Root Me Challenge

https://www.root-me.org/fr/Challenges/Web-Serveur/HTTP-POST

[SOMMAIRE]

Objectif du challenge : Trouver une façon de battre le meilleur score

Synopsis :

> Pour lancer le jeu on clique sur le bouton `Give a try !`.
> Si l'on fait moins que le meilleur score `999999` on perd. Le but étant de battre ce score...

Jeu : départ

Que se passe t'il en cliquant sur le bouton ?
... That is a question.

HTTP

> En cliquant sur le bouton cela va envoyer une requête (demande) d'un certain type au serveur web via le protocol **HTTP** (*hyperText Transfert Protocol*) qui traitera la demande et renverra le résulat dans un navigateur(client). C'est un protocole de communication dit : client / serveur.

- *Il fonctionne sur le port 80 et utilise le protocole TCP comme couche de transport.*
- *HTTP est un protocole de la couche application dans le modèle OSI (couche 5.6.7)*

  Il existe la version HTTPS qui est la variante sécurissée par le chiffrement et l'hauthentification. Cette version utilise le port 443.

POST

> Le type ou la méthode ici est **POST**. La méthode POST est utilisée pour transmettre des données en vue d'un traitement à une ressource (le plus souvent un formulaire HTML).

- *Il existe aussi la méthode GET qui via une requête visible dans l'URL(Uniform Ressource Locator). permet par exemple d'accèder à d'autres pages d'un site.*

  ```
  Faire un teste avec l'inspecteur dans le navigateur sur votre page, en changeant la méthode "P
  ```

- https://www.ionos.fr/digitalguide/sites-internet/developpement-web/get-vs-post/#c251633

  L'URL est un mécanisme utilisé par les navigateurs pour accéder à toute ressource publiée sur le net. l'URL équivaut à l'adresse postale du facteur. Cette adresse est ainsi utilisée pour pouvoir accéder à une page d'un site internet telle que la page d'accueil, la page de contacts...

```
Elle peut-être composée :
```

```
- Du protocol
- D'un nom de domaine et sous-domaine
- D'un chemin
- et de paramètre ou requête (après le ?)
```

- https://www.numacom.fr/blog/qu-est-ce-qu-une-url-definition-et-fonctionnement

HTTP est avec HTML et les URL une des trois inventions fondamentales de Tim Berners-Lee pour créer le World Wide Web.

Une fois la page du jeu affichée :

Le but est de trouver comment afficher le code, pour le hacker, de façon à gagner en faisant plus que 999999.

Méthodologie:

- Ouvrir l'inspecteur (F12).
    - **Trouver la ligne de code qui permet l'envoie de la requête.**
    - Indice ...
        - *Celle-ci est envoyée avec la méthode POST via un formulaire.*

Explication :

```
<form action="" method="post" onsubmit="document.getElementsByName('score')[0].value = Ma
    <input type="hidden" name="score" value="-1" />
    <input type="submit" name="generate" value="Give a try!">
</form>
```

↑ Ce morceau de code HTML avec du Javascript ci-dessus, comprend un formulaire contenant un champ caché et un bouton de soumission.

De façon plus précise ...

1. Balise `<form>`

```
<form action="" method="post" onsubmit="document.getElementsByName('score')[0].value = Ma
<form>
```

La balise `<form>` Définit un formulaire HTML.

- **action=""** : Spécifie l'URL vers laquelle les données du formulaire doivent être envoyées. Une valeur vide signifie que le formulaire sera soumis à la même URL que la page actuelle.
- **method="post"** : Indique que les données du formulaire seront envoyées via une requête HTTP en POST.
- **onsubmit="..."** : Attribut JavaScript, qui spécifie une fonction ou un script à exécuter lorsque le formulaire est soumis. Ici, le script JavaScript change la valeur du champ caché `score` avant la soumission du formulaire.

Fonction JS :

- **Math. floor(x)** renvoie le `plus grand entier` qui est `inférieur ou égal` à un nombre x.
- **Math.random()** renvoie un nombre flottant pseudo-aléatoire, généré entre 0 (inclus) et 1 (**`exclu`**)". Le chiffre généré se situe entre 0 et 0.99 dans ce cas.

---

2. Champ caché `<input>`

```
<input type="hidden" name="score" value="-1" />
```

La balise `<input>` Définit un champ de saisie de données.

- **type="hidden"** : Indique que se champ est caché et ne sera pas visible pour l'utilisateur.
- **name="score"** : Nom du champ utilisé pour identifier les données lors de la soumission.
- **value="-1"** : Valeur initiale du champ, ici définie à "-1".

---

3. Bouton de soumission `<input>`

```
<input type="submit" name="generate" value="Give a try!">
```

La balise `<input>` Définit un champ de saisie de données.

- **type="submit** : Spécifie que ce champ est un bouton de soumission qui envoie un formulaire.
- **name="generate"** : Nom du champ, bien qu'il ne soit généralement pas utilisé pour les boutons de soumission.
- **value="Give a try!** : Texte affiché sur le bouton.

Fonctionnement du code

1. Avant la soumission, l'attribut `onsubmit` exécute le script JavaScript suivant :

```
document.getElementsByName('score')[0].value = Math.floor(Math.random() * 1000001)
```

- **document.getElementsByName('score')[0]** : Sélectionne le premier élément du document avec le nom **`score`**.
- **.value** : Accède à la valeur de cet élément.
- **Math.floor(Math.random() * 1000001)** : Génère un nombre entier aléatoire entre 0 et 1.000.000 et assigne ce nombre aléatoire à la valeur du champ caché **`score`**.

2. Le formulaire sera soumis avec la nouvelle valeur aléatoire du champ `score`.

Conclusion

En cliquant sur le bouton **`Give a try !`** cela va générer un nombre aléatoire entre 0 et 1 000 000 et l'assigner au champ caché `score` avant de soumettre le formulaire.
La valeur du champ caché `input` est à -1.

Donc la valeur aléatoire maximum étant 1 000 000 - la valeur du champ caché qui est `-1`. La valeur maximum sera 999 999.

Img hacker **Pour hacker le code.**

- Pour gagner et hacker le jeu il faut modifier la valeur du coéfficient multiplicateur en rajoutant un zéro par exemple.

```
<form action="" method="post" onsubmit="document.getElementsByName('score')[0].value = Math.floor(M
<form>
```

- Ensuite soumettez de nouveau le formulaire.

Jeu : départ

- Retourner sur la page du challenge et coller le Flag dans la zone de saisie pour réussir le challenge.

Jeu : départ