Challenge: Juggling Facts

# Challenge Description :

**An organization seems to possess knowledge of the true nature of pumpkins. Can you find out what they honestly know and uncover this centuries-long secret once and for all?**

# Context :

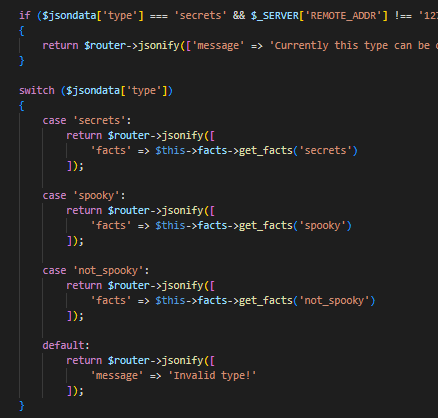
## This is a simple web challenge where you will need to intercept the http requests. We are also given the Source code for this one.

# Notes :

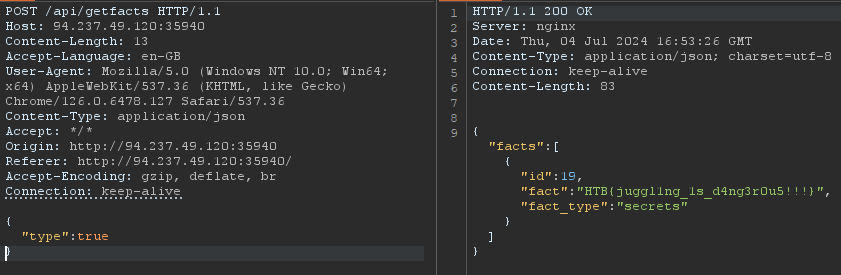
* Tools:
  + - Burpsuite - Using burpsuite to analyze, intercept and forge http requests.
    - Vscode- Used to see the Source code of the web-application, use can also use alternative text based applications like notepad if you want.

# Flag :

* Start the instance, and start up burpsuite, i first check the source code to check for vulnerabilities or anything interesting in the code.
* Going to the IP:PORT of the instance shows a halloween themed page about halloween facts, burpsuite also caught a POST request when we go to click on the other facts.
* Going back to the source code to search for the POST request Query ” Spooky “, takes me to a “ IndexController.php ” page in the Source Code.



* When looking at the result nothing really catches your eyes until you read the logic. The issue lies in the switch function as it uses non-defined types to compare for when it checks, whereas the secret type check employs a strict "===" comparison.
* We can exploit, using Type Juggling, by passing a value that is equal to the logic of both values : ”type != secret and “type == secret“ , the values that should conquer this would be a “True“ statement as its self-explanatory.
* Sending the forged http request with the “ type “ json query being set to “ True “ to replace “spooky“.



* Sending the forged request returns us with a flag :

HTB{juggl1ng\_1s\_d4ng3r0u5!!!}