SEAT

(Search Engine Assessment Tool)

Documentation v.1.0

Midnight
Research Labs

Written by Peter Kacherginsky

iphelix@gmail.com

Table of Contents

0.0.0 Introduction....3
0.1.0 Features....3
0.1.1 Search Engine Abstraction....3
0.1.2 Performance....3
0.1.3 Usability....3
0.1.4 Anonymity....3
0.2.0 Installation....4
0.2.1 Ubuntu....4
0.2.2 Backtrack....4
0.3.0 Running SEAT....5
0.3.1 Assessment process....5
1.0.0 Preparation....6
1.1.0 Targets....6
1.1.1 Targets List....6
1.1.2 Adding a Target....7
1.1.3 Removing a Target....7
1.1.4 Loading Targets....7
1.1.5 Saving Targets....7
1.2.0 Queries....8
1.2.1 Queries List....8
1.2.2 Queries Description....8
1.2.3 Adding a Query....9
1.2.4 Removing a Query....9
1.2.5 Editing a Query....9
1.2.6 Loading Vulnerability Databases 9
1.2.7 Saving Vulnerability Databases....9
1.2.8 Advanced Query....10
2.0.0 Execution....11
2.1.0 Search Engines....11
2.1.1 Search Engines List....12
2.1.2 Adding a Search Engine....12
2.1.3 Removing a Search Engine....12
2.1.4 Editing a Search Engine....12
2.1.5 Loading Search Engines....13
2.1.6 Saving Search Engines....13
2.2.0 Preferences....14
2.2.1 Loading Preferences....15
2.2.2 Saving Preferences....15
2.3.0 Controlling Execution....15
2.4.0 Log Screen....15
2.5.0 Threads and Job Display....15
3.0.0 Analysis....16
3.1.0 Selecting Results....17
3.2.0 Viewing Individual Results....18
3.3.0 Removing Result Targets....18
3.4.0 Recycling Mined Results....18
3.5.0 Saving Results....19
4.0.0 Examples....20
4.1.0 Mining domains....20
4.2.0 Scanning IP Addresses....20
4.3.0 Using Vulnerability Databases....20

0.0.0 Introduction

SEAT (Search Engine Assessment Tool) is the next generation information digging application geared toward the needs of security professionals. SEAT uses information stored in search engine databases, cache repositories, and other public resources to scan web sites for potential vulnerabilities. It's multi-threaded, multi-database, and multi-search-engine capabilities permit easy navigation through vast amounts of information with a goal of system security assessment. Furthermore, SEAT's ability to easily process additional search engine signatures as well as custom made vulnerability databases allows security professionals to adapt SEAT to their specific needs.

0.1.0 Features

The most important strength of SEAT is it's ability to simulate what attackers or malware would do when they anonymously collect potentially harmful public information available on your site. Using SEAT you can perform similar assessments faster with the ability to dig through large sets of information to pinpoint potential vulnerabilities.

0.1.1 Search Engine Abstraction

SEAT utilizes search engine abstraction to automatically adapt queries to multiple search engines. This means that a single signature that could normally be applied to only a single search engine, will be abstracted and adapted to all search engines supported by SEAT. This will increase your chances of finding a vulnerability that would otherwise be missed by a single search engine approach.

0.1.2 Performance

From high performance database which allows you to quickly store and retrieve thousands of mined results and domains to flexible multi-threaded query engine, all parts of SEAT are optimized for quick and reliable performance.

Note: SEAT does not use APIs provided by some search engines, thus avoiding unnecessary limitations in the number of requests made in a given period of time.

0.1.3 Usability

A great deal of time went in to design of a user-friendly and efficient GUI to allow you to get the most from time spent working with the tool. Almost every part of SEAT can be adjusted to fit your individual needs while providing default settings for the beginning users.

0.1.4 Anonymity

SEAT offers a degree of anonymity due to its reliance on publicly available information to assess a target. At no point during its execution SEAT is communicating directly with the target site. This however does not mean you are 100% anonymous, because you are still communicating with various databases which if necessary can and will reveal logs of your activity. You have been warned.

0.2.0 Installation

You will need Perl versions 5.8.0-RC3 and later. Additionally SEAT requires several Perl modules:

- **Gtk2**
- **`threads`**
- **`threads::shared`**
- **`XML::Smart`**

0.2.1 Ubuntu

Default Ubuntu installation comes with both Gtk2 and threads Perl modules. Normally, your installation steps will be limited to the following:

```
sudo apt-get install libxml-smart-perl
```

0.2.2 Backtrack

Backtrack includes perl with ithreads. You will still need to add necessary modules to run the GUI:

```
cpan XML::Smart
cpan Glib
cpan Gtk2
```

0.3.0 Running SEAT

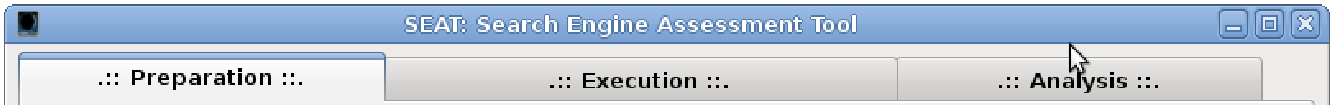
To run SEAT, change your directory to seat/ and execute SEAT with:

```
./seat
```

Note: There is no need for root privileges

0.3.1 Assessment process

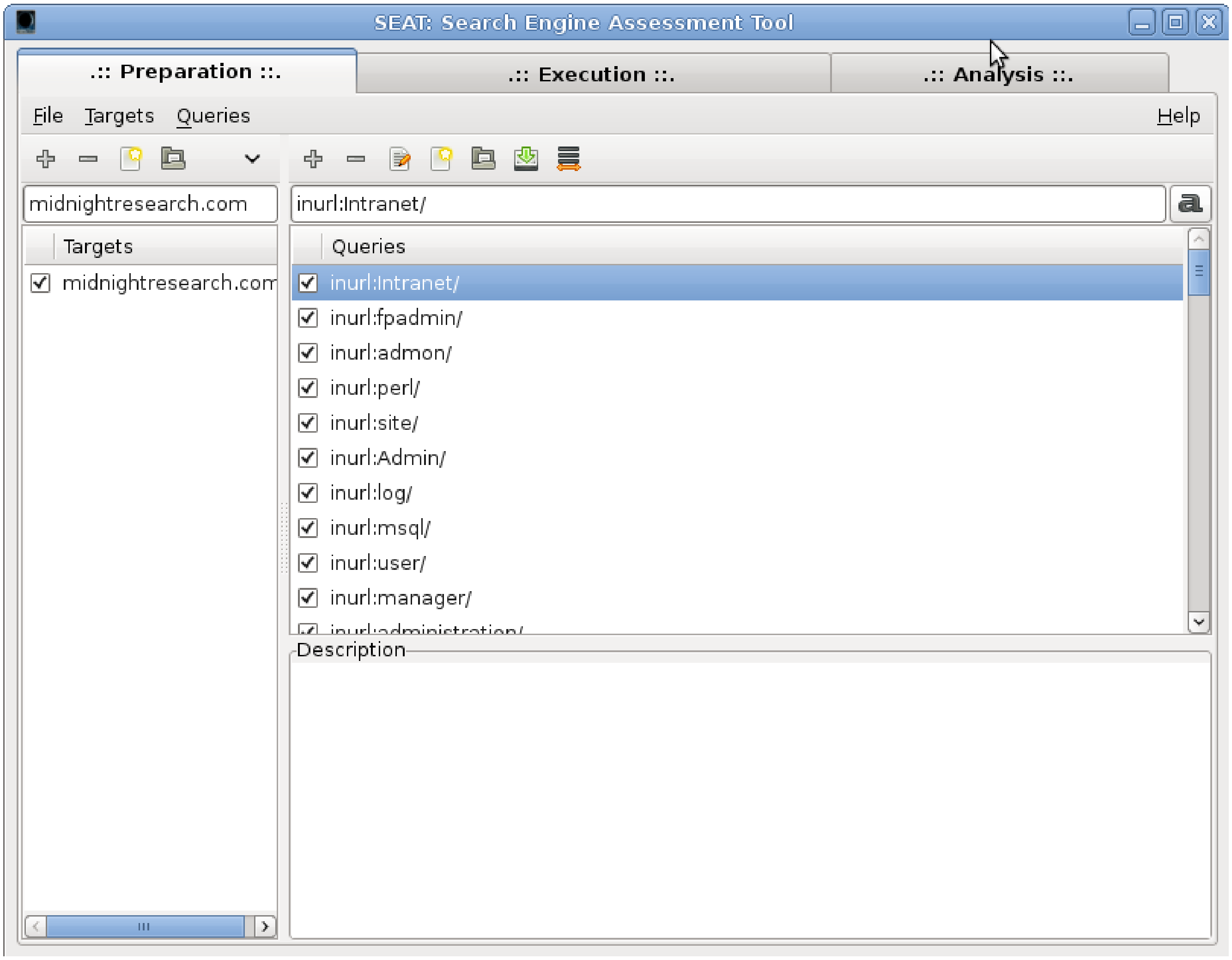
The overall assessment process is divided into three stages: Preparation, Execution, and Analysis. This division allows you to concentrate on one task at hand and not be overwhelmed or distracted by other tasks. Click on a respective tab in order to progress through the assessment.:



Hint: You can switch back and forward between various stages regardless of where are you in the program. This is useful for previewing results as they become available while SEAT is still executing.

1.0.0 Preparation

In the preparation stage your primary goal is to specify a list of targets to analyze, as well as select one or more vulnerability databases that come with SEAT or manually add your own signature.



midnightresearch.com

inurl:Intranet/

- ☑ midnightresearch.com

- ☑ inurl:Intranet/
- ☑ inurl:fpadmin/
- ☑ inurl:admon/
- ☑ inurl:perl/
- ☑ inurl:site/
- ☑ inurl:Admin/
- ☑ inurl:log/
- ☑ inurl:msql/
- ☑ inurl:user/
- ☑ inurl:manager/
- ☑ inurl:administration/

1.1.0 Targets

In the targets section of the GUI, you can specify a list of targets to scan.

1.1.1 Targets List

Targets list allows you to pick and choose which targets to scan. Only targets with a check next to them will be scanned. When adding new targets they will be automatically checked, you can temporarily remove the checkmark to avoid using that target during the scan.

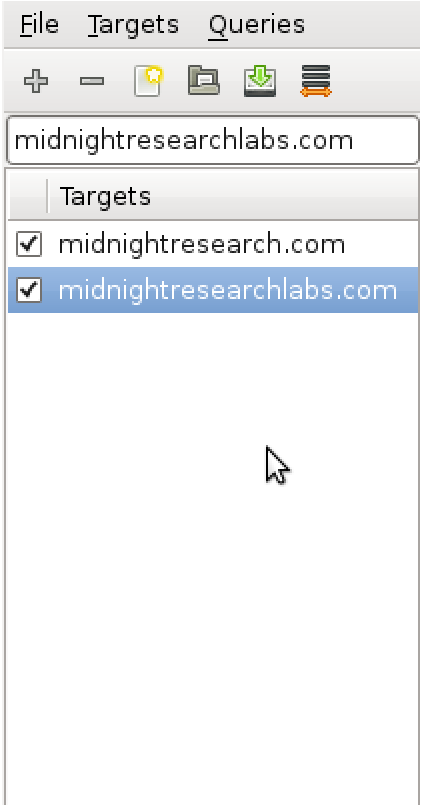
In order to create a fresh new list or simply clear an old one, click on the **New Targets List** button.

Hint: You can reverse targets list selection by clicking on the **Reverse Targets List** button.

Hint: To quickly search for a specific target name hit <control>F and type in a target name into the pop-up entry box.

1.1.2 Adding a Target

You can add a target by entering it into the targets entry box and clicking on the **Add Target** button . The target in the entry box can be either a domain name, an IP address, or even a range of IP addresses in the following format:



midnightresearchlabs.com

	Targets
☑	midnightresearch.com
☑	midnightresearchlabs.com

```
192.168.1.*

10.*.0.*
```

SEAT will automatically expand * wild card into a list of IP addresses.

Note: Although SEAT is a target oriented tool, for special cases during the assessment you may specify a universal target name *_GLOBAL* to indiscriminately scan and mine everything matching some vulnerability signature.

Hint: You can use common keyboard shortcuts to speed up your work. Use [ENTER] key to add a target to the list.

1.1.3 Removing a Target

To remove a target, select it in the targets list below and click on the **Remove Target** button.. The target will be removed from the list and will not be used during the scan.

Hint: You can use common keyboard shortcuts to speed up your work. Use [DEL] or [BACKSPACE] keys to remove a target from the list.

1.1.4 Loading Targets

You can load a targets list by clicking on the **Load Targets List** button. The file can be created by SEAT or any other program. If you would like to import a list of targets from another program or type one up yourself, make sure there is only one target per line:

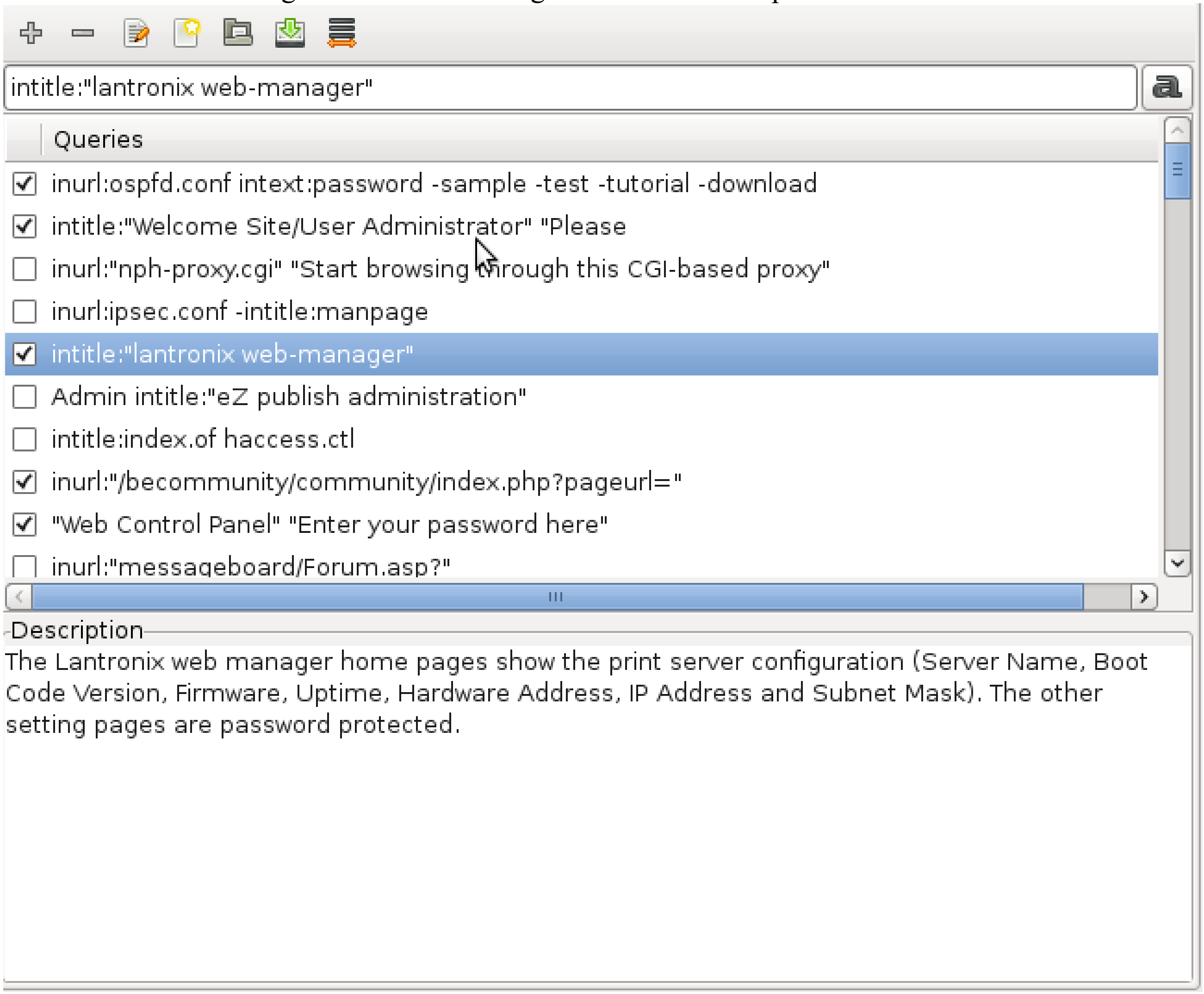
```
midnightresearch.com
midnightresearchlabs.com
...
```

1.1.5 Saving Targets

It is often useful to save targets list for later use. To do that click on the **Save Targets List** button. You will be presented with a dialog to choose where to save the targets list. The file generated will be a simple text file with targets arranged on individual lines.

1.2.0 Queries

In the queries section of the GUI, you can specify which queries to perform on the target. Each query in the list will be checked against all selected targets in order to find potential vulnerabilities.



intitle:"lantronix web-manager"

Queries

☑ inurl:ospfd.conf intext:password -sample -test -tutorial -download
☑ intitle:"Welcome Site/User Administrator" "Please
□ inurl:"nph-proxy.cgi" "Start browsing through this CGI-based proxy"
□ inurl:ipsec.conf -intitle:manpage
☑ intitle:"lantronix web-manager"
□ Admin intitle:"eZ publish administration"
□ intitle:index.of haccess.ctl
☑ inurl:"/becommunity/community/index.php?pageurl="
☑ "Web Control Panel" "Enter your password here"
□ inurl:"messageboard/Forum.asp?"

Description
The Lantronix web manager home pages show the print server configuration (Server Name, Boot Code Version, Firmware, Uptime, Hardware Address, IP Address and Subnet Mask). The other setting pages are password protected.

1.2.1 Queries List

Only queries with the check mark next to them will be scanned. This allows you to quickly add and remove queries to fine tune the scan.

In order to start on a fresh new list or simply clear an old list, click on the **New Query List** button.

Hint: You can reverse queries list selection by clicking on the **Reverse Queries List** button.

Hint: To quickly search for a specific query name hit <control>F and type in a search query name into the pop-up entry box.

1.2.2 Queries Description

If a query has description associated with it, you can view additional information about what it does in the Description box.

1.2.3 Adding a Query

The simplest way to add a query is to enter a query manually into the queries entry box and click on the **Add Query** button. The query will appear in the queries list. When entering queries, there is no need to use syntax specific to any one of the search engines. Simply use common Google-like keywords such as *intitle:*, *inurl*, etc. and SEAT's search engine abstraction engine will take care of adapting your queries to each individual search engine during the execution stage.

Note: For special cases during the assessment you may specify a blank query *_BLANK* to simply make a target request without testing for any particular signature. In fact, if you don't specify any queries at all, *_BLANK* request will be generated for you. This is useful for domain name mining as well as IP range scanning.

Hint: You can use common keyboard shortcuts to speed up your work. Use [ENTER] key to add a query to the list.

1.2.4 Removing a Query

To remove the currently selected query, simply click on the **Remove Query** button. The query will be removed from the queries list and will not be used during the scan.

1.2.5 Editing a Query

If you would like to edit a query or simply add information such as description, click on the **Edit Query** button and you will be presented with a dialog which will allow you to add necessary changes. See Advanced Query section for detailed explanation of the fields.

1.2.6 Loading Vulnerability Databases

SEAT comes with several popular vulnerability databases. Some like GHDB were designed specifically for search engines, others like NIKTO were created for the more traditional CGI scanners. SEAT is capable of importing all of these databases and generating queries for the subsequent scans.

To load a database click on the **Load Queries List** button and you will be presented with a file selection dialog. Signature databases are located in the folder *databases* in SEAT's root directory.

Hint: Load multiple databases for more extensive scans.

When you select a particular database, SEAT will automatically recognize the type of a database and generate appropriate queries.

Hint: Use database filter to narrow your selection to a specific Database type

1.2.7 Saving Vulnerability Databases

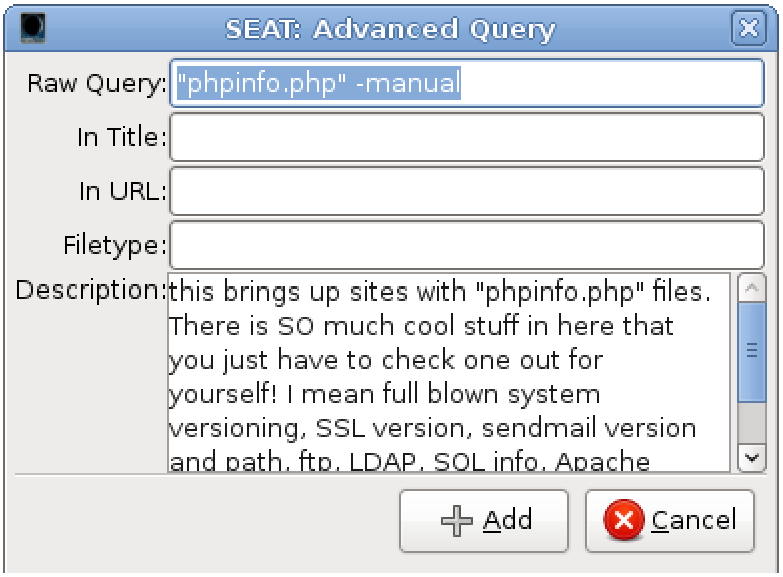
To save a new or modified query list click on the **Save Queries List** button. SEAT will generate an XML vulnerability database in the specified location which will hold your vulnerability signatures.

1.2.8 Advanced Query

To avoid using standard search keywords, you can utilize advanced query menu by clicking on the **Advanced Query** button. This will bring up a dialog that will assist you in generating advanced queries with no previous knowledge of search engine technology required.

The following fields are available in the advanced query menu:

- **Raw Query** – raw query request in the same format as the simple query entry above.
- **In Title** – Search in the Title of a page
- **In URL** – Search in the URL of a page
- **Filetype** – Search for a Filetype
- **Description** – Add a description to this query



Raw Query: "phpinfo.php" -manual

In Title:

In URL:

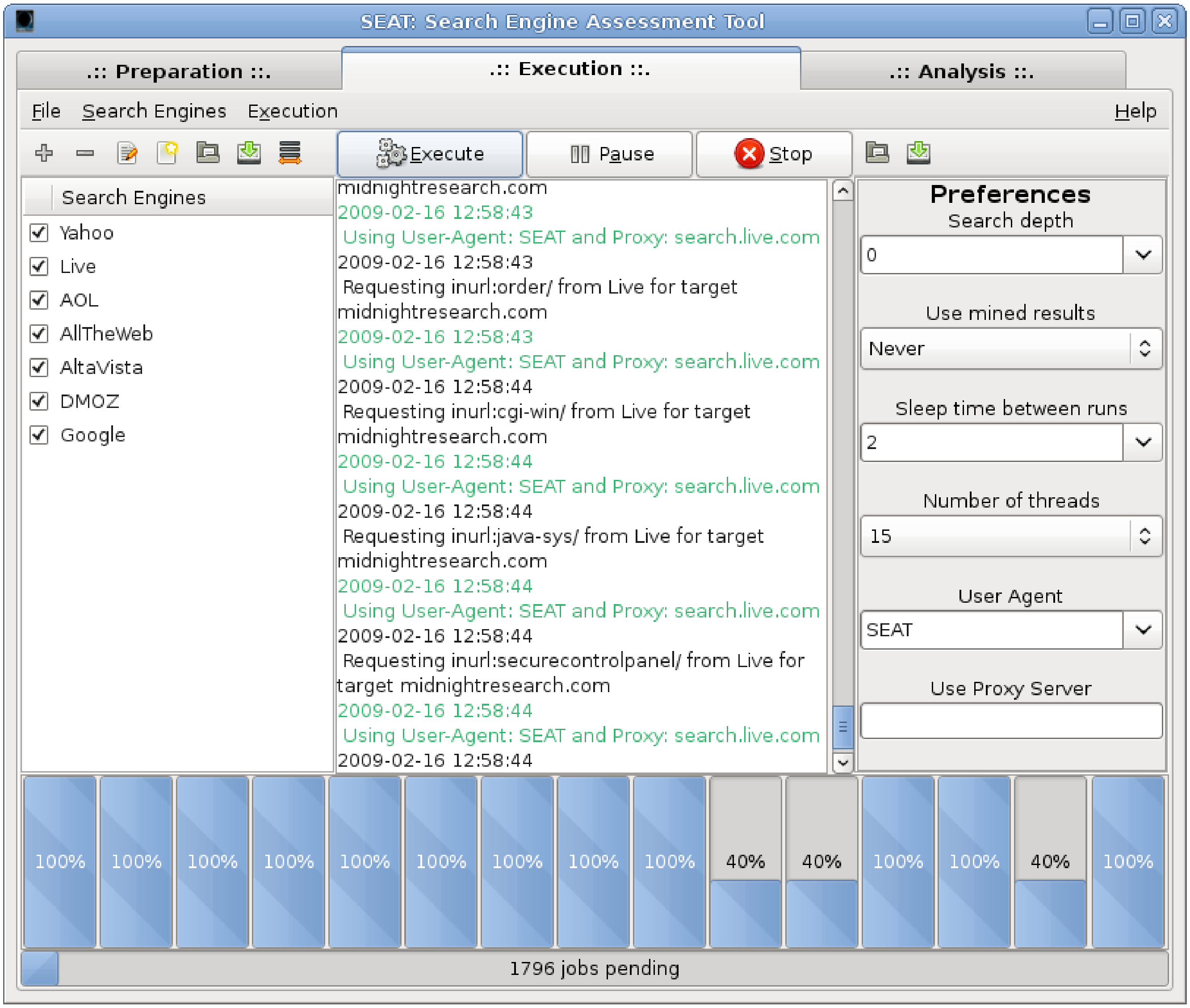
Filetype:

Description: this brings up sites with "phpinfo.php" files. There is SO much cool stuff in here that you just have to check one out for yourself! I mean full blown system versioning, SSL version, sendmail version and path, ftp, LDAP, SQL info, Apache

Hint: When you click on the Add button, the dialog will not close thus allowing you to quickly enter a series of queries.

2.0.0 Execution

During the execution stage, you can specify details to how a particular scan will be performed. You can select and edit Search Engines used for the scan, adjust performance preferences, as well as simulate more realistic scans by using various Proxy Servers and User Agent identifiers. As SEAT runs, you can adjust preferences on the right panel live. Meaning whatever changes you make will immediately take effect without restarting the scan.



Search Engines

☑ Yahoo
☑ Live
☑ AOL
☑ AllTheWeb
☑ AltaVista
☑ DMOZ
☑ Google

```
midnightresearch.com
2009-02-16 12:58:43
 Using User-Agent: SEAT and Proxy: search.live.com
2009-02-16 12:58:43
 Requesting inurl:order/ from Live for target
midnightresearch.com
2009-02-16 12:58:43
 Using User-Agent: SEAT and Proxy: search.live.com
2009-02-16 12:58:44
 Requesting inurl:cgi-win/ from Live for target
midnightresearch.com
2009-02-16 12:58:44
 Using User-Agent: SEAT and Proxy: search.live.com
2009-02-16 12:58:44
 Requesting inurl:java-sys/ from Live for target
midnightresearch.com
2009-02-16 12:58:44
 Using User-Agent: SEAT and Proxy: search.live.com
2009-02-16 12:58:44
 Requesting inurl:securecontrolpanel/ from Live for
target midnightresearch.com
2009-02-16 12:58:44
 Using User-Agent: SEAT and Proxy: search.live.com
2009-02-16 12:58:44
```

Preferences

Search depth: 0

Use mined results: Never

Sleep time between runs: 2

Number of threads: 15

User Agent: SEAT

Use Proxy Server:

100% 100% 100% 100% 100% 100% 100% 100% 100% 40% 40% 100% 100% 40% 100%

1796 jobs pending

2.1.0 Search Engines

In the Search Engines section you can select which Search Engines to use during the scan. Since SEAT relies on search engines to collect information, you will quickly discover that some search engines are better than others for various tasks. For example MSN is great for IP address scanning and co-host detection, while DMOZ is useful for mining unique sub domains. The king of search engines, Google, is great for vulnerability database scanning; however, be on a lookout for false positives.

In addition to simply using available search engines, SEAT allows you to add more search engine signatures or edit the existing ones to further enhance your scans.

2.1.1 Search Engines List

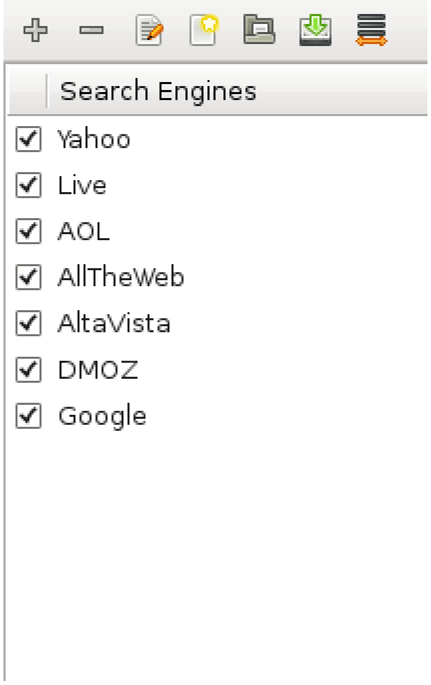
Only Search Engines with the check mark next to them will be used during the scan. This allows you to quickly add and remove search engines to adjust an individual scan.

In order to start on a fresh new list or simply clear an old list, click on the **New Search Engine List** button.

Hint: You can reverse search engines list selection by clicking on the **Reverse Search Engines List** button.

Hint: To quickly search for a specific search engine name hit <control>F and type in a search engine name into the pop-up entry box.

2.1.2 Adding a Search Engine



Search Engines

☑ Yahoo
☑ Live
☑ AOL
☑ AllTheWeb
☑ AltaVista
☑ DMOZ
☑ Google

To add a new Search Engine click on the **Add Search Engine** button. You will be presented with a blank template to specify a complete search engine signature. A few of the fields can be left blank depending on the capabilities of the search engine you are adding.

Hint: It is usually easier to edit an already existing search engine signature as opposed to building one from scratch.

2.1.3 Removing a Search Engine

To remove the currently selected search engine, simply click on the **Remove Search Engine** button. The search engine will be removed from the list and will not be used during the scan.

Hint: You can use common keyboard shortcuts to speed up your work. Use [DEL] key to remove a search engine from the list.

2.1.4 Editing a Search Engine

To edit a search engine click on the **Edit Search Engine** button and you will be presented with a dialog which will allow you to make necessary changes. Below is the explanation for the available fields using Google signature as an example search engine:

- **Name** – search engine's name

  Google

- **Prefix** – standard template to specify a query for the search engine

  `/search?hl=en&q=`

- **Server** – server name where to make requests

  `www.google.com`

- **Matchstring** – regex matchstring to extract the number of hits returned by the search engine

  `Results(?:.*)of\s(?:about\s)?<b>(.*?)<\/b>`

- **Results Matchstring** – regex matchstring to extract resultant sites returned by the search engine

  `<a class=l href=\"(.*?)\">`

- **Next Matchstring** – regex matchstring to extract a link to the next page of results

  `<td\snowrap\sclass=b><a\shref=(.*?)><img\ssrc=\/intl\/en\/nav_next\.gif`

- **Cache Matchstring** – regex matchstring to extract a link to the cached page

  `<a class=fl\shref=\”(.*?)\”>Cached<\/a>`

- **Site** – particular search engine's version of *site:* query keyword to specify target site

  `site:`

- **IP** – particular search engine's version of *ip:* query keyword to specify target IP address

  `site:`

- **In Title** – particular search engine's version of *intitle:* query keyword to specify search in the title of the page

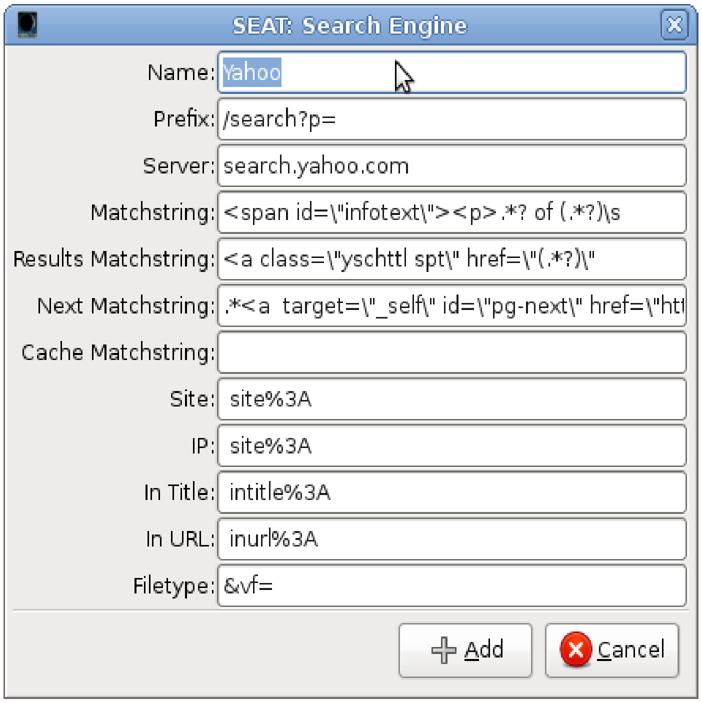
  `intitle:`

- **In URL** – particular search engine's version of *inurl*: query keyword to specify search in the url of the page

  `inurl:`

- **Filetype** – particular search engine's version of *filetype:* query keyword to specify file type of the result

  `filetype:`



SEAT: Search Engine

Name: Yahoo
Prefix: /search?p=
Server: search.yahoo.com
Matchstring: <span id=\"infotext\"><p>.*? of (.*?)\s
Results Matchstring: <a class=\"yschttl spt\" href=\"(.*?)\"
Next Matchstring: .*<a target=\"_self\" id=\"pg-next\" href=\"htt
Cache Matchstring:
Site: site%3A
IP: site%3A
In Title: intitle%3A
In URL: inurl%3A
Filetype: &vf=

Note: If a particular search engine does not support some keyword like filetype or does not have caching available, you can simply leave the two fields blank. Also notice how IP keyword for Google is the same as Site, this is because there is no way to specify an IP address as a target in Google so a standard *site:* is used instead.

2.1.5 Loading Search Engines

To load a search engine signature database click on the **Load Search Engines** button. Search Engine signature databases are located in the folder *searchengines* in SEAT's root directory.

2.1.6 Saving Search Engines

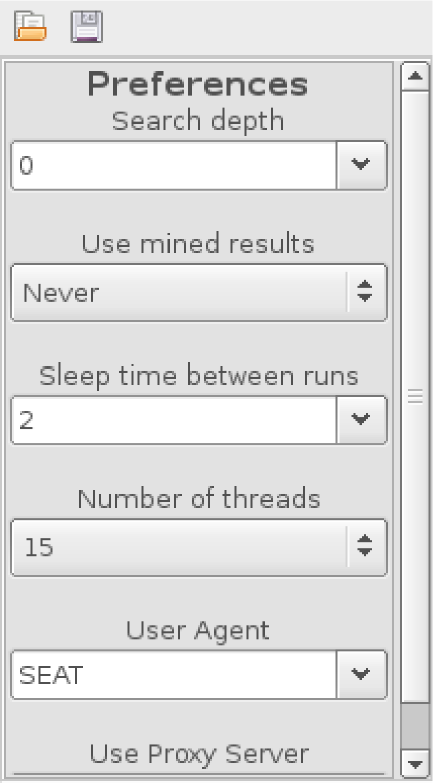
To save a new or modified Search Engines list click on the **Save Search Engines** list button. SEAT will generate an XML file in the specified location which will hold search engine signatures.

Note: SEAT loads *default.xml* signature database on startup.

2.2.0 Preferences

You can use various controls and settings in the Preferences column to fine tune SEAT's operation. All of the settings in the Preferences bar will take effect immediately even during the execution.

- **Search depth** – search depth specifies how many levels of search results SEAT will traverse. If you specify 0, that means SEAT will process results on the first page returned and give up on that particular search query; however, if you specify a higher depth, SEAT will continue digging through pages returned by the search engine. You can use one of the predefined values or type in your own.
- **Use mined results –** during the scan SEAT will try to mine domains that are related to the original target domain. Normally they will simply show up in the Analysis window, but you can also either generate new queries right away and make appropriate requests on the mined sites by selecting *Immediately Request* or simply save them to the targets list in the preparation stage for subsequent searches by selecting *Save for Later* option.



Preferences

Search depth: 0

Use mined results: Never

Sleep time between runs: 2

Number of threads: 15

User Agent: SEAT

Use Proxy Server

- **Sleep Time between runs** – sleep time specifies a time period between two search requests in a single thread. Increasing this number will slow down the scan but spare your and search engine's network bandwidth. Decreasing sleep time will likely get you banned by search engines for overloading their servers. (Use random User-Agents and Proxy servers to avoid the ban). You can use one of the predefined values or type in your own.
- **Number of threads** – with this setting you can control how many simultaneous requests (threads) SEAT will perform during the scan. Just like Sleep Time above, the number of threads should be optimized to your individual network and processing capabilities.
- **User-Agent** – User-Agent string is how SEAT identifies itself to search engines. Some search engines (MSN,Yahoo,etc.) have tendency to return different results for different User-Agent types. There are two special User Agent entries. If you select 'Random Bot' or 'Random Browser', SEAT will use a random User Agent string from its internal list of a few thousand User Agent strings for every request it makes. You can use one of the predefined values or type in your own.

  NOTE: Default search engine signatures are tuned for User-Agent “SEAT”
- **Proxy Server** – In case of a need to proxy all requests through a separate machine, you can specify HTTP proxy server in the following format:

  ```
  IP_or_domain:port_number
  ```

Hint: If you see a lot of “connection error” messages, that means you are overloading Search Engine servers. Simply increase sleep time between runs or decrease the number of simultaneous threads to avoid a long term ban.

2.2.1 Loading Preferences

To load default preferences or previously saved preferences, click on the **Load Preferences** button and select *.conf* file from the file menu.

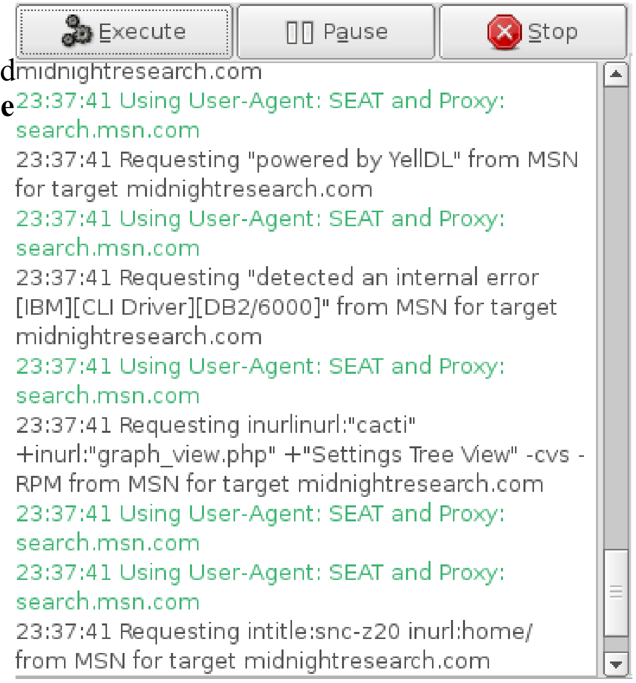
2.2.2 Saving Preferences

To avoid reentering changes made to default preferences, click on the **Save Preferences** button to save changes. You will be presented with a dialog which allows you to choose where to save your preferences file. Preferences are stored in the folder *preferences/* in SEAT's root directory.

Note: SEAT loads *default.conf* preferences file on startup.

2.3.0 Controlling Execution

Once you have finished specifying scan parameters and ready to start the querying engine, click on the **Execute** button to start the scan. In the process of the scan, you may pause execution by clicking on the **Pause** button or stop the scan completely by clicking on the **Stop** button. To resume a paused job, simply click on the **Execute** button again.



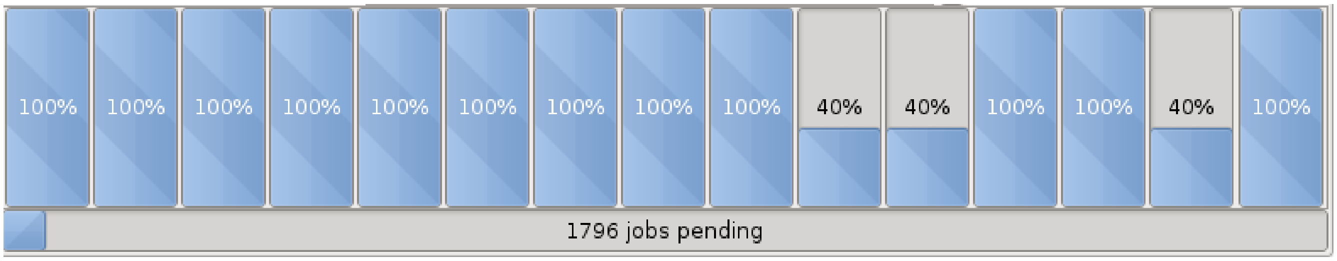
```
midnightresearch.com
23:37:41 Using User-Agent: SEAT and Proxy: search.msn.com
23:37:41 Requesting "powered by YellDL" from MSN for target midnightresearch.com
23:37:41 Using User-Agent: SEAT and Proxy: search.msn.com
23:37:41 Requesting "detected an internal error [IBM][CLI Driver][DB2/6000]" from MSN for target midnightresearch.com
23:37:41 Using User-Agent: SEAT and Proxy: search.msn.com
23:37:41 Requesting inurlinurl:"cacti" +inurl:"graph_view.php" +"Settings Tree View" -cvs -RPM from MSN for target midnightresearch.com
23:37:41 Using User-Agent: SEAT and Proxy: search.msn.com
23:37:41 Using User-Agent: SEAT and Proxy: search.msn.com
23:37:41 Requesting intitle:snc-z20 inurl:home/ from MSN for target midnightresearch.com
```

2.4.0 Log Screen

During the scan, SEAT will output a variety of information about its work. The information printed includes detailed request queries made, successful results collected, possible error messages, and other critical information.

2.5.0 Threads and Job Display

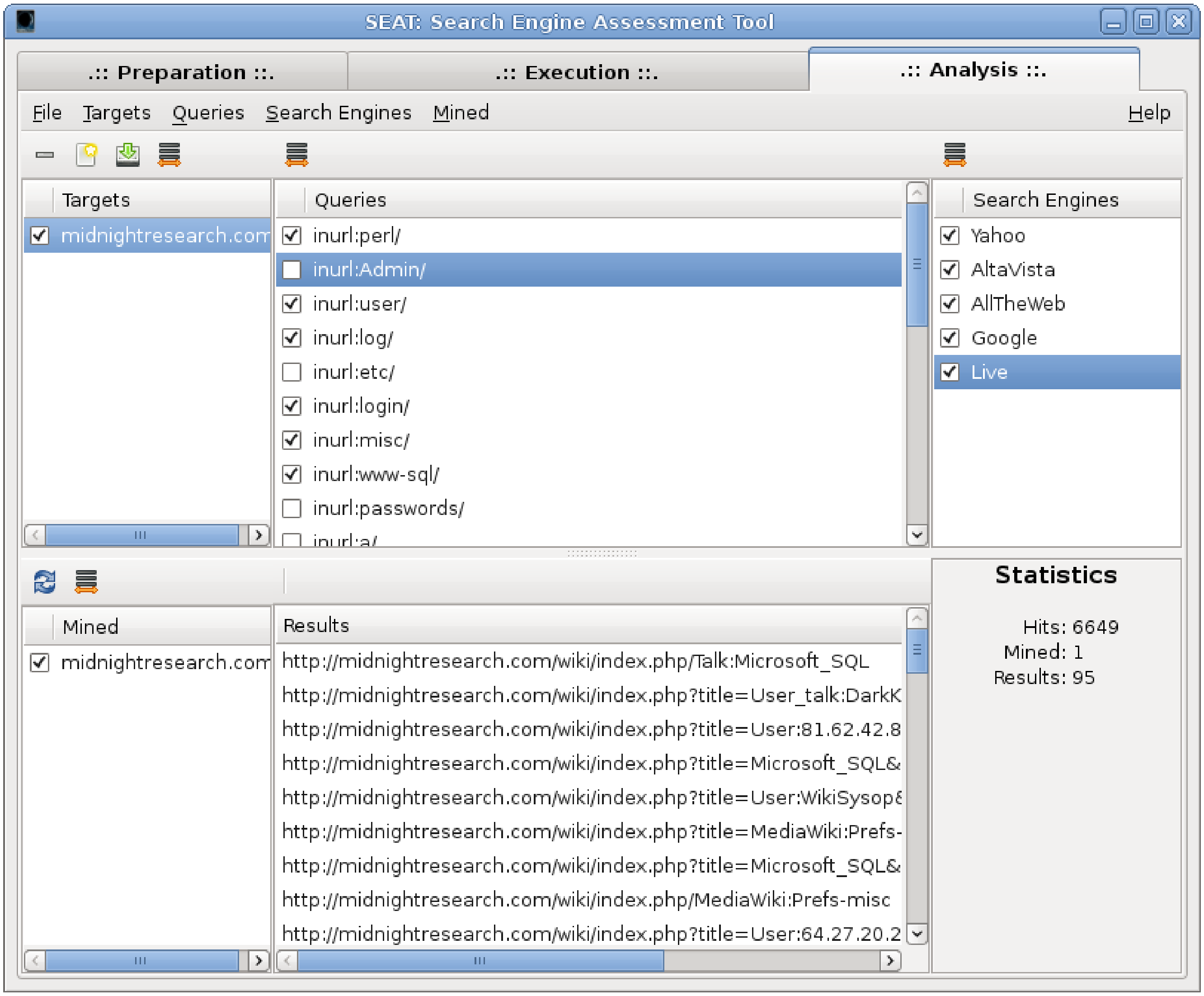
For visualization purposes, SEAT will display separate progress bars for each active thread , the overall progress made, and the number of jobs pending. It is possible to judge both the speed and the scope of the execution by observing this part of the display.



Note: SEAT will attempt to start the querying process as quickly as possible without waiting for all jobs to be generated. Thus in the beginning of the scan the number of jobs pending will actually increase because jobs are still being generated.

3.0.0 Analysis

In the final stage of the scan process, you will be presented with an easy navigation of the collected results. You can mix and match different targets, signatures, and search engines to learn the most about collected results.



Targets

☑ midnightresearch.com

Queries

☑ inurl:perl/
□ inurl:Admin/
☑ inurl:user/
☑ inurl:log/
□ inurl:etc/
☑ inurl:login/
☑ inurl:misc/
☑ inurl:www-sql/
□ inurl:passwords/
□ inurl:a/

Search Engines

☑ Yahoo
☑ AltaVista
☑ AllTheWeb
☑ Google
☑ Live

Mined

☑ midnightresearch.com

Results

http://midnightresearch.com/wiki/index.php/Talk:Microsoft_SQL
http://midnightresearch.com/wiki/index.php?title=User_talk:DarkK
http://midnightresearch.com/wiki/index.php?title=User:81.62.42.8
http://midnightresearch.com/wiki/index.php?title=Microsoft_SQL&
http://midnightresearch.com/wiki/index.php?title=User:WikiSysop&
http://midnightresearch.com/wiki/index.php?title=MediaWiki:Prefs-
http://midnightresearch.com/wiki/index.php?title=Microsoft_SQL&
http://midnightresearch.com/wiki/index.php/MediaWiki:Prefs-misc
http://midnightresearch.com/wiki/index.php?title=User:64.27.20.2

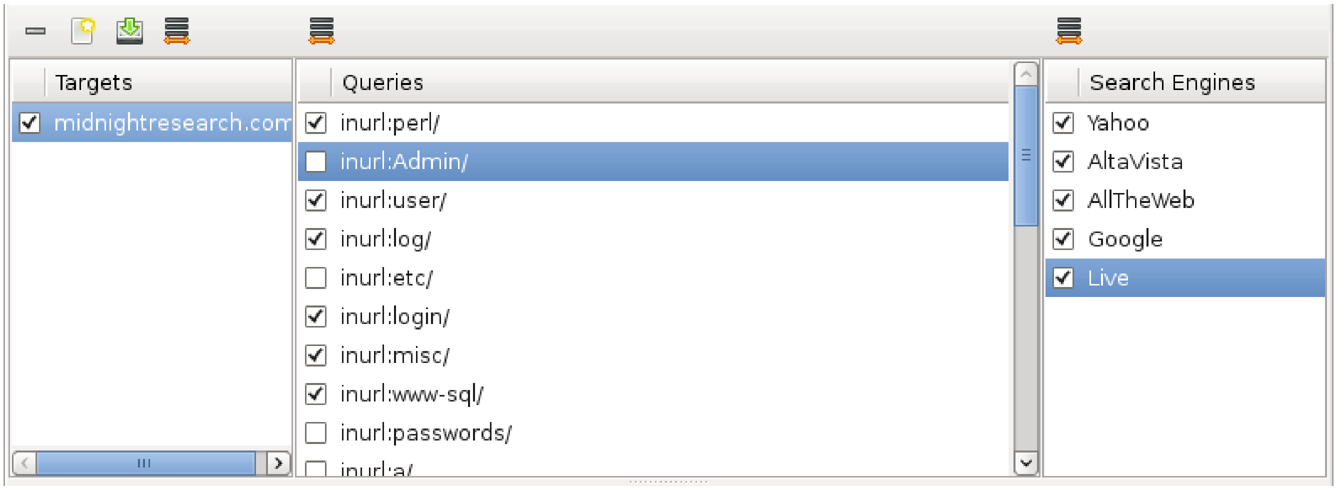
Statistics

Hits: 6649
Mined: 1
Results: 95

Note: You don't have wait for execution to stop before viewing the analysis window. As results are collected and processed, they will be added to the results database and displayed on the analysis database view screen right away.

3.1.0 Selecting Results

On the top half of the Analysis window you can see three different columns. One for each of the major parameters of the scan: Targets, Queries, and Search Engines. You can display varying amounts of information by adding and removing individual database entries.



Targets

☑ midnightresearch.com

Queries

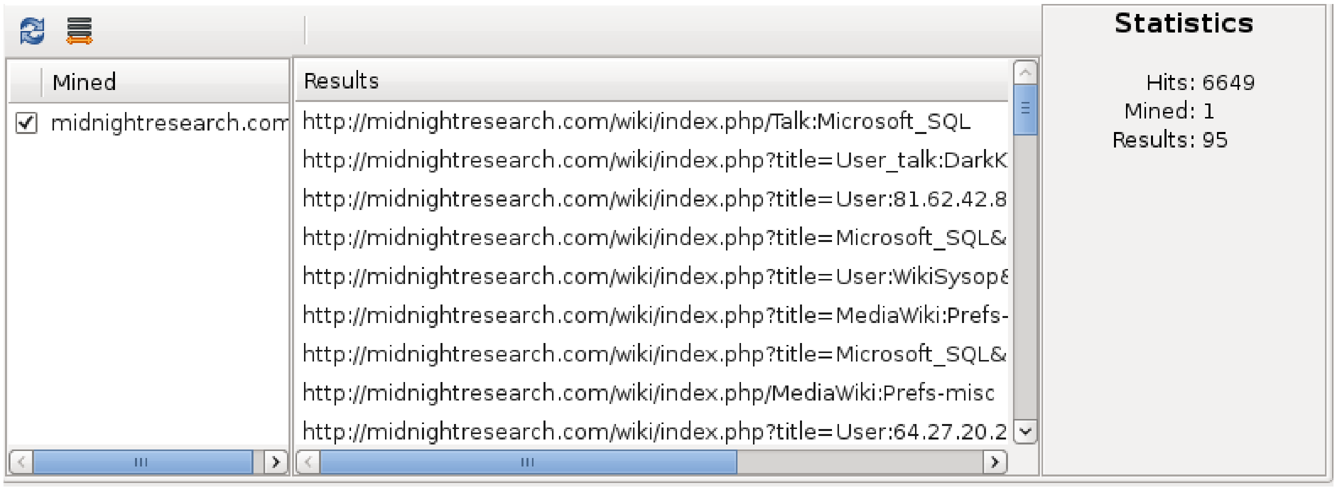
☑ inurl:perl/
□ inurl:Admin/
☑ inurl:user/
☑ inurl:log/
□ inurl:etc/
☑ inurl:login/
☑ inurl:misc/
☑ inurl:www-sql/
□ inurl:passwords/
□ inurl:a/

Search Engines

☑ Yahoo
☑ AltaVista
☑ AllTheWeb
☑ Google
☑ Live

Hint: Use **Inverse Selection** buttons to quickly view all results.

The results themselves will be displayed on the bottom half of the page also split into three columns. Mined domains collected during the scan will be displayed in the first column, exact site results returned by search engines will be displayed in the second column, and statistical information on the number of hits, mined domains, and overall sites collected will be displayed in the last column.



Mined

☑ midnightresearch.com

Results

http://midnightresearch.com/wiki/index.php/Talk:Microsoft_SQL
http://midnightresearch.com/wiki/index.php?title=User_talk:DarkK
http://midnightresearch.com/wiki/index.php?title=User:81.62.42.8
http://midnightresearch.com/wiki/index.php?title=Microsoft_SQL&
http://midnightresearch.com/wiki/index.php?title=User:WikiSysop&
http://midnightresearch.com/wiki/index.php?title=MediaWiki:Prefs-
http://midnightresearch.com/wiki/index.php?title=Microsoft_SQL&
http://midnightresearch.com/wiki/index.php/MediaWiki:Prefs-misc
http://midnightresearch.com/wiki/index.php?title=User:64.27.20.2

Statistics

Hits: 6649
Mined: 1
Results: 95

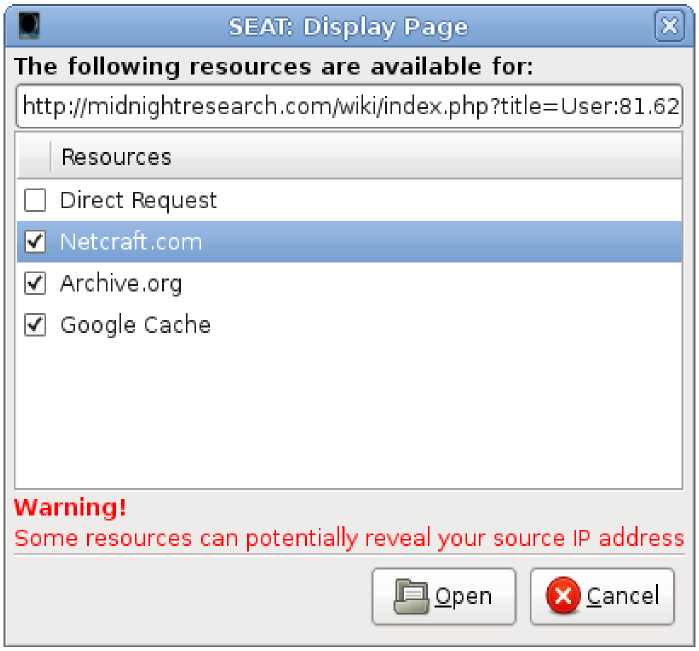
Hint: Use <control>F key combination to search for a specific result.

Note: Some search engines are a bit overzealous in trying to return results to your query, even when a particular query should not return anything at all. This creates a problem of false positives, thus you have to be suspicious if at some point a large number of signatures in the database matches the target

3.2.0 Viewing Individual Results

You can find out more information about an individual result by double-clicking on items in either Mined or Results columns. You will be presented with a dialog of various resources available for this target:

- **Direct Request** – Launches a browser window with the result itself. *This will reveal your source IP to the target site.*
- **Netcraft.com** – Displays information available on that particular site from Netcraft.com. Information includes IP address, WHOIS information, Server and OS version, etc. *Your source IP address will not be revealed to the target site.*
- **Archive.org –** Displays archived information over a long period of time. You may compare and contrast various changes made to learn more about the site. *Your source IP address will not be revealed to the target site.*
- **Google Cache –** Displays information stored in Google Cache. *Your source IP address may be revealed to the target site.*
- **Google Translate –** Displays information using a trick with Google Translate. *Your source IP address may be revealed to the target site.*



SEAT: Display Page

The following resources are available for:

http://midnightresearch.com/wiki/index.php?title=User:81.62

Resources
☐ Direct Request
☑ Netcraft.com
☑ Archive.org
☑ Google Cache

Warning!
Some resources can potentially reveal your source IP address

Depending on the level of anonymity you would like to preserve, choose appropriate resources. Once you have selected one or more of the resources in the list, you may click on the Open button to display those resources in the browser.

3.3.0 Removing Result Targets

If you find that a particular target is not useful and would like to remove it, simply click on the **Remove Target** button. The removed target will not appear in the generated report.

3.4.0 Recycling Mined Results

You can add mined results to the subsequent scans by clicking on the **Recycle Mined Results** button. This will copy all of the selected sites to the targets list in the Preparation window.

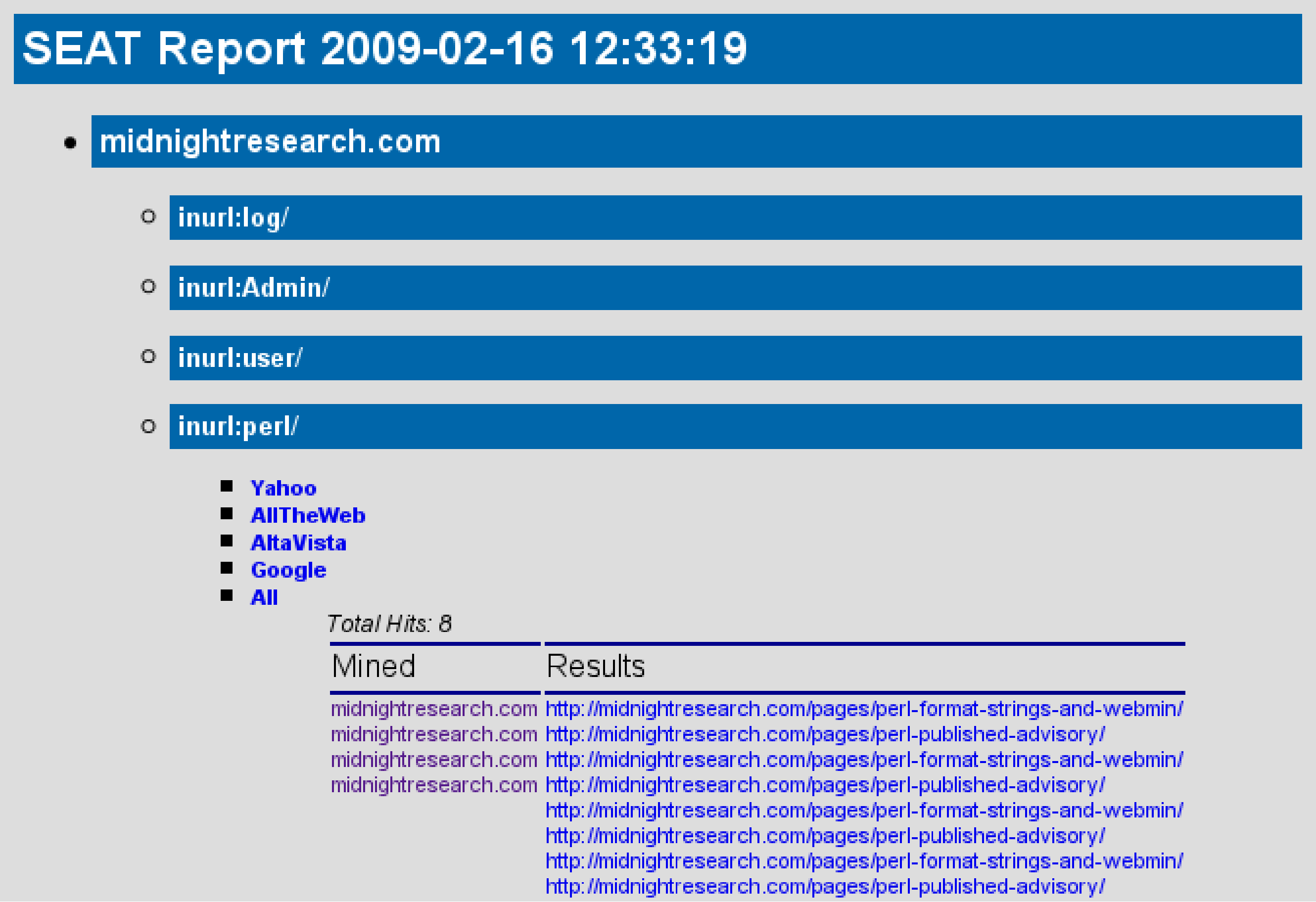
Hint: To make SEAT recycle mined results automatically select appropriate option in the preferences.

3.5.0 Saving Results

To save results database to a file, click on the **Save Results** Button. you will be presented with a dialog where you can choose the location where to save your file, as well as the type of report you would like to generate. You can generate the following report types:

- **HTML** – Generate a complete report in HTML with all collected information in the results database.
- **HTML Mined –** Generate a report in HTML with only Mined results.
- **HTML Results** – Generate a report in HTML with only Results returned by Search Engines.
- **TXT -** Generate a complete report in TXT with all collected information in the results database.
- **TXT Mined –** Generate a report in TXT with only Mined results. This type of report is particularly useful as a source for other applications.
- **TXT Results** – Generate a report in TXT with only Results returned by Search Engines.

Below is a sample HTML report illustrating hierarchical output:



SEAT Report 2009-02-16 12:33:19

- midnightresearch.com
  - inurl:log/
  - inurl:Admin/
  - inurl:user/
  - inurl:perl/
    - Yahoo
    - AllTheWeb
    - AltaVista
    - Google
    - All

Total Hits: 8

Mined	Results
midnightresearch.com	http://midnightresearch.com/pages/perl-format-strings-and-webmin/
midnightresearch.com	http://midnightresearch.com/pages/perl-published-advisory/
midnightresearch.com	http://midnightresearch.com/pages/perl-format-strings-and-webmin/
midnightresearch.com	http://midnightresearch.com/pages/perl-published-advisory/
	http://midnightresearch.com/pages/perl-format-strings-and-webmin/
	http://midnightresearch.com/pages/perl-published-advisory/
	http://midnightresearch.com/pages/perl-format-strings-and-webmin/
	http://midnightresearch.com/pages/perl-published-advisory/

4.0.0 Examples

Below are a few examples of using SEAT. For more details and recorded videos of examples below please visit http://midnightresearch.com/projects/search-engine-assessment-tool.

4.1.0 Mining domains

To increase your chances of finding vulnerabilities, you must use as many unique targets as possible. You can use SEAT to mine for related sites by simply searching for either a domain itself combined with _BLANK query or one or more keywords that are specific to the target site with the target _GLOBAL as a parameter.

Note: Although subdomain.domain.com and domain.com are completely different targets for traditional CGI scanners, for search engines a single scan on domain.com will return results for the domain name itself and all of its subdomains. Thus, all of the collected mined domains are extremely useful for export to CGI scanners as part of a complete assessment process, but only unique mined domain names are useful for SEAT itself.

4.2.0 Scanning IP Addresses

To find out which sites are hosted on a particular IP address or a range of IP addresses, specify an IP address as a target for SEAT and execute it with no queries. SEAT will attempt to mine sites associated with the provided IP address. This is useful for diversifying your primary vulnerability scans as well as learning about relationship among various sites which could not be immediately apparent.

4.3.0 Using Vulnerability Databases

Once you have created a good targets list, it is time to select one or more vulnerability databases and proceed with the scan as previously described in the documentation. Once the execution is complete, you can analyze the collected results or generate a report to look at a later time.