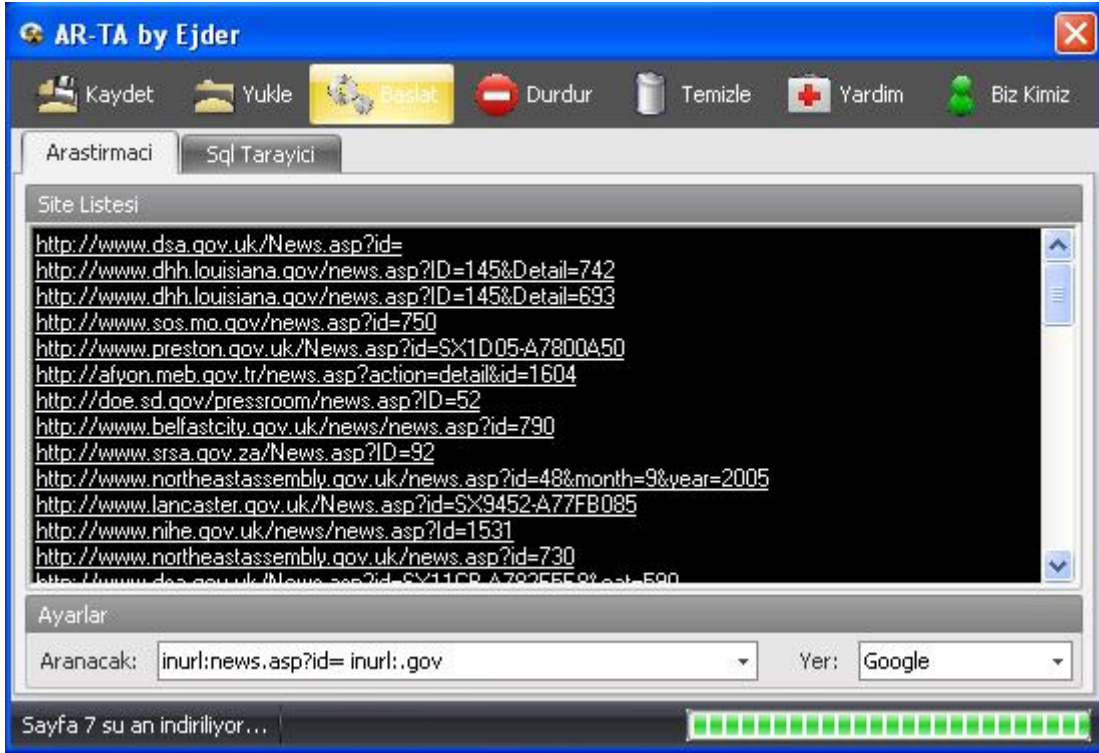


AR-TA (Arastirmaci - Tarayici)

Ar-Ta bir cesit Scanner tarzinda bir yazilimdir. Internetten belirttiginiz parametreler dogrultusunda arama yapip, sonuclarini duzenli kaydedebilme ve bulunan site listesinde Sql injection, tekli rfi taramasi yapilabilen bir yazilim haline geldi. Microsoft .Net Studio 2005 kullanilarak C# dili ile kodlanmis, Microsoft .Net Framework SDK 2.0 ile derlenmistir.



Daha onceden yazdigim Searcher v1, v2 ve SqlFilter v1 yazilimlarinin birlestirilmis, ve sorunlarinin giderilmis halidir. Daha hizli, daha kullanisli, daha kisisel bir program haline getirilmistir. Sabit arama, sabit hata sorgulama degilde, size bagli arama ve tarama imkanlari sunulmaktadır. Vazgecemiyeceginiz bir yazilimdir.

2 kisimdan olusmaktadır.

1- Arastirmaci

Onceden yazdigim Searcher programlarindan daha hizli, gelismis ve kisisellestirilmis halidir. Oncelikle Google ve Yahoo uzerinde istediginiz ozelikteki siteleri bulup, listelemektedir. Bu tur arama ne isimize yarar? Cok isimize yariyor. Belli formattaki siteleri bulmak, sql acik bulunacak potansiyeldeki siteleri listeletmek, elimizde exploiti bulunan forumlarin listesini bulmak vb gibi aramalar icin mukemmel bir yazilimdir.

Tek yapmanız gereken Aranacak kelime yada kalibi seçip, nerde arayacağınızı ayarlayıp Baslat (Cntrl+B) manızdır. Sonucu bulduktan sonra düzenli bir şekilde kaydet (Cntrl+S)ebilirsiniz.

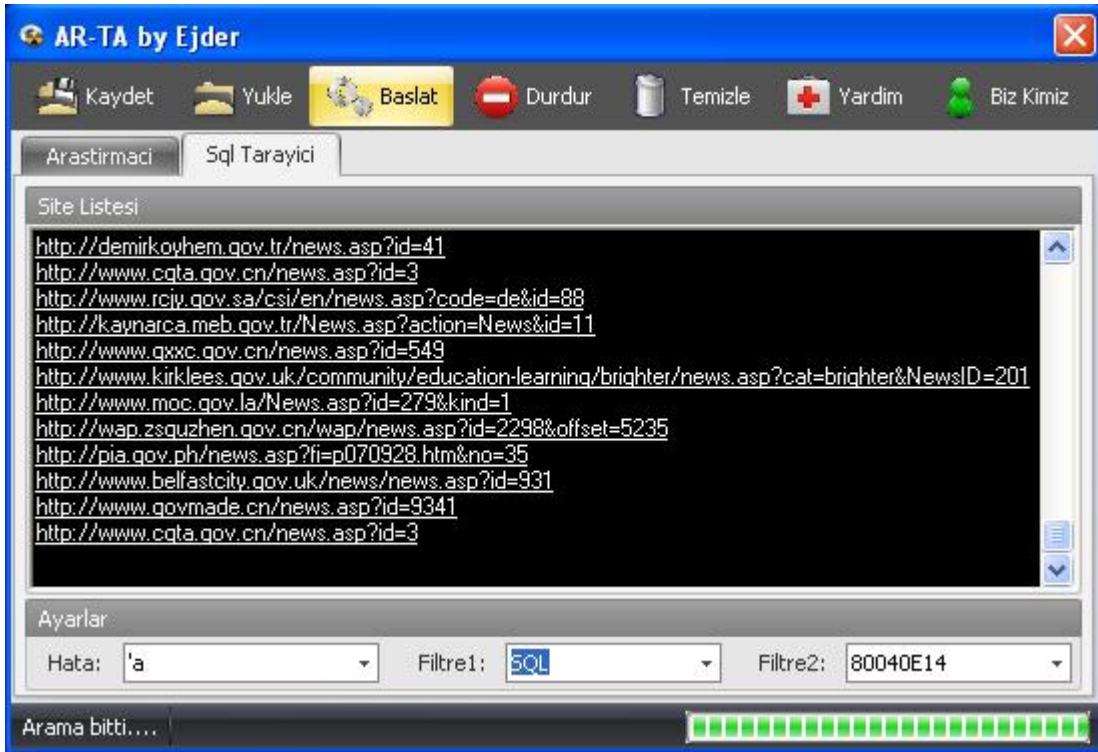
2- Tarayıcı

Önceden yazdığım SqlFilter yazılımının daha gelişmiş, hızlı ve kişiselleştirilmiş halidir. İstedığınız Hatayı verdirebilir ve filtreyebilirsiniz.

Bu kısımda, yukle (Cntrl+O) diginiz site listesinde, her girdiye HATA mesajını eklemektedir. Ve siteden donecek olan sonucda ise Filter1 ve Filter2 deki degerleri tarayacaktır. Eger varsa Listemize ekliyecektir.

Filtreleme olayında illa 2 sinide doldurmak zorunda degilsiniz. Illa listeden bir turde secmeniz gerekmez. İsterseniz birini bos birakabilirsiniz.

Hata kısmında ise, istediğiniz hatayı seçebilir , isterseniz kendi hata turunu seçebilir, yazabilirsiniz. Siteden donecek hatalara karsida, filter kismini duzenlemeniz gerekecektir.



Ornek olarak: Taranacak site -> <http://savsak.com/news.asp?id=4> ve <http://savsak.com/video.asp?id=5&get=all&type=2> seklinde 2 sitede tarama yapilcak mesela.

Hata mesajimiz su sekilde eklenip cagrilcektir;
http://savsak.com/news.asp?id=4+HATA ve
http://savsak.com/video.asp?id=5+HATA&get=all+HATA &type=2+HATA seklinde eklenecektir.

HATA miz = 'a olarak secildi diyelim. O zaman..
http://savsak.com/news.asp?id=4'a ve
http://savsak.com/video.asp?id=5'a&get=all'a&type=2'a seklinde tum parametrelere uygulanacaktır.

Filtreme olayinda ise size birkac taktik verem.

SQL + 80040E14 ikilisi size Sql acik var demektir. Fakat Ole DB, Jet access, mysql 3 ozellikde olabilir.

OLE DB + 80040E14 ikilisi size Sql acik olanlari listeler. Fakat ozellestirilmis bir taramadir. BU tur acik bulunan sitelerde, gelismis Sql injection methodlari uygulanmaktadır. Eger riske girmek istenmiyorsa , daha kesin bir Filtre mumkun oda -> Unclosed + 80040E14 ikilisidir.

JET Database + 80040E14 ikilisinden -> Access db kullanan siteleri bulabilirsiniz..

MySQL + 80040E14 ikilisi ile -> ASP tabanlı fakat Mysql sql hatasi verenleri tarayabilirsiniz..

Kisacasi filte turunu degistirdigimizde, daha ozel taramalar mumkun kilinmaktadır.

Kisaltmalar : Cntrl+S -> Kaydet

Cntrl+O -> Yukle

Cntrl+B -> Baslat

Cntrl+D -> Durdur

F1 -> Yardim

F2 -> Biz Kimiz

Site Listesi ornegi:

http://www.cosmoslac.com/gr/product_list.asp?ID=38

<http://www.nrf.com/GR/CSRA2.asp>

<http://www.nameisp.com/tld.asp?tld=com.gr>

http://www.mobile.com.gr/see_all_articles.asp?id=8

http://www.mobile.com.gr/see_all_articles.asp?id=17

<http://www.pds.com.gr/index.asp?mod=articles&id=86>

<http://www.pds.com.gr/index.asp?mod=articles&id=85>

<http://www.aphrodisia.com.gr/News/PrintArticle.asp?Id=15&Lun=1>

bu sekilde TXT icine kaydedip, yukleyebilirsiniz.



Program EJDER tarafından SAVSAK.COM için yazılmıştır. Tüm hakları Ejder'e aittir. Programın kullanımından dolayı gelecek sorun ve problemlerden dolayı Ejder ve Savsak.com sorumlu tutulamaz..

İrtibat : ejder@savsak.com
Site : www.savsak.com

EJDER was here ;)