Watobo

Information Security Inc.

iSEC
information security inc.

Contents

- About Watobo
- Features
- Testing Environment
- Installing Watobo
- Using Watobo
- References

About Watobo

- WATABO is a security tool for testing web applications. It is intended to enable security professionals to perform efficient (semi-automated) web application security audit

WATOBO

The Webapplication Toolbox

Features

- Powerful session management capabilities! You can define login scripts as well as logout signatures. So you don't have to login manually each time you get logged out
- Can act as a transparent proxy (requires nfqueue)
- Vulnerability checks (SQLinjectin, XSS, LFI) out of the box
- Handles Anti-CSRF-/One-Time-Tokens

WATOBO - THE WEB APPLICATION TOOLBOX

Features

- Supports inline de-/encoding, so you don't have to copy strings to a transcoder and back again. Just do it inside the request/response window with a simple mouse click.
- Smart filter functions, so you can find and navigate to the most interesting parts of the application easily.
- Is written in (FX) Ruby and enables you to easily define your own checks
- Runs on Windows, Linux, MacOS every OS supporting (FX) Ruby

Powered by (FX)Ruby

Testing Environment

- Kali Linux 2017

```
root@kali2017:~# cat /etc/*rel*
DISTRIB_ID=Kali
DISTRIB_RELEASE=kali-rolling
DISTRIB_CODENAME=kali-rolling
DISTRIB_DESCRIPTION="Kali GNU/Linux Rolling"
PRETTY_NAME="Kali GNU/Linux Rolling"
NAME="Kali GNU/Linux"
ID=kali
VERSION="2017.2"
VERSION_ID="2017.2"
ID_LIKE=debian
ANSI_COLOR="1;31"
HOME_URL="http://www.kali.org/"
SUPPORT_URL="http://forums.kali.org/"
BUG_REPORT_URL="http://bugs.kali.org/"
```

Installing Watobo

- apt-get install watobo

```
root@kali2017:~# apt-get install watobo
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  libfox-1.6-0 libfxscintilla20 libnetfilter-queue1 racc ruby-childprocess ruby-fxruby ruby-jwt ruby-mechanize ruby-net-http-pipeline
  ruby-nfnetlink ruby-nfqueue ruby-ntlm ruby-selenium-webdriver ruby-webrobots ruby-websocket
The following NEW packages will be installed:
  libfox-1.6-0 libfxscintilla20 libnetfilter-queue1 racc ruby-childprocess ruby-fxruby ruby-jwt ruby-mechanize ruby-net-http-pipeline
  ruby-nfnetlink ruby-nfqueue ruby-ntlm ruby-selenium-webdriver ruby-webrobots ruby-websocket watobo
0 upgraded, 16 newly installed, 0 to remove and 158 not upgraded.
Need to get 4,106 kB of archives.
After this operation, 23.7 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://ftp.ne.jp/Linux/packages/kali/kali kali-rolling/main amd64 libfox-1.6-0 amd64 1.6.55-1 [876 kB]
```

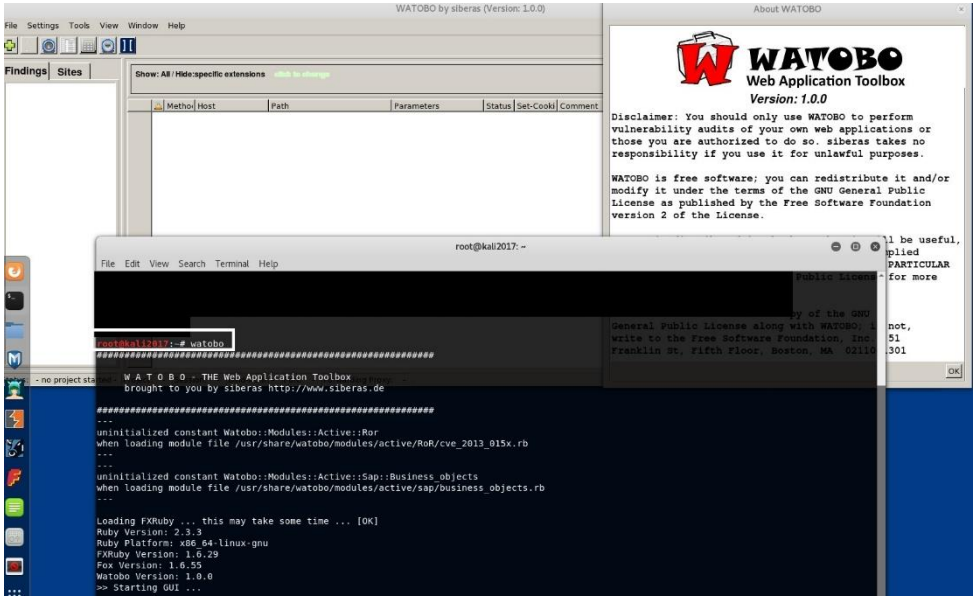
Using Watobo

- Starting Watobo for the first time

```
root@kali2017:~# watobo
#############################################################

     W A T O B O - THE Web Application Toolbox
     brought to you by siberas http://www.siberas.de

#############################################################
Creating WATOBO's working directory /root/.watobo.* create configuration directory '/root/.watobo/conf' ...
OK
* create temp directory '/root/.watobo/tmp' ...
OK
* created workspace folder /root/.watobo/workspace
---
uninitialized constant Watobo::Modules::Active::Ror
when loading module file /usr/share/watobo/modules/active/RoR/cve_2013_015x.rb
---
---
uninitialized constant Watobo::Modules::Active::Sap::Business_objects
when loading module file /usr/share/watobo/modules/active/sap/business_objects.rb
---
Done generating certificate for /C=DE/O=WATOBO/OU=WATOBO CA/CN=Watobo
>> create DH key ...
* creating SSL key (DH 2048) ...

 DONE

Loading FXRuby ... this may take some time ... [OK]
```

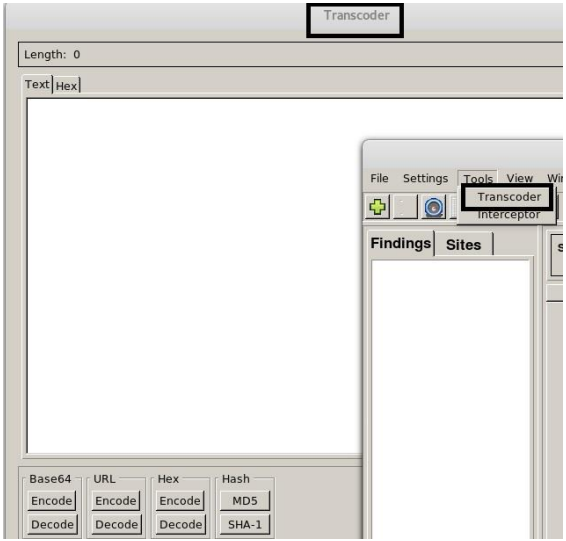
Using Watobo

- Starting Watobo



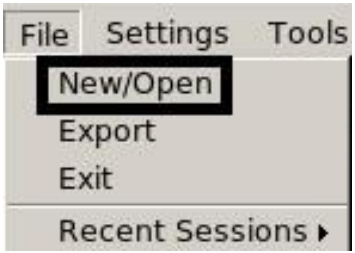
Using Watobo

- Watobo Transcoder



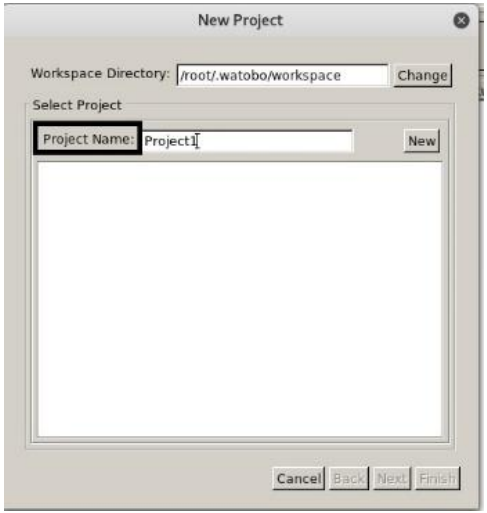
Using Watobo

- Watobo: create a new project => File > New/Open



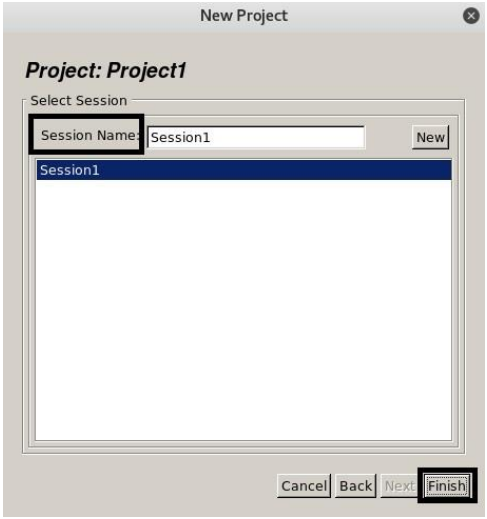
Using Watobo

- Project Name



Using Watobo

- Session Name



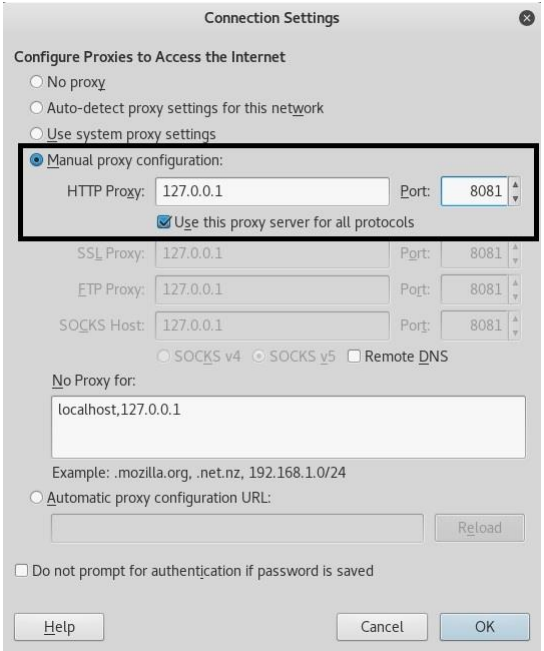
Using Watobo

- Watobo listens on port 8081

```
root@kali2017:~# curl -I 127.0.0.1:8081
HTTP/1.1 555 Watobo Error
WATOBO: Error
Date: 2017-10-15 00:36:36 -0400
Content-Length: 0
Content-Type: text/html
Connection: close
```

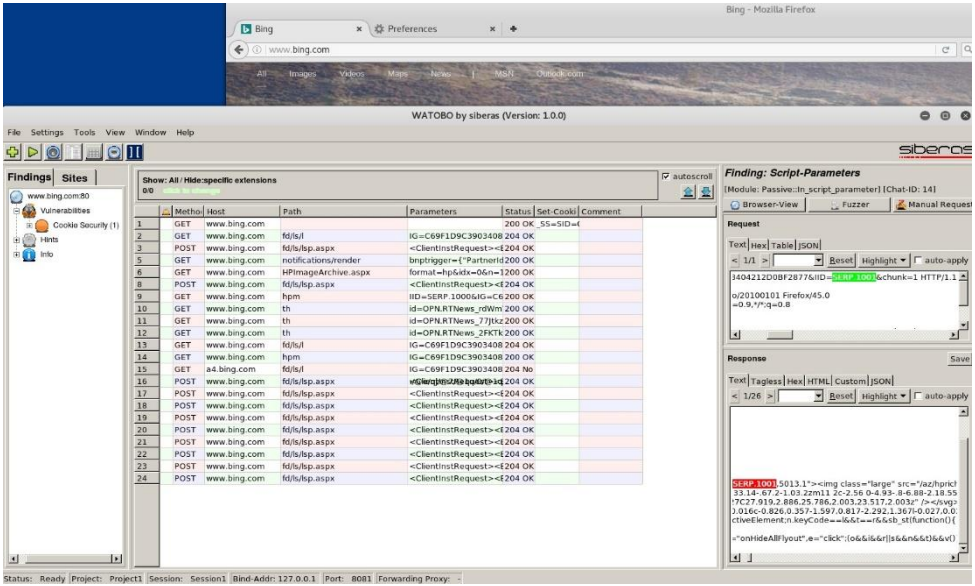
Using Watobo

- Configure browser proxy



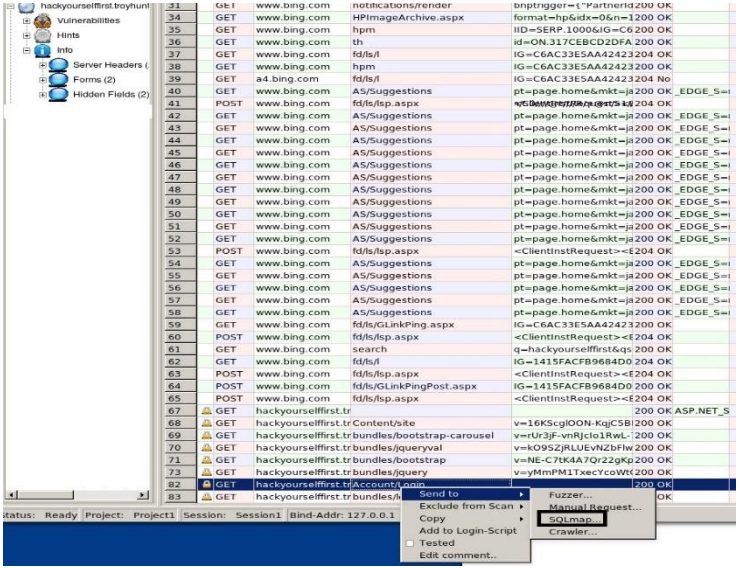
Using Watobo

- Watobo Interceptor



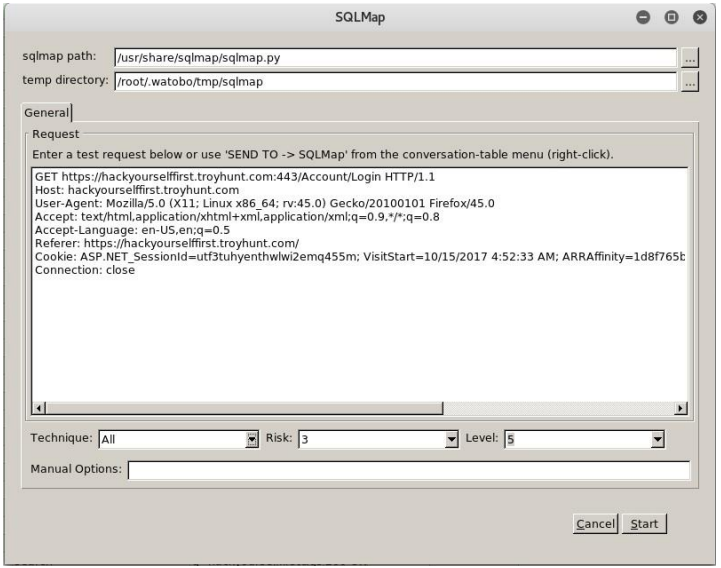
Using Watobo

- Watobo > send to SQLmap



Using Watobo

- Watobo > send to SQLmap



Using Watobo

- Watobo > send to SQLmap

References

- Kitploit
http://www.kitploit.com/2013/08/watobo-0913-web-application-toolbox.html

- Kali Linux
https://www.kali.org/downloads/

- fxruby
https://github.com/larskanis/fxruby