

# Test File Permission (Dosya İznini Test Et)

## Summary (Özet)

Bir kaynak, gerektiğinden daha geniş bir oyuncu yelpazesine erişim sağlayan bir izin ayarı verildiğinde, hassas bilgilerin maruz kalmasına veya bu kaynağın istenmeyen taraflarca değiştirilmesine yol açabilir. Bu, kaynak program yapılandırması, yürütme veya hassas kullanıcı verileri ile ilgili olduğunda özellikle tehlikelidir.

Açık bir örnek, yetkisiz kullanıcılar tarafından yürütülebilen bir infaz dosyasıdır. Başka bir örnekte, bir API'ye erişmek için hesap bilgileri veya bir belirteç değeri - modern web hizmetlerinde veya mikro hizmetlerde giderek daha fazla görülür - izinleri varsayılan olarak kurulumdan dünyaca okunacak şekilde ayarlanmış bir yapılandırma dosyasında saklanabilir. Bu tür hassas veriler, ev sahibinin iç kötü niyetli aktörleri veya hizmeti diğer güvenlik açıklarıyla tehlikeye atan ancak yalnızca normal bir kullanıcı ayrıcalığı elde eden uzak bir saldırgan tarafından ortaya çıkabilir.

## Test Objectives (Test Hedefler)

- Herhangi bir haydut dosya iznini gözden geçirin ve tanımlayın.

## How to Test (Nasıl Test Edilir)

Linux'ta, kullanın `ls` Dosya izinlerini kontrol etmek için emir. Alternatif olarak, `namei` Dosya izinlerini tekrarlamak için de kullanılabilir.

```
$ namei -l /PathToCheck/
```

Dosya izni testi gerektiren dosyalar ve dizinler aşağıdakileri içerir ancak bunlarla sınırlı değildir:

- Web dosyaları/yönlendirme
- Yapılandırma dosyaları/yönlendirme
- Hassas dosyalar (şifreli veriler, şifre, anahtar) / yönerge

- Günlük dosyaları (güvenlik kayıtları, çalışma günlükleri, yönetici günlükleri) / yönerge
- Yürütülebilir maddeler (sıralar, EXE, JAR, sınıf, PHP, ASP) / yönetmenlik
- Veritabanı dosyaları/yönlendirme
- Templi dosyalar / yönerge
- Dosyaları / yönergeyi yükleyin

## **Remediation (Düzeltilme)**

Yetkisiz kullanıcıların kritik kaynaklara gereksiz yere erişememesi için dosya ve dizinlerin izinlerini uygun şekilde ayarlayın.

## **Tools (Araçlar)**

- Windows AccessEnum
- Windows AccessChk
- Linux namei

## **References (Referanslar)**

- CWE-732: Incorrect Permission Assignment for Critical Resource