
    echo system('cat /proc/version');
}

?>
```

mt_rand() 使用 Mersenne Twister 算法返回随机整数。

mt_srand() 播种 Mersenne Twister 随机数生成器。

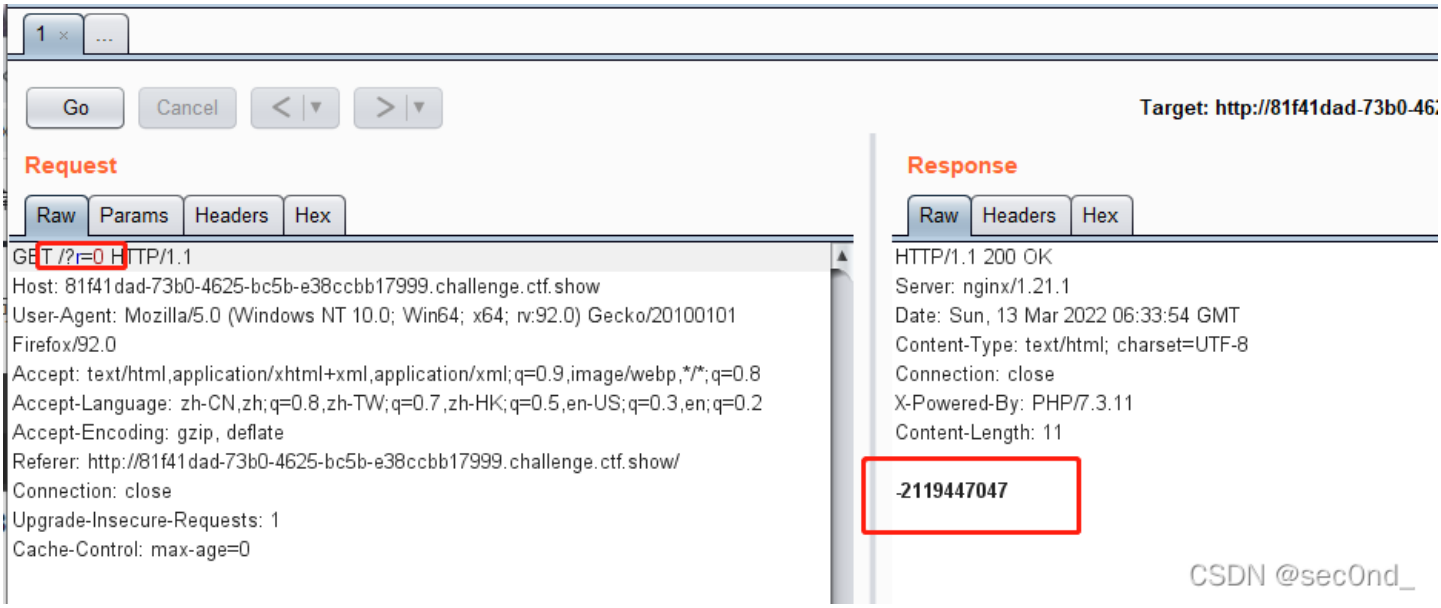
当随机数的种子是个确定值时(如本题),mt_rand()所得到的随机数也是确定的,所以运行后发现mt_rand()=1155388967,传参r=1155388967即可



web25

```php
<?php

error_reporting(0);
include("flag.php");
if(isset($_GET['r'])){
    $r = $_GET['r'];
    mt_srand(hexdec(substr(md5($flag), 0,8)));
    $rand = intval($r)-intval(mt_rand());
    if((!$rand)){
        if($_COOKIE['token']==(mt_rand()+mt_rand())){
            echo $flag;
        }
    }else{
        echo $rand;
    }
}else{
    highlight_file(__FILE__);
    echo system('cat /proc/version');
}
```

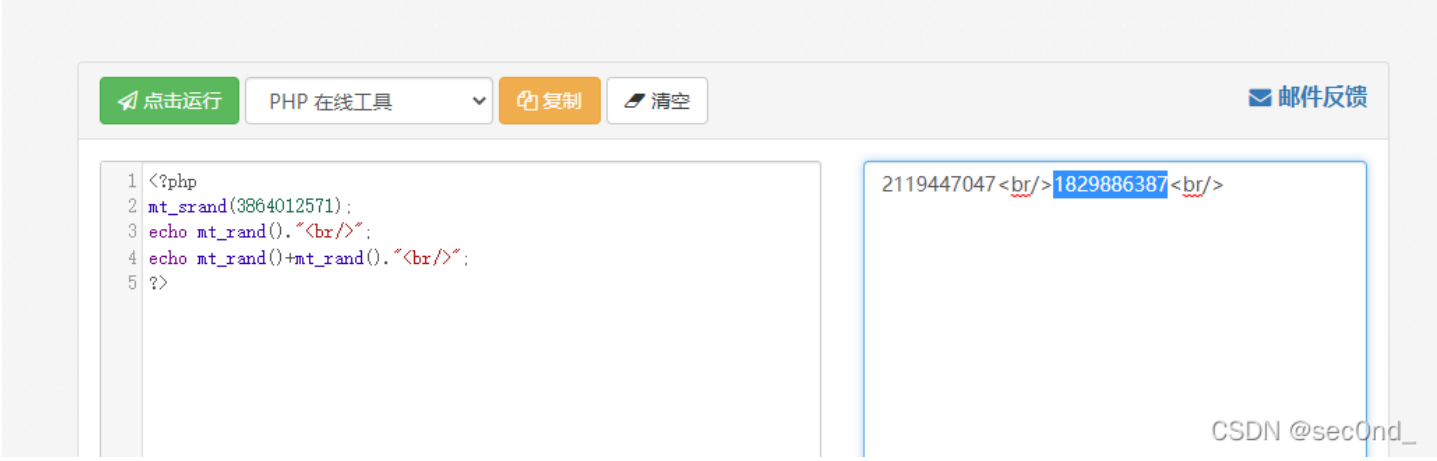
分析代码可以发现，先令r=0，可以得到mt_rand()的随机值 2119447047



得到mt_rand()的值后，需要推算种子seed的值，利用工具

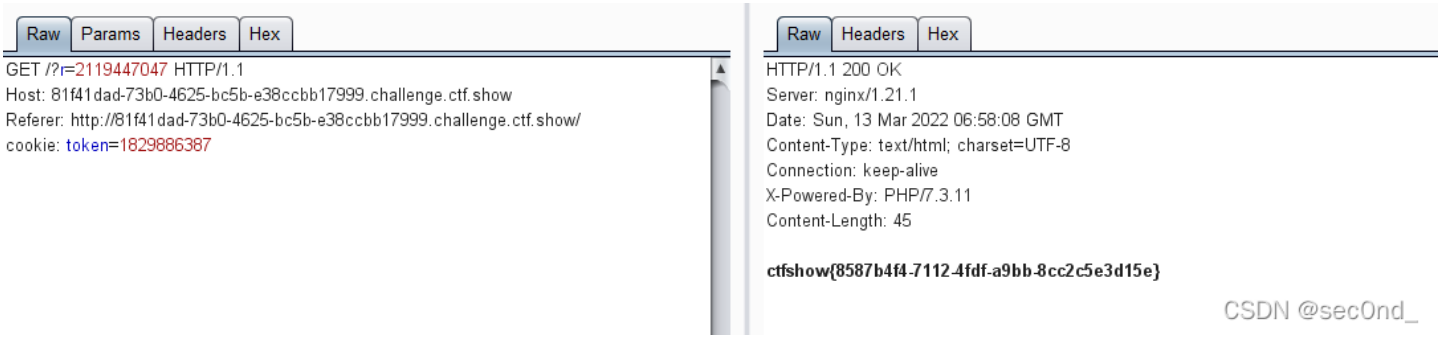
```
└─$ ./php_mt_seed 2119447047
Pattern: EXACT
Version: 3.0.7 to 5.2.0
Found 0, trying 0xfc000000 - 0xffffffff, speed 4450.4 Mseeds/s
Version: 5.2.1+
Found 0, trying 0x2a000000 - 0x2bffffff, speed 35.9 Mseeds/s
seed = 0x2be5cc10 = 736480272 (PHP 5.2.1 to 7.0.x; HHVM)
Found 1, trying 0x8c000000 - 0x8dffffff, speed 35.8 Mseeds/s
seed = 0x8c3f4043 = 2352955459 (PHP 7.1.0+)
Found 2, trying 0xa4000000 - 0xa5ffffff, speed 35.7 Mseeds/s
seed = 0xa4d90a87 = 2765687431 (PHP 7.1.0+)
Found 3, trying 0xe6000000 - 0xe7ffffff, speed 35.7 Mseeds/s
seed = 0xe650271b = 3864012571 (PHP 5.2.1 to 7.0.x; HHVM)
seed = 0xe650271b = 3864012571 (PHP 7.1.0+)
Found 5, trying 0xfe000000 - 0xffffffff, speed 35.6 Mseeds/s
Found 5
```


然后计算mt_rand()的第二、三次的随机值之和。php在线工具



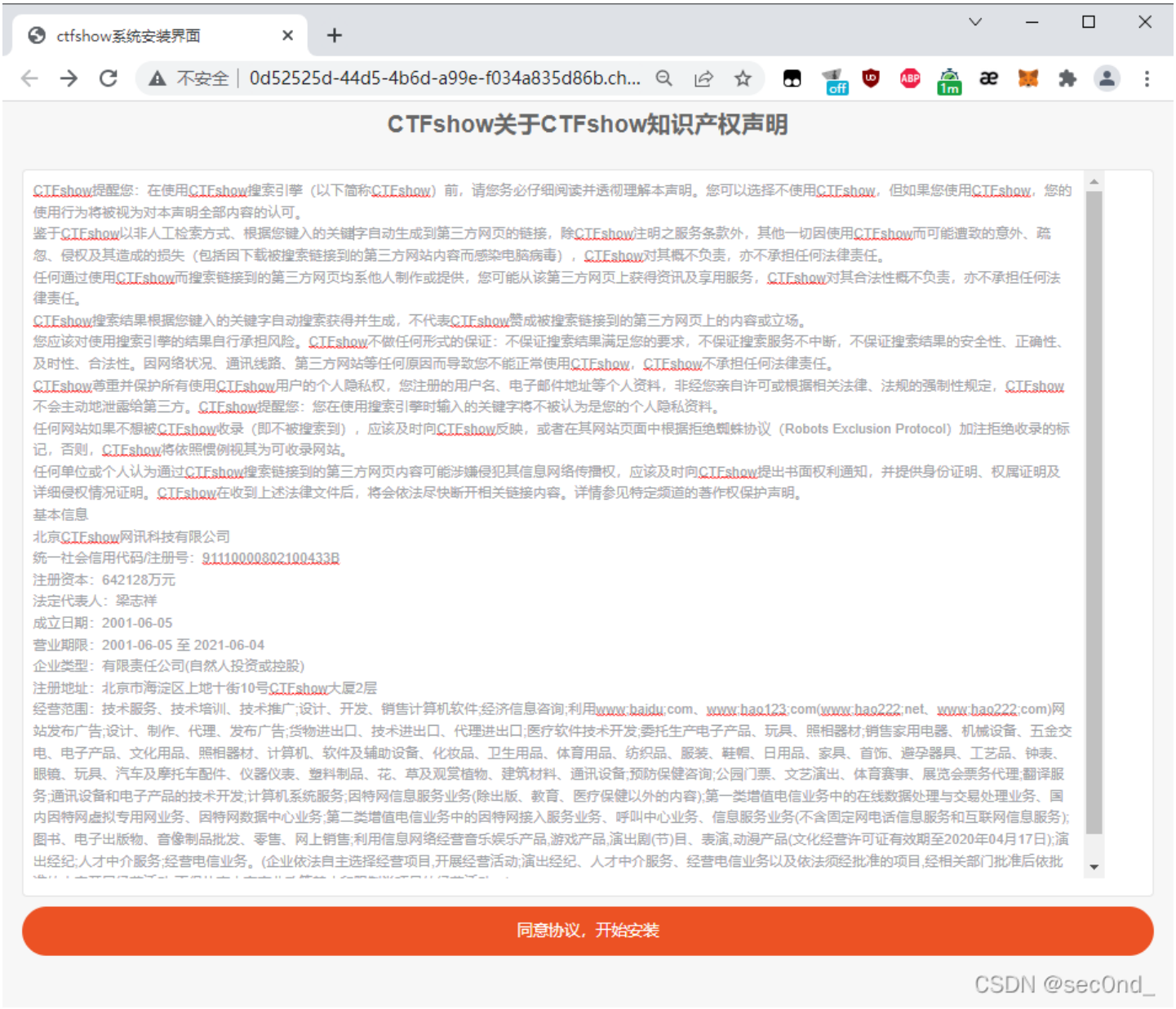
这里的第一个值与r=0的值相等，所有后面就是第二三个随机值的和

令r为mt_rand()的值，令cookie为token=第二、三个随机值的和
（不行就试试后面的seed的值、这是最后一个才有flag的）

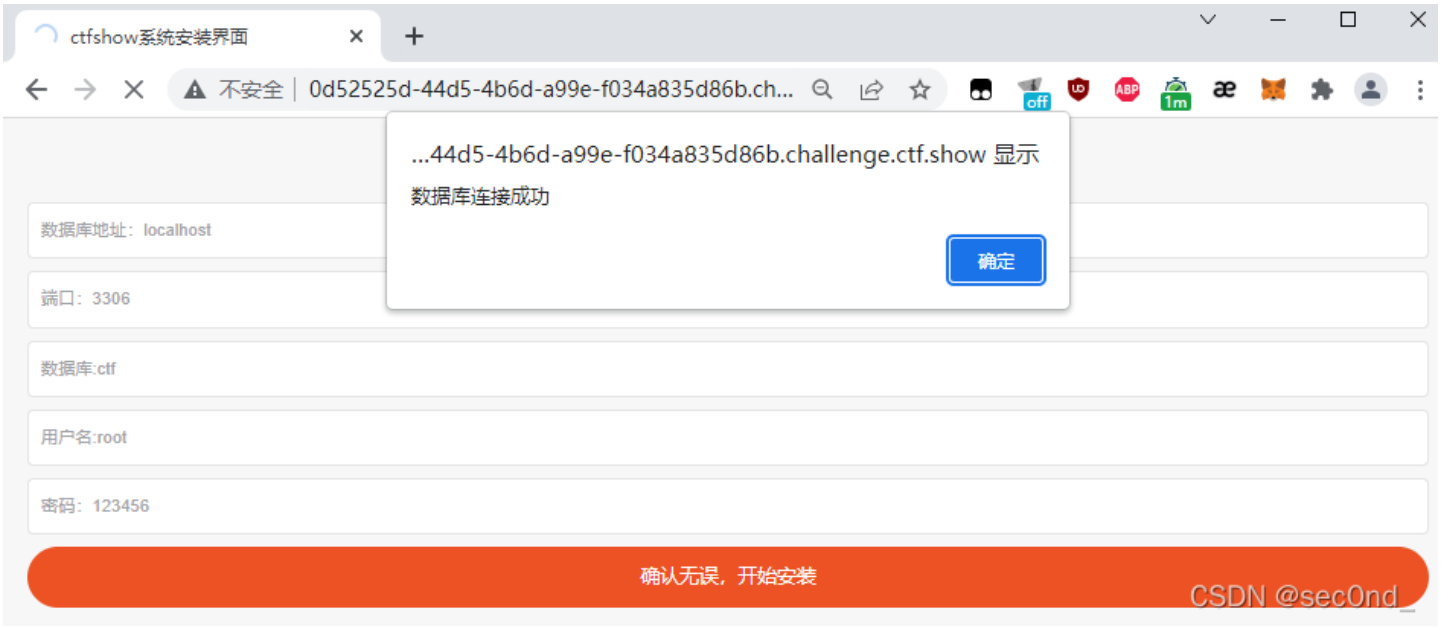


web26

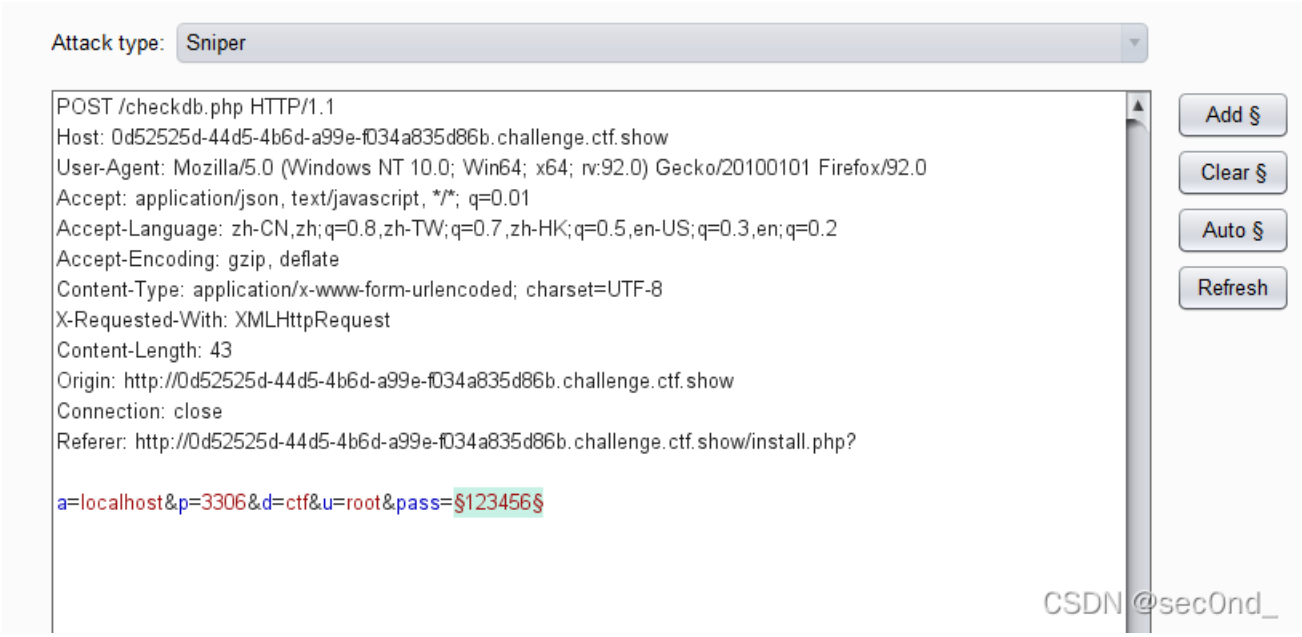
打开后是个安装的界面

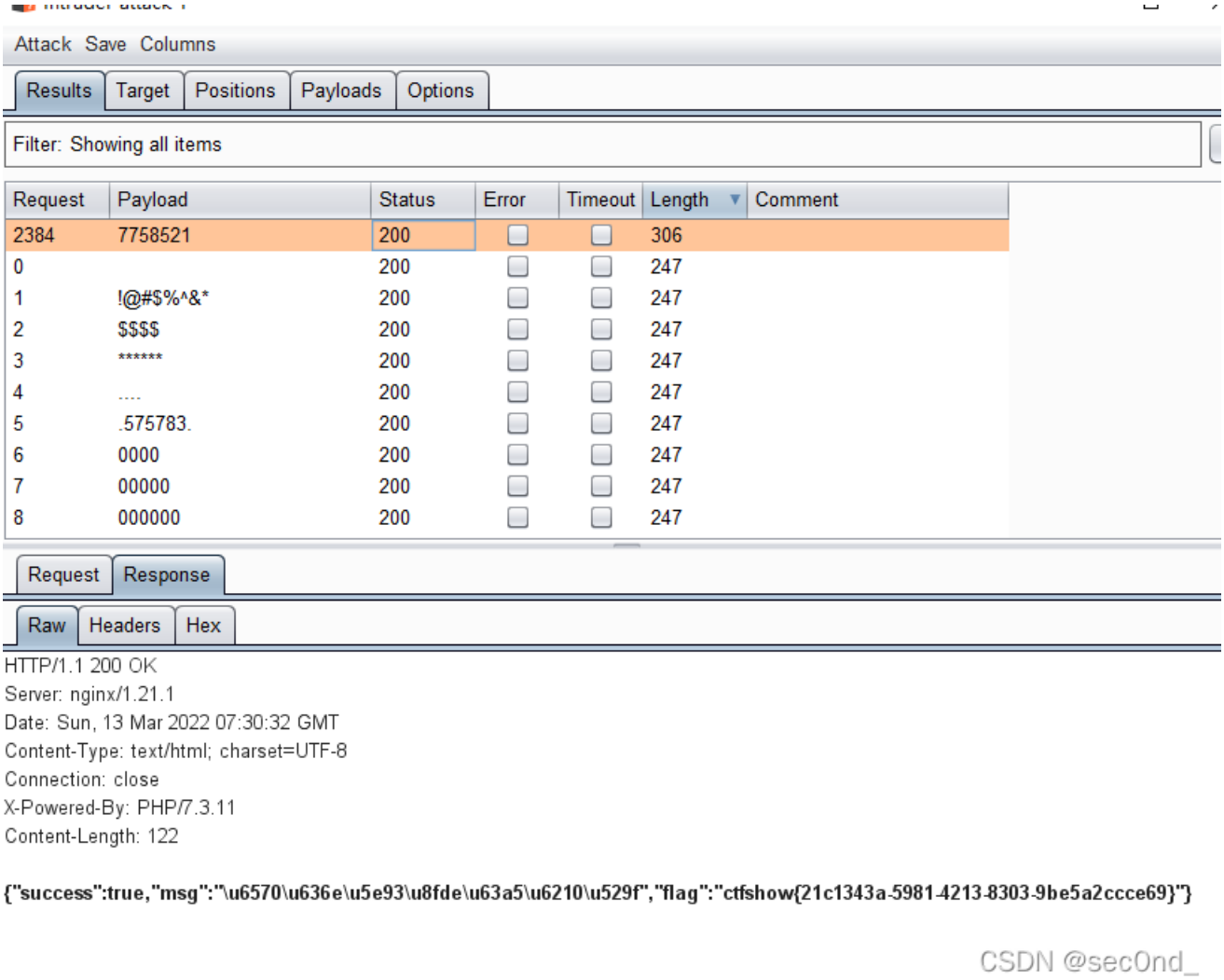

ctfshow系统安装界面
不安全 | 0d52525d-44d5-4b6d-a99e-f034a835d86b.ch...
CTFshow关于CTFshow知识产权声明
CTFshow提醒您：在使用CTFshow搜索引擎（以下简称CTFshow）前，请您务必仔细阅读并透彻理解本声明。您可以选择不使用CTFshow，但如果您使用CTFshow，您的使用行为将被视为对本声明全部内容的认可。
鉴于CTFshow以非人工检索方式、根据您键入的关键字自动生成到第三方网页的链接，除CTFshow注明之服务条款外，其他一切因使用CTFshow而可能遭致的意外、疏忽、侵权及其造成的损失（包括因下载被搜索链接到的第三方网站内容而感染电脑病毒），CTFshow对其概不负责，亦不承担任何法律责任。
任何通过使用CTFshow而搜索链接到的第三方网页均系他人制作或提供，您可能从该第三方网页上获得资讯及享用服务，CTFshow对其合法性概不负责，亦不承担任何法律责任。
CTFshow搜索结果根据您键入的关键字自动搜索获得并生成，不代表CTFshow赞成被搜索链接到的第三方网页上的内容或立场。
您应该对使用搜索引擎的结果自行承担风险。CTFshow不做任何形式的保证：不保证搜索结果满足您的要求，不保证搜索服务不中断，不保证搜索结果的安全性、正确性、及时性、合法性。因网络状况、通讯线路、第三方网站等任何原因而导致您不能正常使用CTFshow，CTFshow不承担任何法律责任。
CTFshow尊重并保护所有使用CTFshow用户的个人隐私权，您注册的用户名、电子邮件地址等个人资料，非经您亲自许可或根据相关法律、法规的强制性规定，CTFshow不会主动地泄露给第三方。CTFshow提醒您：您在使用搜索引擎时输入的关键字将不被认为是您的个人隐私资料。
任何网站如果不想被CTFshow收录（即不被搜索到），应该及时向CTFshow反映，或者在其网站页面中根据拒绝蜘蛛协议（Robots Exclusion Protocol）加注拒绝收录的标记，否则，CTFshow将依照惯例视其为可收录网站。
任何单位或个人认为通过CTFshow搜索链接到的第三方网页内容可能涉嫌侵犯其信息网络传播权，应该及时向CTFshow提出书面权利通知，并提供身份证明、权属证明及详细侵权情况证明。CTFshow在收到上述法律文件后，将会依法尽快断开相关链接内容。详情参见特定频道的著作权保护声明。
基本信息
北京CTFshow网讯科技有限公司
统一社会信用代码/注册号：91110000802100433B
注册资本：642128万元
法定代表人：梁志祥
成立日期：2001-06-05
营业期限：2001-06-05 至 2021-06-04
企业类型：有限责任公司(自然人投资或控股)
注册地址：北京市海淀区上地十街10号CTFshow大厦2层
经营范围：技术服务、技术培训、技术推广;设计、开发、销售计算机软件;经济信息咨询;利用www.baidu.com、www.hao123.com(www.hao222.net、www.hao222.com)网站发布广告;设计、制作、代理、发布广告;货物进出口、技术进出口、代理进出口;医疗软件技术开发;委托生产电子产品、玩具、照相器材;销售家用电器、机械设备、五金交电、电子产品、文化用品、照相器材、计算机、软件及辅助设备、化妆品、卫生用品、体育用品、纺织品、服装、鞋帽、日用品、家具、首饰、避孕器具、工艺品、钟表、眼镜、玩具、汽车及摩托车配件、仪器仪表、塑料制品、花、草及观赏植物、建筑材料、通讯设备;预防保健咨询;公园门票、文艺演出、体育赛事、展览会票务代理;翻译服务;通讯设备和电子产品的技术开发;计算机系统服务;因特网信息服务业务(除出版、教育、医疗保健以外的内容);第一类增值电信业务中的在线数据处理与交易处理业务、国内因特网虚拟专用网业务、因特网数据中心业务;第二类增值电信业务中的因特网接入服务业务、呼叫中心业务、信息服务业务(不含固定网电话信息服务和互联网信息服务);图书、电子出版物、音像制品批发、零售、网上销售;利用信息网络经营音乐娱乐产品,游戏产品,演出剧(节)目、表演,动漫产品(文化经营许可证有效期至2020年04月17日);演出经纪;人才中介服务;经营电信业务。(企业依法自主选择经营项目,开展经营活动;演出经纪、人才中介服务、经营电信业务以及依法须经批准的项目,经相关部门批准后依批
同意协议，开始安装
CSDN @secOnd_


ctfshow系统安装界面
不安全 | 0d52525d-44d5-4b6d-a99e-f034a835d86b.ch...
CTFshow flag管理系统安装
数据库地址：localhost
端口：3306
数据库:ctf
用户名:root
密码：123456
确认无误，开始安装
CSDN @sec0nd_


ctfshow系统安装界面
不安全 | 0d52525d-44d5-4b6d-a99e-f034a835d86b.ch...
...44d5-4b6d-a99e-f034a835d86b.challenge.ctf.show 显示
数据库连接成功
确定
数据库地址：localhost
端口：3306
数据库:ctf
用户名:root
密码：123456
确认无误，开始安装
CSDN @sec0nd_

然后就没有了，根据题目说可以爆破，那有可能是爆破安装的这个密码，用到web21题给的字典库





等好久，终于等到了个不同length的响应

这个题还有一种非预期解 https://oatmeal.vip/writeup/ctfshow/ctfshow-web/

web27

是个教务系统登录，有录取名单和学籍查询

录取名单：

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	元羿谆	PWN	451023********3419	生源地贷款
5	祁落兴	CRYPTO	410927********5570	

学籍查询：

返回登陆

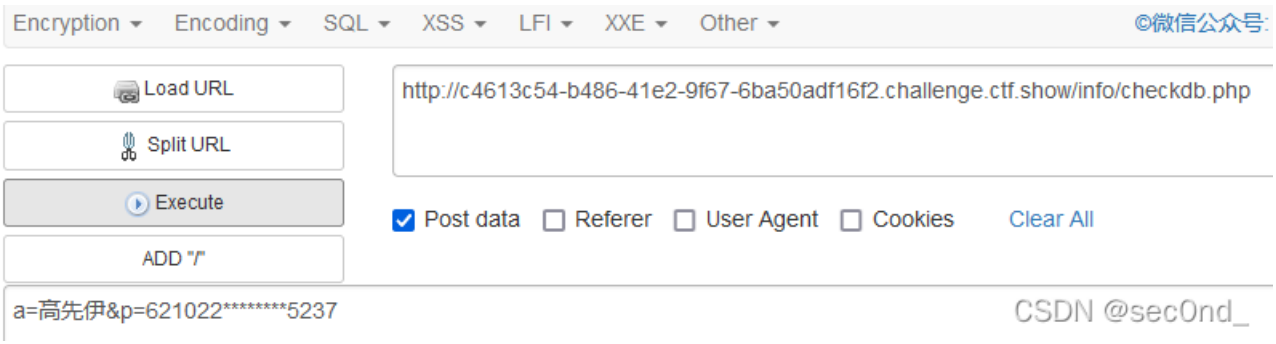
猜测应该是用录取名单的姓名+身份证号登录，查询录取信息
在登陆查询页面查看源代码

```
<script>

    function check(){
        $.ajax({
        url:'checkdb.php',
        type: 'POST',
        dataType:'json',
        data:{
            'a':$('#a').val(),
            'p':$('#p').val()
        },
        success:function(data){
            alert(data['msg']);
        },
        error:function(data){
            alert(data['msg']);
        }
```



```
    });
```

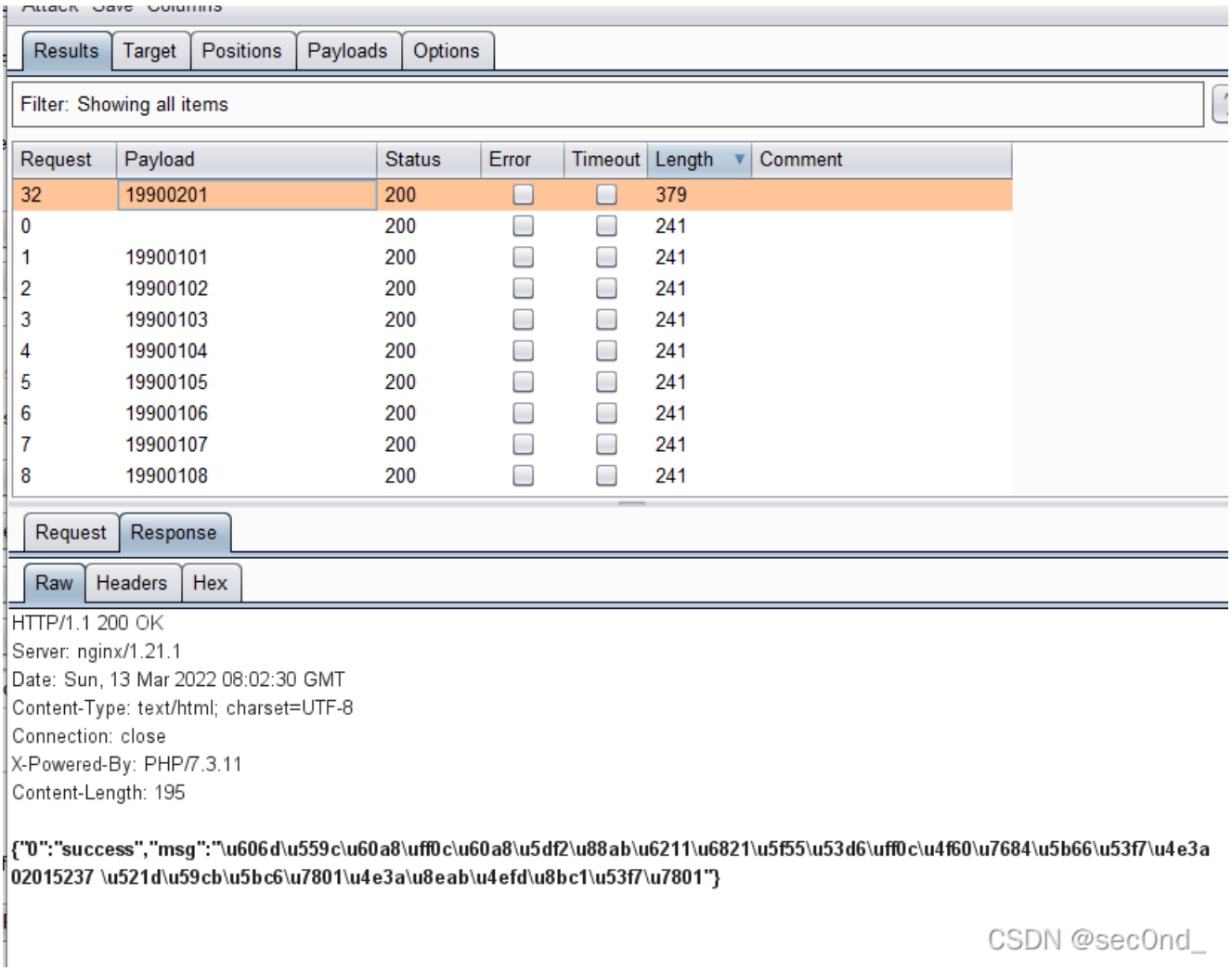
hackbar工具POST提交



4-b486-41e2-9f67-6ba50adf16f2.challenge.ctf.show/info/checkdb.php
ıests: 1

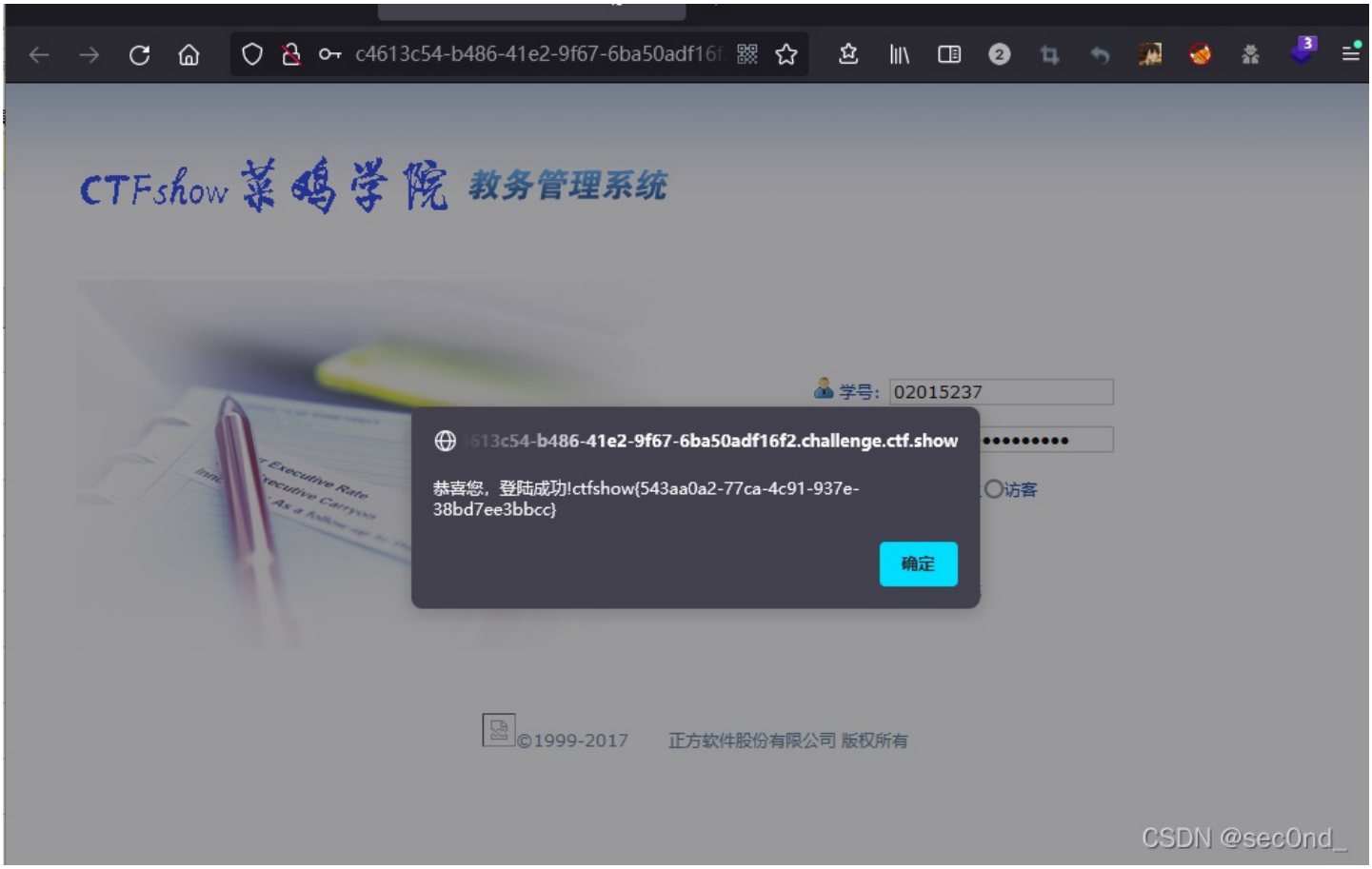
%85%88%E4%BC%8A&p=621022§********§6237

设置好日期范围，开始爆破

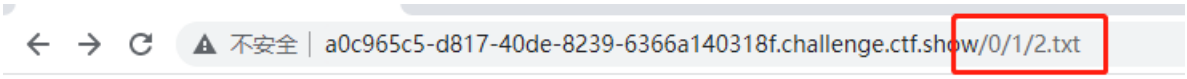


成功爆破，返回的是unicode编码后的，解码一下

得到学号和密码，去刚开始的教务系统登录

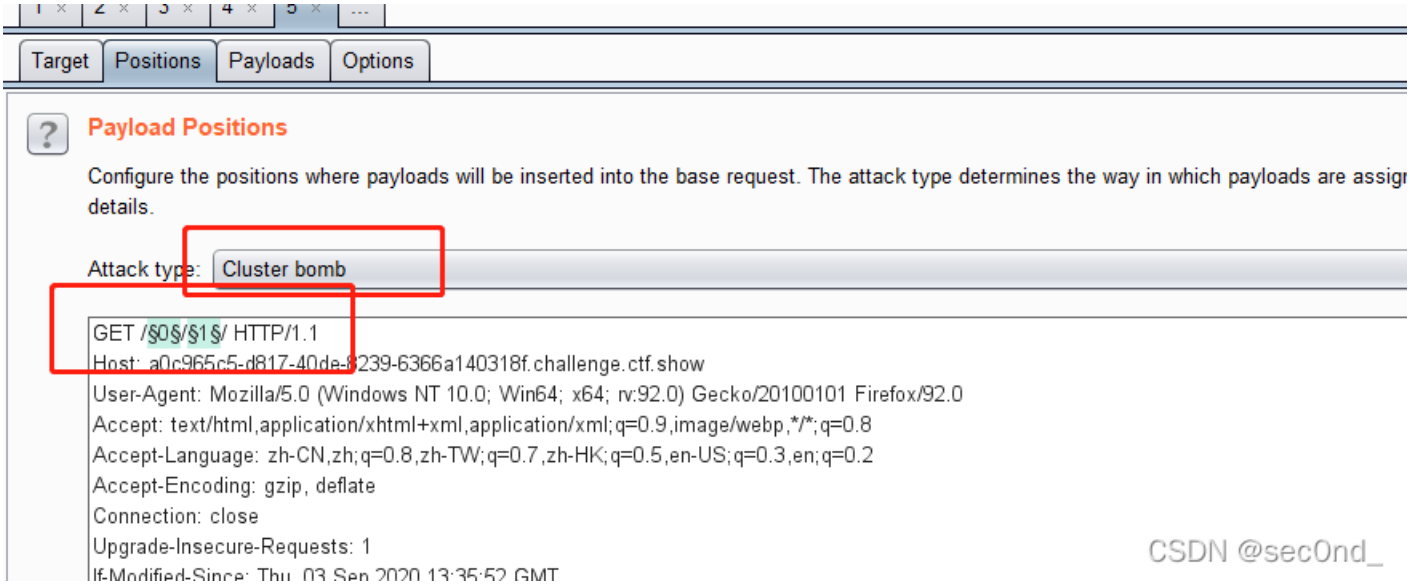


web28

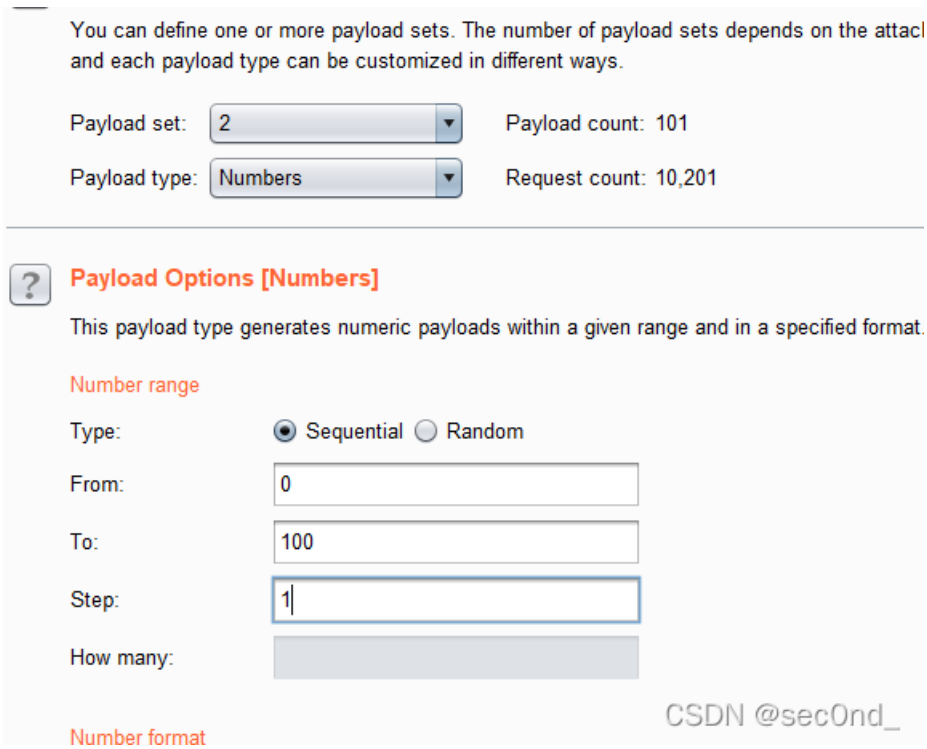



```
web28:where is flag?
```

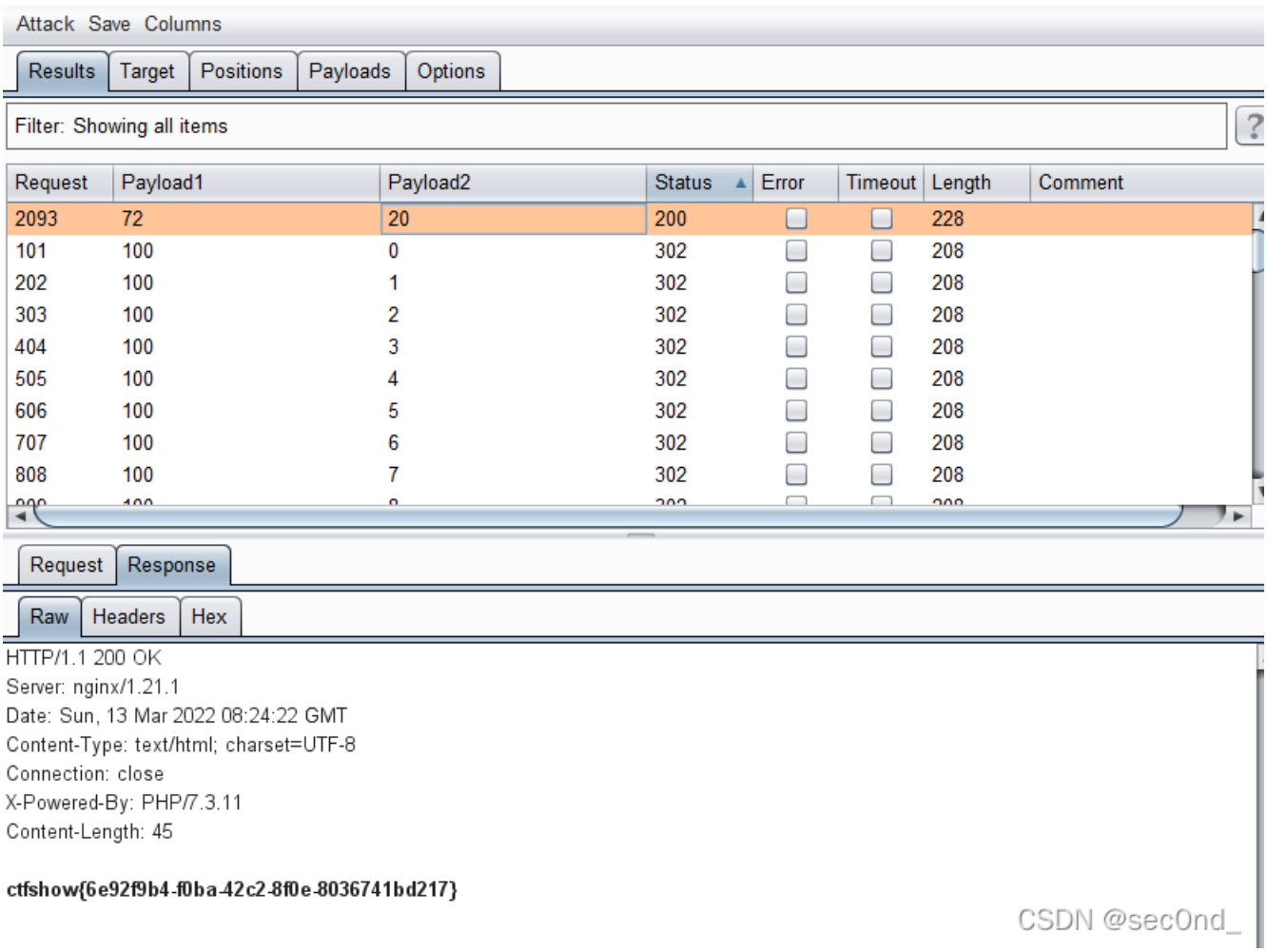
看到这地址之后，应该是去爆破目录



payload1和2一样设置，从0到100



开始爆破



终于在两千多次后成功了