【bugku】 PHP_encrypt_1(ISCCCTF) writeup

原创

perye 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

PHP_encrypt_1(ISCCCTF)

给出了一个 encrypt 函数和一串密文

```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 );
} ?>
output: fR4aHWwuFCYYVydFRxMqHhhCKBseH1dbFygrRxIWJ1UYFhotFjA=
```

根据 encrypt 函数写对应的 decrypt

```php
<?php
function  decrypt( $str ) {
     $mkey  =  "729623334f0aa2784a1599fd374c120d" ;
     $klen  =  strlen ( $mkey );
     $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
     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;
         $char  .=  $mkey [ $x ];   // 从 key 中取二次加密用 key
         $x +=1;
     }
     $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 ]));
     }
     $md_data_source  =  array ();
     $data1  =  "" ;
     $data2  =  "" ;
     foreach  ( $md_data  as  $key  =>  $value ) {  // 对偏移后的密文数据
进行还原
         $i  =  $key ;
         if ( $i  >=  strlen ( $mkey )) { $i  =  $i  -  strlen ( $mkey
);}
         $dd  =  $value ;
```

```php
            $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
            $data2  .=  chr ( $dd - $od );   // 第二种可能，余数直接-key 为回归数
        }
        print  "data1 => " . $data1 . "<br>\n" ;
        print  "data2 => " . $data2 . "<br>\n" ;
}
$str  =  "fR4aHWwuFCYYVydFRxMqHhhCKBseH1dbFygrRxIWJ1UYFhotFjA=" ;
decrypt( $str );
?>
```

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