# w3af'yi Tanıyalım

MUSTAFA SERHAT DÜNDAR, <SERHAT AT SERHATDUNDAR DOT COM>,
28/07/2009

## W3AF NEDİR?

Exploitler hakkında en bilinen framework şüphesiz ki metasploit. Fakat işe yarar bir çok framework daha mevcut. İşte w3af onlardan biri.

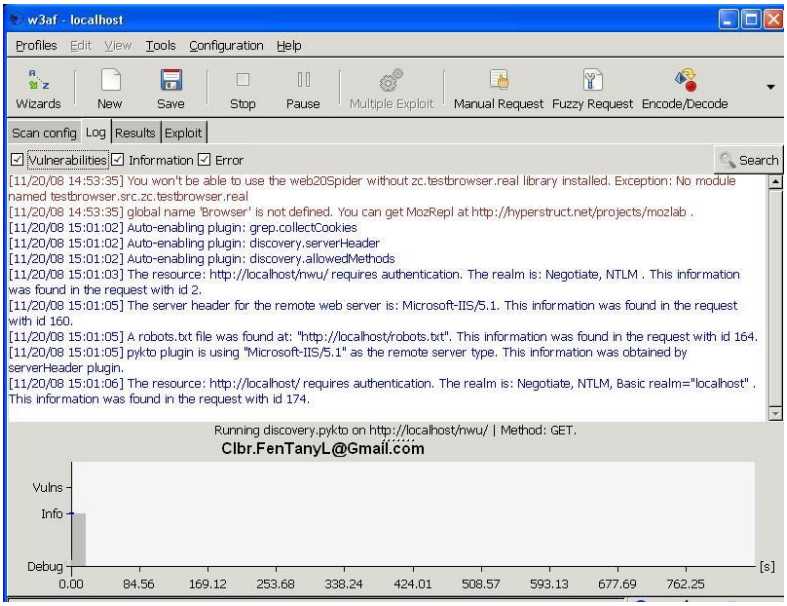
w3af tamamen python tabanlı yazılmış bir programdır. Bu yüzden bilgisayarınızda python yüklü bulunmalıdır. Python.org adresinden download edip, kurabilirsiniz.

SQL injection, cross site scripting (xss), local and remote file inclusion (RFI, LFI) açıklarını tarayan 130'dan fazla plug-in içerir. Bu program sayesinde yazdığınız veya kullandığınız scriptleri taratarak açıklarını bulacak ve saldırı almadan önce güvenlik açıklarınızı kapatma fırsatı bulacaksınız.

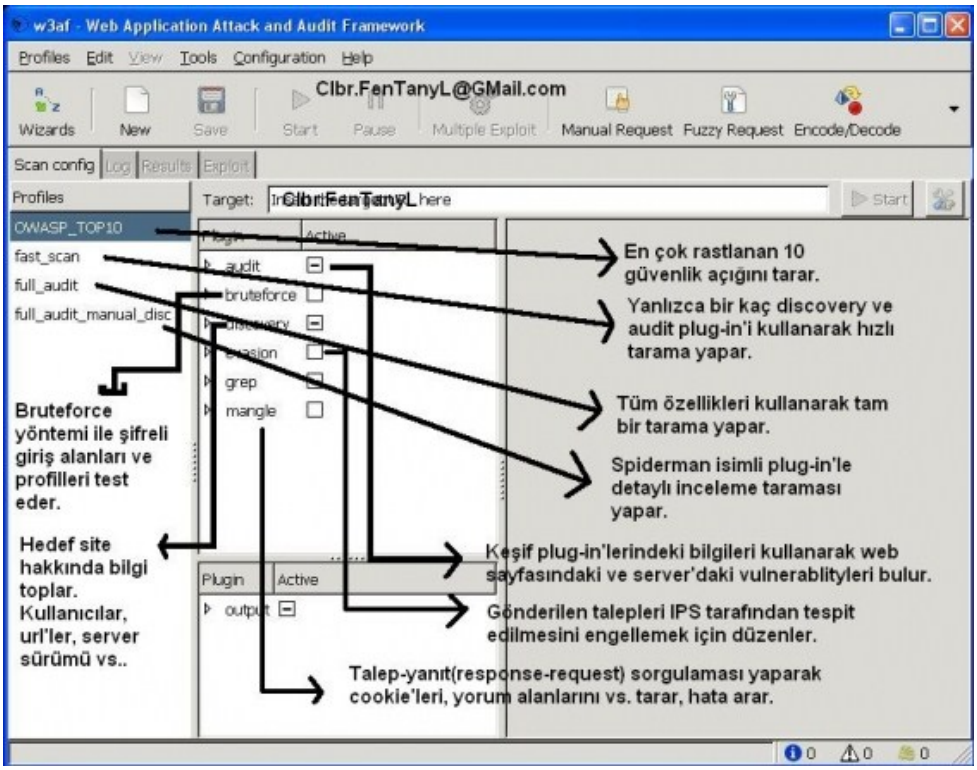
python25 isimli klasörünüze ek olarak Pygtk, pycairo, pygobject, pyOpenSsl, cluster, pyparsing, pywin, pcap, dnet, pyreadline python kütüphanelerini kurar. Sabırla bunlarıda 'next' diyerek yükletelim. En son winpcap ve graphviz programı da yüklenir ve yüklenme işlemi tamamlanmış olur.


** Programı açtığınızda otomatik açılan dos penceresini kapatmayınız.

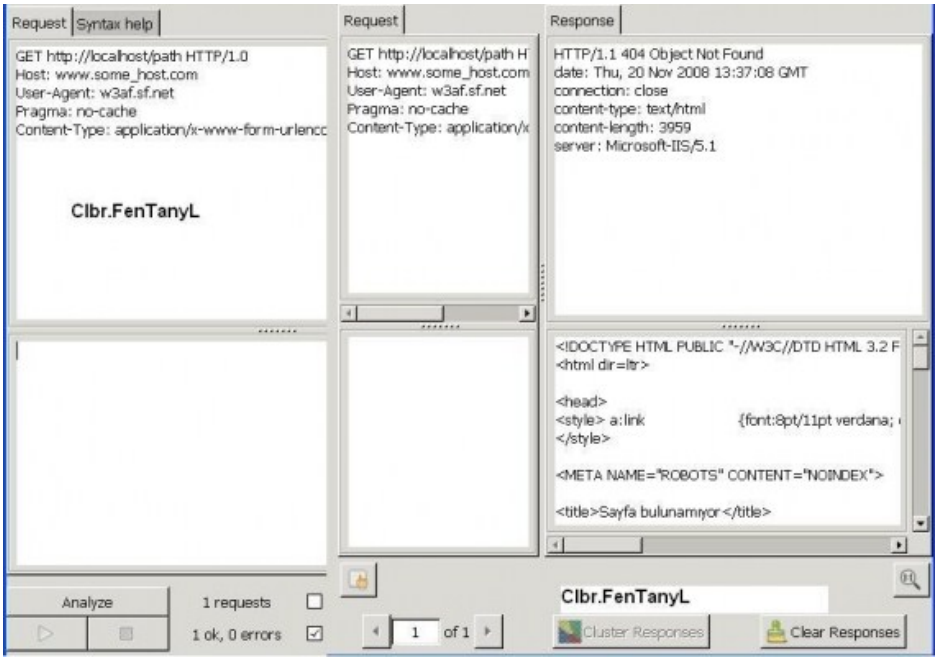
## KENDİ YAZDIĞIM BİR SCRİPTE YAPTIRDIĞIM TARAMA İŞLEMİ :




## PROGRAMIN MENÜLERİ VE İŞLEVLERİ



## FUZZY REQUEST MENÜSÜ :




## PROGRAMIN DİĞER ÖZELLİKLERİ :

## PROGRAMIN GENEL YETENEKLERİ :

- Audit
- SQL injection detection
- XSS detection
- SSI detection
- Local file include detection
- Remote file include detection
- Buffer Overflow detection
- Format String bugs detection
- OS Commanding detection
- Response Splitting detection
- LDAP Injection detection
- Basic Authentication bruteforce
- File upload inside webrot
- htaccess LIMIT misconfiguration
- SSL certificate validation
- XPATH injection detection
- unSSL (HTTPS documents can be fetched using HTTP)
- dav

Discovery
- Pykto, a nikto port to python
- Hmap, http fingerprinting.
- fingerGoogle, finds valid user accounts in google.
- googleSpider, a spider that uses google.
- webSpider, a classic web spider.
- robotsReader
- urlFuzzer
- serverHeader, fetches server header
- allowedMethods, gets a list of allowed HTTP methods.
- crossDomain, get and parse the flash file crossdomain.xml
- error404page, generate a regular expression to match 404 pages.
- sitemapReader, read googles sitemap.xml and parse it.
- spiderMan, using a localproxy and a human, find new URLs for auditing.
- webDiff, find differences between a local and a remote directory.
- wsdlFinder, find and parse WSDL and DISCO files

Grep
- collectCookies
- directoryIndexing
- findComments
- pathDisclosure

- strangeHeaders
- grep for pages using ajax and report them
- domXss, find DOM cross site scripting vulnerabilities.
- errorPages, search for eror pages that are too descriptive.
- fileUpload, find forms with file upload capabilities.
- getMails
- http authentication detection
- objects detection
- privateIP disclosure detection
- wsdlGreper, greps every page searching for WSDL documents.

Output
- console
- htmlFile
- textFile

Mangle
- sed, a stream editor for HTTP requests and responses.

Evasion
- reversedSlashes
- rndCase
- rndHexEncode
- rndParam
- rndPath
- selfReference

Attack
- davShell
- fileUploadShell
- googleProxy
- localFileReader
- mysqlWebShell
- osCommandingShell
- remoteFileIncludeShell
- rfiProxy
- sqlmap
- xssBeef

# KAYNAKÇA :


Programın resmi sitesi

Program iLe ilgili örnek video

Download Adresi (w3af-beta7-windows-r1812.zip isimli dosya win32 için olan dosyadır)

User Guide