PHP_encrypt_1(ISCCCTF) Writeup

原创

丶没胡子的猫 于 2020-10-31 20:36:09 发布 109 收藏

分类专栏： CTF 文章标签： 安全

本文链接：https://blog.csdn.net/weixin_41924764/article/details/109404236

https://ctf.bugku.com/

加密后字符串：

fR4aHWwuFCYYVydFRxMqHhhCKBseH1dbFygrRxlWJ1UYFhotFjA=

题目下载地址：

https://ctf.bugku.com/files/6b8e8eb682d757d851cd5dcdca349668/PHP_encrypt_1.zip

---

下载zip后，获得以下代码并进行分析：

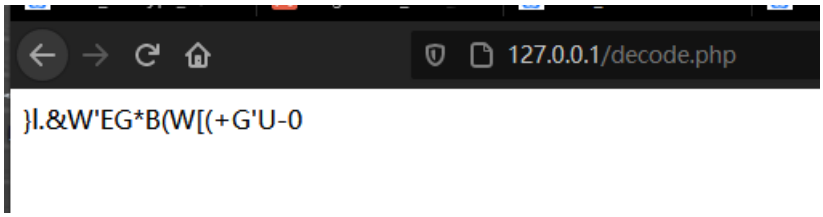
```php
<?php
function encrypt($data,$key)
{
    $key = md5('ISCC');
    $x = 0;
    $len = strlen($data);
    $klen = strlen($key);
    for ($i=0; $i < $len; $i++) {
        if ($x == $klen)
        {
            $x = 0;
        }
        $char .= $key[$x];
        $x+=1;
    }
    for ($i=0; $i < $len; $i++) {
        $str .= chr((ord($data[$i]) + ord($char[$i])) % 128);
    }
    return base64_encode($str);
}
?>
```

脚本逆向分析：

1.从后面往前解析，$str经过了一次base64加密。我们先用decode函数进行解密：

```php
<?php
echo base64_decode("fR4aHWwuFCYYVydFRxMqHhhCKBseH1dbFygrRxIWJ1UYFhotFjA=");
?>
```

得出base64解密后的字符串：



2.`$str`变量生成前，经过了一次for循环：

```php
for ($i=0; $i < $len; $i++) {
        $str .= chr((ord($data[$i]) + ord($char[$i])) % 128);
    }
```

for循环中几个函数与变量：

1. $len =$data字符串的长度（$data的字符串长度就是base64解密后的字符串长度，与原先flag的长度一样，并没有改变。）
2. $char
3. chr()：将一个asill码转换成字符
4. ord():将字符转换成ascii码
5. % : 求余
6. $data：为原先flag

将原先flag的字符串与变量char对应ascii码相加，余128后的ascii码转换成字符，拼接在$str上。

加密公式解析：

（本人数学较差... 正在努力补数学）

将 `ord($data[$i])` 看成 `a`
将 `ord($char[$i]` 看成 `b`
将 `$str` 看成 `c`

```
(a+b)%128=c
```

解密公式：

```
如果 b+c<=128
解：  a=128+c-b

如果 b+c>128
解：如果(c-b)大于128
 a=c-b-128
 如果不大于128
 a=c-b
```

3.分析好for循环中的加密方法后，我们需要知道$char变量内容，继续往上一个for循环分析。

```
$key = md5('ISCC');
$x = 0;
$len = strlen($data);
$klen = strlen($key);
for ($i=0; $i < $len; $i++) {
   if ($x == $klen)
   {
       $x = 0;
    }
    $char .= $key[$x];
    $x+=1;
}
```

函数：

- md5()：将字符串进行MD5加密
- strlen()：获取字符串长度

代码分析：

1. 将ISCC进行MD5加密

```
$key = md5('ISCC');
```

2. 计算$data的字符串长度赋值于$len，计算$key的字符串长度赋值于$klen，
   len变量与前面我们base64解密后的字符串长度一样
   klen变量等于32（因为md5加密后长度为32位）

```
$len = strlen($data);
$klen = strlen($key);
```

3. for循环执行算出$char的值

```
for ($i=0; $i < $len; $i++) { #for循环$len次
   if ($x == $klen)#如果$x等于32,那么$x将等于0
   {
       $x = 0;
    }
    $char .= $key[$x];#char：  如果$data长度为10，那么会将$key的前10位赋值给$char
    $x+=1;
}
```

分析好代码后$char的值后，就可以利用前面`余求值`的解密公式解出data(flag)的值了。

```
<?php
$str= base64_decode("fR4aHWwuFCYYVydFRxMqHhhCKBseH1dbFygrRxIWJ1UYFhotFjA=");

$key = md5('ISCC');
$x = 0;
$len = strlen($str);
$klen = strlen($key);
for ($i=0; $i < $len; $i++) {
        if ($x == $klen)
        {
            $x = 0;
        }
        $char .= $key[$x];
        $x+=1;
}

for ($i=0; $i < $len; $i++) {
 if (ord($char["$i"])+ord($str["$i"])<=128)
 {
  $data.=chr(128+ord($str["$i"])-ord($char["$i"]));
 }else{
  $data1=chr(ord($str["$i"])-ord($char["$i"]));
  if (ord($data1) >128 ){
   $data.=chr(ord($data1)-128);
  }else{
   $data.=$data1;
  }
 }
}

echo $data;
?>
```