Script Kiddie Bezdirme 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.)

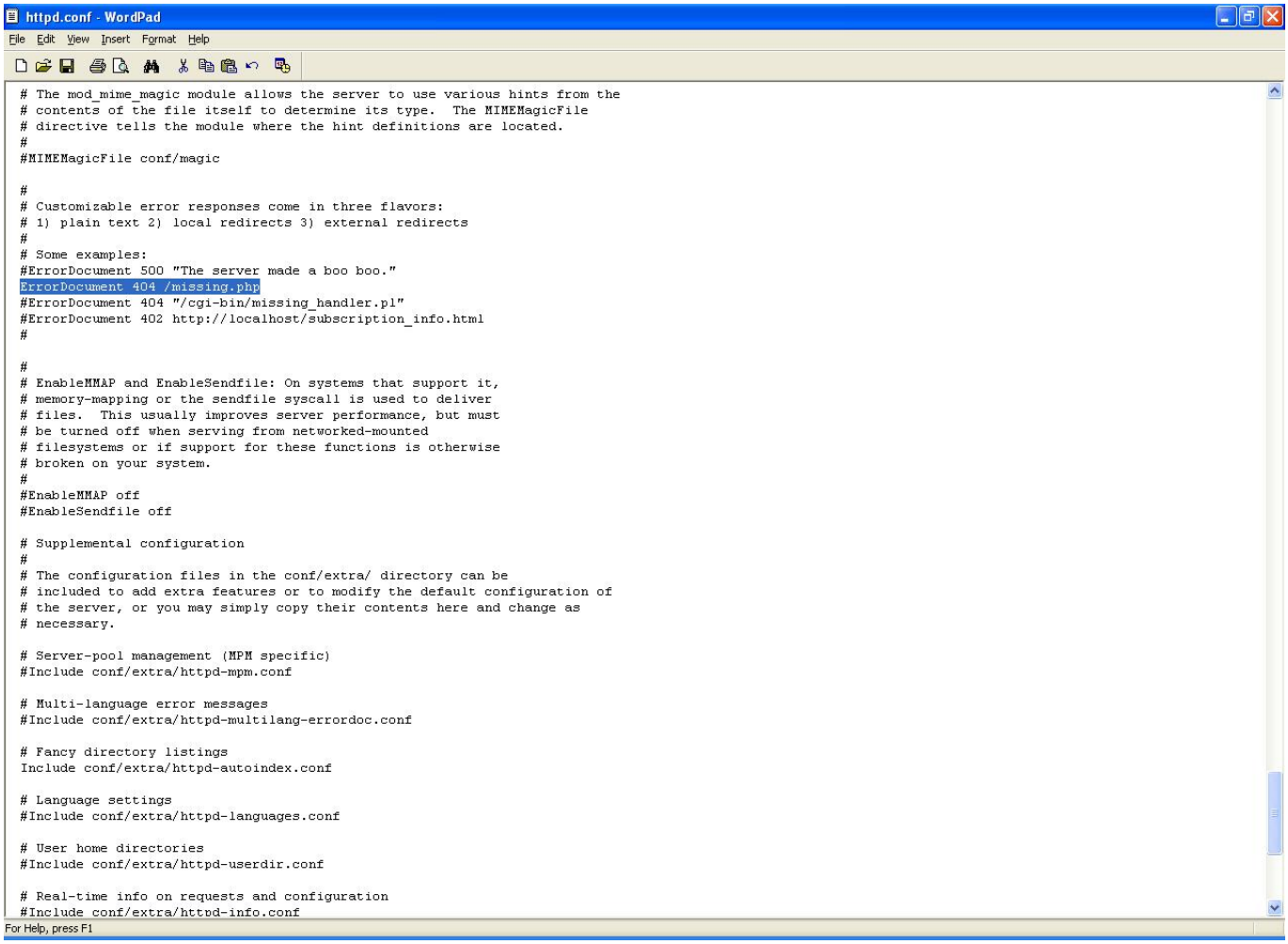
Penetrasyon testlerinde karşılaşmak istemeyeceğiniz durumlardan biri uzun süren taramanın tamamlanmasına yakın tarama aracının göçmesi bir diğeri ise

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.

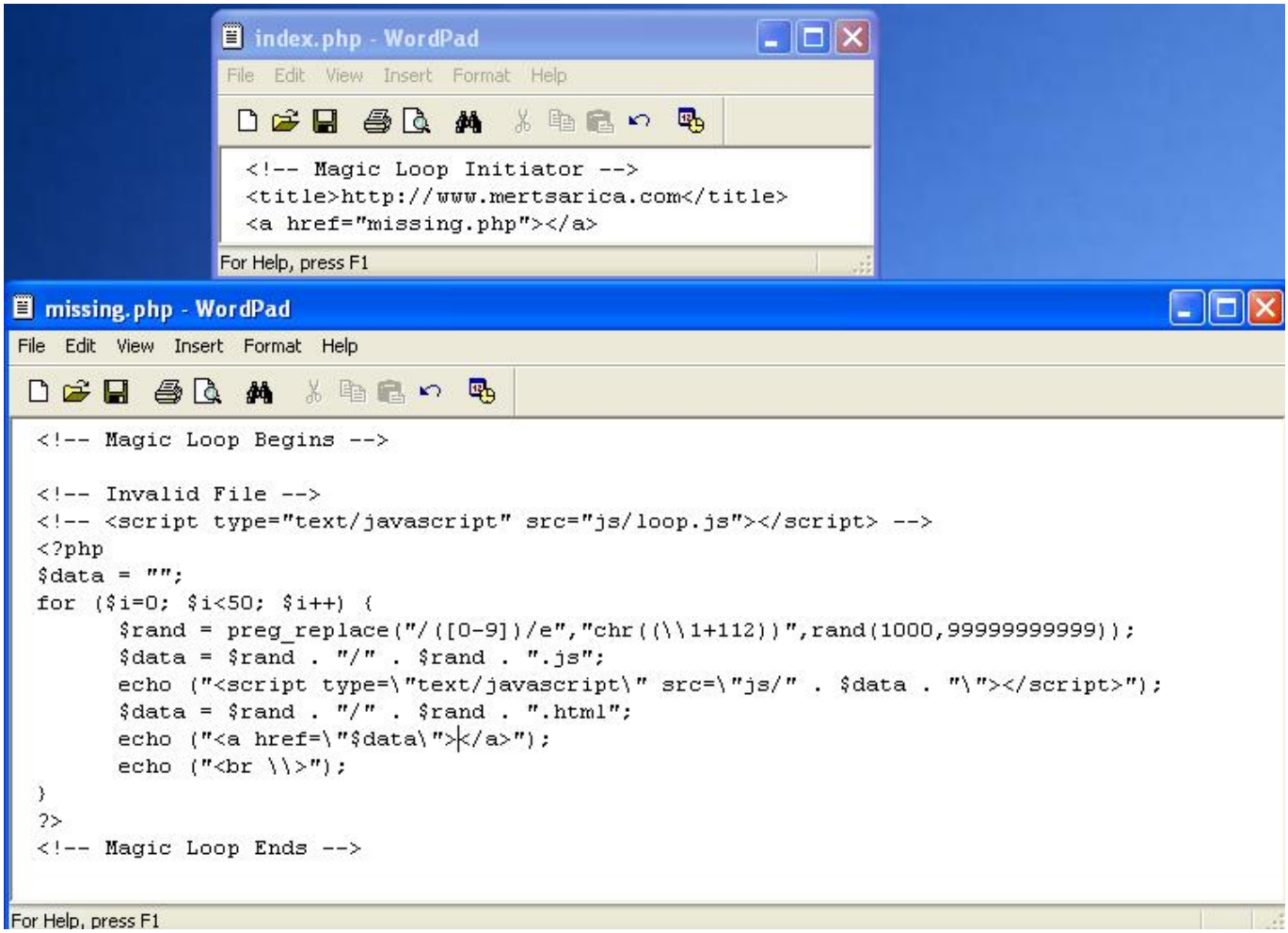
Appscan çalışma prensibi gereği hedef web sitesini taramaya başlamadan önce site üzerinde keşfe çıkmakta ve sitenin haritasını çıkarmaktadır. Keşif aşaması tamamlandıktan hemen sonra tarama işlemine geçmekte ve bu aşamada yeni bir bağlantı adresi (link) ile karşılaşması durumunda bu adresi otomatik olarak 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.

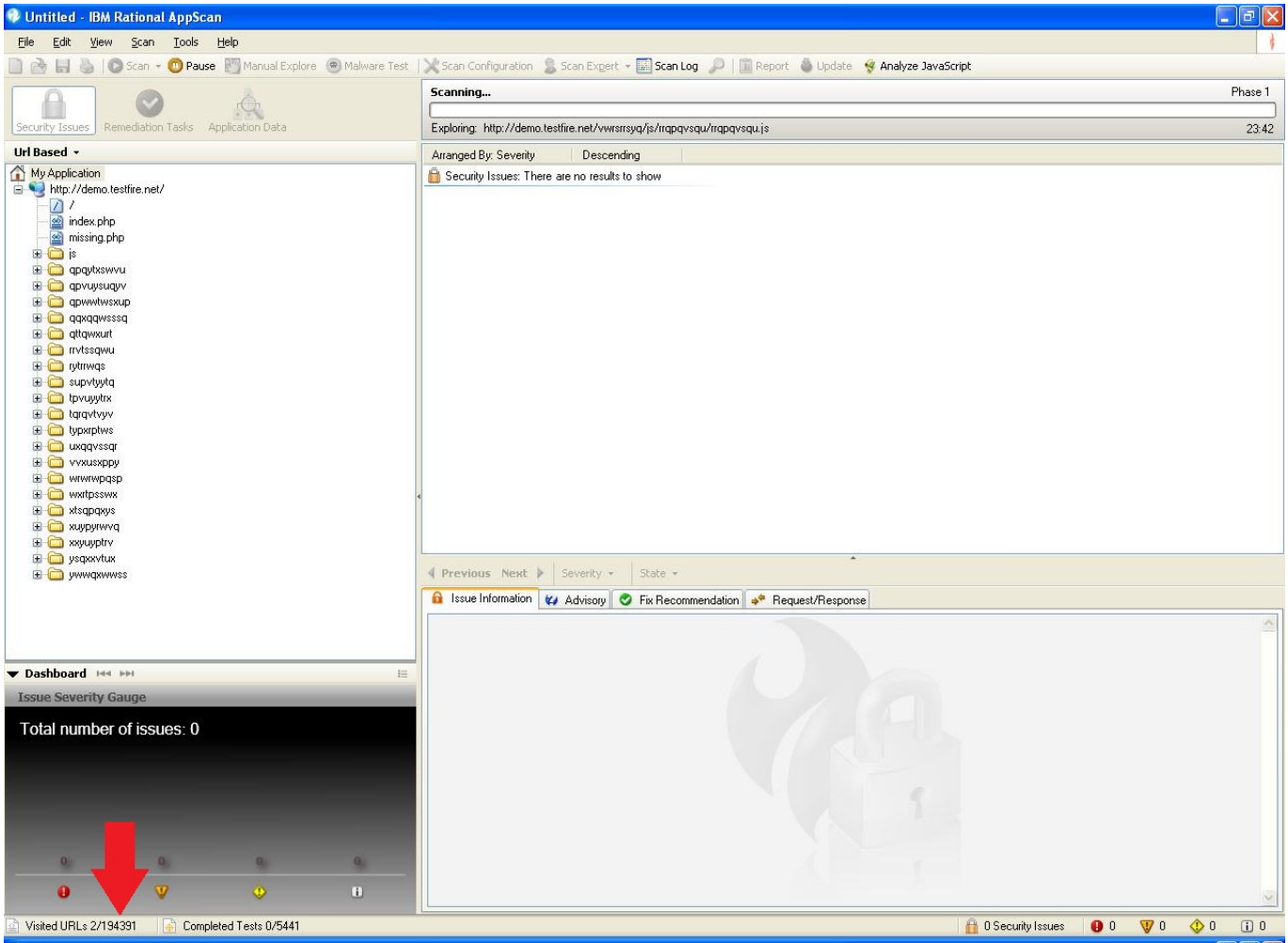
httpd.conf üzerinde özel hata sayfası belirtme:

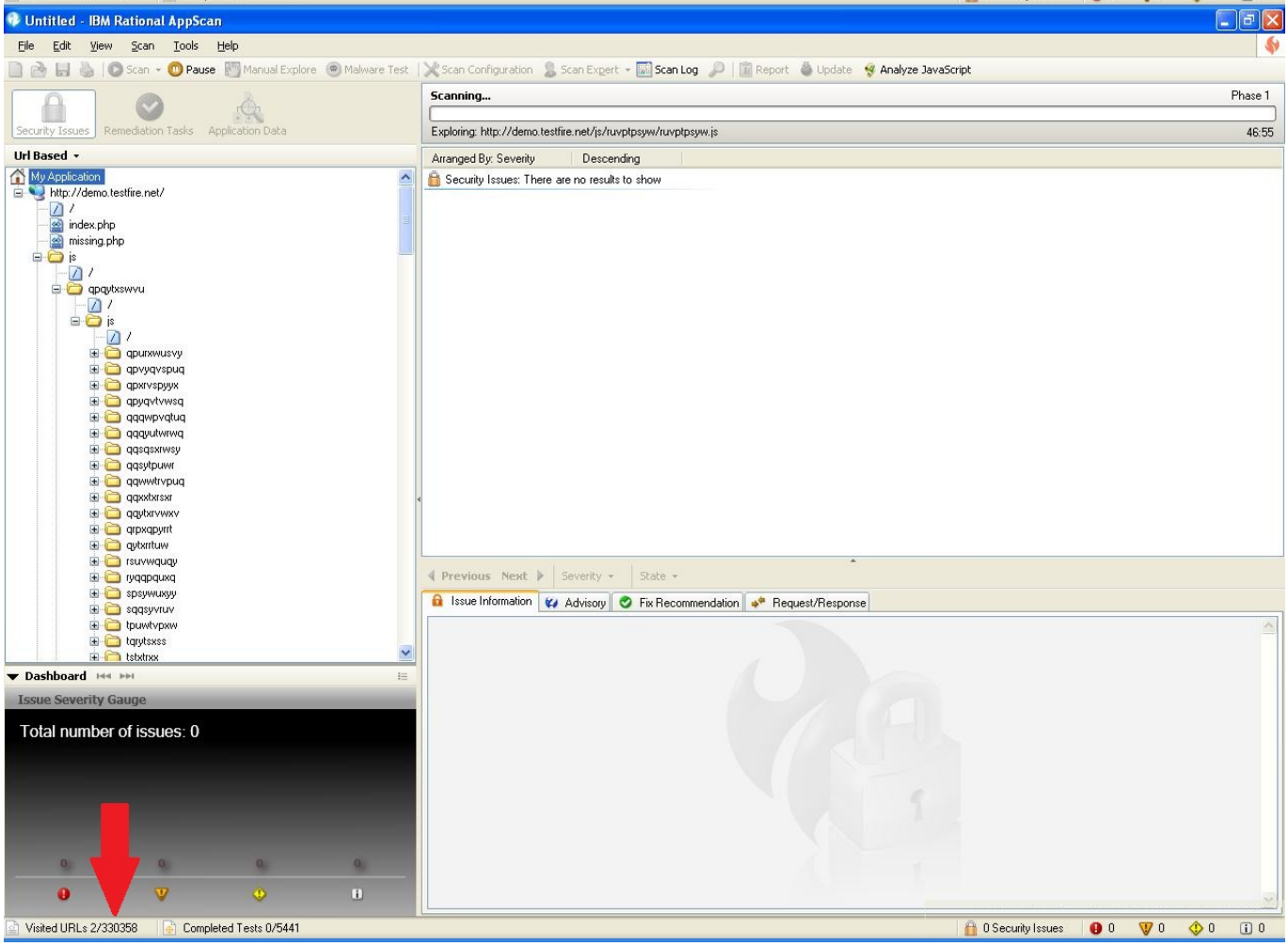


Oluşturduğum web sayfaları:



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 Pause Manual Explore Malware Test Scan Configuration Scan Expert Scan Log Report Update Analyze JavaScript
Security Issues Remediation Tasks Application Data
Scanning... Phase 1
Exploring: http://demo.testfire.net/vwrsrrsyq/js/rrqpqvsqu/rrqpqvsqu.js 23:42
Url Based
Arranged By: Severity Descending
Security Issues: There are no results to show
My Application
http://demo.testfire.net/
/
index.php
missing.php
js
qpqytxswvu
qpvuysuqvv
qpwwtwsxup
qqxqqwsssq
qttqwxurt
rrvtssqwu
rytrrwqs
supvtyytq
tpvuyytrx
tqrqvtvyv
typxrptws
uxqqvssqr
vvxusxppy
wrwrwpqsp
wxrtpsswx
xtsqpqxys
xuypyrwvq
xxyuyptrv
ysqxxvtux
ywwqxwwss
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 Pause Manual Explore Malware Test Scan Configuration Scan Expert Scan Log Report Update Analyze JavaScript
Security Issues Remediation Tasks Application Data
Scanning... Phase 1
Exploring: http://demo.testfire.net/js/ruvptpsyw/ruvptpsyw.js 46:55
Url Based
Arranged By: Severity Descending
Security Issues: There are no results to show
My Application
http://demo.testfire.net/
/
index.php
missing.php
js
/
qpqytxswvu
/
js
/
qpurxwusvy
qpvyqvspuq
qpxrvspyyx
qpyqvtvwsq
qqqwpvqtuq
qqqyutwrwq
qqsqsxrwsy
qqsytpuwr
qqwwtrvpuq
qqxxbxsxr
qqytxrvwxv
qrpxqpyrrt
qytxrrtuw
rsuvwquqy
ryqqpquxq
spsywuxyy
sqqsyvruv
tpuwtvpxw
tqrytsxss
tstxtrxx
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 diğer ticari web uygulaması güvenlik tarayıcılarında var mı diyerek Netsparker ve Acunetix araçlarına baktığımda bunun Appscan'e özgü bir sorun olduğu ve bunun yanında başka bir sorun daha dikkatimi çekti. Misal ekran görüntülerinde yer alan JS klasörünün aslında geçerli, var olan bir klasör olmamasına rağmen Appscan ve Acunetix araçları Netsparker'ın aksine site haritalarına var olmayan klasörleri ekleyerek görüntü kirliliği yaratmakta ve site haritasının kullanımını zorlaştırmaktalar.

Sonuç olarak sitenizin bu tür otomatik araçlar ile taranmasından rahatsız oluyorsanız bu araçları inceleyerek zayıf noktalarını keşfedebilir ve site keşfini zorlaştıracak basit numaralara ile script kiddie'leri canlarından bezdirebilirsiniz :)

Bir sonraki yazıda görüşmek dileğiyle herkese iyi haftasonları dilerim…

Not: Üretilen bağlantı adreslerine benim yaptığım gibi isim (link text) vermez iseniz kullanıcıların yanlışlıkla bu bağlantı adreslerine tıklamasını engelleyebilirsiniz.