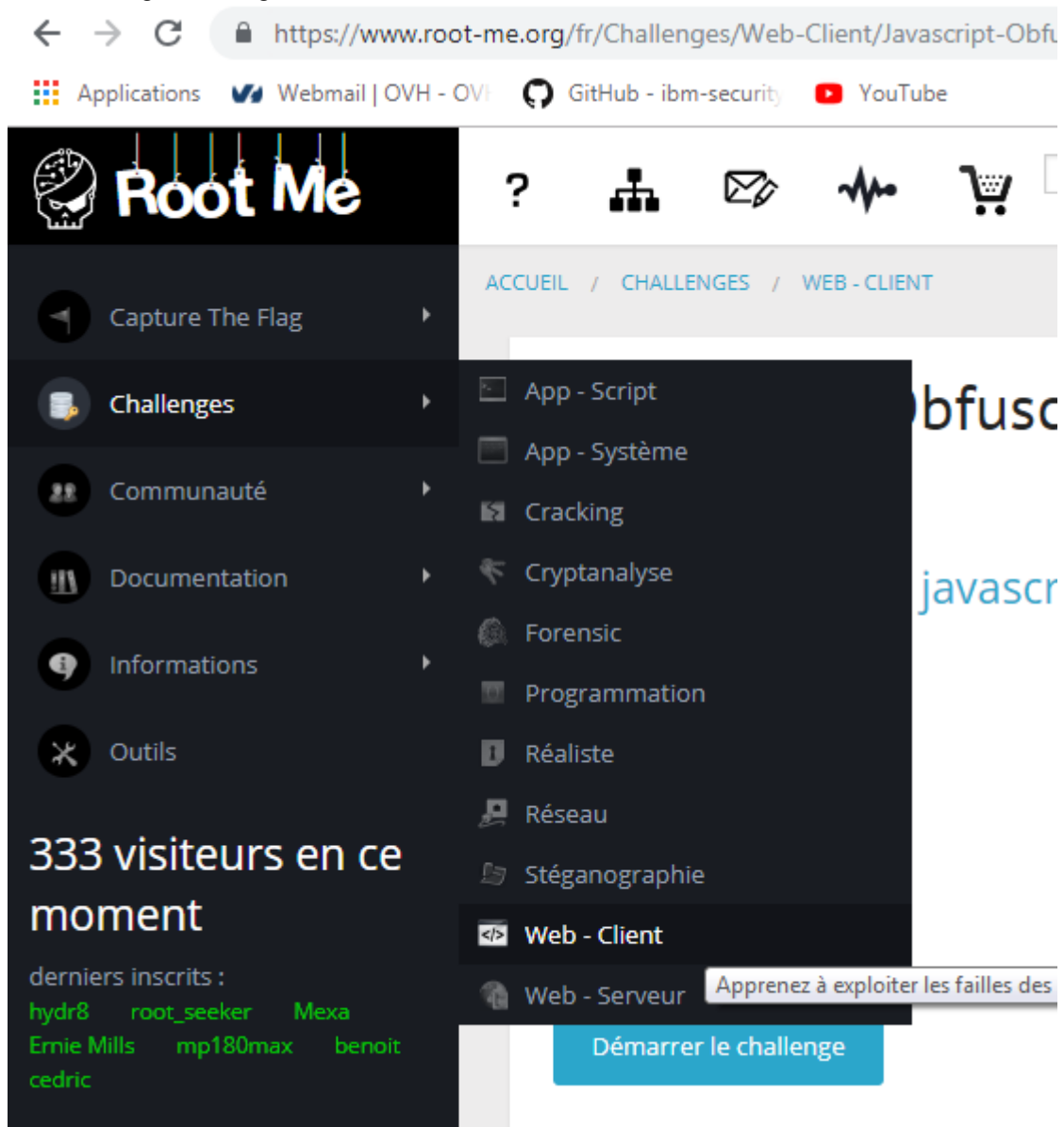


Travaux Pratique
Audit d'application WEB
Enoncé

I) Création d'un compte ROOT-ME :

Se rendre sur le site <http://www.root-me.org> et se créer un compte
Puis se rendre sur l'onglet challenge



- Ce TP ne portera que sur les rubriques Web-client et Web-Serveur

II) Challenges Web-Client :

Objectifs :

Cette rubrique sert à exploiter les failles des applications web pour impacter leurs utilisateurs ou contourner des mécanismes de sécurité côté client. Cette série d'épreuves vous confronte à l'utilisation de langage de script/programmation côté client. Ce sont principalement des scripts à analyser et à comprendre, pour en trouver des vulnérabilités exploitables. Cela permet aussi de se familiariser avec ces langages, dont l'utilisation est très répandue sur Internet.

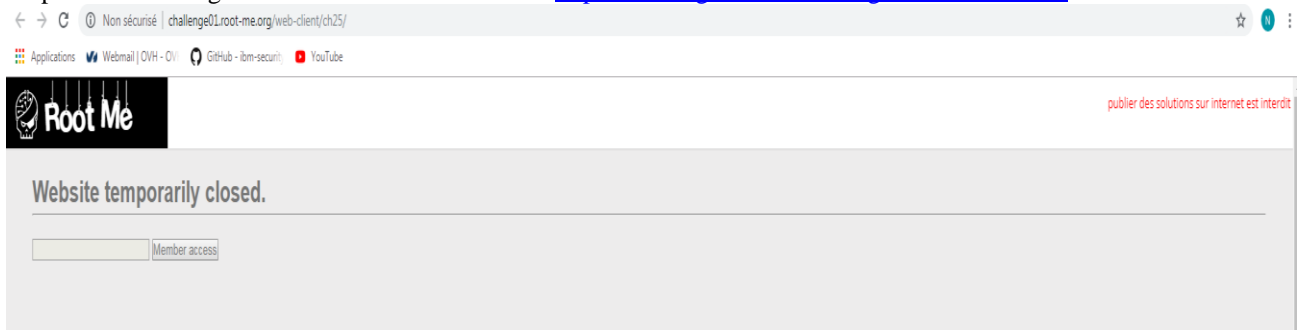
Prérequis :

- Maîtriser un langage de script "web côté client", par exemple javascript ;
- Maîtriser le fonctionnement d'un débogueur, par exemple firebug / console javascript.

A) Challenge 1 : HTML - boutons désactivés :

Enoncé :

Le premier challenge se réalise sur le lien suivant : <http://challenge01.root-me.org/web-client/ch25/>



Il s'agit d'un formulaire désactivé qui ne peut pas être utilisé.

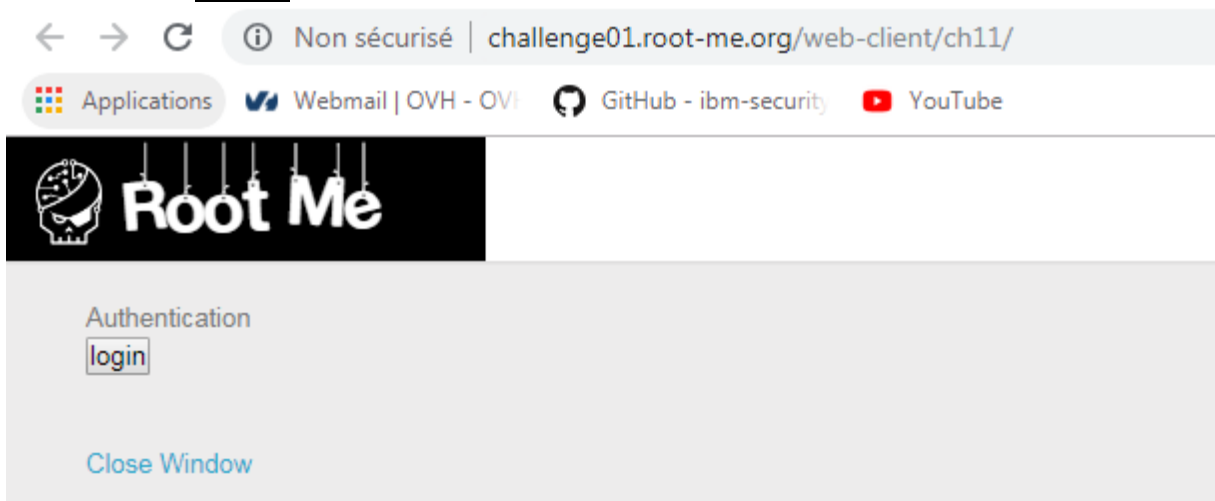
B) Challenge 2 : Javascript – Authentification :

Enoncé :

Il s'agit de retrouver l'identifiant et le mot de passe d'une session pour se connecter sur le site WEB

C) Challenge 3 : Javascript - Authentification 2 :

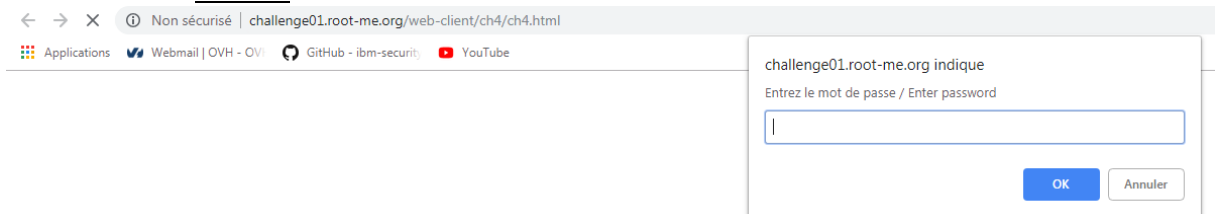
Enoncé :



Ce site semble bloqué. Il faut donc débloquent l'accès pour valider le challenge.

D) Challenge 4 : Javascript - Obfuscation 1 :

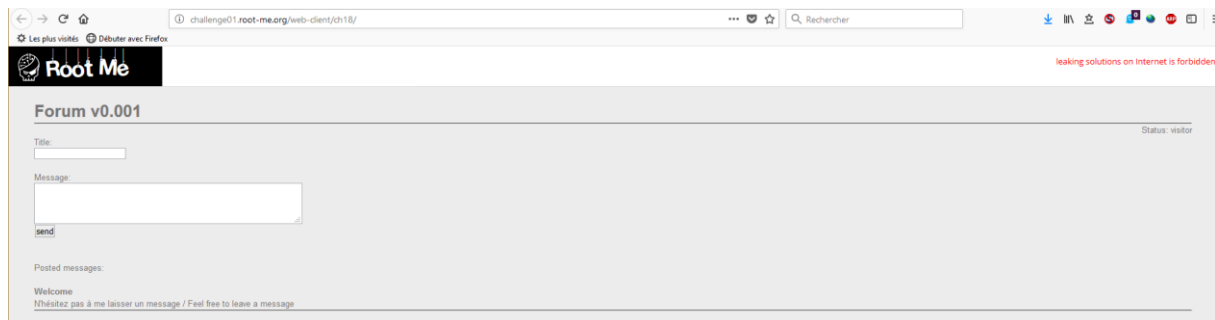
Enoncé :



E) Challenge 5 : XSS - Stockée 1 :

Enoncé :

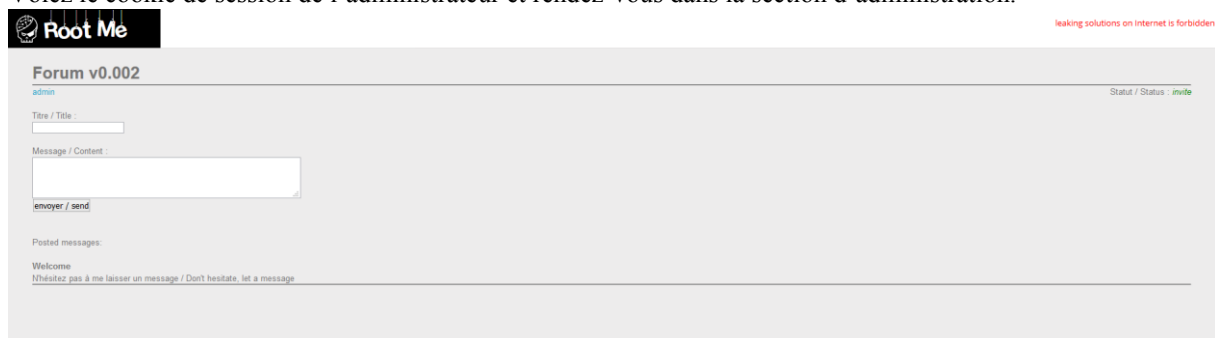
Il s'agit de voler le cookie de session de l'administrateur et de l'utiliser pour valider l'épreuve.



F) Challenge 6 : XSS - Stockée 2

Énoncé :

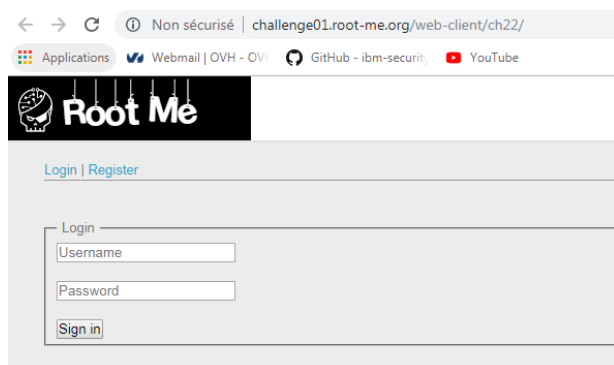
Volez le cookie de session de l'administrateur et rendez-vous dans la section d'administration.



G) Challenge 7 : CSRF - 0 protection :

Énoncé :

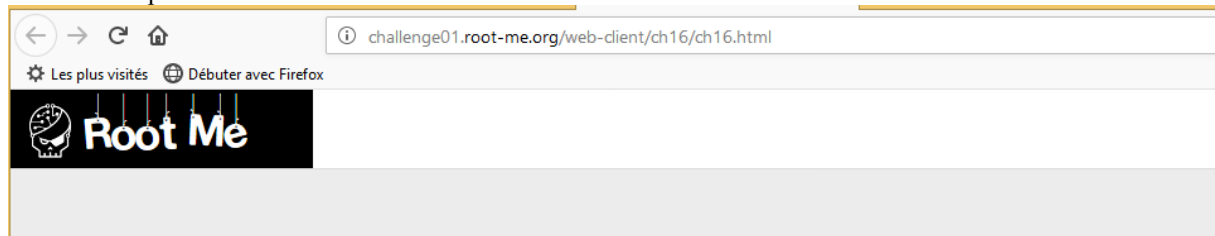
Il s'agit d'activer votre compte pour accéder à l'espace privé de l'intranet.



H) Challenge 8 : Javascript - Native code :

Énoncé:

L'énoncé de précise aucun indice.

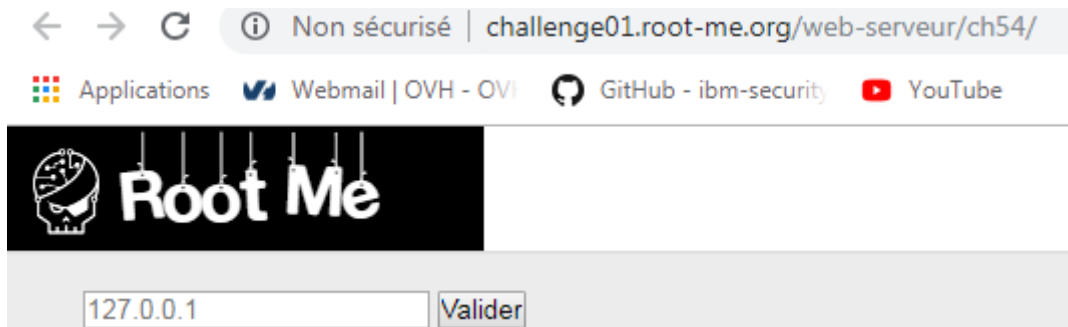


III) Challenge Web-Serveur :

A) Challenge 1 : injection de commande :

Énoncé :

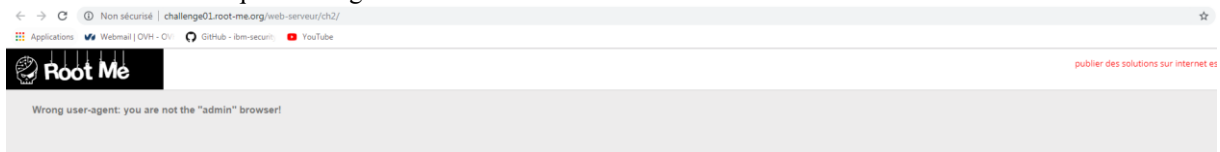
Il s'agit de détourner l'usage premier de ce service. Une indication précise que le mot de passe de validation est dans index.php.



B) Challenge 2 : User-agent :

Enoncé :

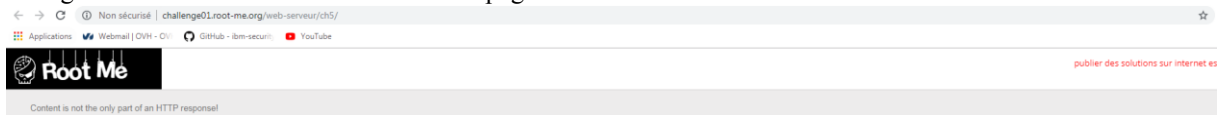
L'admin semble manquer d'imagination.



C) Challenge 3 : http Headers :

Enoncé :

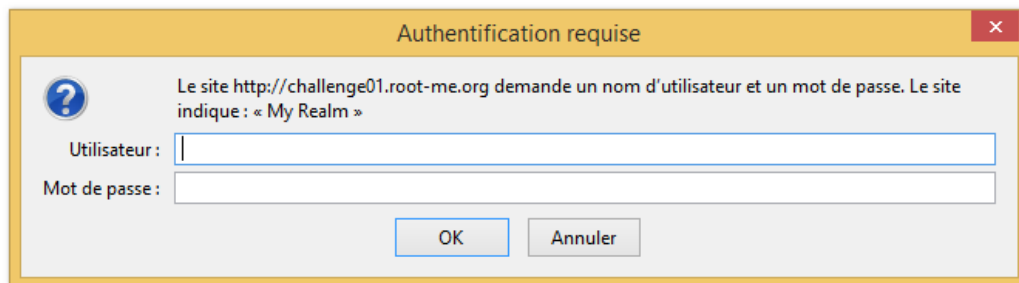
Il s'agit d'obtenir l'accès administrateur à la page.



D) Challenge 4 : http verb tampering :

Enoncé :

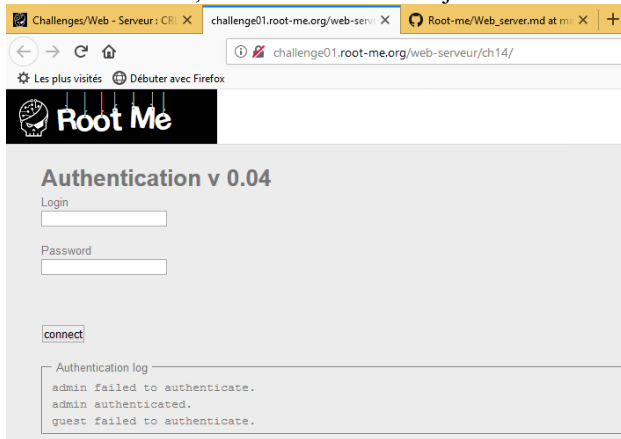
Il suffit de contourner la sécurité mise en place.



E) Challenge 5 : CLRF :

Enoncé :

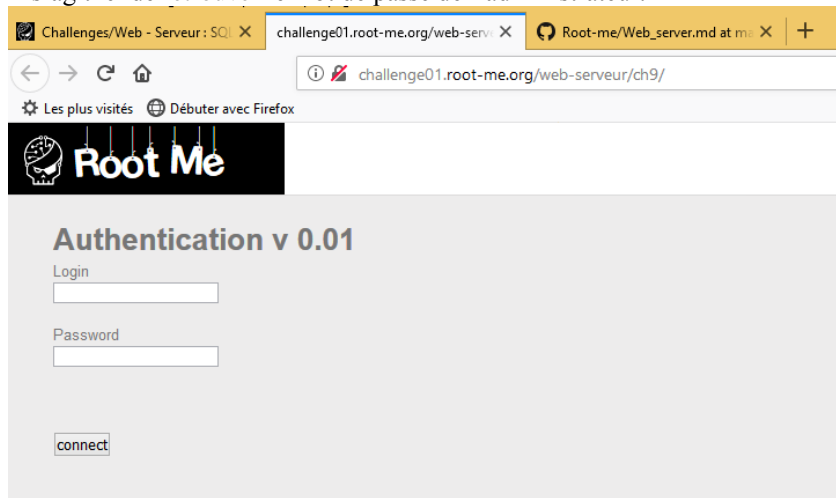
Dans cet exercice, on nous demande d'injecter des données erronées dans le fichier de journalisation.



F) Challenge 6: SQL injection – authentication:

Enoncé:

Il s'agit ici de retrouver le mot de passe de l'administrateur.



The screenshot shows a Firefox browser window with three tabs: "Challenges/Web - Serveur : SQL", "challenge01.root-me.org/web-serveur", and "Root-me/Web_server.md at m...". The address bar shows the URL "challenge01.root-me.org/web-serveur/ch9/". Below the browser window, the Root Me logo is visible. The main content area displays the title "Authentication v 0.01" and a login form with the following elements:

- Label: "Login"
- Input field:
- Label: "Password"
- Input field:
- Button: "connect"