vuln06-远程代码执行

无涯老师

课程大纲

1、什么是远程代码执行?
2、PHP相关函数
3、靶场案例
4、CTF案例
5、防御措施

01 什么是远程代码执行?

远程代码执行

远程代码执行：Remote Code Execute

远程命令执行：Remote Command Execute

为什么要远程执行代码?

- 路由器、防火墙、入侵检测等设备的web管理界面
- 自动化运维的管理系统

漏洞危害

- 获取服务器权限
- 获取敏感数据文件
- 写入恶意文件getshell
- 植入木马病毒勒索软件等

实际漏洞

- CVE-2021-3177　Python RCE漏洞
- CVE-2021-21972　VMWare RCE漏洞
- CVE-2021-25646　Apache Druid RCE漏洞

- CNVD-2020-46552 深信服EDR
- CNVD-2021-30101 网康下一代防火墙
- http://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=RCE

02 PHP RCE涉及函数

命令command注入

函数	作用
system()	执行外部程序，并且显示输出
exec()/shell_exec()	通过 shell 环境执行命令，并且将完整的输出以字符串的方式返回
pcntl_exec()	在当前进程空间执行指定程序
passthru()	执行外部程序并且显示原始输出
popen()	打开进程文件指针
proc_open()	执行一个命令，并且打开用来输入/输出的文件指针

代码code注入

函数	作用
eval()	把字符串 code 作为PHP代码执行
assert()	检查一个断言是否为 false
preg_replace()	执行一个正则表达式的搜索和替换
create_function()	创建一个匿名函数并且返回函数名称
call_user_func()/call_user_func_array()	把第一个参数作为回调函数调用
usort()/uasort()	使用用户自定义的比较函数对数组中的值进行排序并保持索引关联

03 靶场案例

Windows命令拼接符号

符号	含义	示例
&&	左边的命令执行成功，右边的才执行	ping 127.0.0.1 && echo 'hello'
&	简单的拼接	ping 1111 & echo 'hello'
|	上一条命令的输出，作为下一条命令参数	netstat -ano |findstr 3306
||	左边的命令执行失败，右边的才执行	ping baidu.com || ping baidu.net

Linux命令拼接符号

符号	含义	示例
;	没有任何逻辑关系的连接符	
&&	左边的命令执行成功，右边的才执行	cp 1.txt 2.txt && cat 2.txt
|	上一条命令的输出，作为下一条命令参数	netstat -an|grep 3306
||	左边的命令执行失败，右边的才执行	cat 3.txt || cat 2.txt
&	任务后台执行，与nohup命令功能差不多	java -jar test.jar > log.txt &

pikachu

ping payload
127.0.0.1 & ipconfig
127.0.0.1 & whoami

eval payload phpinfo();
POST请求，参数为txt，可以用中国蚁剑连接

DVWA

payload
127.0.0.1 & ipconfig
127.0.0.1 & net user hacker /add

04 CTF题目

ctfhub

见笔记

05 RCE防御

防御

1、尽量不要使用命令执行的函数
2、如果必须使用，需要做白名单处理
3、用正则表达式对用户输入的内容进行处理
4、使用WAF

Thank you for watching

无涯老师