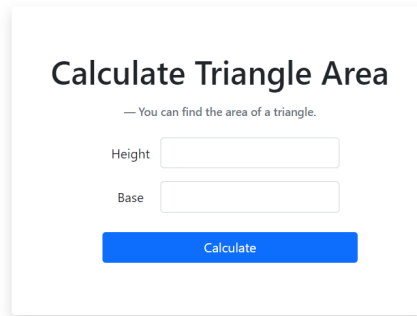


Cross-Site Scripting (XSS)/DOM-Based XSS

Herkese selamlar bu yazımda [Hackviser](#) üzerinde bulunan Web security lablarından biri olan **Cross-Site Scripting (XSS)/DOM-Based XSS labının** çözümünü anlatacağım.

Öncelikle sayfaya gittiğimiz zaman bizi aşağıdaki gibi bir ekran karşılıyor



Sayfanın genel içeriği üçgende alan hesabına dayanıyor.

Acaba kaynak kodu nasıldır diye bir bakıyorum(CTRL U)

```
<div class="row mb-4 justify-content-center">
  <label for="base" class="col-sm-2 col-form-label">Base</label>
  <input type="text" class="form-control w-50 justify-content-center" name="base" id="base">
</div>

<div class="row mb-3 d-grid" style="margin-left:9vh;margin-right:5.5vh;">
  <button class="btn btn-primary" type="submit">Calculate</button>
</div>
</form>

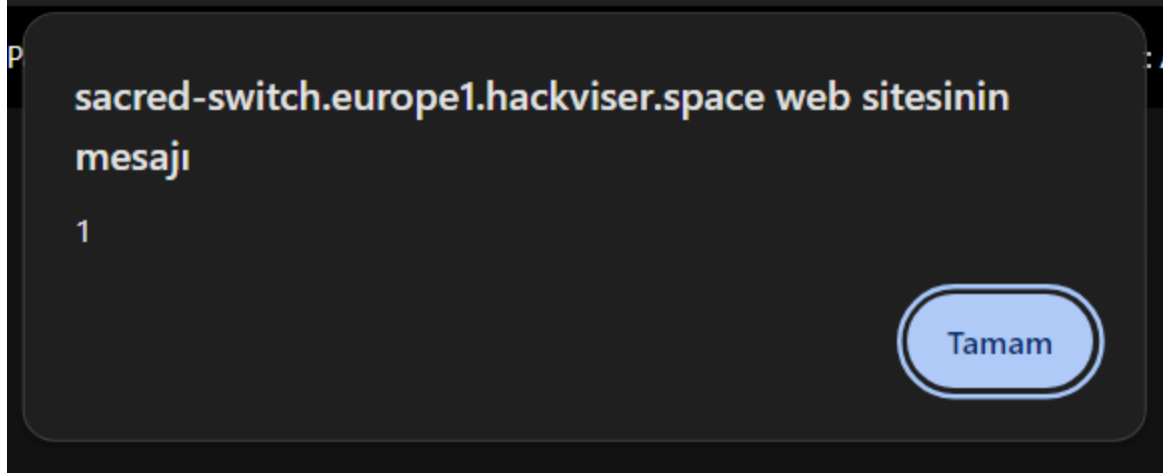
<div class="row justify-content-center text-center mt-4">
  <div class="alert alert-success" id="answer" role="alert" style="text-align: center;"></div>
  <div><script>var height = alert(1);var base = alert(1);var ans = base * height / 2;document.getElementById("answer").innerHTML = "<b>Area:</b> " +ans;</script> </div>
</div>
</body>
</html>
```

Ve burada "Height" ve "Base" kısımlarına girilen inputların herhangi bir filtrelemeden geçmediğini görüyorum

Benim buradaki alana yazacağım herhangi bir ifade direkt olarak script içerisinde işleme alınacak. Bende bu durumu test etmek için `alert(1)` kodunu yazıyorum.

The screenshot shows a web form titled "Calculate Triangle Area" with the subtitle "— You can find the area of a triangle." It has two input fields: "Height" and "Base", both containing the text "alert(1)". Below the inputs is a blue "Calculate" button. At the bottom, a green box displays the result "Area: NaN", indicating that the browser attempted to calculate the area using the injected script instead of treating it as a string.

Benim yazdığım kod parçası herhangi bir filtrelemeye tabii tutulmadığı için direkt işleme alındı ve aşağıdaki gibi bir uyarı aldık



Umarım bu yazıyı sıkılmadan okumuşsunuzdur. Keyifli çalışmalar.