Audit with w3af (console)

Overview

```
$ w3af_console
w3af>>>
```

Move forward by typing a given option Go back by typing back. Type view to see a list of configurable options and use the set command to change the options.

Manual audit

Step 1 - Setup target

```
w3af>>> target
w3af/config:target>>> set target http://example.com
```

Optional : You can setup target OS and Framework

```
w3af/config:target>>> view
|-------------------------------------------------------------------------------
------|
| Setting         | Value   | Description
|
|-------------------------------------------------------------------------------
------|
| targetOS        | unknown | Target operating system (unknown/unix/windows)
|
| targetFramework | unknown | Target programming framework
|
|                 |         | (unknown/php/asp/asp.net/java/jsp/cfm/ruby/perl)
|
| target          |         | A comma separated list of URLs
|
|-------------------------------------------------------------------------------
------|
```

Step 2 - Setup plugins

```
w3af>>> plugins
w3af>>> help
```

```
|-------------------------------------------------------------------------
------|
| list           | List available plugins.
|
|-------------------------------------------------------------------------
------|
| back           | Go to the previous menu.
|
| exit           | Exit w3af.
|
| assert         | Check assertion.
|
|-------------------------------------------------------------------------
------|
| audit          | View, configure and enable audit plugins
|
| auth           | View, configure and enable auth plugins
|
| bruteforce     | View, configure and enable bruteforce plugins
|
| discovery      | View, configure and enable discovery plugins
|
| evasion        | View, configure and enable evasion plugins
|
| grep           | View, configure and enable grep plugins
|
| mangle         | View, configure and enable mangle plugins
|
| output         | View, configure and enable output plugins
|
|-------------------------------------------------------------------------
------|
```

Audit plugins

```
w3af/plugins>>> audit <plugin>
w3af/plugins>>> audit
|-------------------------------------------------------------------------
-----|
| Plugin name       | Status | Conf | Description
|
|-------------------------------------------------------------------------
-----|
| LDAPi             |        |      | Find LDAP injection bugs.
|
| blindSqli         |        | Yes  | Identify blind SQL injection
|
|                   |        |      | vulnerabilities.
|
```

```
| buffOverflow      |        |      | Find buffer overflow vulnerabilities.
|
| dav               |        |      | Verify if the WebDAV module is properly
|
|                   |        |      | configured.
|
| eval              |        | Yes  | Find insecure eval() usage.Andres
Riancho (   |
|                   |        |      | andres.riancho@gmail.com )
|
| fileUpload        |        | Yes  | Uploads a file and then searches for the
|
|                   |        |      | file inside all known directories.
|
| formatString      |        |      | Find format string vulnerabilities.
|
| frontpage         |        | Yes  | Tries to upload a file using frontpage
|
|                   |        |      | extensions (author.dll).
|
| generic           |        | Yes  | Find all kind of bugs without using a
fixed  |
|                   |        |      | database of errors.
|
| globalRedirect    |        |      | Find scripts that redirect the browser
to    |
|                   |        |      | any site.
|
| htaccessMethods   |        |      | Find misconfigurations in the "<LIMIT>"
|
|                   |        |      | configuration of Apache.
|
| localFileInclude  |        |      | Find local file inclusion
vulnerabilities.   |
| mxInjection       |        |      | Find MX injection vulnerabilities.
|
| osCommanding      |        |      | Find OS Commanding vulnerabilities.
|
| phishingVector    |        |      | Find phishing vectors.
|
| preg_replace      |        |      | Find unsafe usage of PHPs preg_replace.
|
| redos             |        |      | Find ReDoS vulnerabilities.
|
| remoteFileInclude |        | Yes  | Find remote file inclusion
vulnerabilities.  |
| responseSplitting |        |      | Find response splitting vulnerabilities.
|
| sqli              |        |      | Find SQL injection bugs.
|
| ssi               |        |      | Find server side inclusion
vulnerabilities.  |
```

```
| sslCertificate    |        | Yes  | Check the SSL certificate validity (if
https |
|                   |        |      | is being used).
|
| unSSL             |        |      | Find out if secure content can also be
|
|                   |        |      | fetched using http.
|
| xpath             |        |      | Find XPATH injection vulnerabilities.
|
| xsrf              |        |      | Find the easiest to exploit xsrf
|
|                   |        |      | vulnerabilities.
|
| xss               |        | Yes  | Find cross site scripting
vulnerabilities.   |
| xst               |        |      | Find Cross Site Tracing vulnerabilities.
|
|-------------------------------------------------------------------------
-----|
```

Output

```
w3af/plugins>>> output <plugin>
w3af/plugins>>> output
|-------------------------------------------------------------------------
-----|
| Plugin name     | Status  | Conf | Description
|
|-------------------------------------------------------------------------
-----|
| console         | Enabled | Yes  | Print messages to the console.
|
| csv_file        |         | Yes  | Export identified vulnerabilities to a
CSV    |
|                 |         |      | file.
|
| emailReport     |         | Yes  | Email report to specified addresses.
|
| export_requests |         | Yes  | Export the fuzzable requests found during
|
|                 |         |      | discovery to a file.
|
| gtkOutput       |         |      | Saves messages to
kb.kb.getData('gtkOutput',  |
|                 |         |      | 'queue') to be displayed in the UI.
|
| htmlFile        |         | Yes  | Print all messages to a HTML file.
|
```

```
| textFile        |         | Yes  | Prints all messages to a text file.
|
| xmlFile         |         | Yes  | Print all messages to a xml file.
|
|-------------------------------------------------------------------------
-----|
```

Discovery

```
w3af/plugins>>> discovery <plugin>
w3af/plugins>>> discovery
|-------------------------------------------------------------------------
-------|
| Plugin name                   | Status | Conf | Description
|
|-------------------------------------------------------------------------
-------|
| afd                           |        |      | Find out if the remote web
server   |
|                               |        |      | has an active filter ( IPS or
WAF   |
|                               |        |      | ).
|
| allowedMethods                |        | Yes  | Enumerate the allowed methods
of an |
|                               |        |      | URL.
|
| archiveDotOrg                 |        | Yes  | Search archive.org to find
new      |
|                               |        |      | pages in the target site.
|
| bing_spider                   |        | Yes  | Search Bing to get a list of
new    |
|                               |        |      | URLs
|
| content_negotiation           |        | Yes  | Use content negotiation to
find new |
|                               |        |      | resources.
|
| detectReverseProxy            |        |      | Find out if the remote web
server   |
|                               |        |      | has a reverse proxy.
|
| detectTransparentProxy        |        |      | Find out if your ISP has a
|
|                               |        |      | transparent proxy installed.
|
| digitSum                      |        | Yes  | Take an URL with a number (
|
```

```
|                              |       |      | index2.asp ) and try to find
|
|                              |       |      | related files (index1.asp,
|
|                              |       |      | index3.asp).
|
| dir_bruter                   |       | Yes  | Finds Web server directories
by     |
|                              |       |      | bruteforcing.
|
| dnsWildcard                  |       |      | Find out if www.site.com and
|
|                              |       |      | site.com return the same
page.      |
| domain_dot                   |       |      | Send a specially crafted
request    |
|                              |       |      | with a dot after the domain
|
|                              |       |      | (http://host.tld./) and
analyze     |
|                              |       |      | response.
|
| dotNetErrors                 |       |      | Request specially crafted
URLs that |
|                              |       |      | generate ASP.NET errors in
order to |
|                              |       |      | gather information.
|
| favicon_identification       |       |      | Identify server software
using      |
|                              |       |      | favicon.
|
| findBackdoor                 |       |      | Find web backdoors and web
shells.  |
| findCaptchas                 |       |      | Identify captcha images on
web      |
|                              |       |      | pages.
|
| findDVCS                     |       |      | Find GIT, Mercurial (HG), and
|
|                              |       |      | Bazaar (BZR) repositories
|
| findGit                      |       |      | Find GIT repositories
|
| findJBoss                    |       |      | Find default Jboss
installations.   |
| findvhost                    |       |      | Modify the HTTP Host header
and try |
|                              |       |      | to find virtual hosts.
|
| fingerBing                   |       | Yes  | Search Bing to get a list of
users  |
```

```
|                              |       |      | for a domain.
|
| fingerGoogle                 |       | Yes  | Search Google using the
Google API  |
|                              |       |      | to get a list of users for a
|
|                              |       |      | domain.
|
| fingerPKS                    |       |      | Search MIT PKS to get a list
of     |
|                              |       |      | users for a domain.
|
| fingerprint_WAF              |       |      | Identify if a Web Application
|
|                              |       |      | Firewall is present and if
possible |
|                              |       |      | identify the vendor and
version.    |
| fingerprint_os               |       |      | Fingerprint the remote
operating    |
|                              |       |      | system using the HTTP
protocol.     |
| frontpage_version            |       |      | Search FrontPage Server Info
file   |
|                              |       |      | and if it finds it will
determine   |
|                              |       |      | its version.
|
| ghdb                         |       | Yes  | Search Google for
vulnerabilities   |
|                              |       |      | in the target site.
|
| googleSpider                 |       | Yes  | Search google using google
API to   |
|                              |       |      | get new URLs
|
| halberd                      |       |      | Identify if the remote server
has   |
|                              |       |      | HTTP load balancers.
|
| hmap                         |       | Yes  | Fingerprint the server type,
i.e    |
|                              |       |      | apache, iis, tomcat, etc.
|
| http_vs_https_dist           |       | Yes  | Determines the network
distance     |
|                              |       |      | between the http and https
ports    |
|                              |       |      | for a target.
|
| importResults                |       | Yes  | Import URLs found by other
tools.   |
```

```
| netcraft                    |        |      | Find out "What's that site
|
|                             |        |      | running?".
|
| oracleDiscovery             |        |      | Find Oracle applications on
the     |
|                             |        |      | remote web server.
|
| phishtank                   |        | Yes  | Search the phishtank.com
database   |
|                             |        |      | to determine if your server
is (or  |
|                             |        |      | was) being used in phishing
scams.  |
| phpEggs                     |        |      | Fingerprint the PHP version
using   |
|                             |        |      | documented easter eggs that
exist   |
|                             |        |      | in PHP.
|
| phpinfo                     |        |      | Search PHP Info file and if
it      |
|                             |        |      | finds it will determine the
version |
|                             |        |      | of PHP.
|
| ria_enumerator              |        | Yes  | Fingerprint Rich Internet
Apps -    |
|                             |        |      | Google Gears Manifest files,
|
|                             |        |      | Silverlight and Flash.
|
| robotsReader                |        |      | Analyze the robots.txt file
and     |
|                             |        |      | find new URLs
|
| serverHeader                |        | Yes  | Identify the server type
based on   |
|                             |        |      | the server header.
|
| serverStatus                |        |      | Find new URLs from the Apache
|
|                             |        |      | server-status cgi.
|
| sharedHosting               |        | Yes  | Use Bing search to determine
if the |
|                             |        |      | website is in a shared
hosting.     |
| sitemapReader               |        |      | Analyze the sitemap.xml file
and    |
|                             |        |      | find new URLs
|
```

```
| slash                          |        |      | Identify if the resource
|
|                                |        |      | http://host.tld/spam/ and
|
|                                |        |      | http://host.tld/spam are the
same.  |
| spiderMan                      |        | Yes  | SpiderMan is a local proxy
that     |
|                                |        |      | will collect new URLs.
|
| urlFuzzer                      |        | Yes  | Try to find backups, and
other     |
|                                |        |      | related files.
|
| urllist_txt                    |        |      | Analyze the urllist.txt file
and    |
|                                |        |      | find new URLs
|
| userDir                        |        | Yes  | Try to find user directories
like   |
|                                |        |      | "http://test/~user/" and
identify   |
|                                |        |      | the remote OS based on the
remote   |
|                                |        |      | users.
|
| webDiff                        |        | Yes  | Compare a local directory
with a    |
|                                |        |      | remote URL path.
|
| webSpider                      |        | Yes  | Crawl the web application.
|
| wordpress_enumerate_users      |        |      | Finds users in a WordPress
|
|                                |        |      | installation.
|
| wordpress_fingerprint          |        |      | Finds the version of a
WordPress    |
|                                |        |      | installation.
|
| wordpress_fullpathdisclosure |        |      | Try to find the path where
the      |
|                                |        |      | WordPress is installed
|
| wsdlFinder                     |        |      | Find web service definitions
files. |
| xssedDotCom                    |        |      | Search in xssed.com to find
xssed   |
|                                |        |      | pages.
|
| zone_h                         |        |      | Find out if the site was
defaced in |
```

```
|                              |        |      | the past.
|
|-------------------------------------------------------------------------
-------|
```

Step 3 - Start scan

```
w3af>>> start
```

Go further

Configuration profiles

Configuration can be saved as profile in ~/w3af/profiles.

```
w3af>>> profiles
w3af/profiles>>> save_as my_profile
Profile saved.
```

Note if the profile use another profile use self-contained to save it.

```
w3af/profiles>>> save_as my_profile self-contained
```

Saved profiles can be used like this :

```
w3af/profiles>>> use my_profile
The plugins configured by the scan profile have been enabled, and their
options configured.
Please set the target URL(s) and start the scan.
```

Built-in profiles :

```
w3af/profiles>>> list
|-------------------------------------------------------------------------
------|
| Profile                | Description
|
|-------------------------------------------------------------------------
------|
| bruteforce             | Bruteforce form or basic authentication access
controls  |
```

```
|                         | using default credentials. To run this profile, set
the  |
|                         | target URL to the resource where the access control
is,  |
|                         | and then click on Start.
|
| audit_high_risk         | Perform a scan to only identify the vulnerabilities
with |
|                         | higher risk, like SQL Injection, OS Commanding,
Insecure |
|                         | File Uploads, etc.
|
| full_audit_manual_disc | Perform a manual discovery using the spiderMan
plugin,   |
|                         | and afterwards scan the site for any known
|
|                         | vulnerabilities.
|
| full_audit              | This profile performs a full audit of the target
|
|                         | website, using only the webSpider plugin for
discovery.  |
| OWASP_TOP10             | The Open Web Application Security Project (OWASP)
is a   |
|                         | worldwide free and open community focused on
improving   |
|                         | the security of application software. OWASP
searched for |
|                         | and published the ten most common security flaws.
This   |
|                         | profile search for this top 10 security flaws. For
more  |
|                         | information about the security flaws:
|
|                         |
http://www.owasp.org/index.php/OWASP_Top_Ten_Project .   |
| fast_scan               | Perform a fast scan of the target site, using only
a few |
|                         | discovery plugins and the fastest audit plugins.
|
| empty_profile           | This is an empty profile that you can use to start
a new |
|                         | configuration from.
|
| web_infrastructure      | Use all the available techniques in w3af to
fingerprint  |
|                         | the remote Web infrastructure.
|
| sitemap                 | Use different online techniques to create a fast
sitemap |
|                         | of the target web application. This plugin will
only     |
```

```
|                       | work if you've got Internet access and the target
web    |
|                       | application is being spidered by Yahoo!
|
|-------------------------------------------------------------------------
------|
```

Authentication

```
w3af/plugins>>> auth
|-------------------------------------------------------------------------
-----|
| Plugin name     | Status    | Conf  | Description
|
|-------------------------------------------------------------------------
-----|
| detailed        |           | Yes   | Detailed authentication plugin.
|
| generic         | Enabled   | Yes   | Generic authentication plugin.
|
|-------------------------------------------------------------------------
-----|
w3af/plugins>>> auth generic
w3af/plugins>>> auth config generic
w3af/plugins/auth/config:generic>>> view
|-------------------------------------------------------------------------
-----|
| Setting        | Value | Description
|
|-------------------------------------------------------------------------
-----|
| username       |       | Username for using in the authentication
|
| check_url      |       | Check session URL - URL in which response body
|
|                |       | check_string will be searched
|
| check_string   |       | String for searching on check_url page to determine
if  |
|                |       | user is logged in the web application
|
| password_field |       | Password HTML field name
|
| username_field |       | Username HTML field name
|
| auth_url       |       | Auth URL - URL for POSTing the authentication
|
|                |       | information
|
```

```
| password       |       | Password for using in the authentication
|
|-------------------------------------------------------------------------
-----|
```

HTTP Headers

Create plain text header file with Key: value syntax.

```
w3af>>> http-settings
w3af/config:http-settings>>> set headersFile header.txt
```

Scripts

w3af can run a script file using the -s argument. Script files are text files with one w3af_console command on each line. An example script file would look like this:

```
plugins
output text_file
output config text_file
set output_file output-w3af.txt
set verbose True
back
```

Example script files can be found inside the scripts/ directory.