

Script Kiddie Bezdırme Mekanizması

written by Mert SARICA | 27 February 2011

Günümüzde internete açık web sitelerinin kaderinde ya Çin üzerinden ya da Rusya üzerinden en az bir defa taranmak vardır. Bunu web uygulamaları üzerindeki zafiyetleri otomatik olarak tespit etmek ve istismar etmek üzere hazırlanmış bir solucan (worm) yaptığı gibi proxy arkasına gizlenmiş meraklı bir script kiddie de yapıyor olabilir.

Benim sitem de zaman zaman meraklı arkadaşların ilgi alanına girmekte ve Netsparker'dan Acunetix'e kadar bir çok ticari web uygulaması güvenlik tarayıcıları (web application security scanner) ile taranmaktadır. Her ne kadar bu zamana dek bu durumdam şikayetçi olmasamda kendimi şikayet edenlerine yerine koyarak "acaba bu script kiddieler'in işlerini mod_security ve benzer karmaşık yöntemlere başvurmadan nasıl zorlaştırabilirim?" sorusuna yanıt aramaya koyuldum.

Script kiddie'nin ticari araçlar ile tarama işlemini simüle etmek için ilk olarak Windows işletim sistemi yüklü olan sanal makine içine bir web sunucusu kurmam gerekiyordu ve seçimimi WAMP'tan yana kullandım. Daha sonra demo sürümü ile bu web sunucusunu tarayabilecek meşhur ticari bir tarama aracı aramaya başladım. Eskiden web uygulaması güvenlik tarayıcısı denilince akla ya HP firmasının satın aldığı Spi Dynamics firmasının Webinspect ürünü ya da IBM firmasının satın aldığı Watchfire firmasının Appscan ürünü gelirdi. Her ne kadar HP satın alana dek Webinspect'in hayranı olsam da bu senaryoda IBM'in Appscan demo ürününü kullanmaya karar verdim.

Başka bir sanal makineye Appscan ürününü kurduktan sonra diğer sanal makinemde kurulu olan web sunucusunu tarayabilmek için ufak bir numara ile <http://demo.testfire.net> sitesini taranacak sanal makinemin ip adresine yönlendirdim ve zorlaştırma yöntemi üzerine düşünmeye başladım. (Webinspect ve Appscan araçlarının demo sürümleri ile sadece kendi demo sitelerini (Appscan için <http://demo.testfire.net> web adresi, Webinspect için <http://zero.webappsecurity.com> web adresi) tarayabilmektesiniz.)

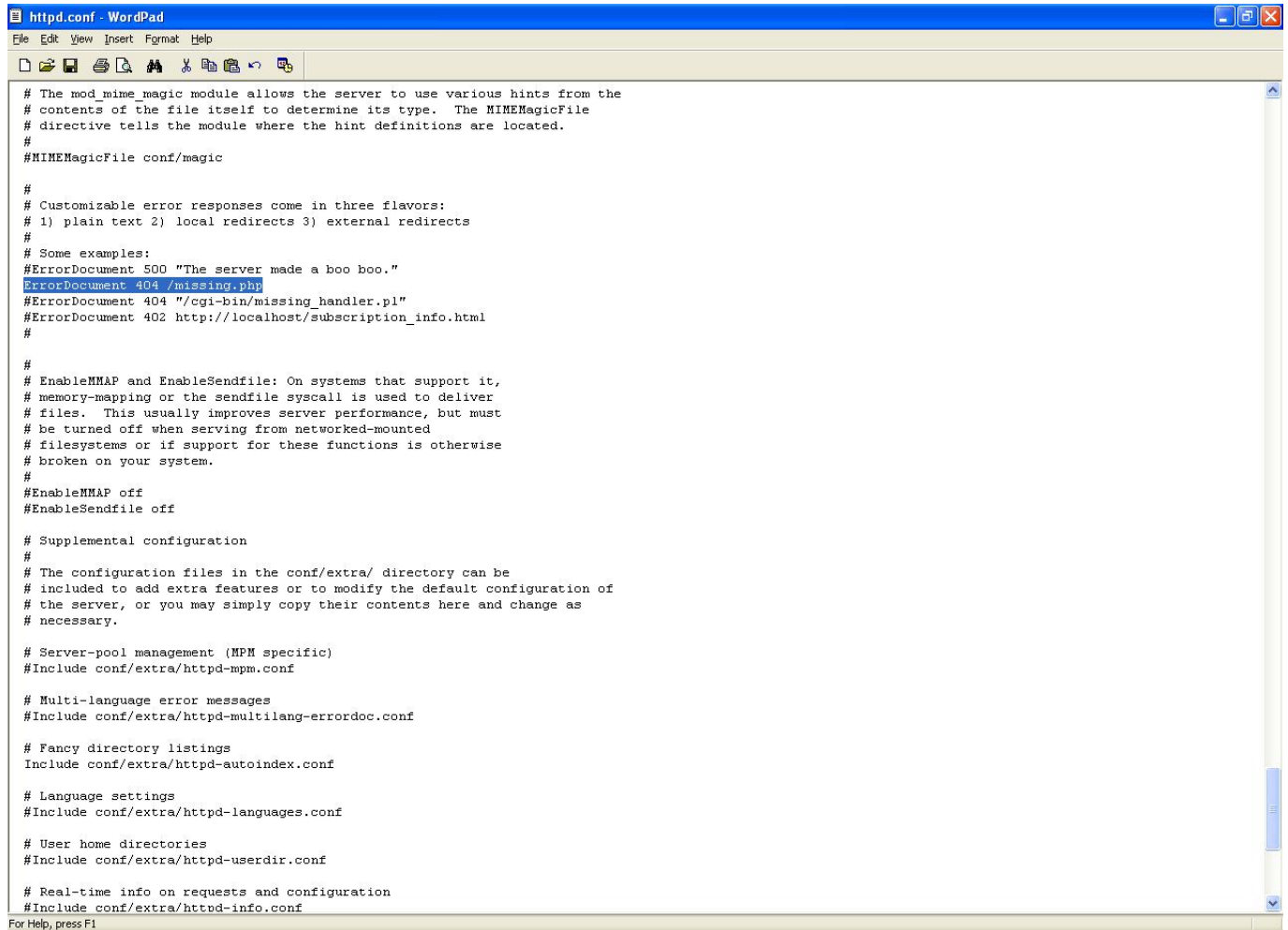
Penetrasyon testlerinde karşılaşmak istemeyeceğiniz durumlardan biri uzun süren taramanın tamamlanmasına yakın tarama aracının göçmesi bir diğeri ise

taranan sitenin çok büyük olması ve isteklere geç yanıt veriyor olması nedeniyle taramanın saatlerce sürmesidir. Korsanlar ve script kiddieler genellikle sabırsız insanlardır bu nedenle hedefe bir an önce sızmak için en kestirme, en hızlı yolu seçmektedirler. Bunu göz önünde bulundurarak tarama aracının 10 dakikada tarayabileceği bir siteyi ufak bir numara ile saatler içinde taramasını sağlayabilmenin script kiddie'yi bezdirebileceği düşüncesiyle Appscan'i biraz etüt etmeye başladım.

Appscan çalışma prensibi gereği hedef web sitesini taramaya başlamadan önce site üzerinde keşfe çıkmakta ve sitenin haritasını çıkarmaktadır. Keşif aşaması tamamlandıktan hemen sonra tarama işlemine geçmekte ve bu aşamada yeni bir bağlantı adresi (link) ile karşılaşması durumunda bu adresi otomatik olarak taranacaklar listesine dahil etmektedir. Durum böyle olunca acaba bir web sayfası hazırlasam ve bu sayfa her ziyaret edildiğinde rastgele bağlantı adresi üretiyor olsa, bu sayfayı ziyaret eden Appscan yeni bağlantı adresi -> tara -> yeni bağlantı adresi -> tara şeklinde sonsuz bir döngüye girer mi sorusuna yanıt aramaya başladım.

Bunun için öncelikle httpd.conf üzerinde özel bir hata sayfası oluşturdum (missing.php) ki bulamadığı her sayfa için otomatik olarak missing.php sayfasına yönlendirilsin ve bu sayfada üretilen rastgele 100 bağlantı adresi sayesinde sonsuz döngüye girebildin. Bir kaç deneme sonucunda Appscan'i döngüye (sonsuz olabilir) sokan sayfayı oluşturdum ve muradıma erdim.

httpd.conf üzerinde özel hata sayfası belirtme:



```
# The mod_mime_magic module allows the server to use various hints from the
# contents of the file itself to determine its type. The MIMEMagicFile
# directive tells the module where the hint definitions are located.
#
#MIMEMagicFile conf/magic

#
# Customizable error responses come in three flavors:
# 1) plain text 2) local redirects 3) external redirects
#
# Some examples:
#ErrorDocument 500 "The server made a boo boo."
#ErrorDocument 404 /missing.php
#ErrorDocument 404 "/cgi-bin/missing_handler.pl"
#ErrorDocument 402 http://localhost/subscription_info.html
#

#
# EnableMMAP and EnableSendfile: On systems that support it,
# memory-mapping or the sendfile syscall is used to deliver
# files. This usually improves server performance, but must
# be turned off when serving from networked-mounted
# filesystems or if support for these functions is otherwise
# broken on your system.
#
#EnableMMAP off
#EnableSendfile off

# Supplemental configuration
#
# The configuration files in the conf/extra/ directory can be
# included to add extra features or to modify the default configuration of
# the server, or you may simply copy their contents here and change as
# necessary.

# Server-pool management (MPM specific)
#Include conf/extra/httpd-mpm.conf

# Multi-language error messages
#Include conf/extra/httpd-multilang-errordoc.conf

# Fancy directory listings
#Include conf/extra/httpd-autoindex.conf

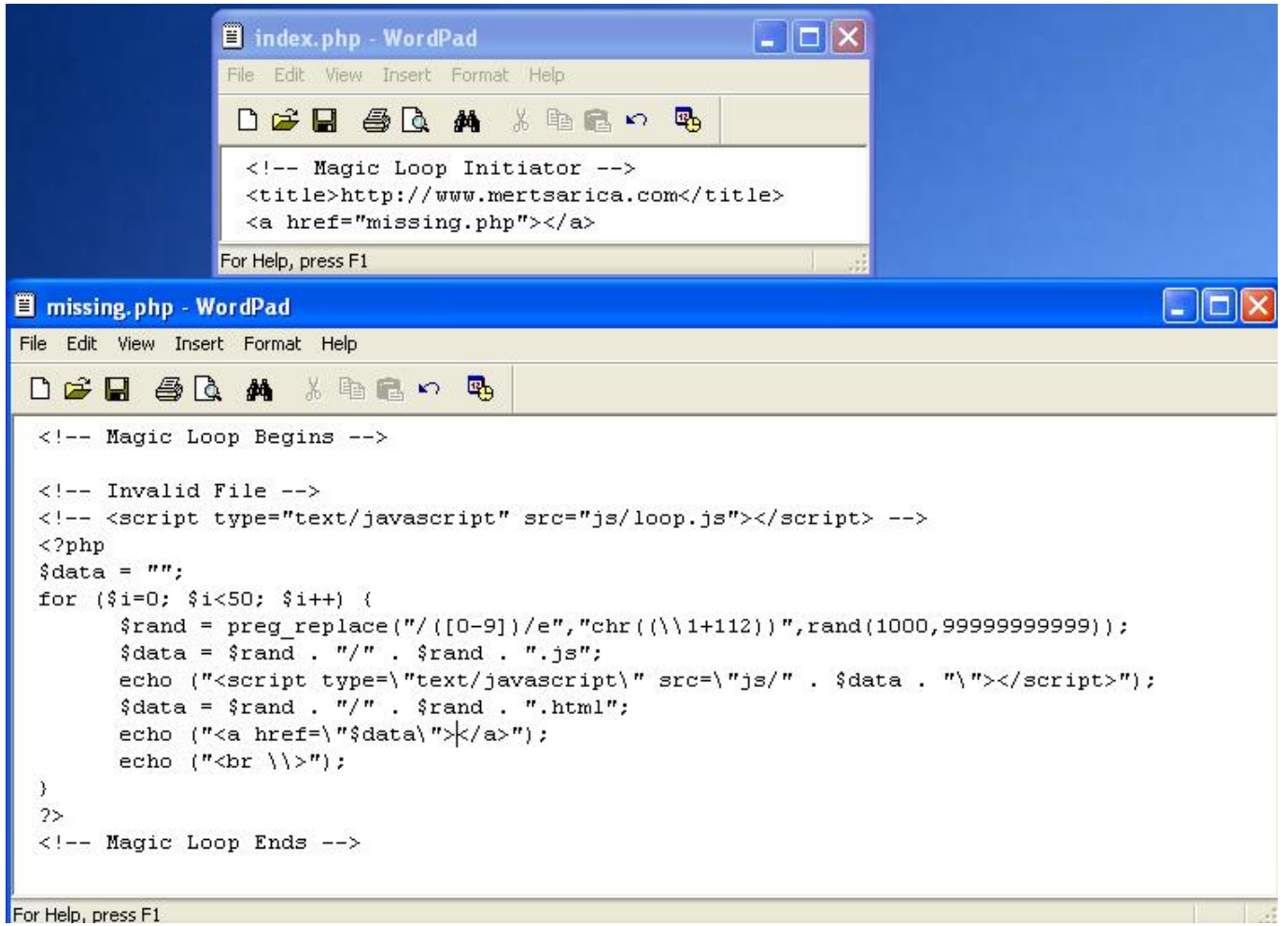
# Language settings
#Include conf/extra/httpd-languages.conf

# User home directories
#Include conf/extra/httpd-userdir.conf

# Real-time info on requests and configuration
#Include conf/extra/httpd-info.conf

For Help, press F1
```

Oluşturduğum web sayfaları:



Normal şartlarda 2 dakikada taranabilen bir sayfa, 46. dakika sonunda halen taranmaya ve ziyaret edilecek URL (resimde sol alt köşeye dikkat) sayısı artmaya devam ediyor. (döngü):

Untitled - IBM Rational AppScan

File Edit View Scan Tools Help

Scan Configuration Scan Expert Scan Log Report Update Analyze JavaScript

Security Issues Remediation Tasks Application Data

Scanning... Phase 1

Exploring: http://demo.testfire.net/vwrsrsyq/s/rqpqvsqu/rqpqvsqu.js 23:42

Arranged By: Severity Descending

Security Issues: There are no results to show

Previous Next Severity State

Issue Information Advisory Fix Recommendation Request/Response

Dashboard

Issue Severity Gauge

Total number of issues: 0

Visited URLs 2/194391 Completed Tests 0/5441 0 Security Issues 0 0 0 0

Untitled - IBM Rational AppScan

File Edit View Scan Tools Help

Scan Configuration Scan Expert Scan Log Report Update Analyze JavaScript

Security Issues Remediation Tasks Application Data

Scanning... Phase 1

Exploring: http://demo.testfire.net/s/uvrptpsyw/uvrptpsyw.js 46:55

Arranged By: Severity Descending

Security Issues: There are no results to show

Previous Next Severity State

Issue Information Advisory Fix Recommendation Request/Response

Dashboard

Issue Severity Gauge

Total number of issues: 0

Visited URLs 2/330358 Completed Tests 0/5441 0 Security Issues 0 0 0 0

Benzer sorun diğ er ticari web uygulaması g venlik tarayıcılarında var mı diyerek Netsparker ve Acunetix araçlarına baktığımda bunun Appscan'e  zg  bir sorun olduėu ve bunun yanında ba ka bir sorun daha dikkatimi  ekti. Misal ekran g r nt lerinde yer alan JS klas r n n aslında ge erli, var olan bir klas r olmamasına raėmen Appscan ve Acunetix araçları Netsparker'ın aksine site haritalarına var olmayan klas rleri ekleyerek g r nt  kirliliėi yaratmakta ve site haritasının kullanımını zorla tırmaktalar.

Sonuc olarak sitenizin bu t r otomatik araçlar ile taranmasından rahatsız oluyorsanız bu araçları inceleyerek zayıf noktalarını ke fedebilir ve site ke fini zorla tıracak basit numaralara ile script kiddie'leri canlarından bezdirebilirsiniz :)

Bir sonraki yazıda g r  mek dileėiyle herkese iyi haftasonları dilerim...

Not:  retilen baėlantı adreslerine benim yaptığım gibi isim (link text) vermez iseniz kullanıcıların yanlışlıkla bu baėlantı adreslerine tıklamasını engelleyebilirsiniz.