Test RIA Cross Domain Policy (DEA Çapraz Etki Alanı İlkesini Test Etme)

Summary (Özet)

Zengin İnternet Uygulamaları (RIA), Oracle Java, Silverlight ve Adobe Flash gibi teknolojileri kullanarak veri ve hizmet tüketimine kontrollü çapraz alan erişimine izin vermek için Adobe'nin crossdomain.xml politika dosyalarını benimsemiştir. Bu nedenle, bir alan, hizmetlerine farklı bir etki alanından uzaktan erişim sağlayabilir. Bununla birlikte, genellikle erişim kısıtlamalarını tanımlayan politika dosyaları kötü yapılandırılmıştır. Politika dosyalarının zayıf yapılandırması, Çapraz Site İstek Sahteci saldırıları sağlar ve üçüncü tarafların kullanıcı için hassas verilere erişmesine izin verebilir.

What are cross-domain policy files? (Koordinata meyilli politika dosyaları nelerdir?)

Bir çapraz-domain politikası dosyası, Java, Adobe Flash, Adobe Reader vb. gibi bir web istemcisinin farklı alanlardaki verilere erişmek için kullandığı izinleri belirtir. Silverlight için Microsoft, Adobe'nin crossdomain.xml'inin bir alt kümesini benimsedi ve ayrıca kendi cross-domain politikası dosyasını oluşturdu: clientaccesspolicy.xml.

Bir web istemcisi, bir kaynağın diğer etki alanından talep edilmesi gerektiğini algıladığında, önce başlıklar da dahil olmak üzere yatılı taleplerin gerçekleştirilip gerçekleştirilmediğini belirlemek için hedef alanda bir politika dosyası arayacaktır ve soket tabanlı bağlantılara izin verilir.

Master politikası dosyaları etki alanının kökünde bulunur. Bir müşteriye farklı bir politika dosyası yüklemesi talimatı verilebilir, ancak ana politika dosyasının talep edilen politika dosyasına izin vermesini sağlamak için önce ana politika dosyasını her zaman kontrol edecektir.

Crossdomain.xml vs. Clientaccesspolicy.xml (Crossdomain.xml vs. Clientaccesspolicy.xml)

Çoğu RIA uygulaması crossdomain.xml'yi destekler. Bununla birlikte, Silverlight durumunda, yalnızca crossdomain.xml herhangi bir etki alanından erişime izin verildiğini belirtirse işe yarayacaktır. Silverlight ile daha ayrıntılı kontrol için, clientaccesspolicy.xml kullanılmalıdır.

Politika dosyaları çeşitli izinler verir:

- Kabul edilen politika dosyaları (Adalet politikası dosyaları belirli politika dosyalarını devre dışı bırakabilir veya kısıtlayabilir)
- Soket izinleri
- Başlık izinleri
- HTTP/HTTPS erişim izinleri
- Kriptografik kimlik bilgilerine dayalı erişime izin vermek

Aşırı izin veren bir politika dosyası örneği:

```
<?xml version="1.0"?>
<!DOCTYPE cross-domain-policy SYSTEM
"http://www.adobe.com/xml/dtds/cross-domain-policy.dtd">
<cross-domain-policy>
   <site-control permitted-cross-domain-policies="all"/>
   <allow-access-from domain="*" secure="false"/>
   <allow-http-request-headers-from domain="*" headers="*" secure="fals
e"/>
</cross-domain-policy>
```

How can cross domain policy files can be abused? (Ara sıra domain politikası dosyaları nasıl kötüye kullanılabilir?)

- Aşırı derecede izin veren çapraz-domain politikaları.
- Çapraz-domain politikası dosyaları olarak ele alınabilecek sunucu yanıtları üretmek.
- Alt-domain politika dosyaları olarak ele alınabilecek dosyaları yüklemek için dosya yükleme işlevselliğini kullanmak.

Impact of Abusing Cross-Domain Access (Kıyamet-Domain Erişimini Kötüye Kullanma Etkisi)

- CSF korumalarını yener.
- Çapraz köken politikalarıyla kısıtlanmış veya başka bir şekilde korunan verileri okuyun.

Test Objectives (Test Hedefleri)

- Politika dosyalarını gözden geçirin ve onaylayın.

How to Test (Nasıl Test Edilir)

Testing for RIA Policy Files Weakness (RIA Politika Dosyaları Zayıflığı için Test)

RIA politika dosyası zayıflığını test etmek için test cihazı, politika dosyalarını crossdomain.xml ve clientaccesspolicy.xml'yi uygulamanın kökünden ve bulunan her klasörden almaya çalışmalıdır.

Örneğin, uygulamanın URL'si ise `http://www.owasp.org` Test cihazı dosyaları indirmeye çalışmalıdır. `http://www.owasp.org/crossdomain.xml` ve `http://www.owasp.org/clientaccesspolicy.xml` . .

Tüm politika dosyalarını aldıktan sonra, izin verilen izinler en az ayrıcalık ilkesi altında kontrol edilmelidir. İstekler yalnızca gerekli olan alanlara, limanlardan veya protokollerden gelmelidir. Aşırı izin veren politikalardan kaçınılmalıdır. İlgili politikalar `*` İçlerinde yakından incelenmelidir.

Example (Örnek)

```
<cross-domain-policy>
   <allow-access-from domain="*" />
</cross-domain-policy>
```

Result Expected (Sonuç Bekleniyor)

- Bulunan politika dosyalarının bir listesi.
- Politikalardaki zayıf ayarların bir listesi.

Tools (Araçlar)

- Nikto'nun

- OWASP Zed Saldırı Proxy Projesi
- W3af'ın

References (Referanslar)

- Adobe: “Cross-domain politikası dosyası spesifikasyonu”
- Adobe: “Flash Player için çapraz domain politikası dosya kullanım önerileri”
- Oracle: “Cross-Domain XML Desteği”
- MSDN: “Eklantı Alanı Sınırları Arasında Hizmet Sunmak”
- MSDN: “Sütlight’ta Net Güvenlik Erişim Kısıtlamaları”
- Stefan Esser: “Flash Crossdomain Politika Dosyaları ile yeni delikler açmak”
- Jeremiah Grossman: “Clossdomain.xml, Çapraz Yamacı Davet Ediyor”
- Google Doctype: “Flash Security’ye Giriş”
- UCSD: Flash Uygulamaların Crossdomain Politikalarını Analiz Etmek