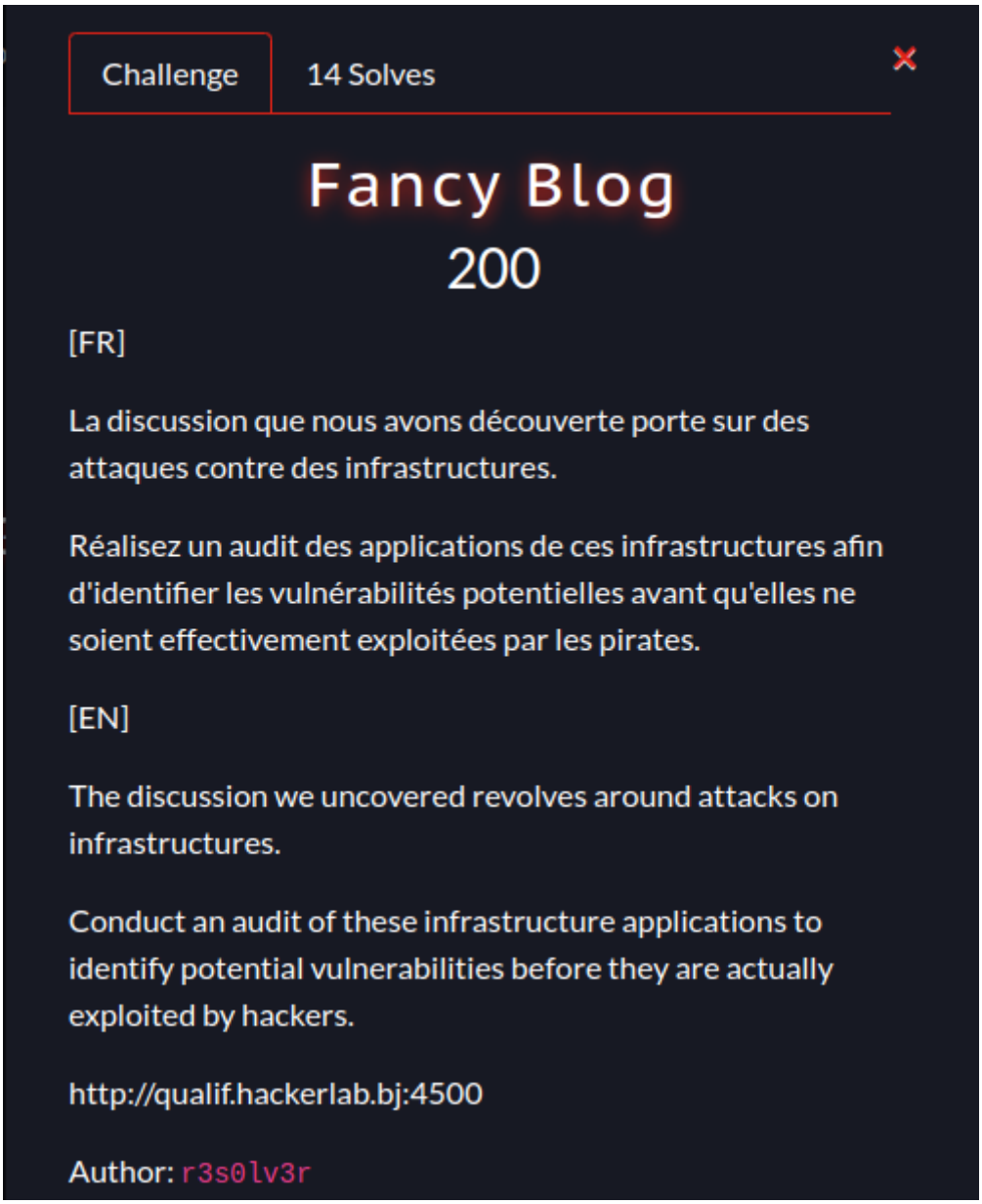
Writeup pour le challenge Fancy Blog de la phase de qualification pour le Hackerlab2024

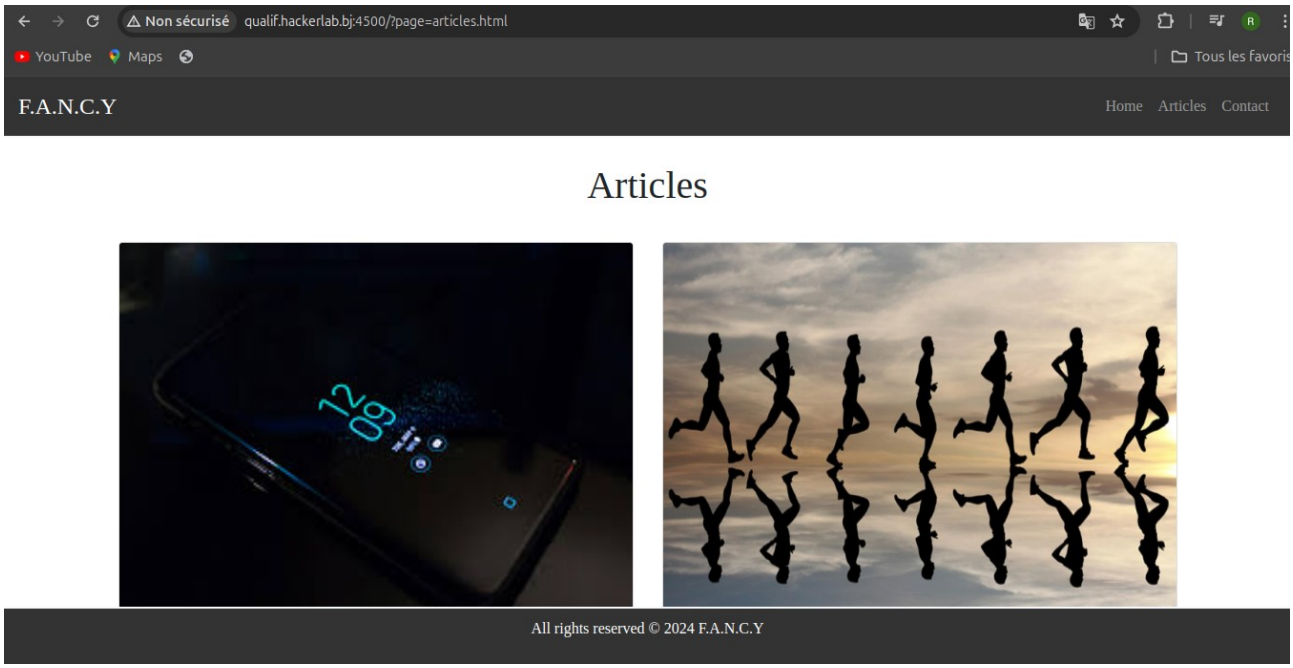
Nom d'utilisateur : takeoff
E-mail : robertohoungbo@gmail.com
Affiliation : IFRI
Pays : Bénin



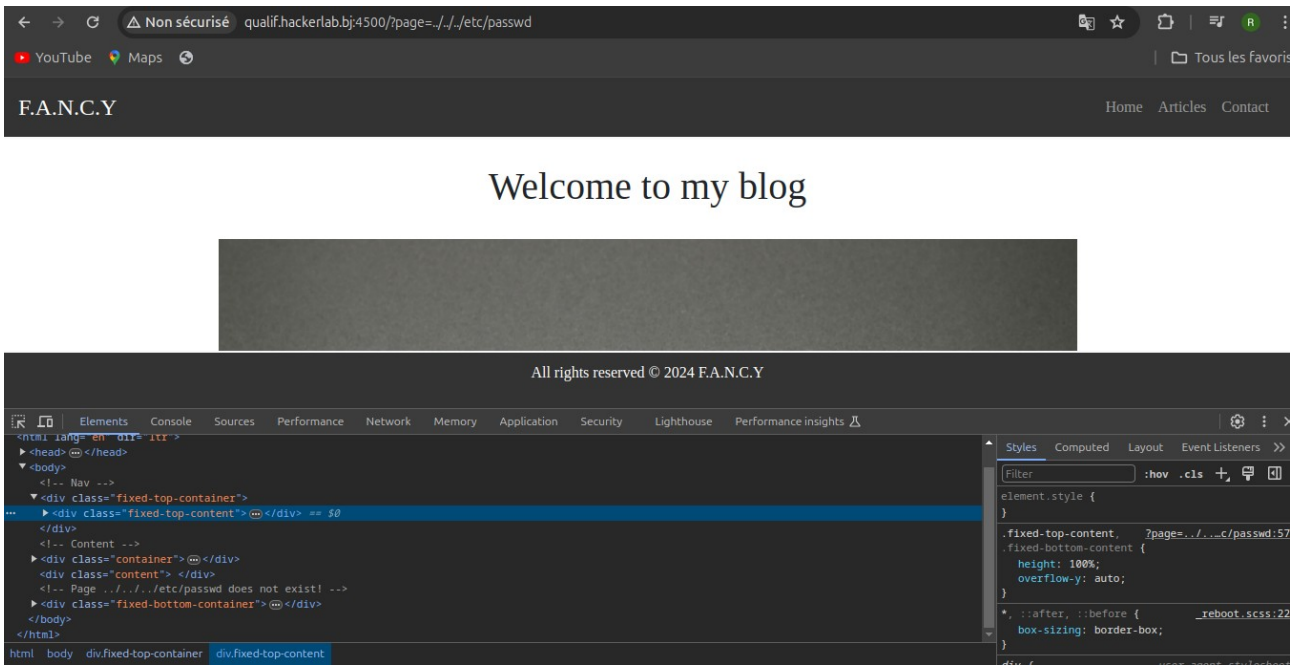
Ce challenge est en lien avec le challenge précédent Trailer. A la fin de ce dernier j'avais découvert le pdf d'une discussion sur l'attaques d'infrastructures critiques du Bénin.

Le but du challenge est de mener un audit sur lesdites infrastructures afin d'identifier des vulnérabilités potentielles.

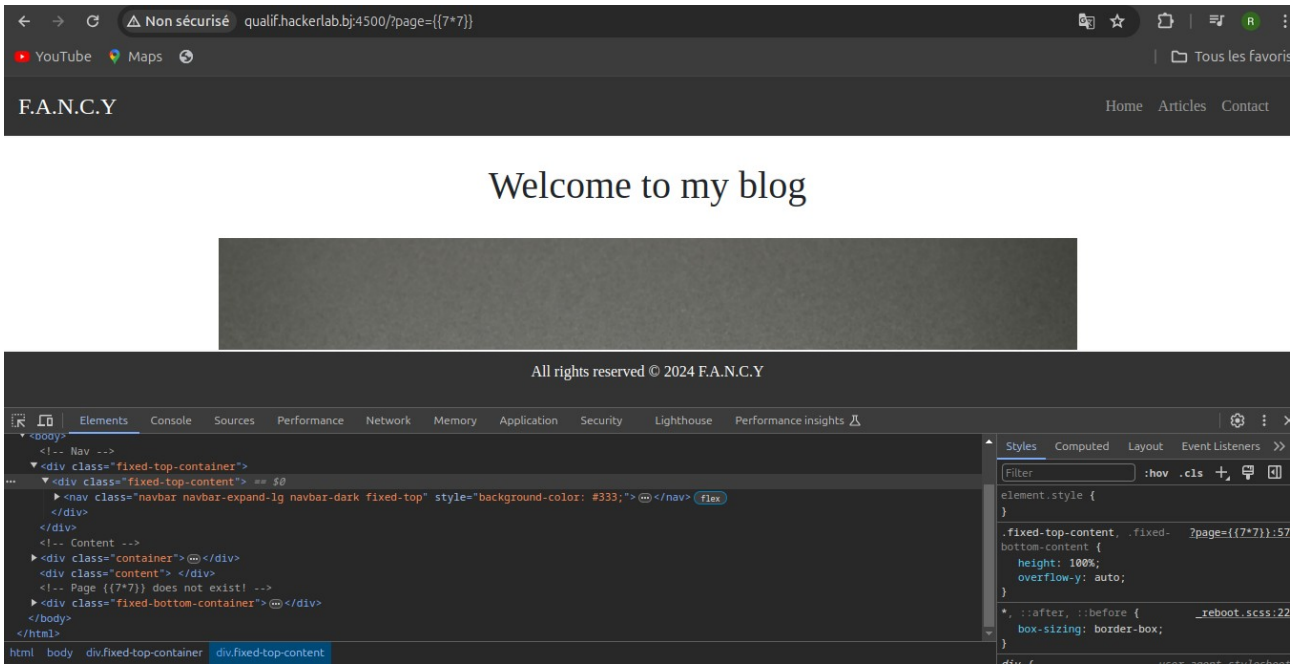
Je me suis rendu sur le lien et j'ai découvert un blog avec trois pages de navigation. Après une reconnaissance des lieux quelque chose a vite attiré mon attention, il s'agit du paramètre ?page de l'url qui permet de changer de page en renseignant le nom de la page cible.



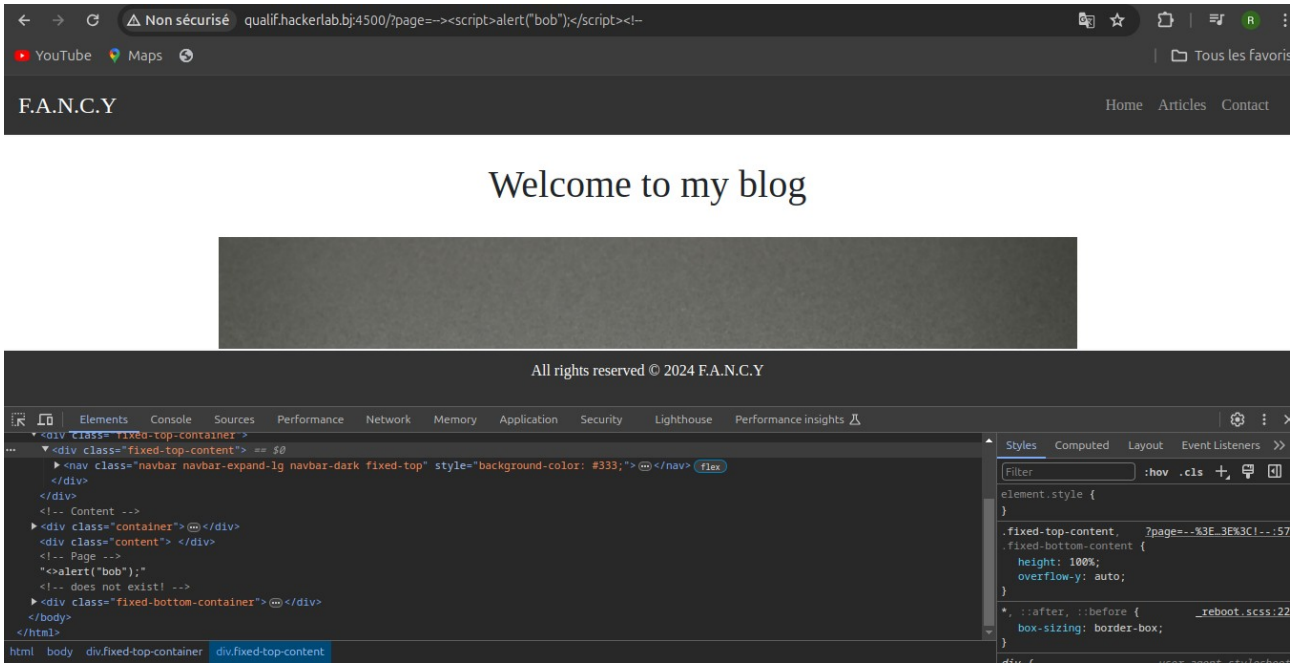
J'ai alors pensé à une vulnérabilité de LFI(Local File Inclusion) et j'ai essayé une longue liste de payloads LFI sans succès, à chaque fois j'étais redirigé vers la page home. Cependant, il y avait quelque chose d'étrange. Lorsque je suis redirigé vers home après avoir renseigné une page qui n'existe pas, je voyais la valeur de mon entrée apparaître en commentaires sur la page home lorsque je consulte l'inspecteur.



Tout d'abord j'ai cru à du SSTI(Server Side Template Injection) vu que la valeur était réfléchie sur la page j'ai donc essayé des payloads comme {{7*7}} mais rien n'y faisait, l'entrée n'était pas interprétée par le navigateur. J'ai vite abandonné cette piste après l'échec des payloads.

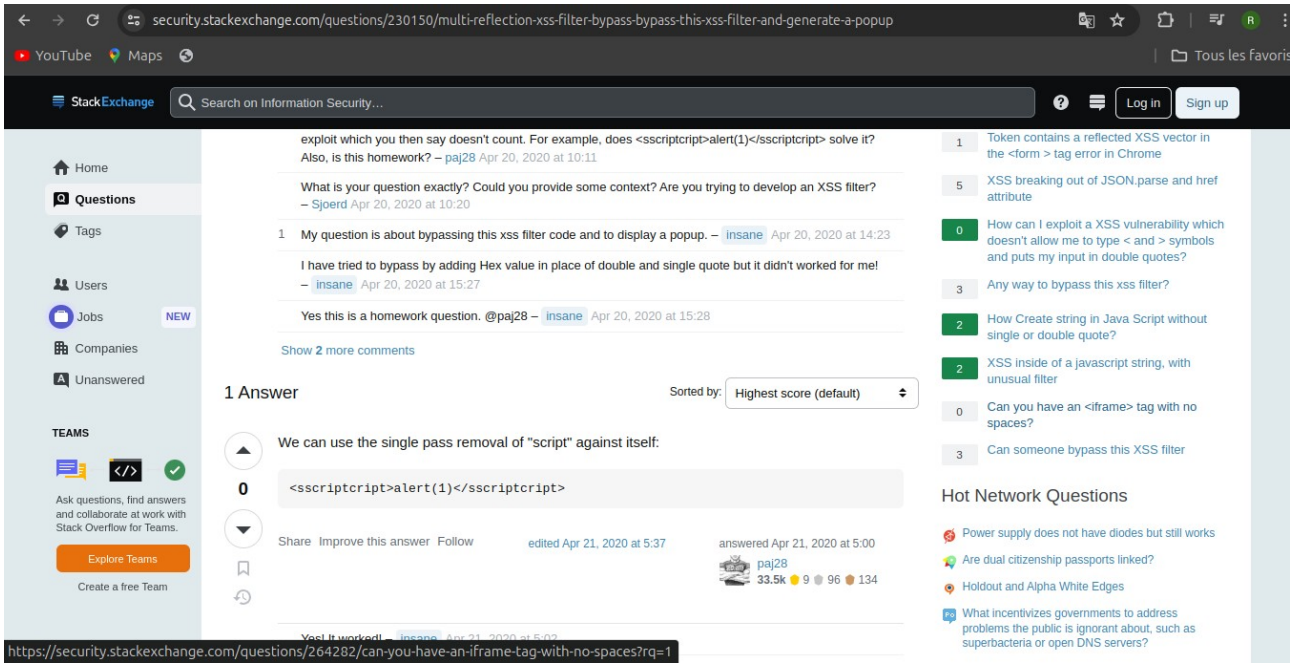


Il ne me restait plus qu'un type d'attaque qui pouvait aboutir, et c'était l'attaque par XSS Réfléchie(Reflected Cross Site Scripting). Vu que ma valeur apparaissait sur la page mais sous forme de commentaires, j'ai contourné les commentaires avec le payload suivant : --><script>alert("bob");</script><!--



Les commentaires ont bien été contournés mais on dirait qu'il y a un filtre sur le mot script qui est remplacé par rien. J'ai alors cherché un payload adéquat pour contourner ce filtre. A force de chercher je suis tombé sur le lien suivant :

https://security.stackexchange.com/questions/230150/multi-reflection-xss-filter-bypass-bypass-this-xss-filter-and-generate-a-popup



J’ai utilisé le payload à la fin de l’article et boom j’ai eu le flag.

FLAG : HLB2024{XSS_INJ3CT10N_1n_C0MM3N7_8898))69}

Merci !