

# Dosya Sistemi

### *Amaç*

Herhangi bir sisteme ait yerel dosya sistemine erişimin izinsiz oluşturma, değiştirme veya silinme işlemlerine karşı korunduğundan emin olmak.

### *Etkilenen ortamlar*

Hepsi.

### *Ilgili COBIT Başlıkları*

DS11 – veri değerlendirme – bütün bölümler gözden geçirilmelidir.

DS11.9 – veri işlemede bütünlük

DS11.20 – depolanmış verilerin sürekli bütünlüğü

### *Tanım*

Dosya sistemi, ortalama saldırgan ve betiklerle oynayan yeni yetme saldırgan için en uygun ortamdır. Saldırılar, ortalama bir websitesi için son derece tehlikeli olabilir ve çoğu kere gerçekleştirilebilecek en kolay saldırı biçimidir.

### *En etkili uygulamalar*

- Unix ortamında “chroot” kilitleme kullanın.
- Bütün ortamlarda en az dosya sistem izni verin.
- Mümkünse sadece okunabilir türden dosya sistemlerinin kullanımına ağırlık verin. (CD-ROM veya kilitli USB anahtarları için)

### *tahrifat*

tahrifat, websitesi saldırılarında en fazla kullanılan yöntemlerden biridir. Saldırgan, belli bir program veya teknik kullanarak, saldırganlık içeriğini, mevcut dosyaların veya yapılanış hataları aracılığıyla yeni dosyaların üzerine yükler. Tahrifatın sonucu utanç verici olabilir, çünkü kullanıcının güvenini sarsabilir veya, websitesinin hafife alınmasına neden olabilir.

Internette tahrifatla ilgili bir sürü arşiv bilgisine rastlanabilir. Çoğu tahrifatın nedeni web sunucularında kullanılan yetersiz yamalardır. Ancak diğer en yaygın tahrifat türü, web uygulamalarındaki açıklardır.

Tehlikeye açık olup olmadığınızı saptama

- Sisteminiz güncellenmiş halde mi ?
- Dosya sistemi, web kullanıcısı tarafından web içeriğine (dizin dahil olmak üzere) yazım izni veriyor mu ?
- Uygulama, dosyaları kullanıcının sağladığı dosya adları ile yazıyor mu ?
- Uygulama kullanım dosya sistemi emirleri arıyor mu yoksa uyguluyor mu (örneğin exec() veya xp?cmdshell() gibi) ?
- Herhangi bir uygulama veya dosya sistemi arama işlemi, ek ve izinsiz emirlerin uygulamasına izin veriyor mu ? ayrıntılı bilgi için İS injection bölümüne bakınız.

**Kendinizi koruma**

- Destekleyici işletim sisteminin ve web uygulama ortamının güncel olduğundan emin olun ya da güncellenmesini önerin.
- Uygulama dosyalarının ve kaynaklarının sadece-okunabilir olduğundan emin olun.
- Yerel dosyalarla çalışırken veya dosya kaydedildiğinde kullanıcının sağladığı dosya adlarının uygulama tarafından alınmadığından emin olun.
- Kullanıcının sağladığı bütün girdilerin ek emirlerin çalışmasını engelleyecek şekilde uygulama tarafından kontrol edildiğinden emin olun.

***Yol aykırılığı***

En basitleri hariç bütün web uygulamaları resimleri temalar, diğer betikler, vs. gibi bütün yerel kaynakları içermek durumundadır. Uygulama her kaynak veya dosya içerişinde, bir saldırganın, tarafınızdan izin verilmemiş bir dosya veya sunucudaki kaynağa ulaşabilme riski mevcuttur.

**Tehlikeye açık olup olmadığınızı saptama**

- Dosya açık, dahil, dosya yarat, dosya sil, vs. içeren kodları gözden geçirin.
- Dosyanın sağlıksız kullanıcı girdisi içerip içermediğini saptayın.
- Içeriyorsa, uygulama risk altında demektir.

**Kendinizi koruma**

- Dosya sistemi çağrıları kullanıldığında, kullanıcı girdisi olmaksızın çalışmayı tercih edin.
- Örnek veya dil dosyaları kullanıldığında, dosya adlarının gerçek kısımları yerine indexleri kullanmayı tercih edin.( yani, kullanıcıdan 'Çekoslovak' ummak yerine Çekoslovak=5 değerini alın)
- Kullanıcının yolun bütün kısımlarını sağlayamayacağından, yolu kendi yol kodunuzla çevreleyerek, emin olun
- Sadece iyi olarak bilinenleri kabul ederek kullanıcının girdisini kabul edin- verileri sağlıksız hale getirmeyin.
- Dosyaların bulunabileceği veya kaydedilebileceği yerlerde, kısıtlama amacıyla chrooted jails ve kod erişim kurallarını kullanın.

***Güvenliksiz izinler***

Geliştiricilerin çoğu uygulamalarının çalışması için programı kabaca çalışır hale getirmeyi tercih eder ve sistem yöneticilerinin çoğu ise, izin-veren dosya sistem ACL'lerinin risk oranının farkında değildir.

**Tehlikeye açık olup olmadığınızı saptama**

- Sistemdeki diğer yerel kullanıcılar web uygulaması tarafından kullanılan dosyaları okuma, değiştırme veya silme yetkisine sahip mi ?

Sahipse, büyük olasılıkla uygulama yerel ve uzaktyan gelecek saldırılara açık demektir.

**Kendinizi koruma**

- Web uygulamalarını geliştirme ve yayma sırasında olabilecek en sıkı izinleri kullanın.
- CD-ROMlarda olduğu gibi, web uygulamalarının çoğu sadece-okuma ortamında yayılabilir.
- Sistem yanlış konfigüre etse bile dosya işletimlerinin tür ve yerini denetlemek ve sınırlamak için chroot jails ve kod erişim güvenlik kurallarını kullanmayı gözardı etmeeyin.
- Windows'taki bütün 'Herkes : Tam kontrol' ACLlerini ve Unix'teki tüm mod 777 (dünya yazılabilir dizinleri) veya mod 666 dosyalarını (dünya yazılabilir dizinleri) kaldırın.
- Mümkün olan heryerde dünya yazılabilir izinlerini, 'misafir' ve 'herkes'i ayırmayı gözardı etmeyin.

### *Güvenliksiz indexleme*

Google masaüstü arama motoru ve macintosh Spotlight çok yaygın araçlardır. Bu harika araçlar, kullanıcıların hard sürücüde istedikleri herşeyi bulmalarını sağlar. Aynı harika teknoloji, saldırganlara, uygulamanın derinliklerinde saklı olanları tam olarak saptama fırsatını da sağlar.

### Tehlikeye açık olup olmadığınızı saptama

- Google ve diğer arama motorlarını websitenizde birşeyler, örneğin meta tag veya saklı dosya, vs. aramak için kullanın.
- Dosya bulunuyorsa, uygulamanız tehlikede demektir.

### Kendinizi koruma

- robots.txt kullanın– bu, arama motorlarının çoğunun düşündüğünüzün dışında birşeyler aramasını engelleyecektir.
- Websitenizde kullandığınız arama motorunun aktivitelerini sık sık denetleyin, örneğin IIS arama motoru, Sharepoint, google appliance, vs.
- Websitenizde aranabilir bir index'e ihtiyacınız yoksa, kullanıma açılmış olabilecek bütün arama fmksiyonlarını iptal edin.

### *Eşlenmemiş dosyalar*

Web uygulama iskeletleri, sadece kendi dosyalarını kullanıcıya yorumlatacak, diğer uygulamaların tümünü HTML veya sadece yazı dosyası olarak gösterecektir. Bu ise, saldırganın başarıyla saldırabileceği gizlilikleri ve konfigürasyonu açığa çıkaracaktır.

#### Tehlikeye açık olup olmadığınızı saptama

Config.xml veya benzeri, normalde görümez olan bir konfigürasyon dosyasını yükleyin ve web browseri kullanarak açmaya çalışın. Dosya içeriği görünürse veya ortaya çıkarsa, uygulamanız tehlikede demektir.

#### Kendinizi koruma

- Web köküne ait olmayan bütün dosyaları silin veya başka yere aktarın.
- Içerik dosyalarını normal uzantı olacak şekilde yeniden adlandırın(örneğin foo.inc → foo.jsp veya foo.aspx)
- .xml, .cfg gibi, kalması gereken bütün dosyaları, dosya içeriklerini göstermeyecek bir hata işleyici veya renderera eşleyin. Bu işlemin, uygulama iskeletinin konfigürasyon alanında ve/veya web sunucunun konfigürasyonunda yapılması gerekebilir.

### *Geçici dosyalar*

Uygulamalar genelde sonuc veya raporlari dıske yazmak durumundadır. Geçici dosyalar izinsiz kullanıcıların eline geçerse özel bilgilere de giriş yapabilirler veya saldırının boyutuna bağlı olarak, saldırganı izinli kullanıcı haline getirebilirler.

#### Tehlikeye açık olup olmadığınızı saptama

Uygulamanızın geçici dosyaları kullanıp kullanmadığını saptayın. Kullanıyorsa, aşağıdakileri kontrol edin :

- dosyalar web kaynağında mı yeralıyor ? öyle ise, sadece browser aracılığıyla erişilmesi mümkün mü ? öyle ise, giriş yapılmadan da dosyalara erişmek mümkün mü ?
- eski dosyalar açıkta mı ? eski dosyaları silip atacak bir sistem veya benzeri bir mekanizma var mı ?
- Dosyalara erişim uygulamaya erişim anlamına geliyor mu veya özel bilgilere mi ulaşılıyor ?

Tehlikeye açık olma seviyesi verilerin kabul ediliş sınıflandırmasından türetilmektedir.

**Kendinizi koruma**

Geçici dosya kullanımı sadece izinsiz erişime karşı koruma açısından önemli değildir. Orta-yüksek risk kullanımı için, özellikle dosyalar uygulamanın iç işleyişine veya özel kullanıcı ilgilerine erişirse, aşağıdaki kontroller gözönüne alınmalıdır :

- Geçici dosya rutinleri, işlem sırasında içeriği oluştururken dosya sistemine depolanma yerine yeniden yazılmalıdır.
- Bütün kaynakların izinsiz kullanıcılarr tarafından ulaşılamaz olduğundan emin olun ve kullanıcıların sadece kendi dosyalarına girme iznine sahip olmalarını sağlayın.
- Geçici dosyaları silmek için, örneğin her 20 dakikada veya belli bir sürede veya işlem sonunda silinen dosyaları toplayan bir sistem kullanın.
- Unix türü işletim sistemlerinde yeralıyorsa, chroot jails kullanarak uygulamayı birincil işletim sisteminden izole edin. Windows sisteminde ise, ACL desteği ile IIS kullanıcılarının dosyalara doğrudan erişimini veya dosyaların üzerine yeni bilgi girmelerini engelleyin.
- Dosyaları web kaynağı dışına taşıyarak sadece-browserdan kaynaklanan saldırıları engelleyin.
- Tehlike seviyesi yüksek  ikiyüzlü saldırıları azaltmak için rastgele dosya adları kullanın.

***Eski, referanslandırılmamış dosyalar***

Sistem yöneticileri ve geliştiricilerin  geçici eski dosya yaratmak için düzenleyici programlar veya diğer araçları kullanması yaygındır. Bu dosyaların uzantıları veya erişim kontrol izinleri değişirse, saldırgan kaynak ve konfigürasyon verilerini okuyabilir.

**Tehlikeye açık olup olmadığınızı saptama**

Dosya sistemini aşağıdaki kalemler için kontrol edin :

- Düzenleyici programlar veya çalışmayan programlarca yaratılmış geçici dosyalar (core, ~foo, blah.tmp, vs. gibi)
- 'Yedek', 'eski' veya 'kopya' adlı dosyalar
- foo.php.old türü ek uzantılı dosyalar
- ara sonuçlu geçici dosyalar

**Kendinizi koruma**

- dosyaların eski kopyalarını saklamamak için kaynak kodu kontrolü kkullanın.
- Web kaynağındaki bütün dosyaların gerçekten gerekip gerekmediğini periyodik olarak kontrol edin.
- Uygulamanın geçici dosyalarına web kaynağından ulaşmanın imkansız olduğundan emin olun.

***Ikinci tür içeri atma? Second Order Injection***

Web uygulaması başka bir işlem, diyelim kesikli veya zamanı belirlenmiş bir işlem tarafından işletiliyorsa, o zaman ikinci işlem saldırıya açık olabilir. Ilk kullanım öncesi geçerli olan girdinin arkadaki işlemde olması az görülen bir uygulamadır.

**Tehlikeye açık olup olmadığınızı saptama**

- Kullanıcının verilerini işlemede uygulama gerideki/kesikli/zamanı belirlenmiş işlemler kullanıyor mu ?
- Bu program kullanıcı girdilerini işletim öncesinde geçerli kılıyor mu ?

**Kendinizi koruma**



- Herşeyin ötesinde programların işletim öncesi kullanıcı girdilerini kontrol ettiğinden emin olun.
- En az imtiyaz ile uygulamayı çalıştırın- özellikle kesikli uygulama son dosya, network veya benzeri için yazma yetkisine gerek duymamalıdır.
- Kaynakları ve arka plandaki uygulamanın kullanabileceği özellikleri kısaltmak/durdurmak için içdil veya işletim sistemi kullanın. Örneğin, kesikli programlar nadiren network erişimine gerek duyar.
- Izinsiz dosya yaratımını saptamak için misafir tabanlı saldırı saptama sistemleri ve virus yoketme sistemleri kullanın.

***Ileri okuma***

- Klein, A., güvenliksiz indexleme http://www.webappsec.org/projects/articles/022805-clean.html
- MySQL dünya okunabilir log dosyaları http://www.securityfocus.com/advisories/3803
- Oracle 8i ve 9i Servlet sunucu dosya görüntülemeye izin verir http://online.securityfocus.com/advisories/3964

**Dökümanın Aslı :** OWASP GUIDE 2.0.1

**Çeviri** **:** Billur C. Yılmazyiğit - info@biledge.com