攻防世界 web2 writeup

原创

tothemoon_2019 于 2020-03-04 10:34:46 发布 124 收藏

分类专栏： 攻防世界 write up web2 文章标签： php 字符串

本文链接：https://blog.csdn.net/qq_43478096/article/details/104647731

http://39.96.86.88/2020/04/03/攻防世界-web2-writeup/

```php
<?php
$miwen="a1zLbgQsCESEIqRLwuQAyMwLyq2L5VwBxqGA3RQAyumZ0tmMvSGM2ZwB4tws";

function  encode($str){
        $_o=strrev($str);
        //  echo  $_o;

        for($_0=0;$_0<strlen($_o);$_0++){

                $_c=substr($_o,$_0,1);
                $__=ord($_c)+1;
                $_c=chr($__);
                $_=$_.$_c;
        }
        return  str_rot13(strrev(base64_encode($_)));
}

highlight_file(__FILE__);
/*
      逆向加密算法，解密$miwen就是flag
*/
?>
```


打开页面就是源码，结合注释里的提示，这是一道代码审计的题。根据给出的加密方法将$miwen还原出来。

先解释一下里面的几个函数：

```
strrev($str);        //反转str字符串
substr($_o,$_0,1); //返回的字符串  取头不取尾 在这里是的作用是从头到尾一个一个取出字符
ord($_c)+1;    //返回字符串的ascii然后加1
chr($__);     //将上面加1后的ascii码转为字符
return str_rot13(strrev(base64_encode($_)));//先base64解码 -> 反转字符串 -> 只把字母向前移动13位
```

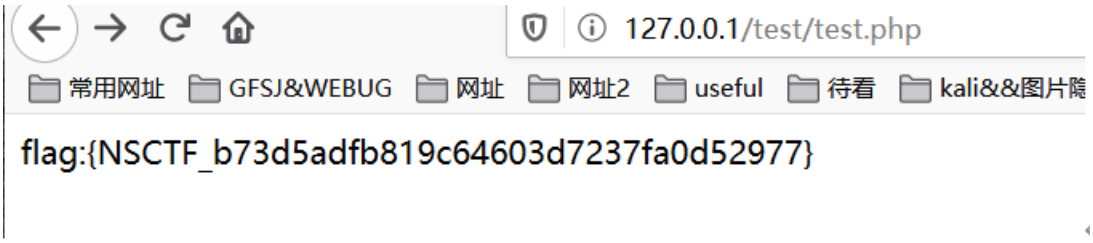
这里需要注意的是：
1.for循环的作用就是将字符串字符从头到尾依次取出，然后将它变为ascii码加1的字符，这样就完成了加密的主要部分。
2.因为字母有26个所以再次调用str_rot13()即可将字母还原。

上解密脚本

```
<?php
 $miwen="a1zLbgQsCESEIqRLwuQAyMwLyq2L5VwBxqGA3RQAyumZ0tmMvSGM2ZwB4tws";
 function decode($str)
 { //因为字母有26个所以再次调用str_rot13()即可将字母还原为之前的
     $_o = base64_decode(strrev(str_rot13($str)));
     echo $str_1;
     for($_0=0;$_0<strlen($_o);$_0++){
      //只需要将字符串里的每个字符变为ascii码-1的字符即可
         $_c=substr($_o,$_0,1);//返回的字符串  取头不取尾 这里是从头一个一个取到尾
         $__=ord($_c)-1;//返回ascii+1
         $_c=chr($__);//和ord相反
         $_=$_.$_c;   //连接
             echo strrev($_);

     }
 }

 decode($miwen);
 highlight_file(__FILE__);
 ?>
```



flag:
{NSCTF_b73d5adfb819c64603d7237fa0d52977}