

CLUB ETHICAL HACKING



Challenge #2
W3bmast3r_n00b
Part.2

21 Mars 2019

Pré-requis

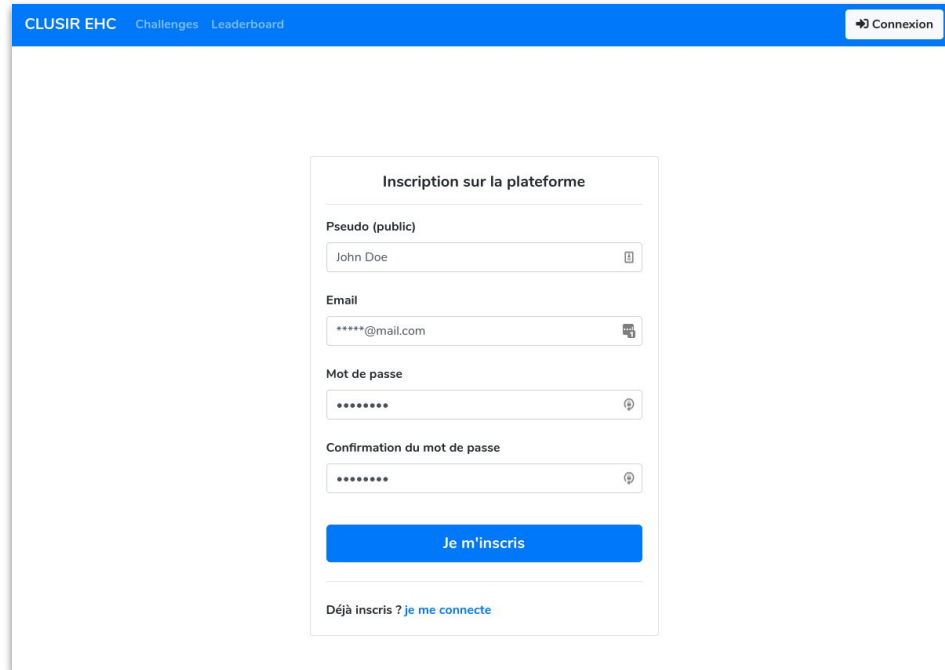
- Machine Linux (Kali, Debian, etc.)
- Docker (+ docker-compose)
- Quelques connaissances en MySQL / Linux / Web

Installation du challenge (environnement Linux):

```
curl -sSL
```

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

<https://clusir-ehc.firebaseio.com>



The image shows a web browser window displaying the registration page for CLUSIR EHC. The page has a blue header with the text "CLUSIR EHC" and navigation links for "Challenges" and "Leaderboard". A "Connexion" button is located in the top right corner. The main content area features a registration form titled "Inscription sur la plateforme". The form includes four input fields: "Pseudo (public)" with the value "John Doe", "Email" with the value "****@mail.com", "Mot de passe" (password), and "Confirmation du mot de passe" (password confirmation). A blue "Je m'inscris" button is positioned below the form. At the bottom of the form, there is a link that says "Déjà inscrit ? je me connecte".

CLUSIR EHC Challenges Leaderboard Connexion

Inscription sur la plateforme

Pseudo (public)
John Doe

Email
****@mail.com

Mot de passe

Confirmation du mot de passe

Je m'inscris

Déjà inscrit ? je me connecte

<https://clusir-ehc.firebaseio.com>



Challenges

Web admin noob

[2019-02-21]

Web Admin Noob - Part 2

[2019-03-21]



<https://clusir-ehc.firebaseio.com>

CLUSIR EHC Challenges Leaderboard

Web admin noob

Vous avez entendu parlé du nouveau service PVEX par un ami se plaignant de l'incompétence de leur webmaster. Sur le ton de la rigolade, il vous propose d'obtenir un accès administrateur à son site en l'échange d'une tournée ! C'est donc avec beaucoup de conviction que vous jetez un coup d'oeil à leur site web ...

2019-02-21

Flags trouvés 2 / 5
20 / 120 points

Flag	flag	✓
	[Redacted]	10 points
	[Redacted]	10 points

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