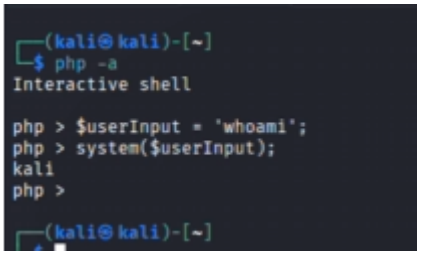
10 - Command Injection - Introduction

This is a very serious vulnerability. Essentially the application is taking input from the user, and passing it to a function that executes it as code. This goes against security development principle of not mixing data and code.

"Eval is evil." This is one of the functions that executes data that is passed to it.

We can test eval in the developer tools, in the console tab. We can type "eval()", and make a statement in the parenthesis like 1+1 or some other math operation or even other commands, eval will execute that command.



Whenever writing code for an application, make sure to have this in mind, and do not trust user input, or let users execute commands in the underlying system.