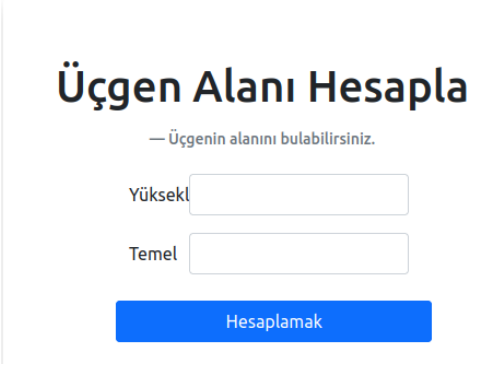
# XSS

**1.3 DOM-Based XSS Nedir;** Kötü niyetli bir kullanıcının web sayfasının Document Object Model'ine (DOM) müdahale ederek zararlı JavaScript kodlarını çalıştırmasıyla oluşan bir güvenlik açığıdır. Bu tür XSS saldırılarında, kötü amaçlı kod sunucudan değil, kullanıcı tarayıcısındaki sayfa yapısından gelir.
**Önlem ;** Bu saldırıyı önlemek için, JavaScript ile kullanıcıdan gelen veriler işlenirken güvenlik kontrolleri yapılmalı ve `innerHTML` gibi tehlikeli fonksiyonlar yerine `textContent` veya güvenli DOM API'leri kullanılmalıdır. Ayrıca, dış kaynaklardan gelen veri girişleri her zaman güvenli hale getirilmelidir.

## ÇÖZÜM

Matematiksel işlem kullanarak Üçgenin alanını hesablamak için bir sayfa bizi karşılıyor buraya int değer girmemizi istiyor. Deniyelim ve verecek output sonuca bakalım yorum yapalım.





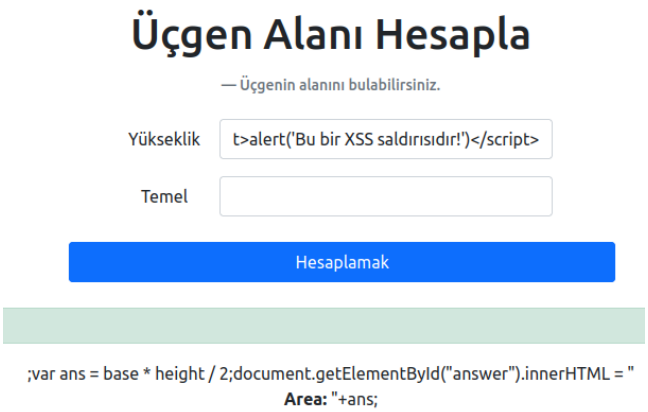
100 e 50 girdim ve hesaplayım bana Üçgenin alanını verdi "2500" müş.
Kaynak koduna baktığım zaman 2500 ü bulamıyorum çünkü veritabından hesaplayıp getiriyor, o kadar bir backendi görmemiz mümkün değil doğal olarak ama güvenlik zafiyetleri ile müdahele edebiliyoruz.
Eğer kaynak kodda yoksa ve input alanımız int istiyorsa hiç bunlara bulaşmadan url'e göz atalım urlde neler oldu neler bitti.

1.hackviser.space/?height=100&base=50

Verdiğimiz değerleri urlde gösteriyor kullanıcıdan aldığı backend kısmında height ve base değişkenleri kullanılıyor buralar normalde null boştur , kullanıcıdan veriyi ister biz verdik ve değişkenlerimiz ile birlikte verdiğimiz int değer karşımızda.

Genelde = eşittir sonrası bir int değer geldiğinde aklımıza , xss ,idor , sql gelir.
Veya = eşittir sonrası bir path varsa burda da genelde LFI RFI zafiyetleri aklımıza gelebilir.
Biz buradan makinemizin xss olduğunu bilerek xss den devam edelim.
Ama atladığımız bir kısım oldu bizden istedği değer alanına payloadımızı yazalım ve response bir bakalım.

.




Hesablamıyor ve payloadımız'da çalışmadı urlden devale edelim.

e/?height=alert(1)&base=50

Payloadımı height değişkenin içerisine enjekte ettim ve entere basalım bakalım ne olucak.


Eğer 2 değişkene de payload girersek ilk 1. değişkeni sonra 2. değişkeni ekrana verdiricek.

=alert(1)&base=alert(2)

**Cevap:** **alert(1)**