云演-Web文件下载-writeup

原创

秋风瑟瑟... 于 2020-06-15 11:19:33 发布 333 收藏

分类专栏： 云演

本文链接：https://blog.csdn.net/qq_45628145/article/details/106758709

听首歌吧

页面里面有两个歌曲下载链接，发现下载的url是这样的

```
download.php?url=T25lIExvdmUubXAz
```

后面是对应文件名的base64编码，按照这个规律，下载一个download.php看看

```
download.php?url=ZG93bmxvYWQucGhw
```

```php
<?php
error_reporting(0);
include("hereiskey.php");
$url=base64_decode($_GET[url]);
if( $url=="hereiskey.php" || $url=="choubaguai.mp3" || $url=="One Love.mp3" || $url=="download.php"){
 $file_size = filesize($url);
 header ( "Pragma: public" );
 header ( "Cache-Control: must-revalidate, post-check=0, pre-check=0" );
 header ( "Cache-Control: private", false );
 header ( "Content-Transfer-Encoding: binary" );
 header ( "Content-Type:audio/mpeg MP3");
 header ( "Content-Length: " . $file_size);
 header ( "Content-Disposition: attachment; filename=".$url);
 echo(file_get_contents($url));
 exit;
}
else {
 echo "Access Forbidden!";
}
?>
```

下载**hereiskey.php**，得到flag

```php
<?php
// key is d0wnload_0k
?>
```