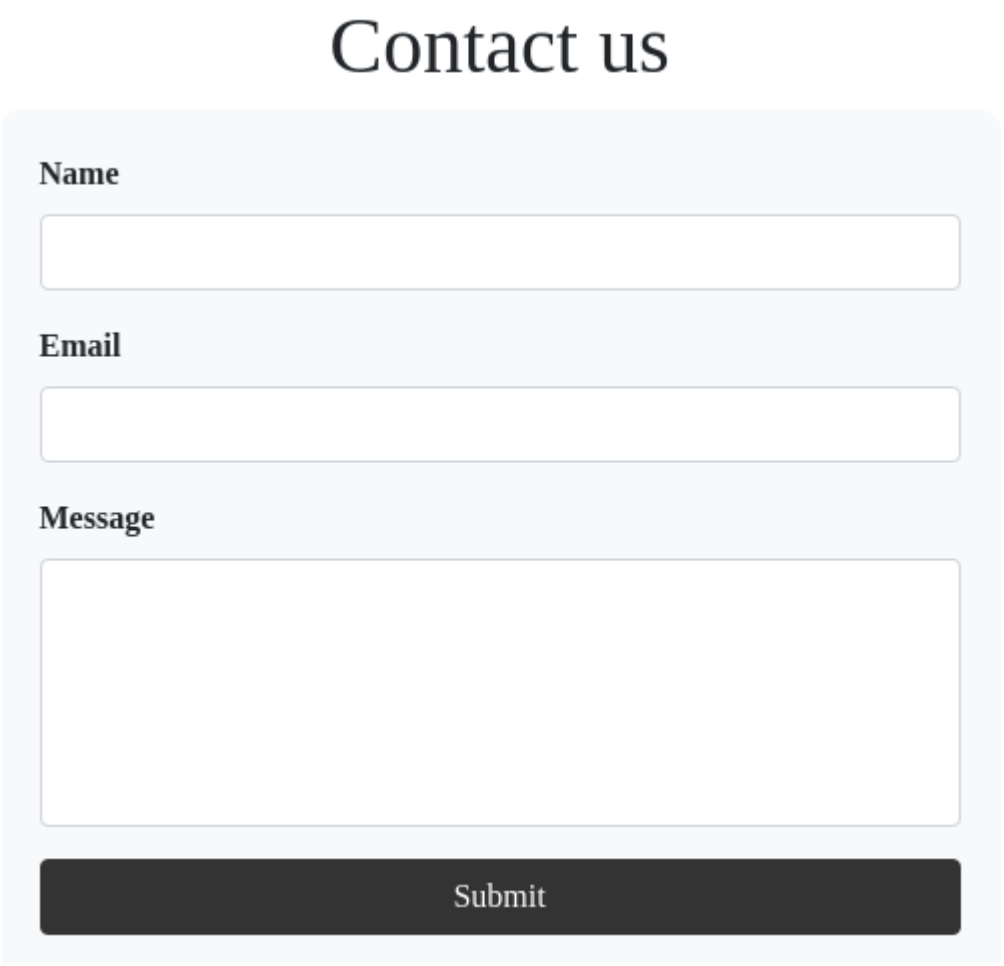
Korp_station

Writeup pour Fancy Blog

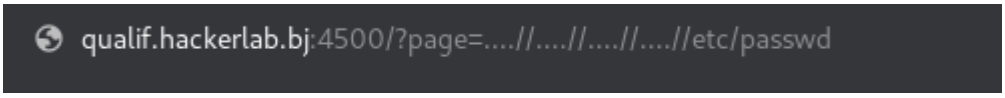
Le lien nous mène vers un site nous m-ne vers un site simple avec trois pages index,articles et contact.html.

Ce n'était pas vraiment un défi difficile mais j'ai passé beaucoup de temps à identifier la vulnérabilité.

1ère tentative : xxs dans le formulaire de contact pour obtenir le cookie (perte de temps)

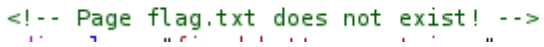


2ème tentative : Path Traversal dans le paramètre page (perte de temps)



3ème tentative : XSS dans le paramètre page

En faisant le path traversal j'ai constaté ce commentaire dans la réponse



Ce qui montre clairement que le paramètre page était vulnérable à du Refleted XSS car il renvoie directement les données que nous avons soumis dans la réponse. J'envoie une alerte classique et je constate que notre entrée est filtrée et qu'on ne pouvait pas utiliser directement les scripts habituels. Évasion du filtre OWASP pour XSS nous donne des commandes à essayer pour échapper ces filtres. Après plusieurs essaies

GET /?page=--><sscriptcript>alert('XSS')</sscriptcript> HTTP/1.1 voilà la commande que j'ai envoyé pour obtenir le flag HLB2024{XSS_INJ3CT10N_1n_C0MM3N7_8898))69}