CLUB
ETHICAL HACKING

Challenge #2
W3bmast3r_n00b
Part.2

21 Mars 2019

Pré-requis

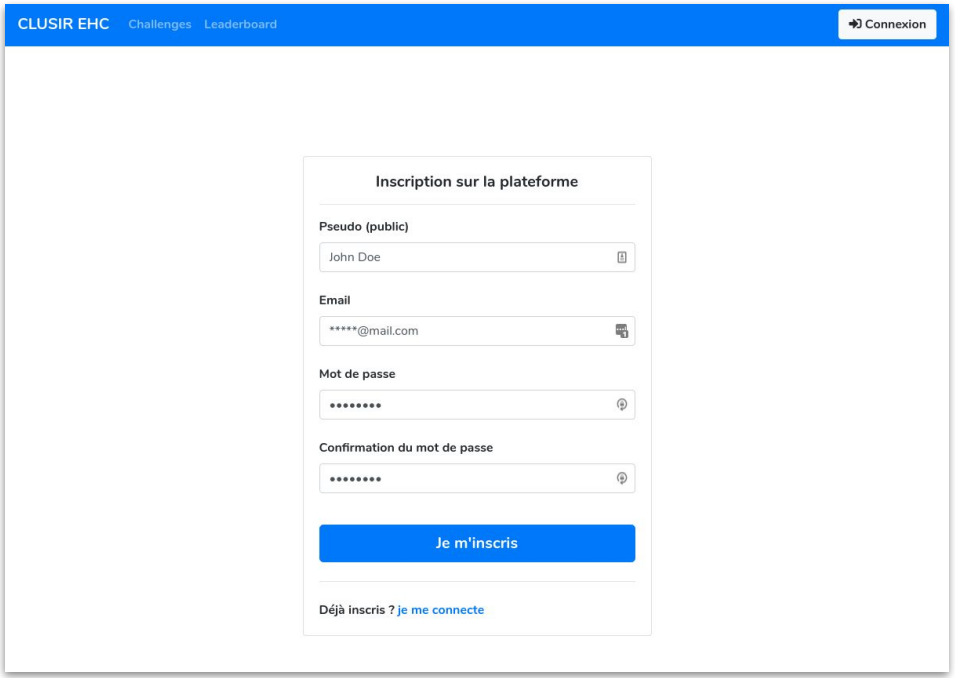
- Machine Linux (Kali, Debian, etc.)
- Docker (+ docker-compose)
- Quelques connaissances en MySQL / Linux / Web

Installation du challenge (environnement Linux):

```
curl -sSL https://gist.githubusercontent.com/remiallain/b4b588d6ddc28266c488a24c8cce117f/raw/e3030696ba6d3724a5c04bf6b431ef3bf3c9cdbe/run2.sh | sh
```

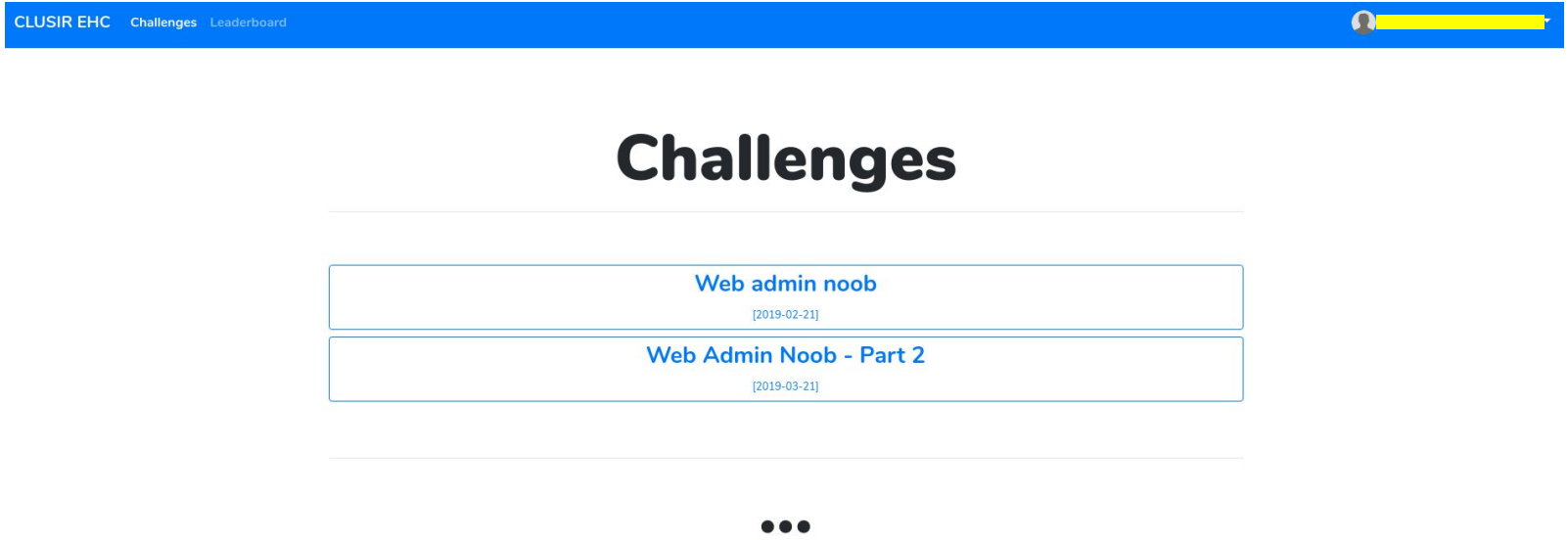
Plateforme de points

https://clusir-ehc.firebaseapp.com



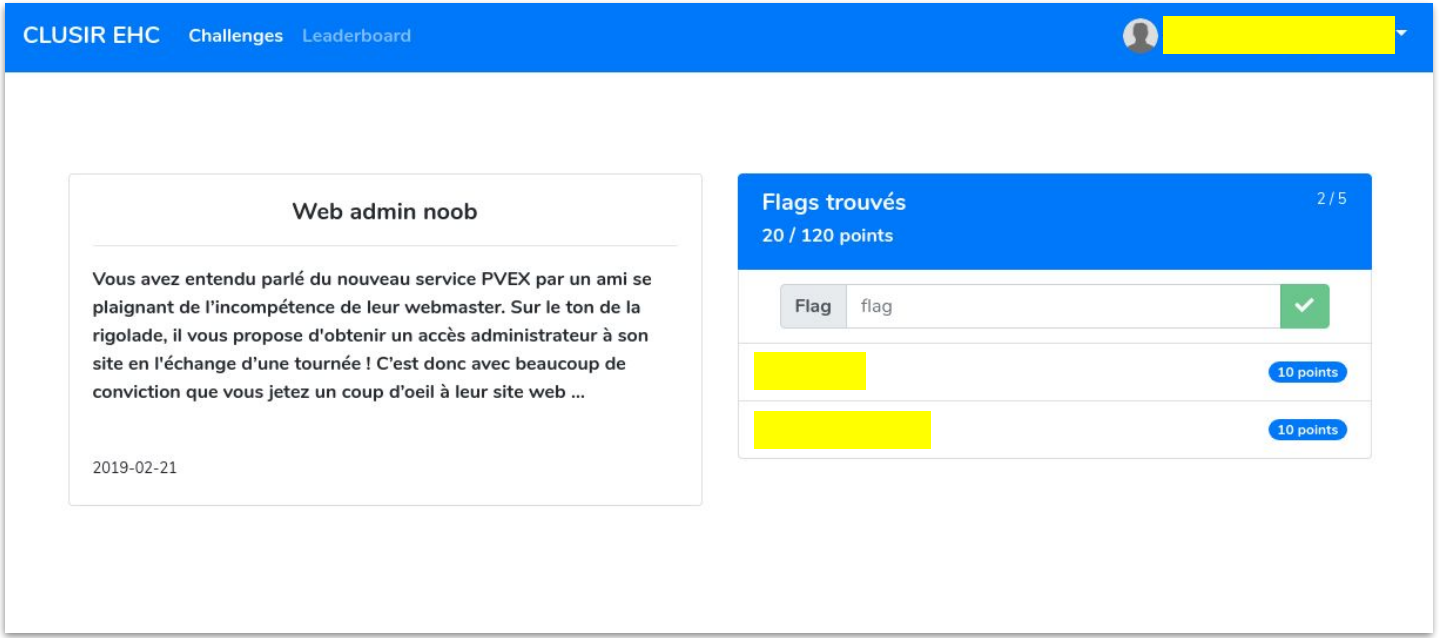
Plateforme de points

https://clusir-ehc.firebaseapp.com



Plateforme de points

https://clusir-ehc.firebaseapp.com



Objectifs

Suite à vos attaques, Les webmasters de PVEX ont pris des mesures pour sécuriser leur site. Mais ont-elles été efficaces ?

→ *(En local - via Docker)* `http://172.16.2.100`

→ *(Si vous n'avez pas Docker - AWS)* `http://?.?.?.?` *(l'ip sera affichée le jour j)*

Vous aurez à trouver 3 flags au format **${CEH_flag}**

ATTENTION

Pour ceux travaillant sur AWS, lors de la dernière étape, vous pouvez compromettre la machine (ex: changement de mot de passe).

Merci de respecter vos collègues et de réaliser des actions non-bloquantes pour les autres challengers.

Des questions ? → **rallain@cyberprotect.one**