OS COMMAND INJECTION

Friday, January 31, 2020 12:20 AM

1.NORMAL=>inject command using '&' character and display the output to check

2.BLIND=>

- A) To check blind input a ping coomand for 10 sec "ex=>ping+-c+10+127.0.0.1" and use "||" these chracters at the front and back of command .
- To check try to redirect output to domain that you can control. ex=> nslookup domain
- To check blind based try to create a file in the dirctory that can be accessed and saved that file.now open the file and access the result. Ex=> Cmd> directory address.

  - Try submitting the following values in turn as each targeted parameter:
    ;echo%20111111
    echo%20111111
    response.write%20111111
    :response.write%20111111
  - You can use commands like this .ex=>"system(‘ping%20127.0.0.1’)"
  - For php applicaton use this to identify .ex=> "phpinfo()"