PHP Exploit Derlemek

MUSTAFA SERHAT DÜNDAR, <SERHAT AT SERHATDUNDAR DOT COM>,
21/06/2009

Php exploitleri derlemek ve çalıştırmak için genelde PHP 5.2.0 kullanılıyor. Bizde yazımızda bundan yararlanacağız.

http://tr2.php.net/distributions/php-5.2.0-win32-installer.msi adresine girip 18.44MB'lık dosyayı kaydedin.

Yükleme aşamasında bütün yerleri 'next' diyerek geçebilirsiniz. Web Server Setup bölümü geldiğinde ise 'Do not setup a web server' seçiniz.

Örnek olarak securityfocus.com'dan bir tane php exploit buldum.

http://www.securityfocus.com/archive/1/472205

Kodları boş bir 'Not Defteri' sayfasına yapıştıralım ve exploit.php olarak kaydedelim.

NOT :

```
# This file require the PhpSploit class.
# If you want to use this class, the latest
# version can be downloaded from acid-root.new.fr.
# Note: The new version is compatible with PHP 4 by default.
################################################
error_reporting(E_ALL ^ E_NOTICE);
require('phpsploitclass.php');
```

Exploit.php dosyasını C:Program Files/PHP klasörüne koyalım. Tabi eğer siz install sırasında başka bir dosya yolu belirttiyseniz oraya koyunuz.

Şuan bize gereken her şey hazır artık geldik exploitimizi çalıştırmaya.

Hemen Başlat (Start) / Çalıştır (Run)'a giriyoruz ve cmd yazıp enterlıyoruz.

MSDos komut sisteminde cd C:PHP komutu ile C dizinine kurduğumuz PHP klasörüne indik.

Siz Program Files'a kurduysanız cd C:Program Files/PHP yazarak enterlayınız.

Daha sonra C:PHP/php.exe C:PHP/exploit.php yazarak enterlayınız.

Evet artık exploiti yazan kişinin verdiği bilgilerden yola çıkacağız. Usage – Params – Option – Dork – Example gibi kısımlar bize exploitler hakkında bilgiler verir.

```
C:\PHP>C:\PHP\php.exe C:\PHP\e.php

------------ Pluxml 0.3.1 Remote Code Execution Exploit ------------
--------------------------------------------------------------------
Credits: DarkFig <gmdarkfig (at) gmail (dot) com [email concealed]>
URL: acid-root.new.fr || mgsdl.free.fr
IRC: #acidroot (at) irc.worldnet (dot) net [email concealed]
Note: Coded for fun 8)
--------------------------------------------------------------------
Usage: C:\PHP\e.php -url <> -ip <> [Options]
Params: -url For example http://victim.com/pluxml0.3.1/
-ip The IP that will be bound to the socket
Options: -port The socket will listen on this port (default=80)
-proxy If you wanna use a proxy <proxyhost:proxyport>
-proxyauth Basic authentification <proxyuser:proxypwd>
--------------------------------------------------------------------
```

Geri kalan kısımlar size kalmış. Her exploit farklı bilgiler verir. Bu exploitimizin kullanımını usage kısımdan öğrenebilirsiniz. Bazı exploitlerde extradan Dork yani google'da arama yapacağımız kodu içeren bölümüde olur. Dork yardımıyla siteleri bulup usage kısımdaki gibi uygularsanız hedefinize ulaşmış olursunuz.

MUSTAFA SERHAT DÜNDAR