[ACTF2020 新生赛]Exec 1 命令注入

原创

一只Traveler 已于 2022-04-04 13:22:57 修改 706 收藏
文章标签： php 安全
于 2022-04-04 12:22:51 首次发布

题后总结：

关于命令注入；

刷题到目前为止，只知道一个sql注入，所以拿到一个非sql注入的题就会毫无办法；

对于网站的渗透测试来讲，远不止只有sql注入；参考博文

BUUCTF-[ACTF2020 新生赛]Exec1__Monica_的博客-CSDN博客

CTF-web 第十三部分 命令注入_iamsongyu的博客-CSDN博客_ctf命令注入

总结到网站注入攻击有：

命令注入(Command Injection)

Eval 注入(Eval Injection)

客户端脚本攻击(Script Insertion)

跨网站脚本攻击(Cross Site Scripting, XSS)

SQL 注入攻击(SQL injection)

动态函数注入攻击(Dynamic Variable Evaluation)

序列化注入&对象注入

其中这里命令注入为最最最简单的命令：

那么是怎么判断使用命令注入的呢；通参考资料可以知道，可以通过不同语言包含的不同的代码来判断：比如：

在PHP中的以下函数就可能存在命令注入：

system

exec

shell_exec

passthru

这道题题目就含有提示exec，所以就考你用命令注入来解题；

在python语言中含有可能命令注入的函数：

```
-*-command: system\popen\subprocess.call\spawn
```

```
-*-code: map\filter\reduce\...
```

```
# python 函数名可以直接作为普通函数的参数的，理论上，如果定义了这样的函数都危险def myreduce(funcname,param):
```

```
return funcname(param)
```

在java中：

-*-command：java.lang.Runtime.getRuntime().exec(command)

在本题中，只使用了简单的cd ../；ls来查看有哪些目录，然后发现有Flag 目录，使用cat命令打开目录；