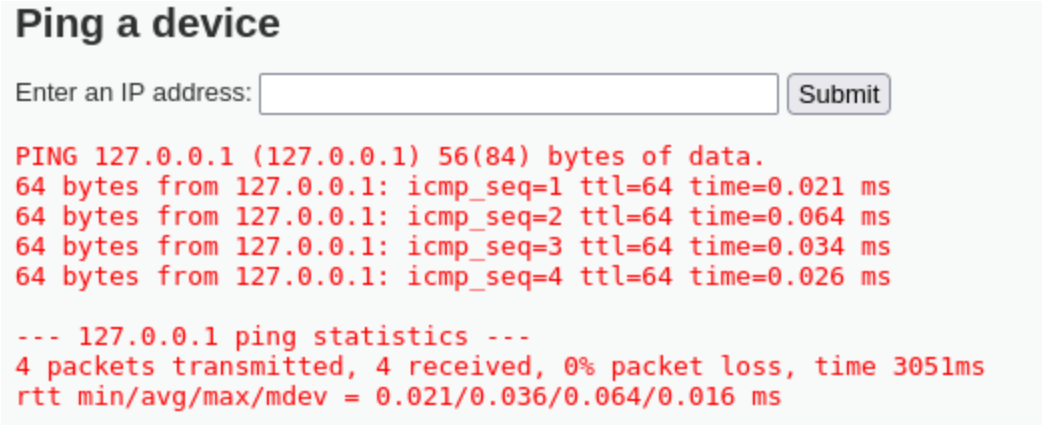
Command Injection

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



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

```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}</pre>";
}

?>
```

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