XSS (Cross-Site Scripting) Nedir ve Nasıl Korunulur?

# 📌 XSS (Cross-Site Scripting) Nedir?

XSS (Cross-Site Scripting), kötü niyetli kişilerin bir web uygulamasına zararlı script kodları enjekte ederek diğer kullanıcıların tarayıcılarında bu kodları çalıştırmasına neden olan güvenlik açığıdır.

# 🧠 XSS Türleri

- Stored XSS: Zararlı kod sunucuya/veritabanına kalıcı olarak kaydedilir.

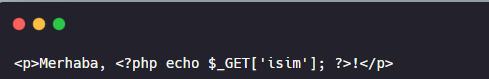
- Reflected XSS: Zararlı kod, URL ile gönderilir ve doğrudan kullanıcıya yansıtılır.

- DOM-Based XSS: Zararlı kod, JavaScript ile DOM üzerinde işlenerek oluşur.

# 🧪 Örnek Senaryo (Reflected XSS)

Zayıf Kod:

<p>Merhaba, <?php echo $\_GET['isim']; ?>!</p>



Zararlı URL:

[https://site.com/?isim=<script>alert('XSS')</script](https://site.com/?isim=%3cscript%3ealert('XSS')%3c/script)>

metin, ekran görüntüsü, yazı tipi, grafik içeren bir resim

Yapay zeka tarafından oluşturulmuş içerik yanlış olabilir.

Sonuç: Kullanıcı bu bağlantıya tıkladığında tarayıcıda bir uyarı kutusu (alert) görünür.

# 🛠️ Korunma Yöntemleri

- Girdi doğrulama (input validation)  
- Çıktı kodlama (output encoding)  
- Content Security Policy (CSP) kullanımı  
- HTTPOnly ve Secure cookie ayarları  
- Framework'lerin güvenlik özelliklerini kullanma

# 💡 Güvenli Kod Örneği (PHP)

<p>Merhaba, <?php echo htmlspecialchars($\_GET['isim'], ENT\_QUOTES, 'UTF-8'); ?>!</p>

metin, ekran görüntüsü, yazı tipi içeren bir resim

Yapay zeka tarafından oluşturulmuş içerik yanlış olabilir.

# 📎 Sonuç

XSS, özellikle kullanıcı girdilerinin işlendiği web uygulamalarında çok sık karşılaşılan bir açıklıktır. Doğru giriş doğrulama ve çıktılarda kodlama işlemleri ile bu tür saldırılara karşı etkili şekilde korunmak mümkündür.