php writeup,PHP_encrypt_1(ISCCCTF) Writeup

转载

口口子茶叶蛋 于 2021-03-29 05:50:33 发布 61 收藏
文章标签： php writeup

PHP_encrypt_1(ISCCCTF) Writeup

PHP_encrypt_1(ISCCCTF) Writeup

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：

```
function encrypt($data,$key)
{
$key = md5('ISCC');
$x = 0;
$len = strlen($data);
$klen = strlen($key);
for ($i=0; $i < $len; $i++) {
if ($x == $klen)
```

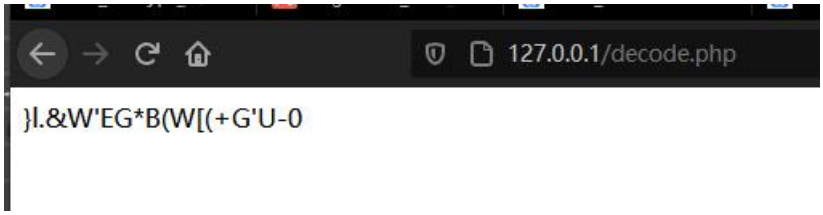
```
{
$x = 0;
}
$char .= $key[$x];
$x+=1;
}
for ($i=0; $i < $len; $i++) {
$str .= chr((ord($data[$i]) + ord($char[$i])) % 128);
}
return base64_encode($str);
}
?>
```

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：

```
echo base64_decode("fR4aHWwuFCYYVydFRxMqHhhCKBseH1dbFygrRxlWJ1UYFhotFjA=");
?>
```

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：

```
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：

$len =$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。)

$char

chr()：将一个asill码转换成字符

ord():将字符转换成ascii码

% : 求余

$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：

将ISCC进行MD5加密

$key = md5('ISCC');

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);

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。

$str= base64_decode("fR4aHWwuFCYYVydFRxMqHhhCKBseH1dbFygrRxlWJ1UYFhotFjA=");

$key = md5('ISCC');

$x = 0;

$len = strlen($str);

$klen = strlen($key);

for ($i=0; $i < $len; $i++) {

if ($x == $klen)

{

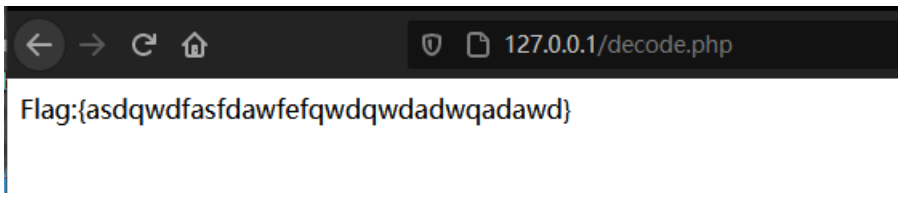
$x = 0;

}

$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;
?>
```



PHP_encrypt_1(ISCCCTF) Writeup相关教程

nginx如何配置index.php 隐藏

nginx配置index.php隐藏的方法：首先找到并打开“nginx.conf”配置文件；然后添加代码为“location / {if (!-e $request_filename) {...}}”并保存即可。 推荐：《PHP视频教程》 ThinkPHP5.0的nginx配置隐藏入口文件index.php 只需要在配置文件nginx.conf添

php如何安装openssl扩展

php安装openssl扩展的方法：首先在PHP安装包中找到curl扩展目录；然后将config0.m4文件重命名；接着运行phpize；最后编译安装，并设置PHP配置文件php.ini即可。 推荐：《PHP视频教程》 关于openssl OpenSSL是一个安全套接字层密码库，囊括主要的密码算法、常

ubuntu 怎么安装 php curl

ubuntu安装php curl的方法：首先下载curl安装包；然后安装cURL；最后打开开关“–with-curl=/usr/local/curl”即可。 推荐：《PHP视频教程》 ubuntu下php安装curl扩展库 如果php已经在系统编译好，后来又需要添加新的扩展，一种方式就是重新完全编译php，另

搭建 PHP 开发环境(手把手图文教程)

搭建 PHP 开发环境(手把手图文教程) 都 2020 年了，你还在老老实实地按照 下载Apache、安装MySQL、安装PHP、配置Apache 步骤来搭建PHP开发环境吗？ 下面介绍一种一键配置方法：炒鸡好用的 phpStudy 我们在这里可以看到，phpStudy 内置了apache、nginx、mysq

PHP 数据库操作

PHP 数据库操作 PHP操作数据库的2种形式 使用 PDO 扩展类库(推荐) 使用 Mysqli 扩展类库(这是Mysql类库的升级版，但已经不推荐使用) PDO 扩展包含哪三个类 PDO PDOStatement PDOException PDO 与 Mysqli 区别 PDO 可以支持多种数据库，而且操作方法一致 M

PHP的OpenSSL加密扩展学习(一)：对称加密

PHP的OpenSSL加密扩展学习(一)：对称加密 PHP的OpenSSL加密扩展学习(一)：对称加密 我们已经学过不少 PHP 中加密扩展相关的内容了。而今天开始，我们要学习的则是重点中的重点，那就是 OpenSSL 加密扩展的使用。为什么说它是重点中的重点呢？一是 OpenSSL

XTCTF Web_php_wrong_nginx_config

XTCTF Web_php_wrong_nginx_config 知识点 目录扫描 cookie 文件包含 nginx配置有问题导致存在目录遍历。PHP混淆加密及其逆向利用 代码审计 python脚本 WP 进入环境先扫目录，这题扫目录挺重要的。 可以扫到/admin,login.php,robots.txt,/admin/admin.php之

基于Thinkphp使用同一个域名，PC和M端访问不同模板

基于Thinkphp使用同一个域名，PC和M端访问不同模板 一、首先目录结构展示：(主要修改这几个文件) 二、更改入口文件 index.php require DIR . ‘./isMobile.php’; 三、在入口文件index.php同级目录下，增加common.php文件，代码为： ?phpfunction isMobile