Test File Extensions Handling for Sensitive Information (Hassas Bilgiler için Dosya Uzantılarının İşlenmesini Test Edin)

Summary (Özet)

Web isteğini yerine getirmek için hangi teknolojilerin, dillerin ve eklentilerin kullanılması gerektiğini kolayca belirlemek için web sunucularında dosya uzantıları yaygın olarak kullanılır. Bu davranış RFC'ler ve Web Standartları ile tutarlı olsa da, standart dosya uzantıları kullanmak, penetrasyon test cihazına bir web cihazında kullanılan temel teknolojiler hakkında yararlı bilgiler sağlar ve saldırı senaryosunu belirli teknolojilerde kullanma görevini büyük ölçüde basitleştirir. Buna ek olarak, web sunucularının yanlış yapılandırılması, erişim kimlik bilgileri hakkında gizli bilgileri kolayca ortaya çıkarabilir.

Uzatma kontrolü genellikle yüklenecek dosyaları doğrulamak için kullanılır, bu da beklenmedik sonuçlara yol açabilir, çünkü içerik beklenen şey değildir veya beklenmedik işletim sistemi işleme nedeniyle.

Web sunucularının farklı uzantılara sahip dosyalara karşılık gelen talepleri nasıl ele aldığını belirlemek, erişilen dosyalara bağlı olarak web sunucusu davranışını anlamanıza yardımcı olabilir. Örneğin, hangi dosya uzantılarının sunucu tarafı yürütmeye neden olanlara karşı metin veya düz olarak iade edildiğini anlamaya yardımcı olabilir. İkincisi, web sunucuları veya uygulama sunucuları tarafından kullanılan teknolojilerin, dillerin veya eklentilerin göstergesidir ve web uygulamasının nasıl tasarlandığı konusunda ek bilgiler sağlayabilir. Örneğin, bir “.pl” uzantısı genellikle sunucu tarafı Perl desteği ile ilişkilendirilir. Ancak, dosya uzantısı tek başına aldatıcı olabilir ve tam olarak kesin olmayabilir. Örneğin, Perl sunucu tarafı kaynakları, gerçekten de Perl ile ilgili oldukları gerçeğini gizlemek

için yeniden adlandırılabilir. Sunucu tarafı teknolojilerini ve bileşenlerini tanımlamak için daha fazla “web sunucusu bileşenleri” ile ilgili bir sonraki bölüme bakın.

Test Objectives (Test Hedefleri)

- Çek veri (örneğin*e.g.*, komut dosyaları, ham veriler, kimlik bilgileri vb.) içeren hassas dosya uzantıları veya uzantılar).
- Belirlenen kurallar üzerinde hiçbir sistem çerçevesinin bulunmadığını doğrulayın.

How to Test (Nasıl Test Edilir)

Forced Browsing (Zorla Tarama)

İstekleri farklı dosya uzantıları ile gönderin ve nasıl ele alındıklarını doğrulayın. Doğrulama web dizini bazında olmalıdır. Senaryo yürütmesine izin veren dizinleri doğrulayın. Web sunucusu dizinleri, tanınmış dizinlerin varlığını arayan araçları tarayarak tanımlanabilir. Ayrıca, web sitesi yapısını yansıtmak, test cihazının uygulama tarafından sunulan web dizinlerinin ağacını yeniden yapılandırmasını sağlar.

Web uygulama mimarisi yük dengeli ise tüm web sunucularını değerlendirmek önemlidir. Bu, dengeleyici altyapının yapılandırılmasına bağlı olarak kolay olabilir veya olmayabilir. Yedek bileşenleri olan bir altyapıda, bireysel web veya uygulama sunucularının yapılandırılmasında hafif değişiklikler olabilir. Bu, web mimarisi heterojen teknolojileri kullanırsa gerçekleşebilir (bir yük dengeleme yapılandırmasında bir dizi IIS ve Apache web sunucusunu düşünün, bu da aralarında hafif asimetrik davranış ve muhtemelen farklı güvenlik açıkları getirebilir).

Örnek

Testçi, adı geçen bir dosyanın varlığını tespit etti `connection.inc`. . Ona doğrudan erişmeye çalışmak, içeriği geri verir, bunlar:

```
<?
   mysql_connect("127.0.0.1", "root", "password")
      or die("Could not connect");
?>
```

Test cihazı, bir MySQL DBM arka ucunun varlığını ve web uygulaması tarafından ona erişmek için kullanılan (zayıf) kimlik bilgilerini belirler.

Aşağıdaki dosya uzantıları hiçbir zaman bir web sunucusu tarafından iade edilmemelidir, çünkü hassas bilgiler veya hizmet edilmesi için hiçbir neden olmayan dosyalarla ilgilidir.

- `.asa`
- `.inc`
- `.config`

Aşağıdaki dosya uzantıları, erişildiklerinde tarayıcı tarafından görüntülenen veya indirilen dosyalarla ilgilidir. Bu nedenle, bu uzantıları olan dosyalar, gerçekten hizmet edilmesi gerektiğini (ve artık olmadıklarını) ve hassas bilgiler içermediklerini doğrulamak için kontrol edilmelidir.

- `.zip`, `.tar`, `.gz`, `.tgz`, `.rar`, vb.: (Sıkışık) arşiv dosyaları
- `.java`: Java kaynak dosyalarına erişim sağlamak için hiçbir neden yok
- `.txt`: Metin dosyaları
- `.pdf`: PDF belgeleri
- `.docx`, `.rtf`, `.xlsx`, `.pptx`, vb.: Ofis belgeleri
- `.bak`, `.old` ve yedekleme dosyalarının göstergesi olan diğer uzantılar (örneğin: `~` Emacs yedekleme dosyaları için)

Yukarıda verilen liste sadece birkaç örneği detaylandırır, çünkü dosya uzantıları burada kapsamlı bir şekilde ele alınamayacak kadar çoktur. Daha kapsamlı bir uzantı veritabanı için FILExt'e bakın.

Belirli bir uzantıya sahip dosyaları tanımlamak için tekniklerin bir karışımı kullanılabilir. Bu teknikler arasında Güvenlik Açığı Tarayıcılar, örümcekleme ve yansıtma aletleri, uygulamayı manuel olarak
inceler (bu otomatik örümceklemedeki sınırlamaların üstesinden gelir), arama motorlarını sorgulamak
(bkz. Test: Örümcek ve google). Ayrıca, “unutulmuş” dosyalarla ilgili güvenlik sorunlarıyla ilgilenen Eski, Yedekleme ve Referanssız Dosyalar için Test yapın.

File Upload (Dosya Yükle)

Windows 8.3 eski dosya işleme bazen dosya yükleme filtrelerini yenmek için kullanılabilir.

Kullanım Örnekleri:

1. `file.phtml` PHP kodu olarak işlenir.
2. `FILE~1.PHT` Servis edilir, ancak PHP ISAPI işleyicisi tarafından işlenmez.
3. `shell.phPWND` Yüklenebilir.
4. `SHELL~1.PHP` OS kabuğu tarafından genişletilecek ve iade edilecek, ardından PHP ISAPI işleyicisi tarafından işlenecektir.

Gray-Box Testing (Gri-Kutu Testi)

Dosya uzantıları işlemeye karşı beyaz kutu testi yapmak, web uygulama mimarisine katılan web sunucularının veya uygulama sunucularının yapılandırmalarını kontrol etmek ve farklı dosya uzantıları sunmaları için nasıl talimat verildiğini doğrulamak için tutar.

Web uygulaması yük dengeli, heterojen bir altyapıya dayanıyorsa, bunun farklı davranışlar getirip getiremeyeceğini belirleyin.

Tools (Araçlar)

Nessus ve Nikto gibi savunmasızlık tarayıcıları, tanınmış web dizinlerinin varlığını kontrol eder. Testçinin web site yapısını indirmesine izin verebilir, bu da web dizinlerinin yapılandırılmasını ve bireysel dosya uzantılarının nasıl sunulduğunu belirlemeye çalışırken yararlıdır. Bu amaç için kullanılabilecek diğer araçlar şunları içerir:

- wget
- Curl
- Google'da "web mirroring tools".