




# 攻防世界答题

原创

时~  于 2021-11-12 22:05:27 发布  2965  收藏 1

分类专栏: [笔记](#) 文章标签: [php](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: [https://blog.csdn.net/m0\\_62782839/article/details/121216267](https://blog.csdn.net/m0_62782839/article/details/121216267)

版权



[笔记](#) 专栏收录该内容

7 篇文章 0 订阅

订阅专栏

## 第一题

使用ctrl+u或者使用F12+fn键(笔记本)

## 第二题

roots协议即爬虫协议, 可以使用roots.txt查看

roots作用即告知服务器什么可以看, 什么不可以看(通俗来讲)

## 第三题

备份文件的查看方式

即第三题的考察方式: 后面+index.php.bak

## 第四题

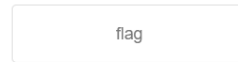
先查找cookie

发现需要查询cookie.php

弹出

## 第五题

## 一个不能按的按钮



cyberpeace{3d76813a34db4baf9e70efe8fda5c09f}

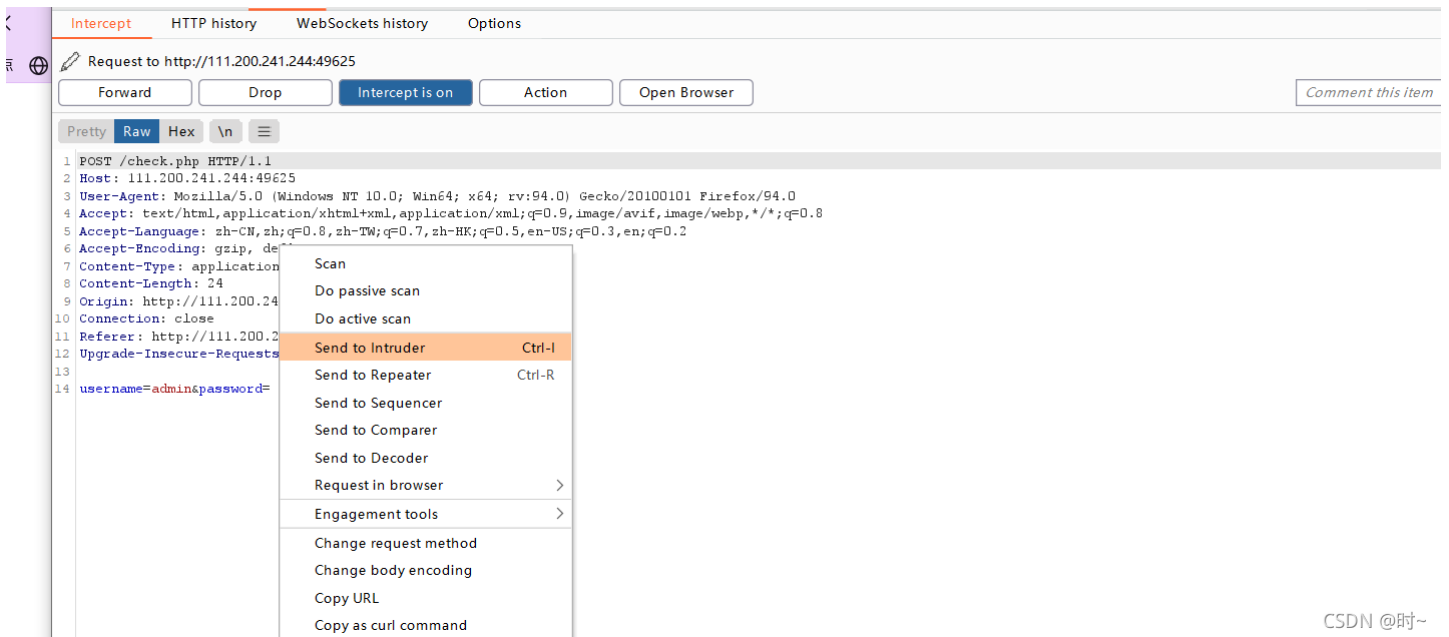


发现存在一个disabled input，将其更改后便能够点击flag了

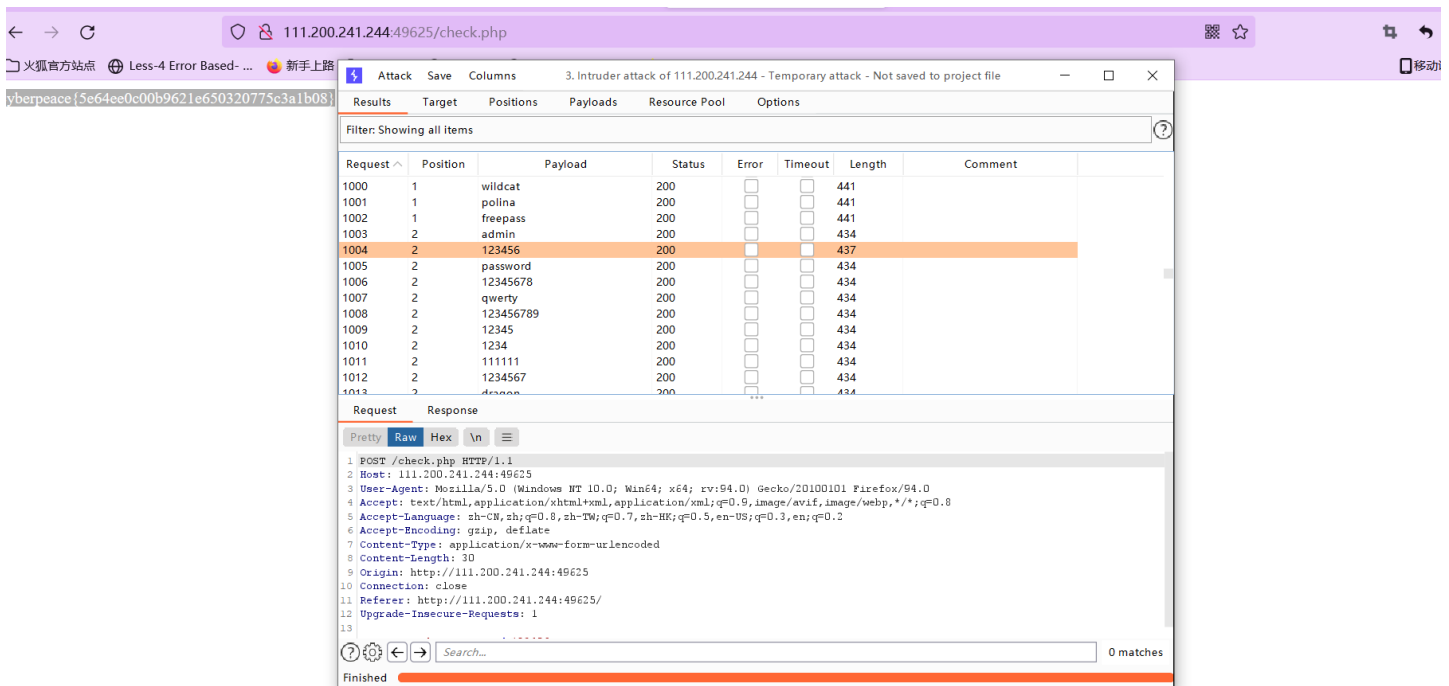
## 第六题

## 进行密码爆破

打开界面，随便输入。发现提示为请输入“admin”的用户名。接着进行密码爆破，需要使用到密码词典。先进行抓包，接着发送到intruder模块，按load加载键添加密码词典，然后爆破，根据长度进行判断。



CSDN @时~



CSDN @时~

## ## 第七题

## 第九题

大狐官方站点 LESS-4 Error Based-... 新手上路 常用网址 京东商城 WHERE IS THE FLAG 大狐王典

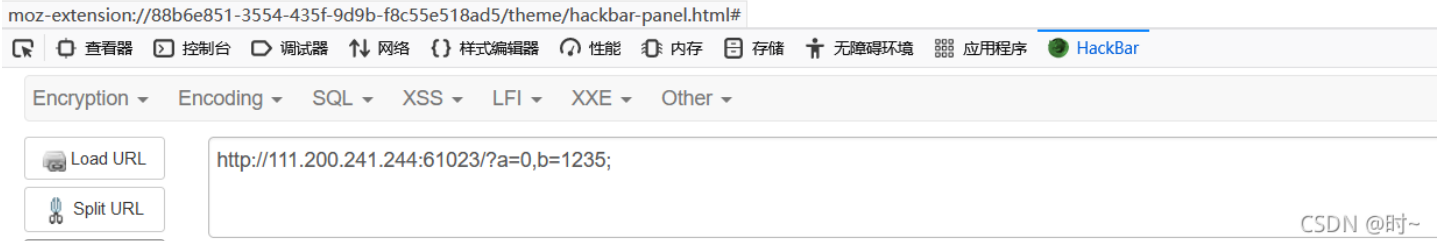
```
<?php
show_source(__FILE__);
include("config.php");
$a=$_GET['a'];
$b=$_GET['b'];
if($a==0 and $a){
    // ...
}
```

```

        echo $flag1;
    }
    if(is_numeric($b)){
        exit();
    }
    if($b>1234){
        echo $flag2;
    }
}
?>

```

Cyberpeace{647E37C7627CC3E401



由题目可知道为get传参方式，可以先得到flag1前半部分，在得到flag2后半部分。前半部分可以根据语句如果a=0，输出flag1得到

```

<?php
show_source(__FILE__);
include("config.php");
$a=@$_GET['a'];
$b=@$_GET['b'];
if($a==0 and $a){
    echo $flag1;
}
if(is_numeric($b)){
    exit();
}
if($b>1234){
    echo $flag2;
}
?>

```

Cyberpeace{647E37C7627CC3E401



第二个函数is\_numeric，如果检测到为数字和数字字符串就执行exit()函数，跳出脚本。可以直接不关注此，输出一个大于1234的b的值即可得到flag2

```

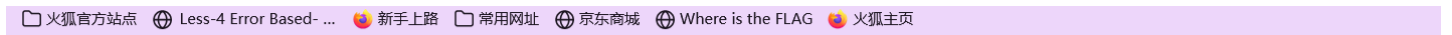
if($b>1234){
    echo $flag2;
}
?>

```

9EC69324F66C7C}



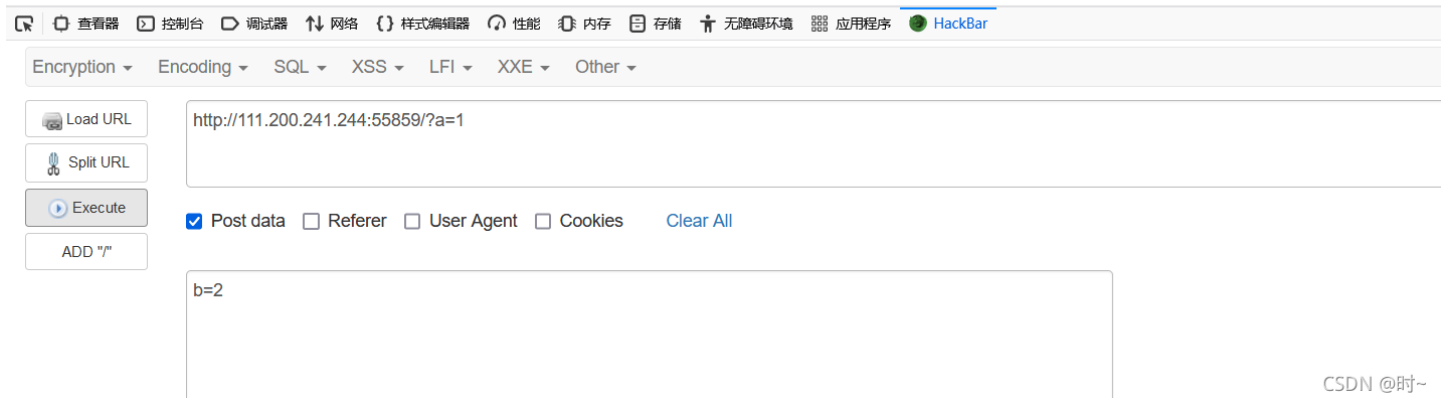
## 第八题



请用GET方式提交一个名为a,值为1的变量

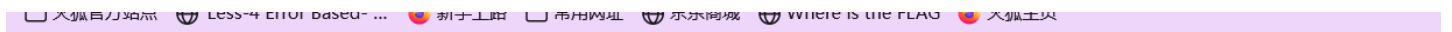
请再以POST方式随便提交一个名为b,值为2的变量

cyberpeace{a8c52b4d2d69d4d4641d4874010cd392}



上方get, 下方post.

## 第九题



```
<?php
show_source(__FILE__);
include("config.php");
$a=@$_GET['a'];
$b=@$_GET['b'];
if($a==0 and $a){
    echo $flag1;
}
if(is_numeric($b)){
    exit();
}
if($b>1234){
    echo $flag2;
}
?>
```

Cyberpeace{647E37C7627CC3E401}



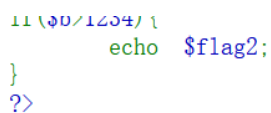
由题目可知为get传参方式，可以先得到flag1前半部分，在得到flag2后半部分。前半部分可以根据语句如果a=0，输出flag1得到



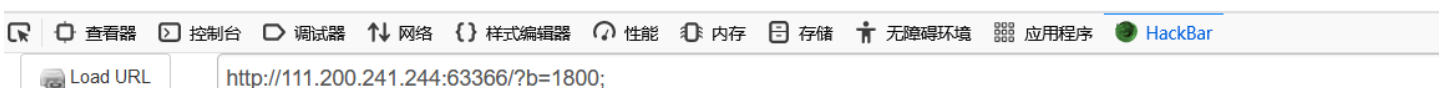
Cyberpeace{647E37C7627CC3E401





第二个函数is\_numeric，如果检测到为数字和数字字符串就执行exit()函数，跳出脚本。可以直接不关注此，输出一个大于1234的b的值即可得到flag2



9EC69324F66C7C}



 Split URL

 Execute

Post data

Referer

User Agent

Cookies

[Clear All](#)

CSDN @时~

## 第九题