

# 【bugku】 PHP\_encrypt\_1(ISCCCTF) writeup

原创

[peryc](#) 于 2018-02-27 10:49:50 发布 4504 收藏 2

分类专栏: [ctf](#) 文章标签: [ctf网络安全](#) [bugku](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: [https://blog.csdn.net/qq\\_19861715/article/details/79385075](https://blog.csdn.net/qq_19861715/article/details/79385075)

版权



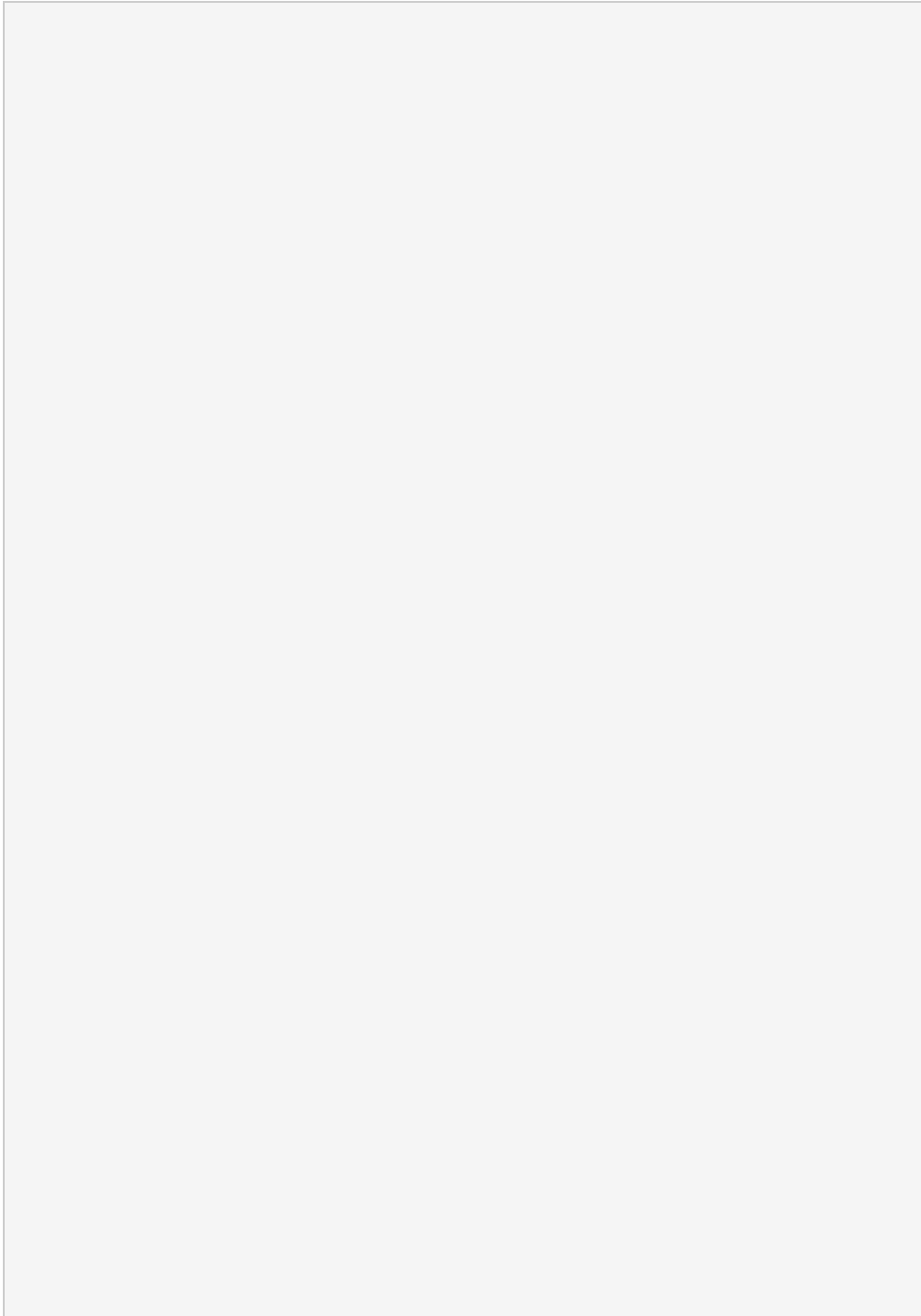
[ctf专栏收录该内容](#)

12 篇文章 0 订阅

订阅专栏

## PHP\_encrypt\_1(ISCCCTF)

给出了一个 encrypt 函数和一串密文



```

1 <?php
  function encrypt( $data , $key )
  {
2     $key = md5( 'ISCC' );
    $x = 0;
    $len = strlen ( $data );
    $klen = strlen ( $key );
3     for ( $i =0; $i < $len ; $i ++ ) {
        if ( $x == $klen )
4         {
            $x = 0;
        }
        $char .= $key [ $x ];
5         $x +=1;
    }
6     for ( $i =0; $i < $len ; $i ++ ) {
        $str .= chr ((ord( $data [ $i ] ) + ord( $char [ $i ] )) %
128);
    }
7     return base64_encode ( $str );
  } ??
  output: fR4aHWwuFCYVYdFRxMqHhCKBseH1dbFygrRxIWJ1UYFhotFjA=
8
9
10
11
12
13
14
15
16
17
18
19
20
21

```

根据 encrypt 函数写对应的 decrypt

```

1 <?php
  function decrypt( $str ) {
    $mkey = "729623334f0aa2784a1599fd374c120d" ;
    $klen = strlen ( $mkey );
2    $tmp = $str ;
    $tmp = base64_decode ( $tmp ); // 对 base64 后的字符串 decode
    $md_len = strlen ( $tmp ); //获取字符串长度
3    for ( $i =0; $i < $md_len ; $i ++ ) { // 取二次加密用 key;
        if ( $x == $klen ) // 数据长度是否超过 key 长度检测
            $x = 0;
4        $char .= $mkey [ $x ]; // 从 key 中取二次加密用 key
        $x +=1;
    }
5    $md_data = array ();
    for ( $i =0; $i < $md_len ; $i ++ ) { // 取偏移后密文数据
        array_push ( $md_data , ord( $tmp [ $i ] ));
6    }
    $md_data_source = array ();
    $data1 = "" ;
    $data2 = "" ;
7    foreach ( $md_data as $key => $value ) { // 对偏移后的密文数据
  进行还原
8        $i = $key ;
        if ( $i >= strlen ( $mkey )) { $i = $i - strlen ( $mkey
9    );}
        $dd = $value ;

```

```
10     $od = ord( $mkey [ $i ] );
    array_push ( $md_data_source , $dd );
    $data1 .= chr ( ( $dd +128)- $od ); // 第一种可能, 余数+128-
key 为回归数
11     $data2 .= chr ( $dd - $od ); // 第二种可能, 余数直接-key 为
回归数
    }
    print "data1 => " . $data1 . "<br>\n" ;
12     print "data2 => " . $data2 . "<br>\n" ;
}
13 $str = "fR4aHwWuFCYyVydFRxMqHhCKBseH1dbFygrRxIWJ1UYFhotFjA=" ;
decrypt( $str );
?>

14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
```

FLAG -> Flag:{asdqw\*fasfd\*wfefq\*dqwdadwq\*daw\*}



[创作打卡挑战赛](#) >

[赢取流量/现金/CSDN周边激励大奖](#)