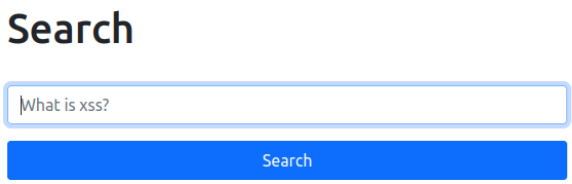
XSS

1.1 Reflected XSS;

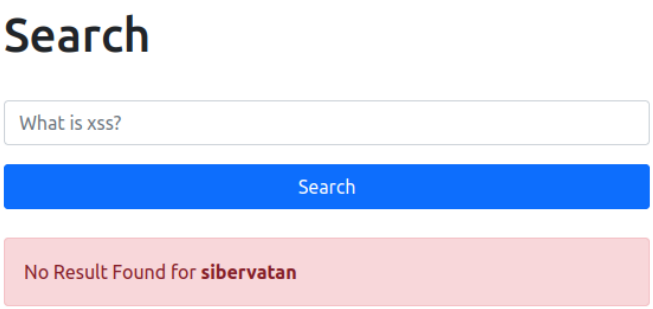
Reflected XSS Nedir; **Reflected XSS**, kullanıcıdan gelen zararlı girdilerin doğrulanmadan web sayfasına yansıtıldığı bir güvenlik açığıdır. Bu saldırıda zararlı kod, genellikle bir URL parametresi aracılığıyla tarayıcıda çalıştırılır. Sonuç olarak, saldırgan kötü niyetli işlemler gerçekleştirebilir.
Nasıl Önlenir ;Önlenmesi: Kullanıcı girdilerini doğrulayıp temizlemek, HTML kodlaması yapmak ve güvenlik politikaları (**CSP**) kullanmak bu tür saldırıları önleyebilir.

CTF ÇÖZÜMÜ



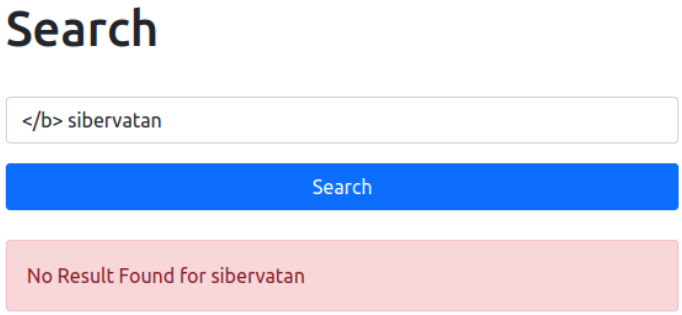
Bu şekilde bir arama motorumuz var , buraya “ **sibervatan** “ yazalım.

Sonuç bulamadı dedi,herhangi bir sonuca varmamız mı gerekiyor bilgim yok, ancak verdiğimiz inputu string değerini yani sibervatan değerimizi sayfa kaynağında nasıl tutuyor bakalım.



```
<div class="alert alert-danger mt-4" role="alert">
      No Result Found for <b>sibervatan</b>
    </div>
```

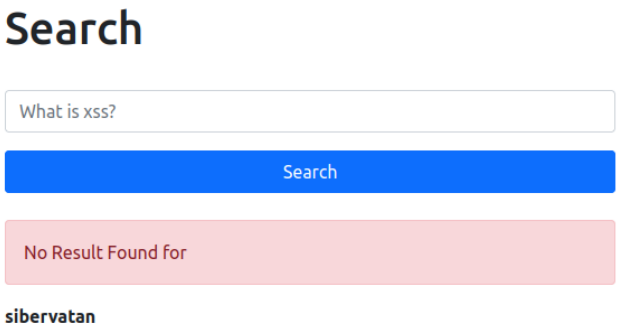
Div etiketleri içerisinde <b> etiketi içerisinde tutuyor bunu buradan çıkarmaya çalışalım başta b etiketinden başlayalım. Amacımız yansıtmak ama öğrenelim.



Sayfa kaynağını inceliyelim.

```
<div class="alert alert-danger mt-4" role="alert">
      No Result Found for <b></b> sibervatan</b>
    </div>
```

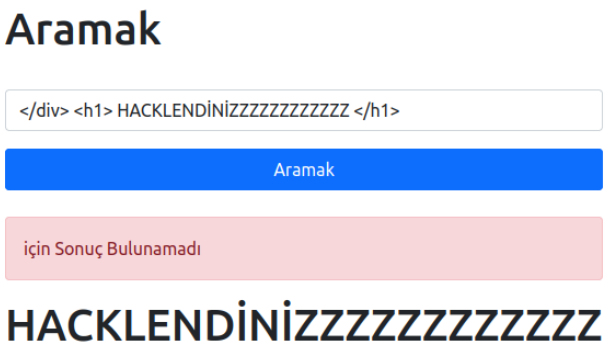
Kod dizimi bu şekilde oldu ancak div içerisinden ekrana bir şey yansıtamıyoruz, birde etiketini kapatmayı deniyelim.



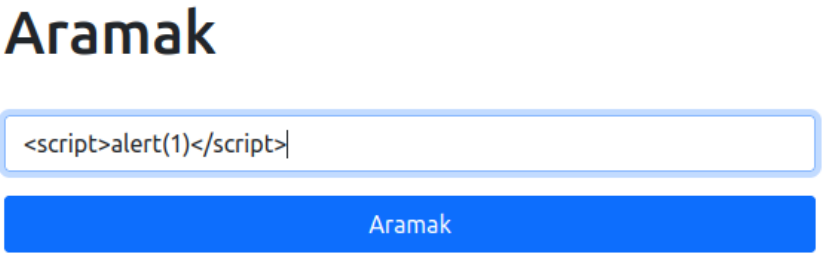
Ekrana sibervatan çıktısını bastırdık F5 çeksemde gitmiyor yazı ancak bu sadece bende gözüküyor, arka planına göz atalım birde.

```
    <div class="alert alert-danger mt-4" role="alert">
          No Result Found for <b></div> sibervatan</b>
        </div>
</div>
```

Burada etiketi class fonksiyonu ile başlayıp resimde ki en alt satırda kapanmış fonksiyon ve dizi kapanıyor, ama biz burada kapanması gereken fonksiyonu daha erken kapatıyoruz ve bir adet fazlalık oluyor bu şekilde ekrana yazı yazımızı yazdırabiliyoruz. Bunu istersek daha fantastik şekilde kullanabiliriz;



Ve çözüme geçelim.



Bu bir javascript kodudur, herhangi bir zararı yok sadece backend kısmına müdahalede bulunabiliyor muyuz diye kontrol ettiğimiz basit bir xss 101 seviye payload çeşitidir, amacı ekrana alert fonksiyonu ile ekrana 1 uyarısını verdirmek. "<script>" ifadesini kullanmamızın nedeni ise, bu kodun çalışması için azönce ki gibi html de div kapatmıştık, burada da javascript bloğu açıyoruz.

Cevabımız; **<script>alert(1)</script>**