Test Upload of Unexpected File Types (Beklenmeyen Dosya Türlerinin Yüklenmesini Test Edin)

Summary (Özet)

Birçok uygulamanın iş süreçleri, dosya üzerinden gönderilen verilerin yüklenmesine ve
manipülasyonuna izin verir. Ancak iş süreci dosyaları kontrol etmeli ve yalnızca belirli “onaylanmış” dosya türlerine izin vermelidir. Hangi dosyaların “onaylandığına” karar vermek iş mantığına göre belirlenir ve uygulamaya / sisteme özeldir. Bu risk, kullanıcıların dosya yüklemesine izin vererek, saldırganlar, web sitesini tahrip edebilecek, uzaktan komutları yerine getirebilecek, sistem dosyalarına göz atabilecek, yerel kaynaklara göz atabilecek, diğer sunuculara saldırabilecek veya yerel güvenlik açıklarından yararlanabilecek saldırılar yoluyla uygulanabilecek ve uygulamayı veya sistemi olumsuz yönde etkileyebilecek beklenmedik bir dosya türü sunabilir.

Beklenmedik dosya türlerinin yüklenmesiyle ilgili güvenlik açıkları, yüklemenin belirli bir uzantıya sahip değilse bir dosyayı hızlı bir şekilde reddetmesi gerektiği konusunda benzersizdir. Ek olarak, bu, kötü amaçlı dosyaları yüklemekten farklıdır, çünkü çoğu durumda yanlış bir dosya biçimi kendi başına doğal olarak “kötü niyetli” olmayabilir, ancak kaydedilen verilere zarar verebilir. Örneğin, bir uygulama Windows Excel dosyalarını kabul ederse, benzer bir veritabanı dosyası yüklenirse okunabilir, ancak veriler çıkarılmış olarak yanlış konumlara taşınır.

Uygulama, işlem için yalnızca belirli dosya türlerinin yüklenmesini bekliyor olabilir. `.csv` ya da `.txt` Dosyalar. Uygulama, yüklenen dosyayı uzatmaya (düşük güvence dosyası doğrulaması için) veya içerik (yüksek güvence dosyası doğrulama) ile doğrulamayabilir. Bu, uygulama / sistem içinde beklenmedik sistem veya veritabanı sonuçları ile sonuçlanabilir veya saldırganlara uygulama / sistemden yararlanmak için ek yöntemler verebilir.

Example (Örnek)

Bir resim paylaşım uygulamasının kullanıcıların bir yük yüklemesine izin verdiğini varsayalım `.gif` ya da `.jpg` Web sitesine grafik dosya. Ya bir saldırgan bir HTML dosyasını bir ile yükleyebilirse ne `<script>` Etiket mi, PHP dosyası mı? Sistem, dosyayı geçici bir konumdan PHP kodunun artık uygulamaya veya sisteme karşı yürütülebileceği son konuma taşıyabilir.

Test Objectives (Test Hedefleri)

- Sistem tarafından reddedilen dosya türleri için proje belgelerini gözden geçirin.
- İstenmeyen dosya türlerinin reddedildiğini ve güvenli bir şekilde ele alındığını doğrulayın.
- Dosya partisi yüklemelerinin güvenli olduğunu ve belirlenen güvenlik önlemlerine karşı herhangi bir baypasa izin vermediğini doğrulayın.

How To Test (Nasıl Test Edilir)

Specific Testing Method (Özel Test Yöntemi)

- Uygulamaları mantıksal gerekliliklerini inceleyin.
- Dosya içeren dosya içeren dosyaları içeren yükleme için “onaylanmamış” bir dosya kütüphanesi hazırlayın: jsp, exe veya script içeren HTML dosyaları.
- Başvuruda dosya gönderim veya yükleme mekanizmasına gidin.
- Yükleme için “onaylanmamış” dosyayı gönderin ve yüklemelerinin düzgün bir şekilde engellendiğini doğrulayın
- Web sitesinin yalnızca dosya tipini istemci tarafı JavaScript'te kontrol edip etmediğini kontrol edin
- Web sitesinin yalnızca HTTP isteğinde dosya türünü “İçerik Tipi” ile kontrol edip etmediğini kontrol edin.
- Web sitesinin yalnızca dosya uzantısına göre olup olmadığını kontrol edin.
- Yüklenen diğer dosyalara doğrudan belirtilen URL ile erişilip erişilemeyeceğini kontrol edin.

- Yüklenen dosyanın kod veya komut dosyası enjeksiyonu içerip ekleyemeyeceğini kontrol edin.
- Yüklenen dosyalar için herhangi bir dosya yolu olup olmadığını kontrol edin. Özellikle, bilgisayar korsanları ZIP'te belirtilen yol ile dosyaları sıkıştırabilir, böylece fermuarsız dosyalar yüklenip fermuarsız çıktıktan sonra amaçlanan yola yüklenebilir.

Related Test Cases (İlgili Test Vakaları)

- Hassas Bilgiler için Test Dosyası Uzantıları Ele Alın
- Kötü Niyetli Dosyaların Yüklenmesini Test Edin

Remediation (Düzeltme)

Uygulamalar, yalnızca uygulama işlevselliğinin geri kalanının ele almaya ve beklemeye hazır olduğu “kabul edilebilir” dosyaları kabul edecek ve manipüle etmek için mekanizmalarla geliştirilmelidir. Bazı özel örnekler şunları içerir: dosya uzantılarının listelerini reddetmek veya başlıktan “İçerik Tipi” kullanarak veya bir dosya türü tanıyı kullanarak, yalnızca belirtilen dosya türlerini sisteme izin vermek için.

References (Referanslar)

- OWASP - Sınırsız Dosya Yükleme
- Dosya yükleme güvenliği en iyi uygulamaları: Kötü amaçlı dosya yüklemesini engelleyin
- Kötü amaçlı PHP dosyalarını formlar aracılığıyla yükleyen kişileri durdurun
- CWE-434: Tehlikeli Tip ile Sınırsız Dosya Yüklemesi