Testing for JavaScript Execution (JavaScript Yürütme Testi)

Summary (Özet)

Bir JavaScript enjeksiyonu güvenlik açığı, kurbanın tarayıcısının içindeki uygulama tarafından yürütülen keyfi JavaScript kodunu enjekte etme yeteneğini içeren bir çapraz site komut dosyası (XSS) alt türüdür. Bu güvenlik açığı, kurbanı taklit etmek için kullanılabilecek bir kullanıcının
oturum çerezlerinin ifşası gibi birçok sonuç doğurabilir veya daha genel olarak, saldırganın mağdurlar tarafından görülen sayfa içeriğini veya uygulamanın davranışını değiştirmesine izin verebilir.

JavaScript enjeksiyonu güvenlik açıkları, uygulama uygun kullanıcı tarafından sağlanan giriş ve çıkış doğrulamasından yoksun olduğunda ortaya çıkabilir. JavaScript, web sayfalarını dinamik olarak doldurmak için kullanıldığından, bu enjeksiyon bu içerik işleme aşamasında gerçekleşir ve sonuç olarak kurbanı etkiler.

Bu güvenlik açığını test ederken, bazı karakterlerin farklı tarayıcılar tarafından farklı muamele gördüğünü düşünün. Referans olarak, DOM tabanlı XSS'ye bakın.

İşte değişkenin herhangi bir doğrulamasını yapmayan bir senaryo örneği `rr`. . Değişken, sorgu dizisi aracılığıyla kullanıcı tarafından sağlanan girdi içerir ve ayrıca herhangi bir kodlama biçimi uygulamaz:

```
var rr = location.search.substring(1);
if(rr) {
   window.location=decodeURIComponent(rr);
}
```

Bu, bir saldırganın aşağıdaki sorgu dizesini göndererek JavaScript kodunu enjekte edebileceği anlamına gelir: `www.victim.com/?javascript:alert(1)`. .

Test Objectives (Test Hedefleri)

- Pusuları ve olası JavaScript enjeksiyon noktalarını belirleyin.

How To Test (Nasıl Test Edilir)

Aşağıdakileri göz önünde bulundurun: DOM XSS egzersizi

Sayfa aşağıdaki senaryoyu içerir:

```
<script>
function loadObj(){
   var cc=eval('('+aMess+')');
   document.getElementById('mess').textContent=cc.message;
}

if(window.location.hash.indexOf('message')==-1) {
   var aMess='({"message":"Hello User!"})';
} else {
   var aMess=location.hash.substr(window.location.hash.indexOf('message=')+8
}
</script>
```

Yukarıdaki kod bir kaynak içerir `location.hash` Bu, doğrudan içine enjekte edebilen saldırgan tarafından kontrol edilir. `message` Kullanıcı tarayıcısının kontrolünü ele geçirmek için bir JavaScript Koduna değer verin.