sait.ca

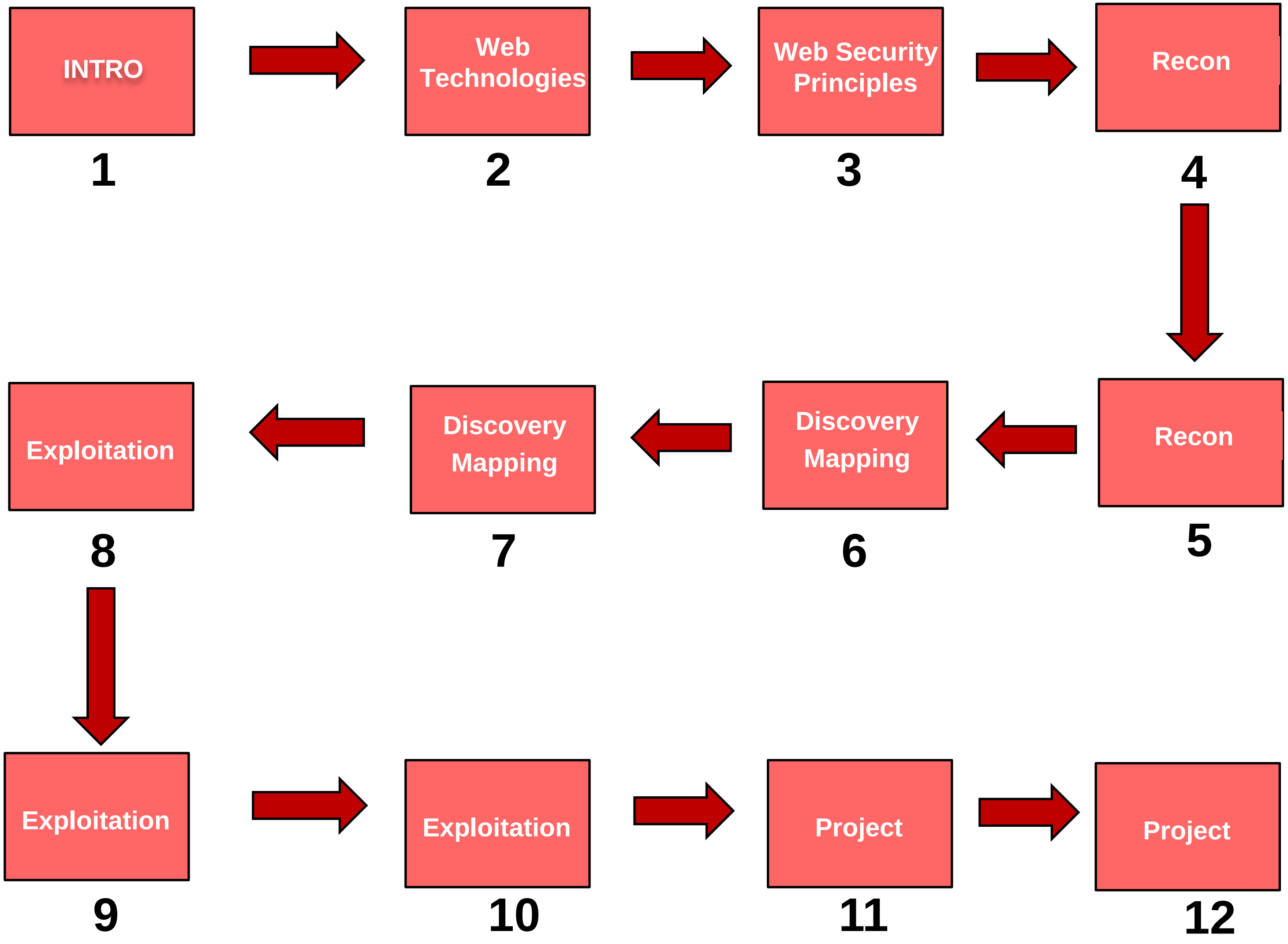
SAIT POLYTECHNIC

FURTHER YOUR PASSION

Web App & Data Base Security

Discovery

Web App & Data Base Security



Agenda

- Web app vulnerability scanner;
- Choosing the right Plugins;
- Nikto for scanning the web servers;
- Grendel-scan web app scanner;
- W3af web app scanner;
- LAB 1: Playing with Nikto;
- LAB 2: Scanning web application with Grendel-scan and w3af.

Web App Vulnerability Scanners

- Web app vulnerabilities scanners are different from scanners like Nessus;
- Web scanners interact with the site, through spidering or proxies;
- The interaction changes the way the plugins send traffic;
  - Grendel-Scan;
  - W3af;
  - **Skipfish;**
  - **Websecurify.**

Find more information about these two tools

Choosing Plug-ins

- Automated tools require multiple scans of the target;
- Selecting all the plugins at once is not a good idea:
  - Causes crashes due to resource limits;
  - Overwhelm the tools and the tester with lots of information.
- Each scan should us similar or grouped plugins:
  - Spider + Information Gathering;
  - Spider + SQL Injection + OS Command injection;
  - Spider + XSS + XSRF.

Nikto

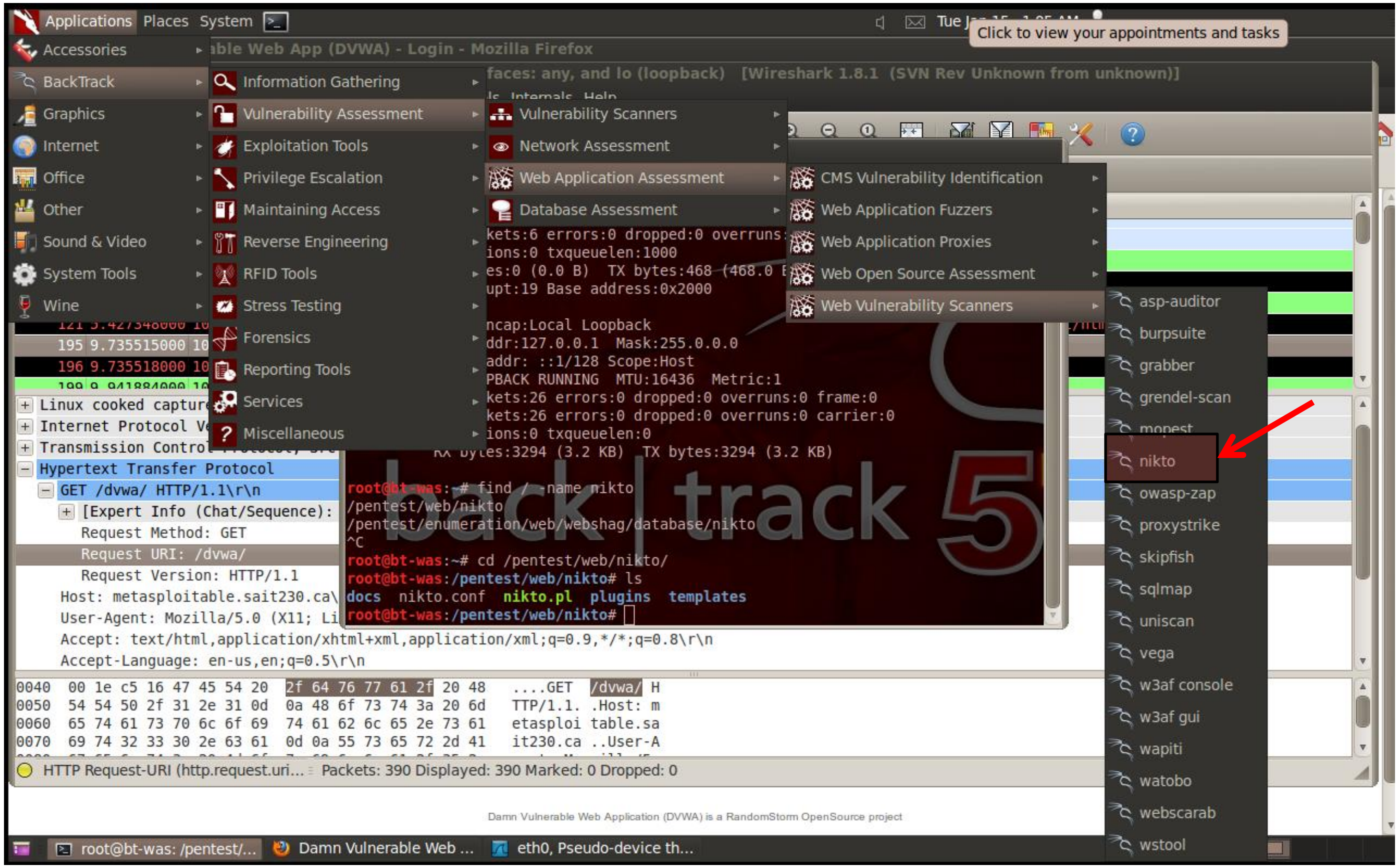
After running a port scan and discovering a service running on port 80 or 443, one of the first tools that should be used to evaluate the service is Nikto.

- It automates the process of scanning web servers for out-of-date and unpatched software;
- Searching for dangerous files that may reside on the web servers;
- It is capable of identifying a wide range of specific issues;
- Checks for server configuration issues.

Nikto

Discovering

NIKTO: a web server vulnerability scanner



```
kets:6 errors:0 dropped:0 overruns:
ions:0 txqueuelen:1000
es:0 (0.0 B)  TX bytes:468 (468.0 B
upt:19 Base address:0x2000

ncap:Local Loopback
ddr:127.0.0.1  Mask:255.0.0.0
addr: ::1/128 Scope:Host
PBACK RUNNING  MTU:16436  Metric:1
kets:26 errors:0 dropped:0 overruns:0 frame:0
kets:26 errors:0 dropped:0 overruns:0 carrier:0
ions:0 txqueuelen:0
     RX bytes:3294 (3.2 KB)  TX bytes:3294 (3.2 KB)

root@bt-was:~# find / -name nikto
/pentest/web/nikto
/pentest/enumeration/web/webshag/database/nikto
^C
root@bt-was:~# cd /pentest/web/nikto/
root@bt-was:/pentest/web/nikto# ls
docs  nikto.conf  nikto.pl  plugins  templates
root@bt-was:/pentest/web/nikto# 
```

```
121 5.427348000 10
195 9.735515000 10
196 9.735518000 10
199 9.941884000 10
+ Linux cooked captur
+ Internet Protocol Ve
+ Transmission Contro
- Hypertext Transfer Protocol
  - GET /dvwa/ HTTP/1.1\r\n
    + [Expert Info (Chat/Sequence):
      Request Method: GET
      Request URI: /dvwa/
      Request Version: HTTP/1.1
    Host: metasploitable.sait230.ca\
    User-Agent: Mozilla/5.0 (X11; Li
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
    Accept-Language: en-us,en;q=0.5\r\n

0040  00 1e c5 16 47 45 54 20  2f 64 76 77 61 2f 20 48   ....GET  /dvwa/ H
0050  54 54 50 2f 31 2e 31 0d  0a 48 6f 73 74 3a 20 6d   TTP/1.1. .Host: m
0060  65 74 61 73 70 6c 6f 69  74 61 62 6c 65 2e 73 61   etasploi table.sa
0070  69 74 32 33 30 2e 63 61  0d 0a 55 73 65 72 2d 41   it230.ca ..User-A

HTTP Request-URI (http.request.uri...  Packets: 390 Displayed: 390 Marked: 0 Dropped: 0
```

Found on:#pentest/web/nikto

Nikto

Discovering

NIKTO: a web server vulnerability scanner

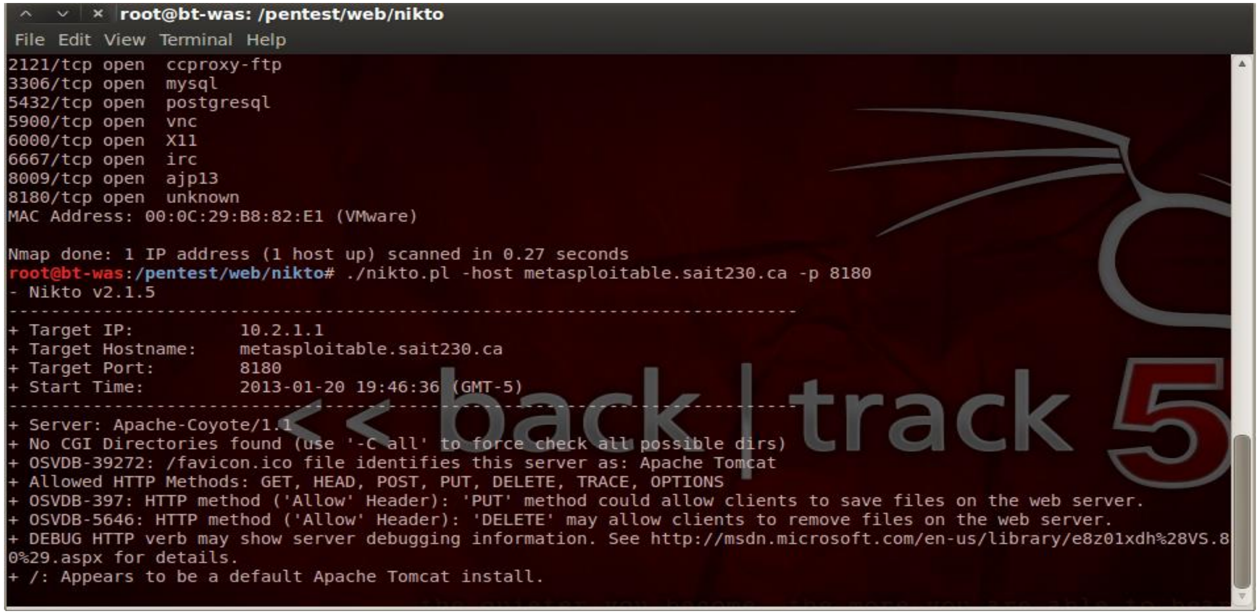
Syntax

:/pentest/web/nikto# ./nikto.pl [options] hostname

EXAMPLE

[root@sait /pentest/web/nikto]#./nikto.pl –host metasploitable.sait230.ca –p 8180

Results



```
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 00:0C:29:B8:82:E1 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.27 seconds
root@bt-was:/pentest/web/nikto# ./nikto.pl -host metasploitable.sait230.ca -p 8180
- Nikto v2.1.5
---------------------------------------------------------------------------
+ Target IP:          10.2.1.1
+ Target Hostname:    metasploitable.sait230.ca
+ Target Port:        8180
+ Start Time:         2013-01-20 19:46:36 (GMT-5)
---------------------------------------------------------------------------
+ Server: Apache-Coyote/1.1
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ OSVDB-39272: /favicon.ico file identifies this server as: Apache Tomcat
+ Allowed HTTP Methods: GET, HEAD, POST, PUT, DELETE, TRACE, OPTIONS
+ OSVDB-397: HTTP method ('Allow' Header): 'PUT' method could allow clients to save files on the web server.
+ OSVDB-5646: HTTP method ('Allow' Header): 'DELETE' may allow clients to remove files on the web server.
+ DEBUG HTTP verb may show server debugging information. See http://msdn.microsoft.com/en-us/library/e8z01xdh%28VS.8
0%29.aspx for details.
+ /: Appears to be a default Apache Tomcat install.
```

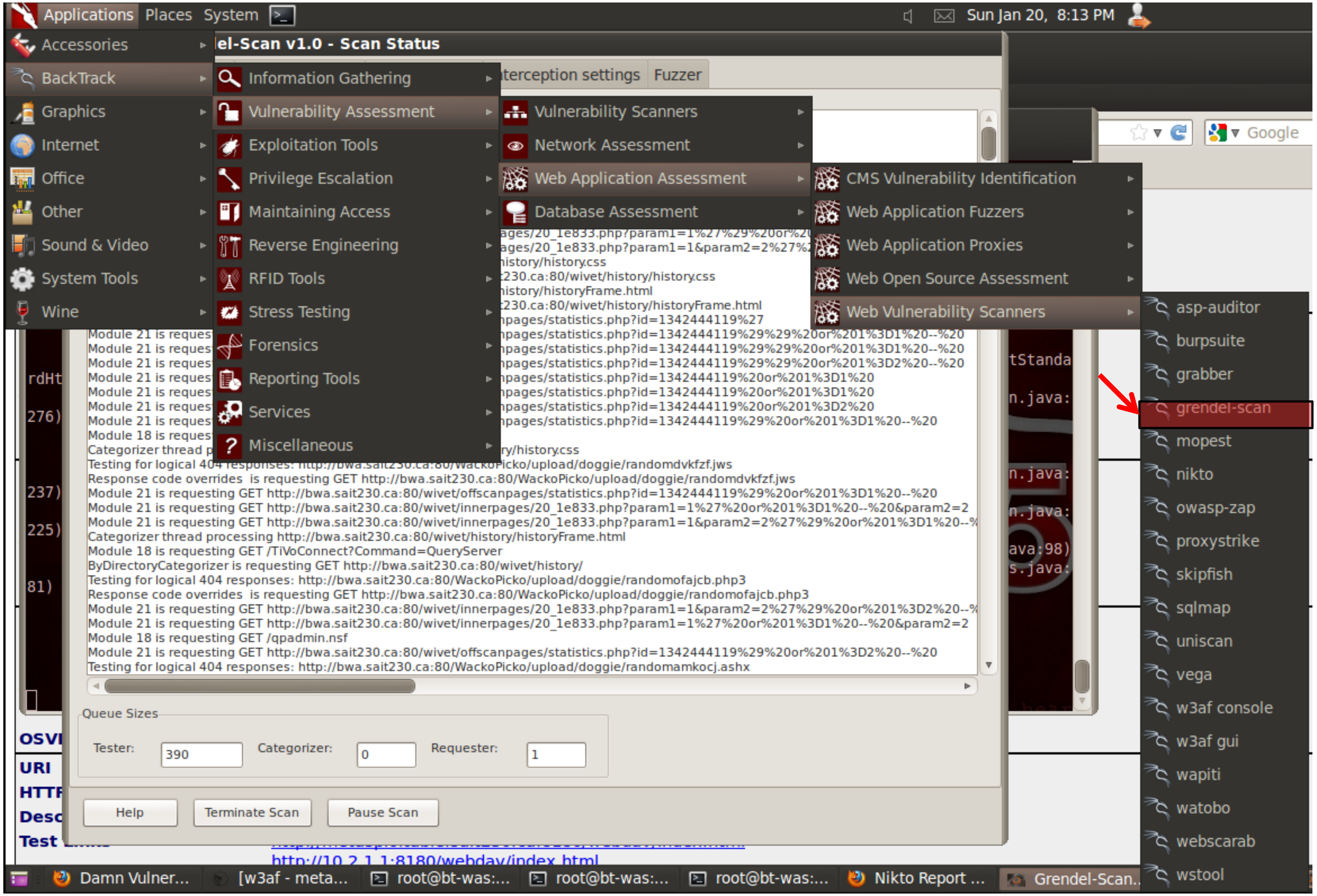
Add –o /tmp/results.html to specifies the output.

Grendel-Scan

- Grendel-Scan is a cross-platform application that automates a large portion of the discovery step;
- It scans, detects and exploits the common web application vulnerabilities;
- It spiders web sites similarly to other spiders already covered;
- Found on sourceforge.net/projects/grendel.

Grendel-Scan

Discovering



```
ages/20_1e833.php?param1=1%27%29%20or%20
ages/20_1e833.php?param1=1&param2=2%27%2
istory/history.css
230.ca:80/wivet/history/history.css
istory/historyFrame.html
230.ca:80/wivet/history/historyFrame.html
pages/statistics.php?id=1342444119%27
Module 21 is reques    pages/statistics.php?id=1342444119%29%29%20or%201%3D1%20--%20
Module 21 is reques    pages/statistics.php?id=1342444119%29%29%20or%201%3D1%20--%20
Module 21 is reques    pages/statistics.php?id=1342444119%29%29%20or%201%3D2%20--%20
Module 21 is reques    pages/statistics.php?id=1342444119%20or%201%3D1%20
Module 21 is reques    pages/statistics.php?id=1342444119%20or%201%3D1%20
Module 21 is reques    pages/statistics.php?id=1342444119%20or%201%3D2%20
Module 21 is reques    pages/statistics.php?id=1342444119%29%20or%201%3D1%20--%20
Module 18 is reques
Categorizer thread p    ry/history.css
Testing for logical 404 responses: http://bwa.sait230.ca:80/WackoPicko/upload/doggie/randomdvkfzf.jws
Response code overrides  is requesting GET http://bwa.sait230.ca:80/WackoPicko/upload/doggie/randomdvkfzf.jws
Module 21 is requesting GET http://bwa.sait230.ca:80/wivet/offscanpages/statistics.php?id=1342444119%29%20or%201%3D1%20--%20
Module 21 is requesting GET http://bwa.sait230.ca:80/wivet/innerpages/20_1e833.php?param1=1%27%20or%201%3D1%20--%20&param2=2
Module 21 is requesting GET http://bwa.sait230.ca:80/wivet/innerpages/20_1e833.php?param1=1&param2=2%27%29%20or%201%3D1%20--%
Categorizer thread processing http://bwa.sait230.ca:80/wivet/history/historyFrame.html
Module 18 is requesting GET /TiVoConnect?Command=QueryServer
ByDirectoryCategorizer is requesting GET http://bwa.sait230.ca:80/wivet/history/
Testing for logical 404 responses: http://bwa.sait230.ca:80/WackoPicko/upload/doggie/randomofajcb.php3
Response code overrides  is requesting GET http://bwa.sait230.ca:80/WackoPicko/upload/doggie/randomofajcb.php3
Module 21 is requesting GET http://bwa.sait230.ca:80/wivet/innerpages/20_1e833.php?param1=1&param2=2%27%29%20or%201%3D2%20--%
Module 21 is requesting GET http://bwa.sait230.ca:80/wivet/innerpages/20_1e833.php?param1=1%27%20or%201%3D1%20--%20&param2=2
Module 18 is requesting GET /qpadmin.nsf
Module 21 is requesting GET http://bwa.sait230.ca:80/wivet/offscanpages/statistics.php?id=1342444119%29%20or%201%3D2%20--%20
Testing for logical 404 responses: http://bwa.sait230.ca:80/WackoPicko/upload/doggie/randomamkocj.ashx
```

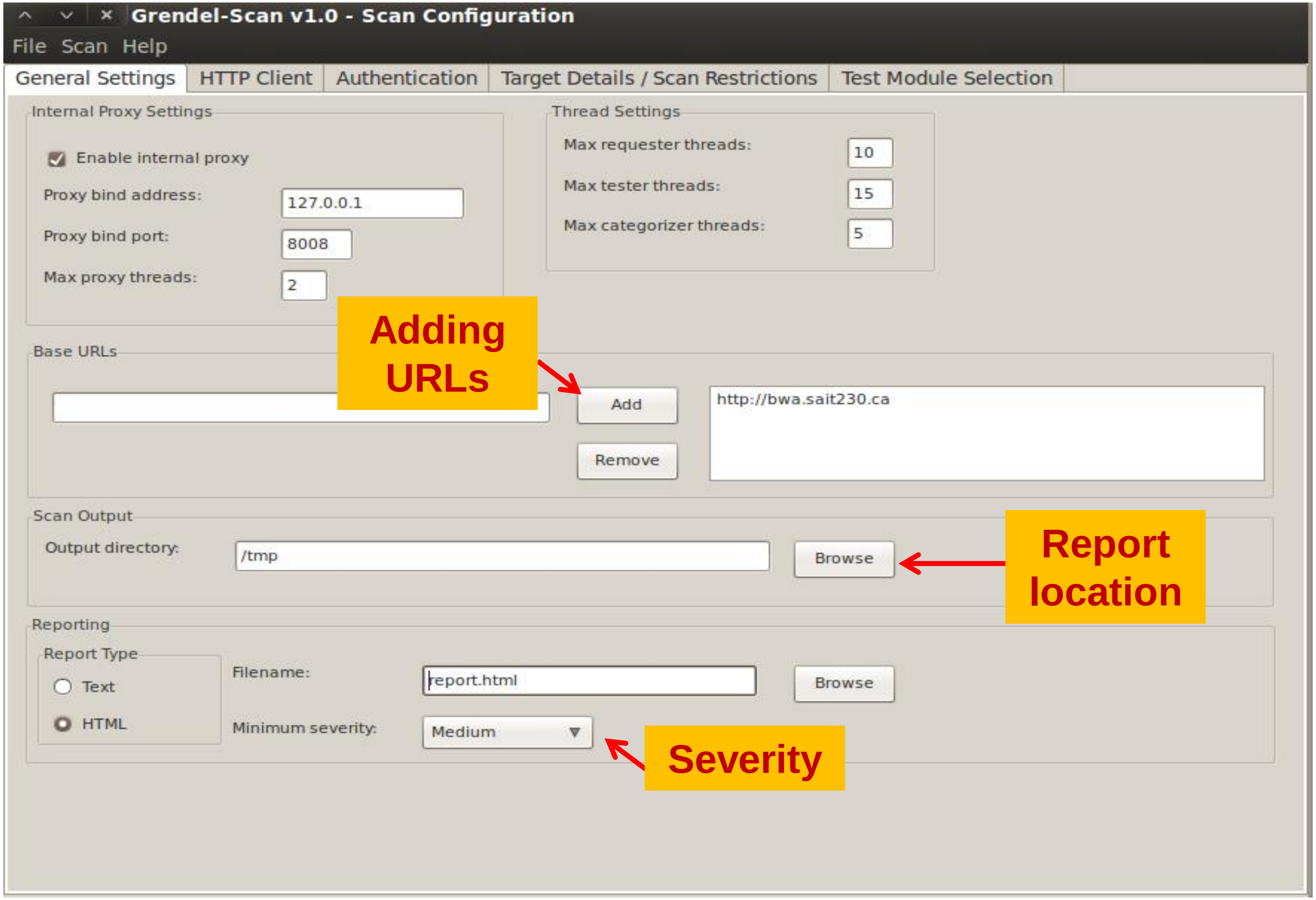
Queue Sizes

Tester: 390 Categorizer: 0 Requester: 1

FURTHER YOUR PASSION

Grendel-Scan – General Settings

Discovering



Internal Proxy Settings

☑ Enable internal proxy

Proxy bind address: 127.0.0.1

Proxy bind port: 8008

Max proxy threads: 2

Thread Settings

Max requester threads: 10

Max tester threads: 15

Max categorizer threads: 5

Base URLs

http://bwa.sait230.ca

Scan Output

Output directory: /tmp

Reporting

Report Type

○ Text

● HTML

Filename: report.html

Minimum severity: Medium

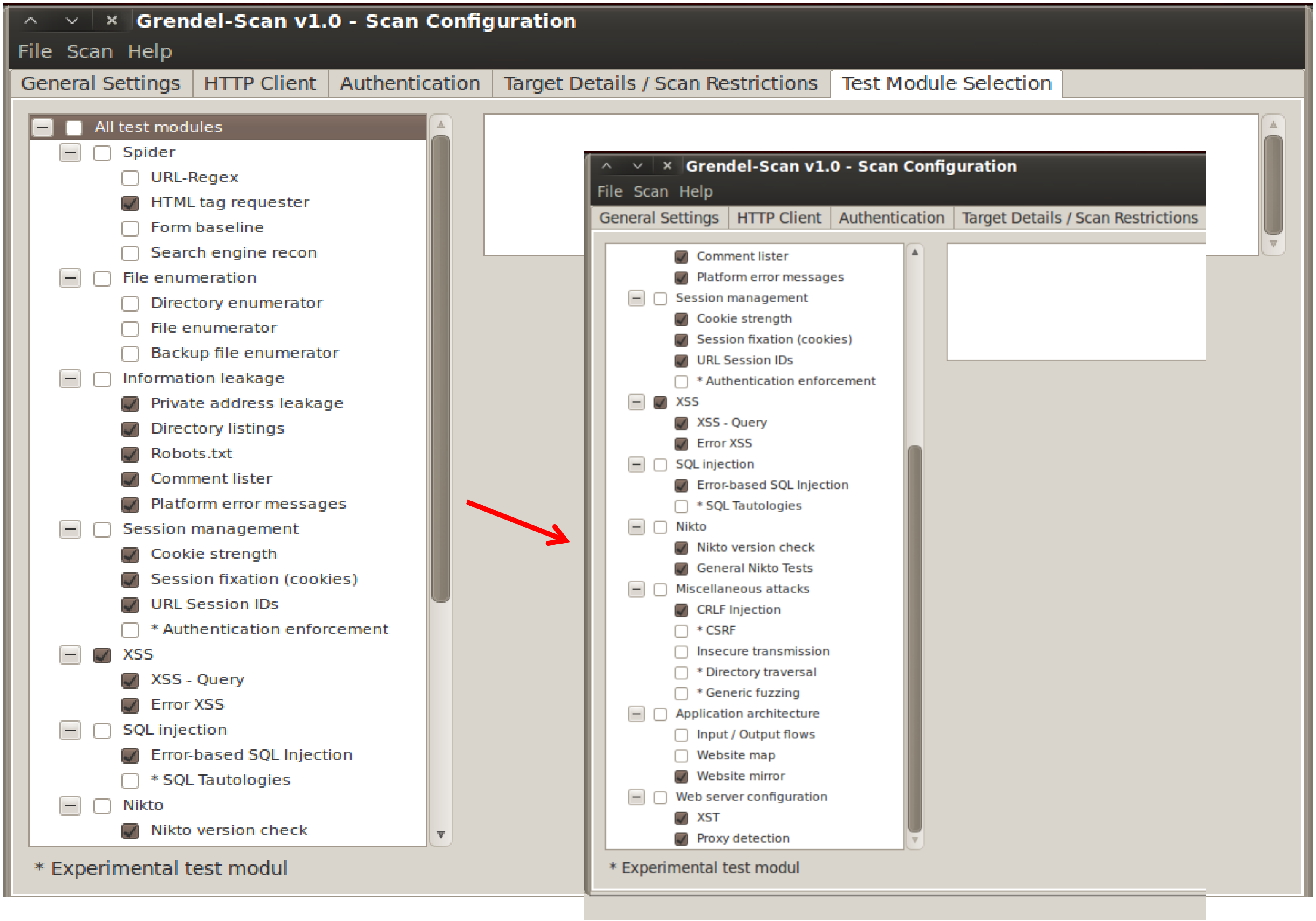
Adding URLs

Report location

Severity

Grendel-Scan - Plugins

Discovering



Grendel-Scan v1.0 - Scan Configuration
File Scan Help
General Settings | HTTP Client | Authentication | Target Details / Scan Restrictions | Test Module Selection

- □ All test modules
  - □ Spider
    - □ URL-Regex
    - ☑ HTML tag requester
    - □ Form baseline
    - □ Search engine recon
  - □ File enumeration
    - □ Directory enumerator
    - □ File enumerator
    - □ Backup file enumerator
  - □ Information leakage
    - ☑ Private address leakage
    - ☑ Directory listings
    - ☑ Robots.txt
    - ☑ Comment lister
    - ☑ Platform error messages
  - □ Session management
    - ☑ Cookie strength
    - ☑ Session fixation (cookies)
    - ☑ URL Session IDs
    - □ * Authentication enforcement
  - ☑ XSS
    - ☑ XSS - Query
    - ☑ Error XSS
  - □ SQL injection
    - ☑ Error-based SQL Injection
    - □ * SQL Tautologies
  - □ Nikto
    - ☑ Nikto version check

* Experimental test modul

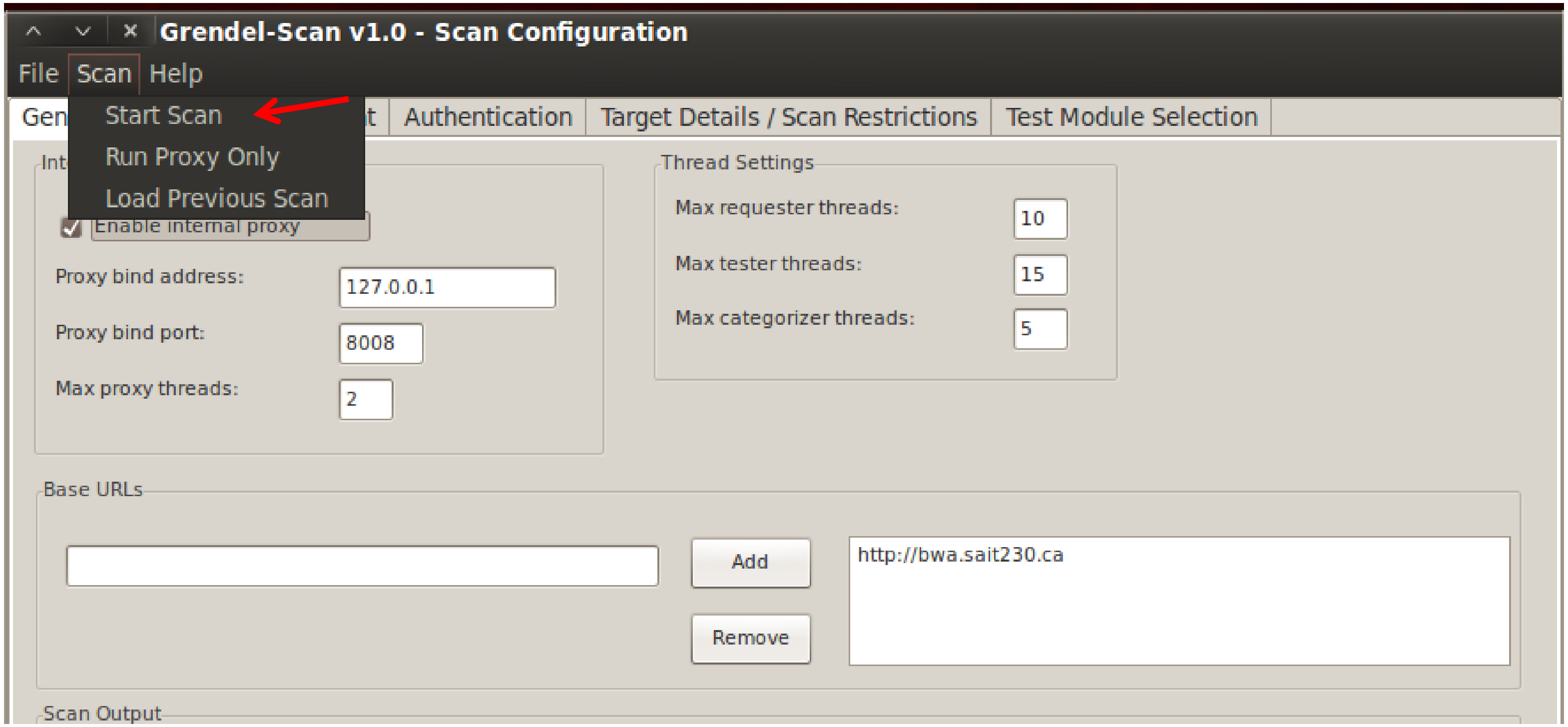
Grendel-Scan v1.0 - Scan Configuration
File Scan Help
General Settings | HTTP Client | Authentication | Target Details / Scan Restrictions

- ☑ Comment lister
- ☑ Platform error messages
- □ Session management
  - ☑ Cookie strength
  - ☑ Session fixation (cookies)
  - ☑ URL Session IDs
  - □ * Authentication enforcement
- ☑ XSS
  - ☑ XSS - Query
  - ☑ Error XSS
- □ SQL injection
  - ☑ Error-based SQL Injection
  - □ * SQL Tautologies
- □ Nikto
  - ☑ Nikto version check
  - ☑ General Nikto Tests
- □ Miscellaneous attacks
  - ☑ CRLF Injection
  - □ * CSRF
  - □ Insecure transmission
  - □ * Directory traversal
  - □ * Generic fuzzing
- □ Application architecture
  - □ Input / Output flows
  - □ Website map
  - ☑ Website mirror
- □ Web server configuration
  - ☑ XST
  - ☑ Proxy detection

* Experimental test modul

Grendel-Scan – Start Scan

Discovering



Grendel-Scan v1.0 - Scan Configuration

Int

☑ Enable internal proxy

Proxy bind address: 127.0.0.1

Proxy bind port: 8008

Max proxy threads: 2

Thread Settings

Max requester threads: 10

Max tester threads: 15

Max categorizer threads: 5

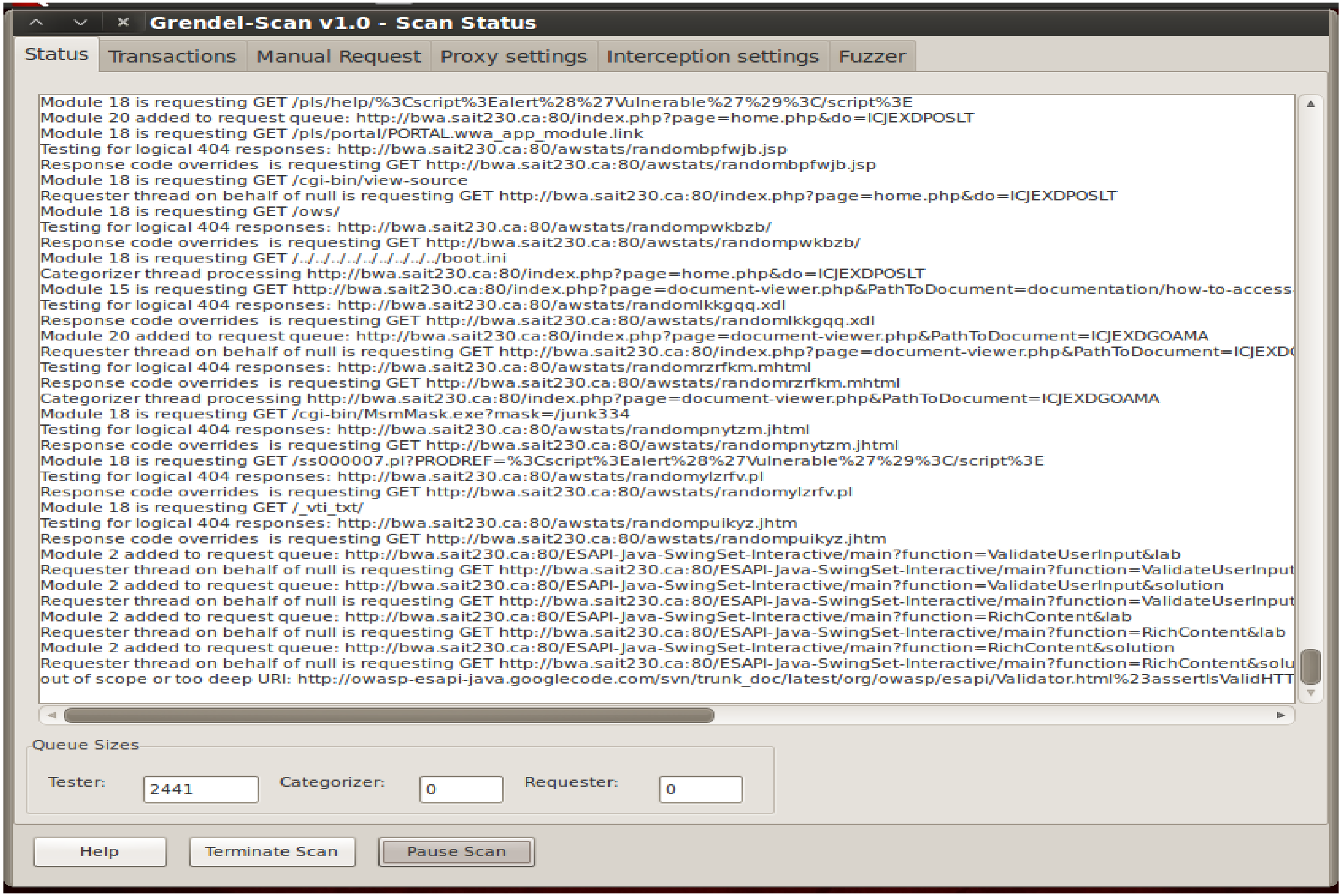
Base URLs

http://bwa.sait230.ca

Scan Output

Grendel-Scan – Start Scan

Discovering



```
Module 18 is requesting GET /pls/help/%3Cscript%3Ealert%28%27Vulnerable%27%29%3C/script%3E
Module 20 added to request queue: http://bwa.sait230.ca:80/index.php?page=home.php&do=ICJEXDPOSLT
Module 18 is requesting GET /pls/portal/PORTAL.wwa_app_module.link
Testing for logical 404 responses: http://bwa.sait230.ca:80/awstats/randombpfwjb.jsp
Response code overrides  is requesting GET http://bwa.sait230.ca:80/awstats/randombpfwjb.jsp
Module 18 is requesting GET /cgi-bin/view-source
Requester thread on behalf of null is requesting GET http://bwa.sait230.ca:80/index.php?page=home.php&do=ICJEXDPOSLT
Module 18 is requesting GET /ows/
Testing for logical 404 responses: http://bwa.sait230.ca:80/awstats/randompwkbzb/
Response code overrides  is requesting GET http://bwa.sait230.ca:80/awstats/randompwkbzb/
Module 18 is requesting GET /../../../../../../../../../boot.ini
Categorizer thread processing http://bwa.sait230.ca:80/index.php?page=home.php&do=ICJEXDPOSLT
Module 15 is requesting GET http://bwa.sait230.ca:80/index.php?page=document-viewer.php&PathToDocument=documentation/how-to-access-
Testing for logical 404 responses: http://bwa.sait230.ca:80/awstats/randomlkkgqq.xdl
Response code overrides  is requesting GET http://bwa.sait230.ca:80/awstats/randomlkkgqq.xdl
Module 20 added to request queue: http://bwa.sait230.ca:80/index.php?page=document-viewer.php&PathToDocument=ICJEXDGOAMA
Requester thread on behalf of null is requesting GET http://bwa.sait230.ca:80/index.php?page=document-viewer.php&PathToDocument=ICJEXD
Testing for logical 404 responses: http://bwa.sait230.ca:80/awstats/randomrzrfkm.mhtml
Response code overrides  is requesting GET http://bwa.sait230.ca:80/awstats/randomrzrfkm.mhtml
Categorizer thread processing http://bwa.sait230.ca:80/index.php?page=document-viewer.php&PathToDocument=ICJEXDGOAMA
Module 18 is requesting GET /cgi-bin/MsmMask.exe?mask=/junk334
Testing for logical 404 responses: http://bwa.sait230.ca:80/awstats/randompnytzm.jhtml
Response code overrides  is requesting GET http://bwa.sait230.ca:80/awstats/randompnytzm.jhtml
Module 18 is requesting GET /ss000007.pl?PRODREF=%3Cscript%3Ealert%28%27Vulnerable%27%29%3C/script%3E
Testing for logical 404 responses: http://bwa.sait230.ca:80/awstats/randomylzrfv.pl
Response code overrides  is requesting GET http://bwa.sait230.ca:80/awstats/randomylzrfv.pl
Module 18 is requesting GET /_vti_txt/
Testing for logical 404 responses: http://bwa.sait230.ca:80/awstats/randompuikyz.jhtm
Response code overrides  is requesting GET http://bwa.sait230.ca:80/awstats/randompuikyz.jhtm
Module 2 added to request queue: http://bwa.sait230.ca:80/ESAPI-Java-SwingSet-Interactive/main?function=ValidateUserInput&lab
Requester thread on behalf of null is requesting GET http://bwa.sait230.ca:80/ESAPI-Java-SwingSet-Interactive/main?function=ValidateUserInput
Module 2 added to request queue: http://bwa.sait230.ca:80/ESAPI-Java-SwingSet-Interactive/main?function=ValidateUserInput&solution
Requester thread on behalf of null is requesting GET http://bwa.sait230.ca:80/ESAPI-Java-SwingSet-Interactive/main?function=ValidateUserInput
Module 2 added to request queue: http://bwa.sait230.ca:80/ESAPI-Java-SwingSet-Interactive/main?function=RichContent&lab
Requester thread on behalf of null is requesting GET http://bwa.sait230.ca:80/ESAPI-Java-SwingSet-Interactive/main?function=RichContent&lab
Module 2 added to request queue: http://bwa.sait230.ca:80/ESAPI-Java-SwingSet-Interactive/main?function=RichContent&solution
Requester thread on behalf of null is requesting GET http://bwa.sait230.ca:80/ESAPI-Java-SwingSet-Interactive/main?function=RichContent&solu
out of scope or too deep URI: http://owasp-esapi-java.googlecode.com/svn/trunk_doc/latest/org/owasp/esapi/Validator.html%23assertIsValidHTT
```

Queue Sizes

Tester: 2441 Categorizer: 0 Requester: 0

Web App Attack and Audit Framework (w3af)

Discovering

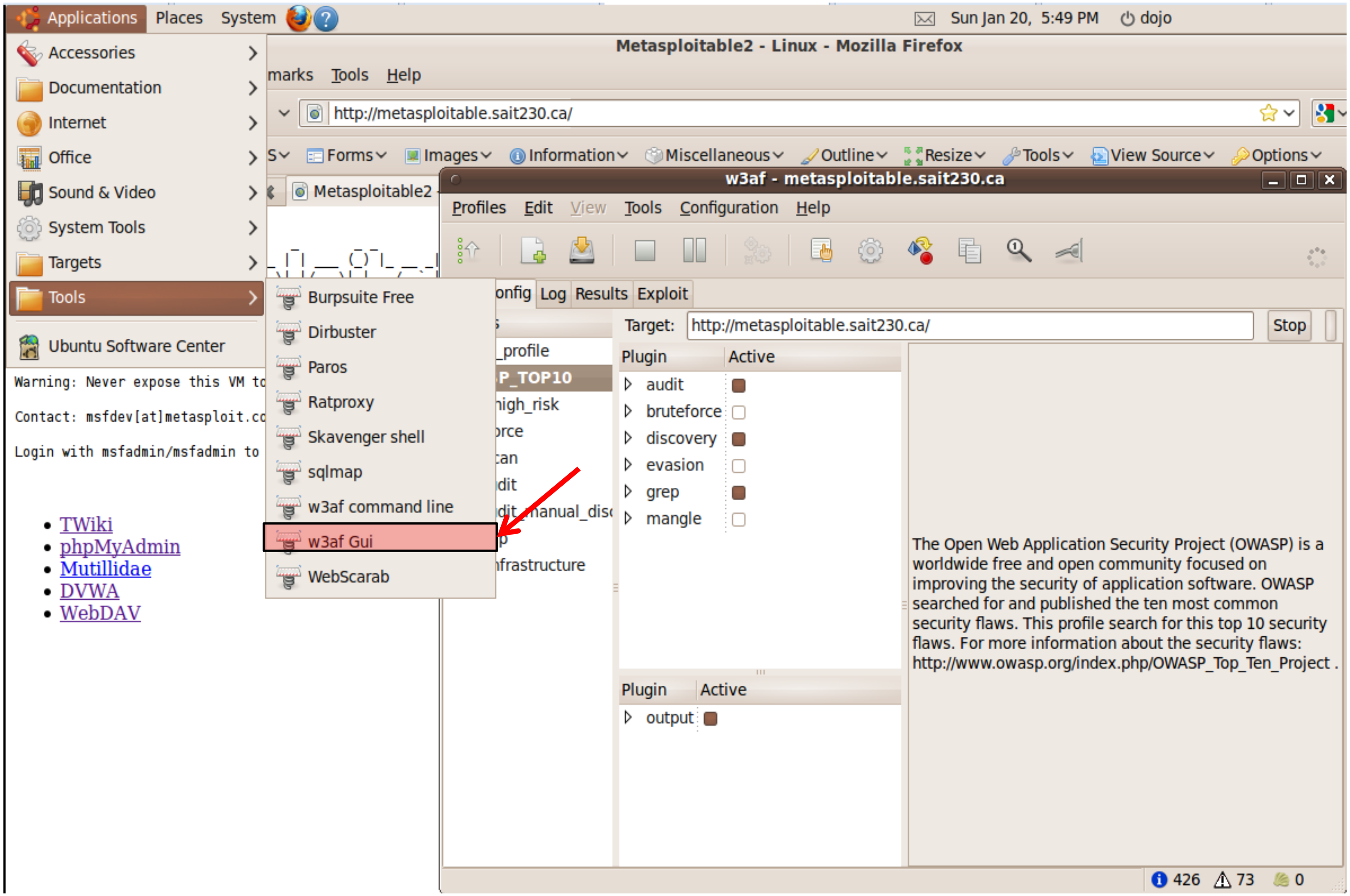
- W3af is an open web application scanner;
- It’s a web application attack and audit framework;
- It’s available at http://w3af.sourceforge.net;
- It is written in python and has both a GUI and command-terminal console interface;
- W3af is designed to perform the spidering part of mapping, all the server-side vulnerability discovery and exploitation;
- It bundles multiple tools such as sqlmap and BeEF to accomplish all of this.

Web App Attack and Audit Framework (w3af) – Plugins

- There are a variety of plugins available within w3af;
- They are python scripts that use the w3af framework;
- Audit plugins:
  - XSS;
  - SQL Injection.
- Brute force plugins:
  - Find credentials for the site.
- Discovery plugins:
  - Robots reader (reads robot.txt file);
  - Detect transparent proxy.

Web App Attack and Audit Framework (w3af) - GUI

Discovering



```
Warning: Never expose this VM to
Contact: msfdev[at]metasploit.co
Login with msfadmin/msfadmin to
```

Target: http://metasploitable.sait230.ca/

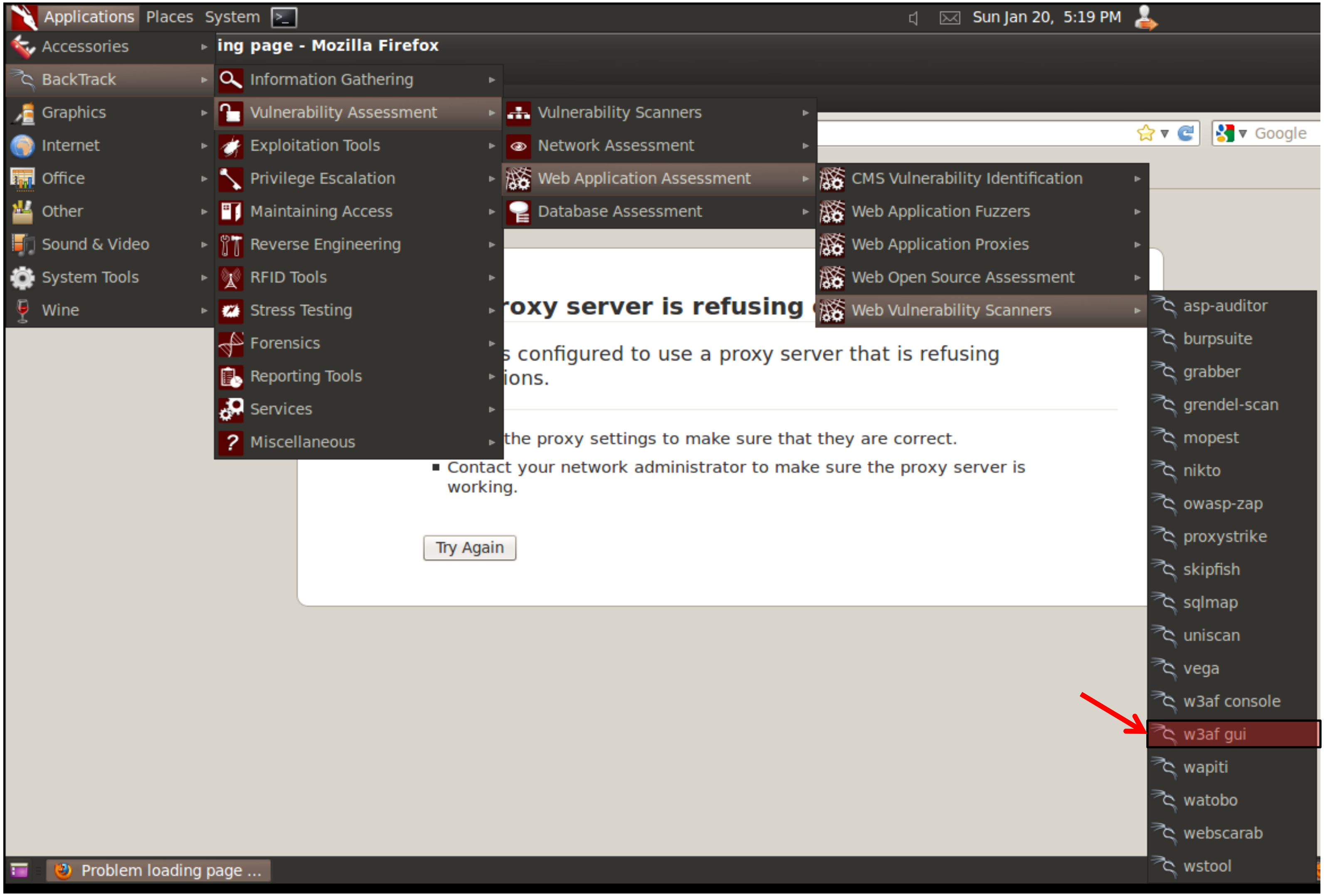
Plugin	Active
audit	■
bruteforce	□
discovery	■
evasion	□
grep	■
mangle	□

Plugin	Active
output	■

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 .

Discovering

Web App Attack and Audit Framework (w3af) - GUI



ing page - Mozilla Firefox

roxy server is refusing

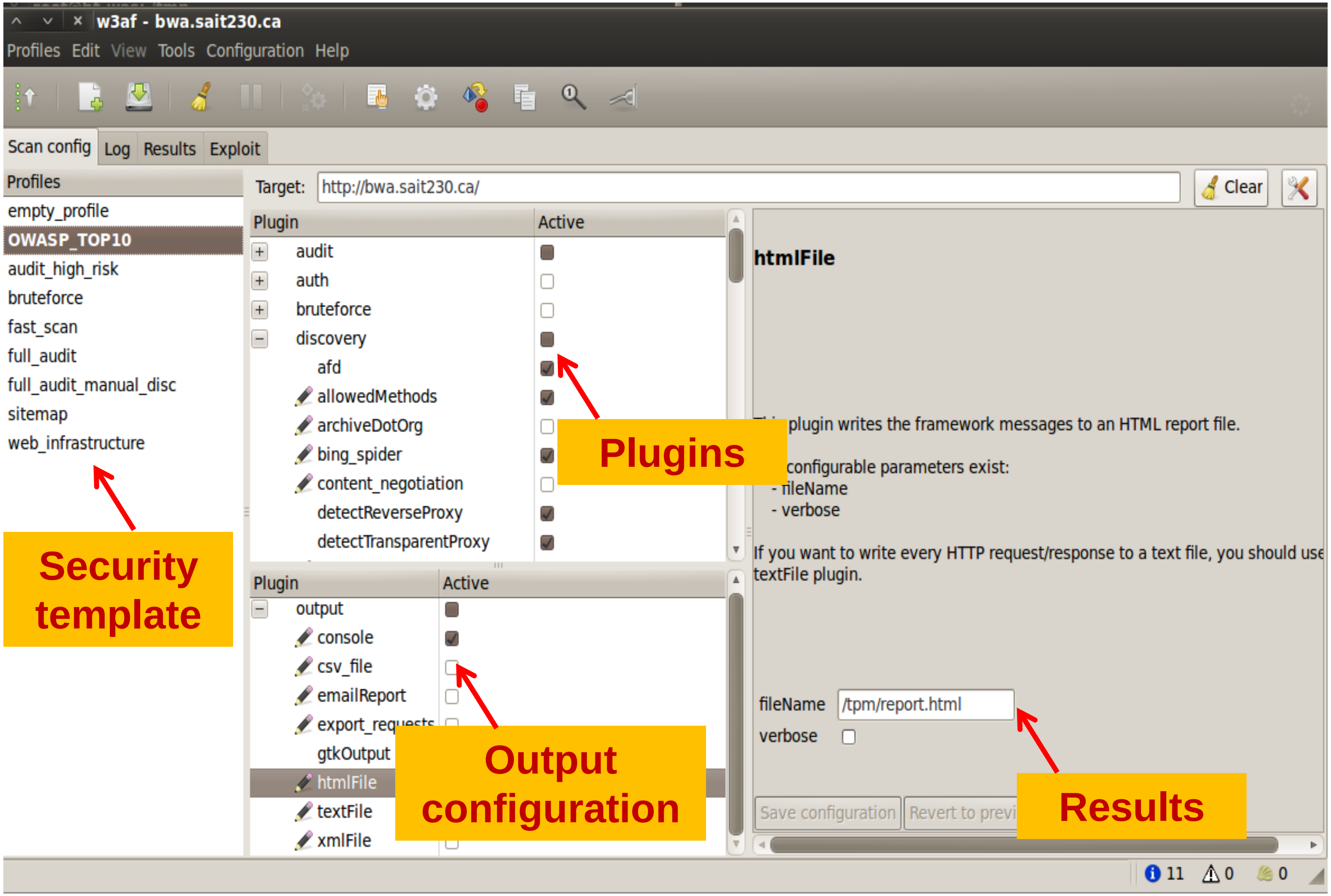
s configured to use a proxy server that is refusing ions.

the proxy settings to make sure that they are correct.

- Contact your network administrator to make sure the proxy server is working.

Web App Attack and Audit Framework (w3af) - GUI

Discovering



Profiles

- empty_profile
- OWASP_TOP10
- audit_high_risk
- bruteforce
- fast_scan
- full_audit
- full_audit_manual_disc
- sitemap
- web_infrastructure

Target: http://bwa.sait230.ca/

Plugin	Active
+ audit	■
+ auth	□
+ bruteforce	□
− discovery	■
afd	☑
allowedMethods	☑
archiveDotOrg	□
bing_spider	☑
content_negotiation	□
detectReverseProxy	☑
detectTransparentProxy	☑

Plugin	Active
− output	■
console	☑
csv_file	□
emailReport	□
export_requests	□
gtkOutput	
htmlFile	
textFile	
xmlFile	□

htmlFile

plugin writes the framework messages to an HTML report file.

configurable parameters exist:
- fileName
- verbose

If you want to write every HTTP request/response to a text file, you should use textFile plugin.

fileName /tpm/report.html

verbose □

Plugins

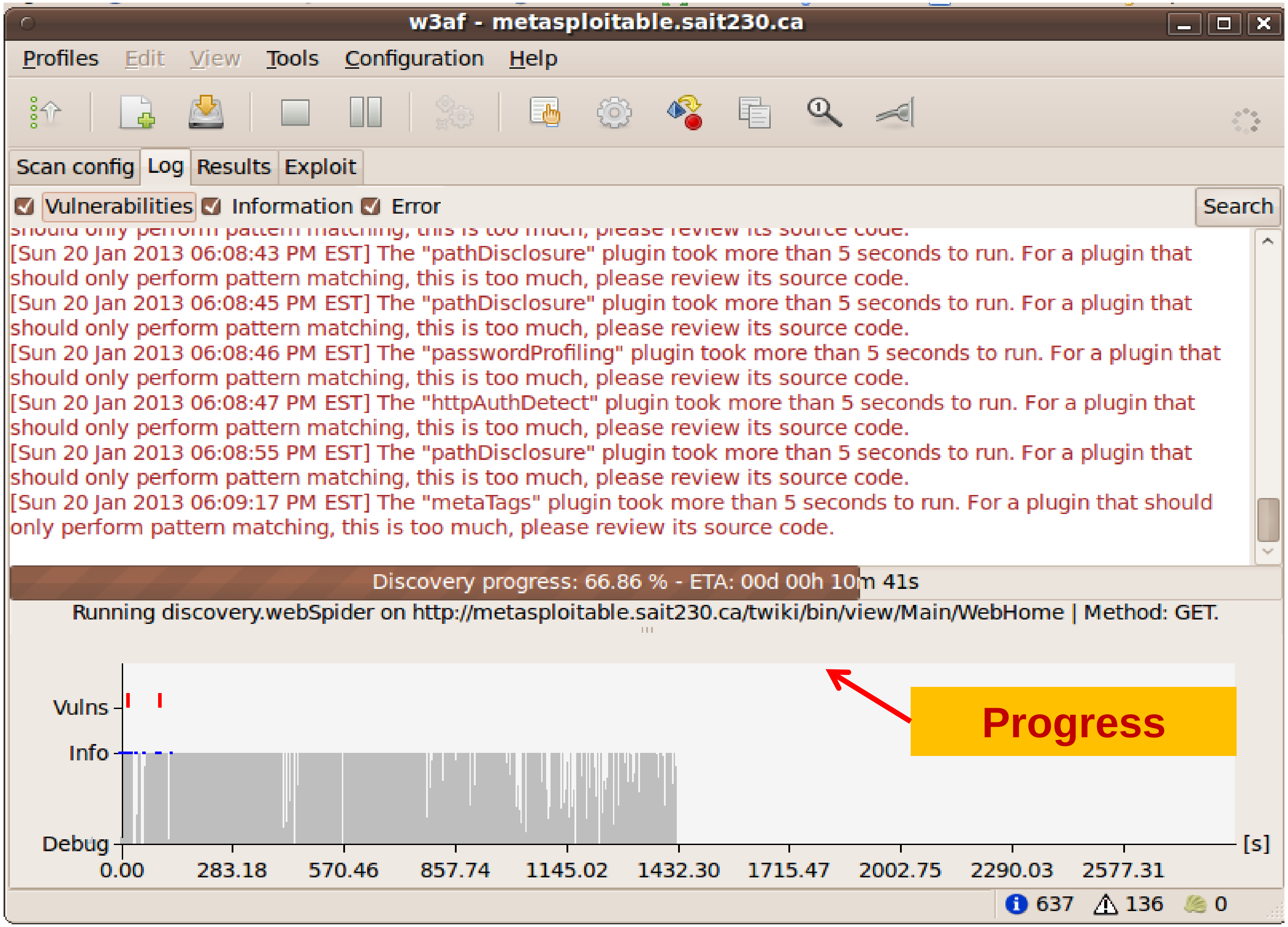
Security template

Output configuration

Results

Web App Attack and Audit Framework (w3af) - GUI

Discovering



w3af - metasploitable.sait230.ca
Profiles Edit View Tools Configuration Help
Scan config Log Results Exploit
☑ Vulnerabilities ☑ Information ☑ Error
Search

```
should only perform pattern matching, this is too much, please review its source code.
[Sun 20 Jan 2013 06:08:43 PM EST] The "pathDisclosure" plugin took more than 5 seconds to run. For a plugin that
should only perform pattern matching, this is too much, please review its source code.
[Sun 20 Jan 2013 06:08:45 PM EST] The "pathDisclosure" plugin took more than 5 seconds to run. For a plugin that
should only perform pattern matching, this is too much, please review its source code.
[Sun 20 Jan 2013 06:08:46 PM EST] The "passwordProfiling" plugin took more than 5 seconds to run. For a plugin that
should only perform pattern matching, this is too much, please review its source code.
[Sun 20 Jan 2013 06:08:47 PM EST] The "httpAuthDetect" plugin took more than 5 seconds to run. For a plugin that
should only perform pattern matching, this is too much, please review its source code.
[Sun 20 Jan 2013 06:08:55 PM EST] The "pathDisclosure" plugin took more than 5 seconds to run. For a plugin that
should only perform pattern matching, this is too much, please review its source code.
[Sun 20 Jan 2013 06:09:17 PM EST] The "metaTags" plugin took more than 5 seconds to run. For a plugin that should
only perform pattern matching, this is too much, please review its source code.
```

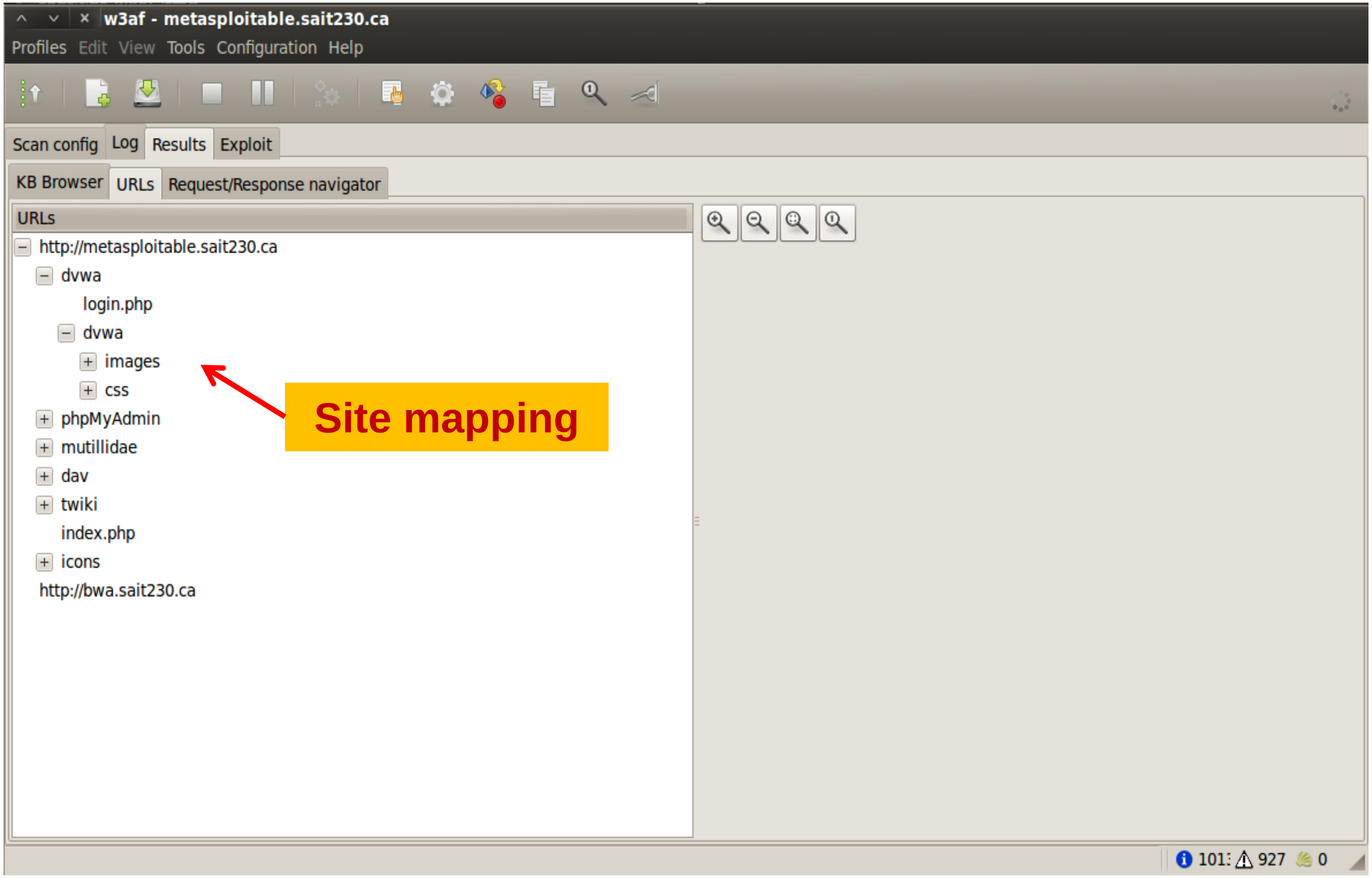
Discovery progress: 66.86 % - ETA: 00d 00h 10m 41s

Running discovery.webSpider on http://metasploitable.sait230.ca/twiki/bin/view/Main/WebHome | Method: GET.

Progress

Web App Attack and Audit Framework (w3af) - GUI

Discovering

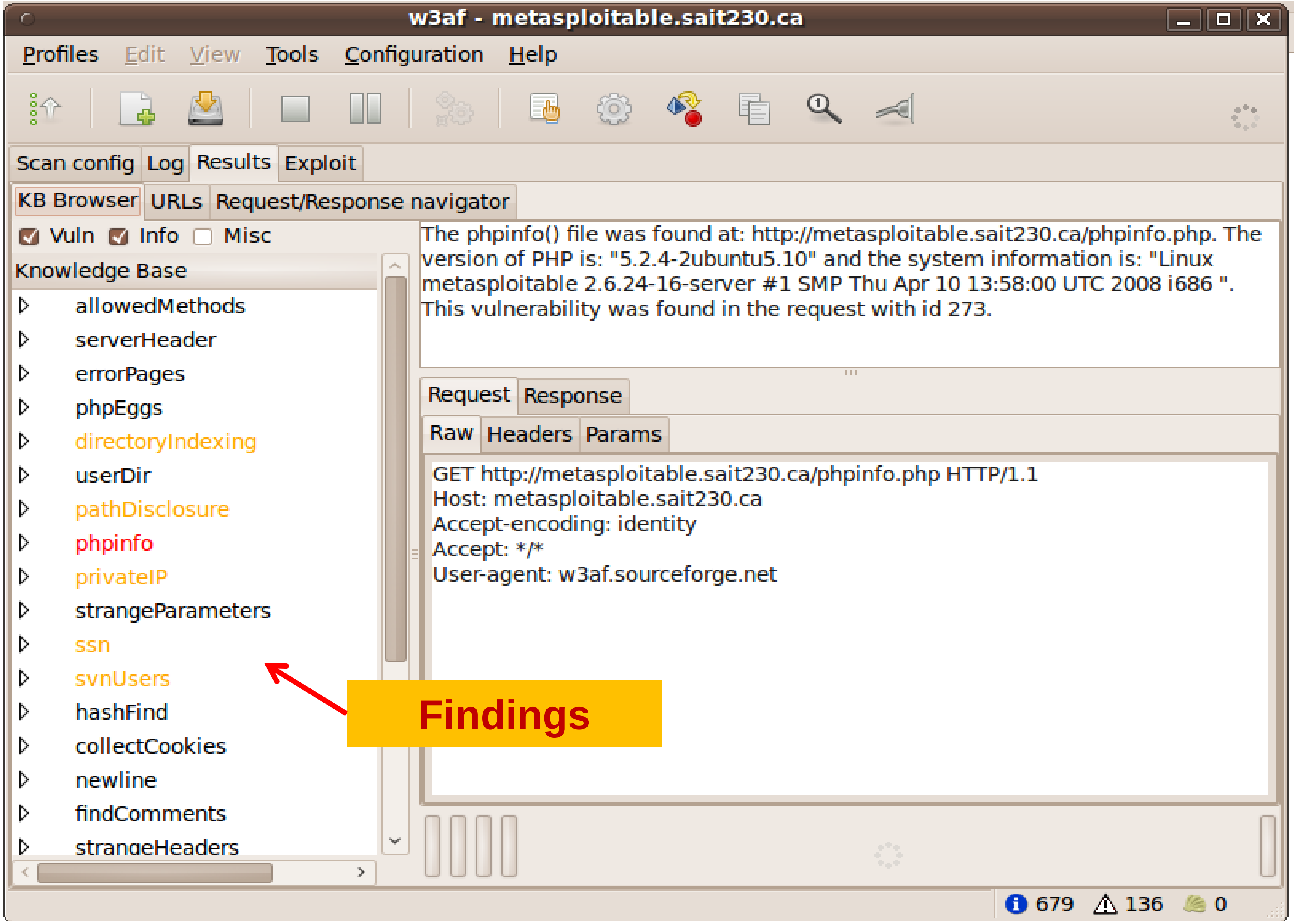


```
− http://metasploitable.sait230.ca
    − dvwa
          login.php
        − dvwa
            + images
            + css
    + phpMyAdmin
    + mutillidae
    + dav
    + twiki
      index.php
    + icons
  http://bwa.sait230.ca
```

Site mapping

Web App Attack and Audit Framework (w3af) - GUI

Discovering



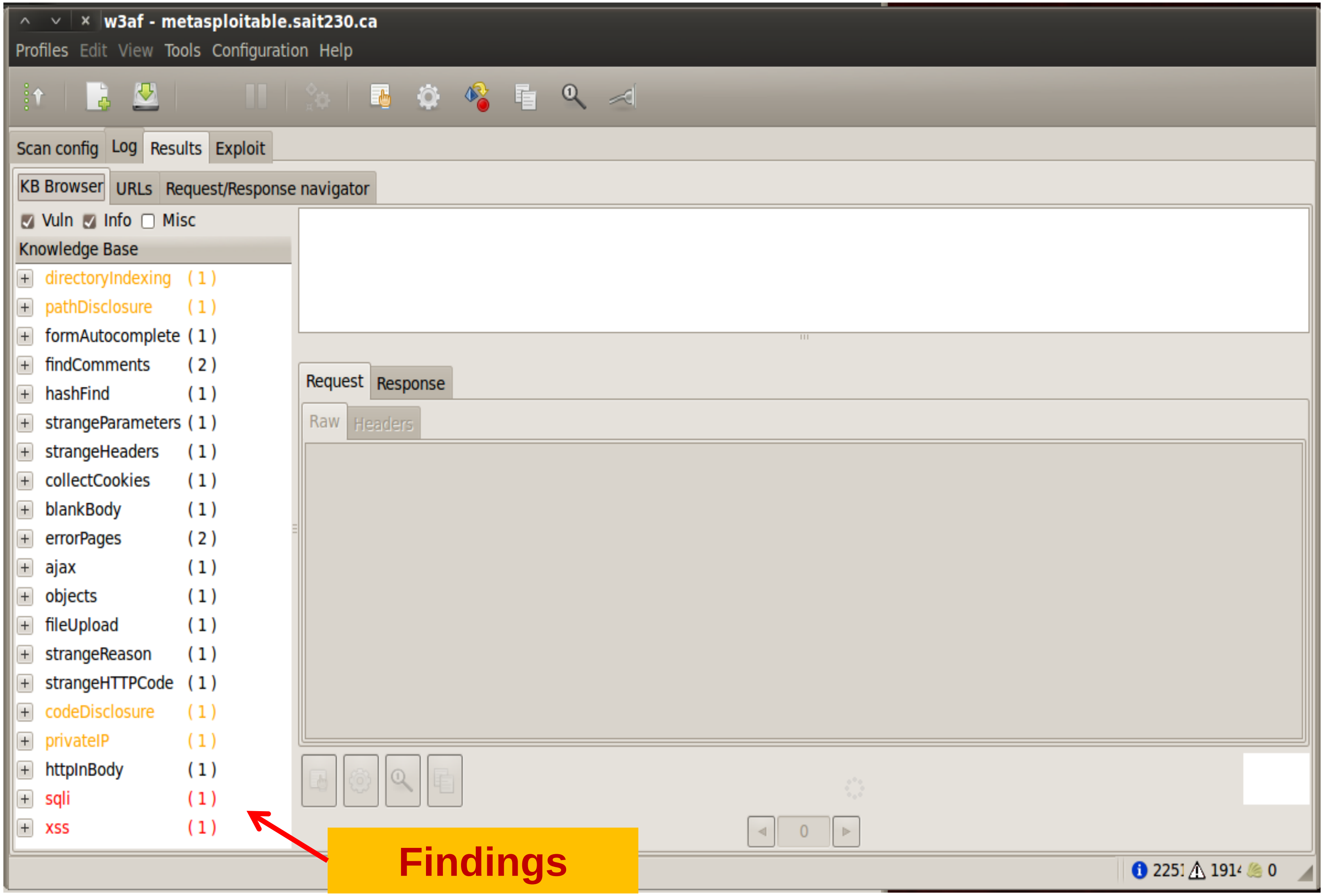
The phpinfo() file was found at: http://metasploitable.sait230.ca/phpinfo.php. The version of PHP is: "5.2.4-2ubuntu5.10" and the system information is: "Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 ". This vulnerability was found in the request with id 273.

```
GET http://metasploitable.sait230.ca/phpinfo.php HTTP/1.1
Host: metasploitable.sait230.ca
Accept-encoding: identity
Accept: */*
User-agent: w3af.sourceforge.net
```

Findings

Web App Attack and Audit Framework (w3af) - GUI

Discovering



☑ Vuln ☑ Info □ Misc

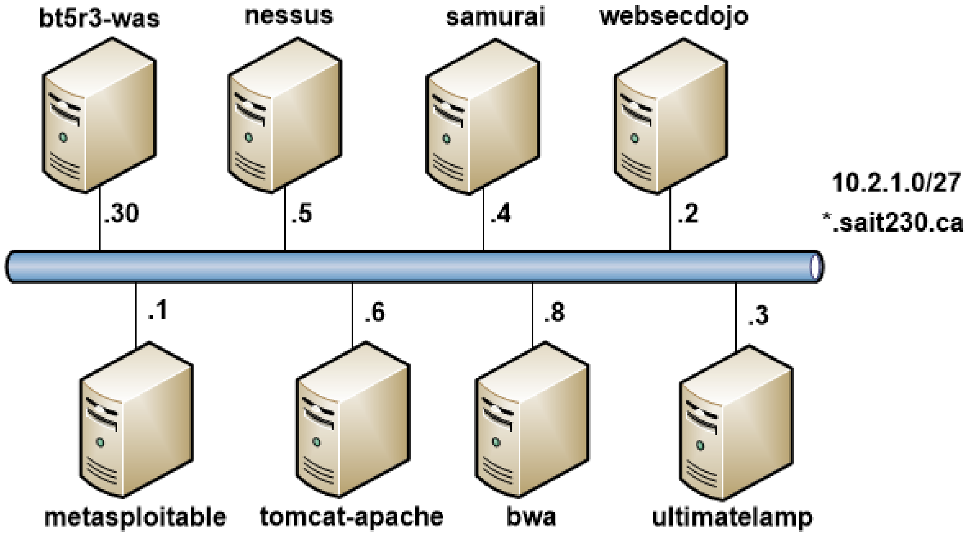
Knowledge Base	
directoryIndexing	(1)
pathDisclosure	(1)
formAutocomplete	(1)
findComments	(2)
hashFind	(1)
strangeParameters	(1)
strangeHeaders	(1)
collectCookies	(1)
blankBody	(1)
errorPages	(2)
ajax	(1)
objects	(1)
fileUpload	(1)
strangeReason	(1)
strangeHTTPCode	(1)
codeDisclosure	(1)
privateIP	(1)
httpInBody	(1)
sqli	(1)
xss	(1)

Findings

Project – Phase 2: Discovery

Discovering

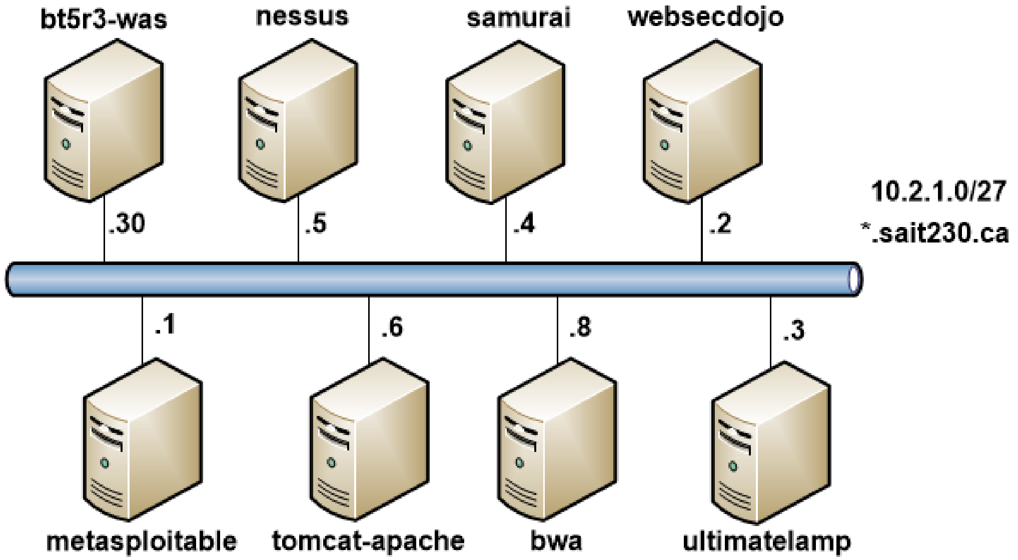
- Use Nikto to scan each server on the network on the following ports:
    - TCP 80, 808X, 800X, 8180, 443.
- Save the report on /tmp/nikto-results/report.html.



Project – Phase 2: Discovery

Discovering

- Use Grendel-Scan and w3af to scan the following servers:
  - metasploitable.sait230.ca;
  - bwa.sait230.ca.



Note: Probably it has be completed at home since the scan takes time to complete.

Project – Phase 2: Discovery

Discovering

Hostname	Web App	Vulnerabilities	Exploitable?

Questions