Project: WebSlayer

The web application Brute forcer

Christian Martorella
Edge-Security

Overview

- WebSlayer is a Web application Brute forcer, based on wfuzz. It’s an evolution by the need of analyzing the results in a convenient way. Also, it adds new functionality, like a Payload generator, results visualization and easy of use.
  - Run in multiple platforms (Linux, Windows and OS X)
  - Multi Threading
  - Python and QT
  - Fast

Objectives

- The main objective is to provide to the security tester a tool to perform highly customized brute force attacks, and a useful results analysis interface. It was designed thinking in the professional tester.

- The tool could be used for:
  - Parameter Fuzzing and brute forcing (Headers, Get, Post)
  - Login/Password brute force (Password policy testing)
  - Predictable Resource Location (Directory and files discovery)
  - Cookie and Session brute forcer
  - Generate Custom Payloads

Objectives

- Easy customization
- Enhanced results presentation
- Provide an environment for analyzing the results

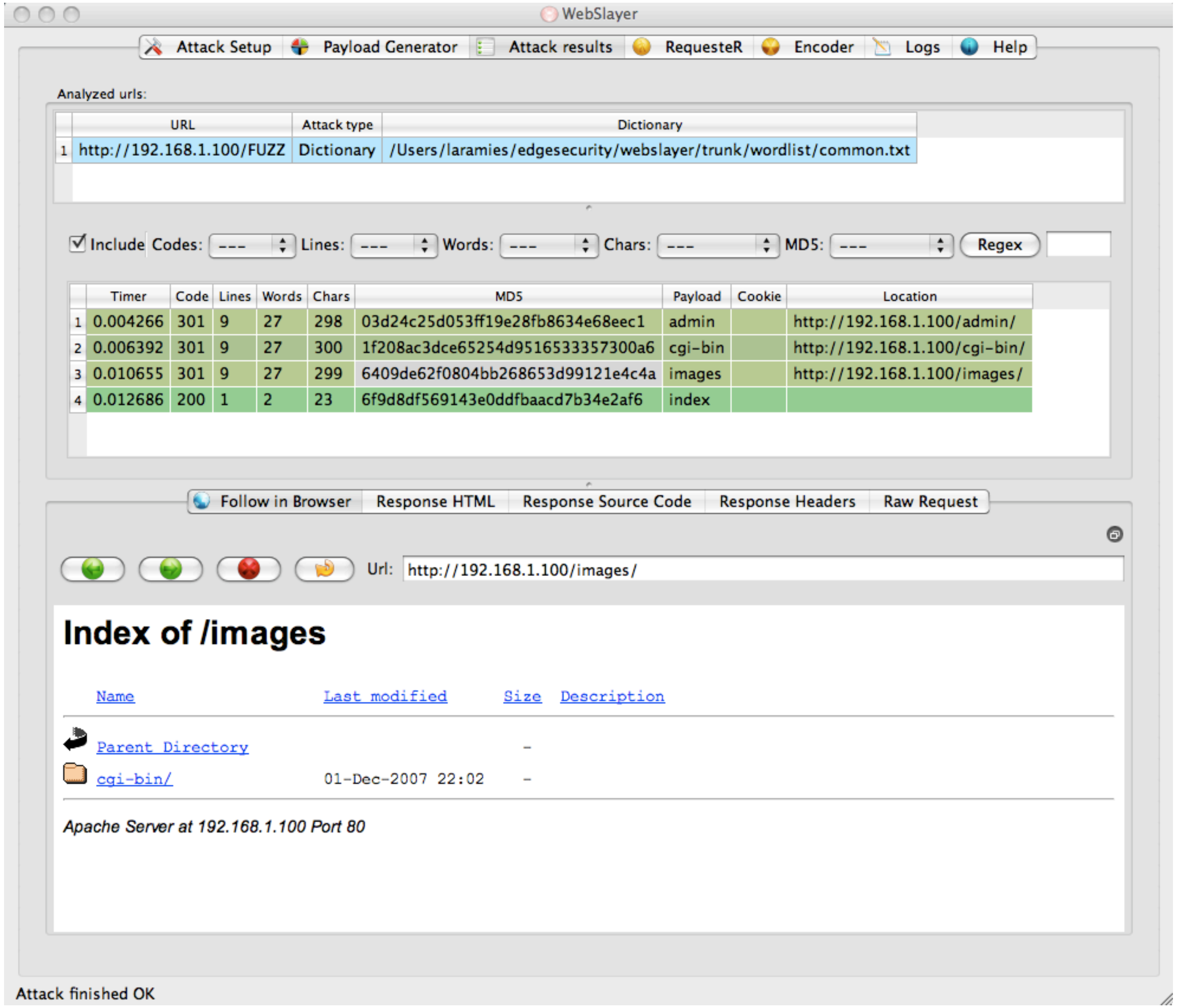
Features

- Multithreading
- Multiple payloads (now 2, but will be unlimited)
- Proxy support (w/authentication)
- Encodings (15)
- Integrated a full fledge Web browser (Webkit)

Features

- Resource location prediction:
  - Recursion
  - Non standard code error detection
  - Lots of dictionaries for known applications and servers (dirb)
- Payload generator
  - Usernames, Credit Card numbers, Permutations, Character blocks, Range
  - Pattern creator and regular expression

A taste of WebSlayer - Results



Analyzed urls:

	URL	Attack type	Dictionary
1	http://192.168.1.100/FUZZ	Dictionary	/Users/laramies/edgesecurity/webslayer/trunk/wordlist/common.txt

☑ Include Codes: --- Lines: --- Words: --- Chars: --- MD5: --- Regex

	Timer	Code	Lines	Words	Chars	MD5	Payload	Cookie	Location
1	0.004266	301	9	27	298	03d24c25d053ff19e28fb8634e68eec1	admin		http://192.168.1.100/admin/
2	0.006392	301	9	27	300	1f208ac3dce65254d9516533357300a6	cgi-bin		http://192.168.1.100/cgi-bin/
3	0.010655	301	9	27	299	6409de62f0804bb268653d99121e4c4a	images		http://192.168.1.100/images/
4	0.012686	200	1	2	23	6f9d8df569143e0ddfbaacd7b34e2af6	index		

Url: http://192.168.1.100/images/

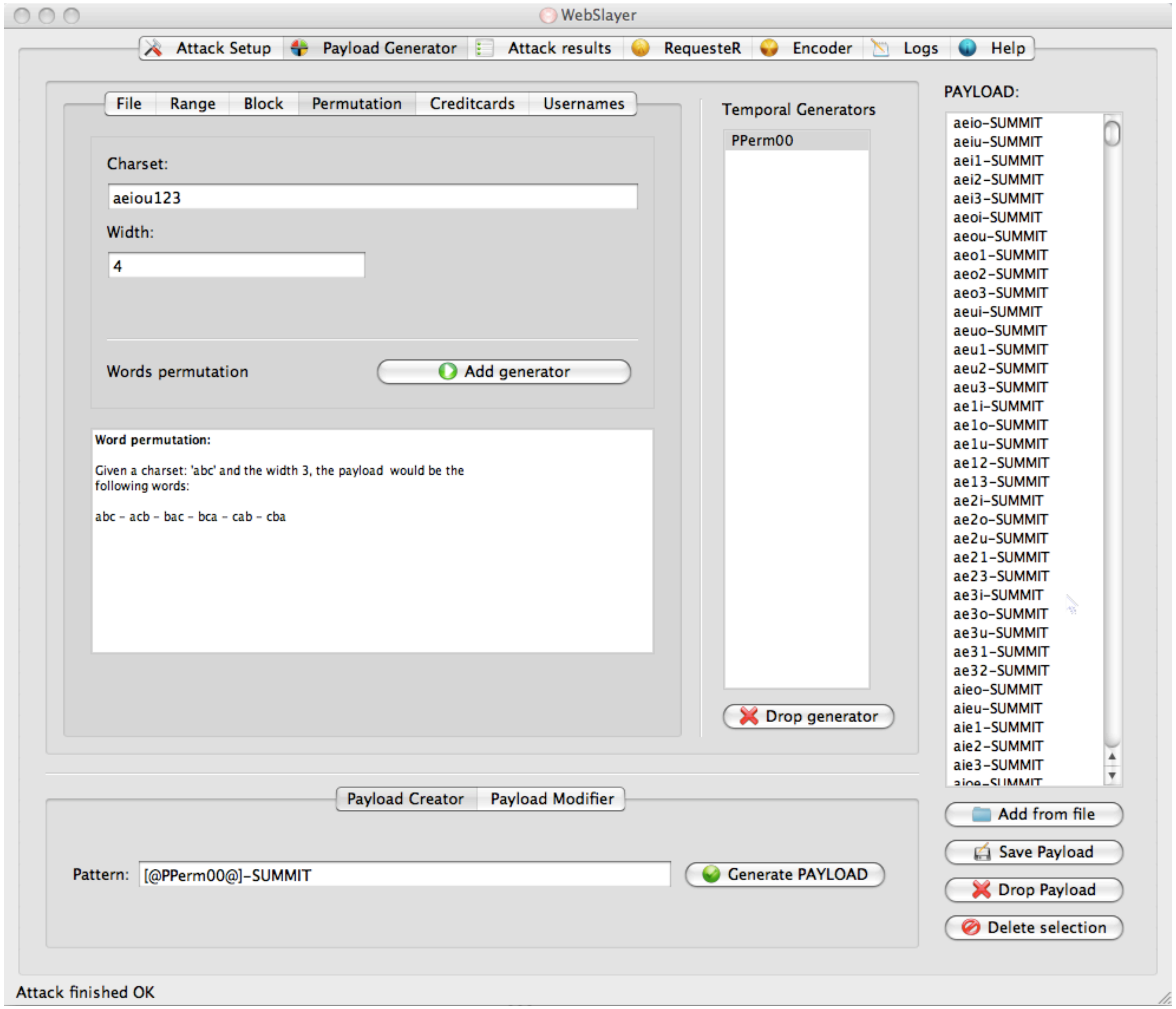
Index of /images

Name	Last modified	Size	Description
Parent Directory		-	
cgi-bin/	01-Dec-2007 22:02	-	

Apache Server at 192.168.1.100 Port 80

Attack finished OK

A taste of WebSlayer – Payload Generator



Charset: aeiou123

Width: 4

Word permutation:

Given a charset: 'abc' and the width 3, the payload would be the following words:

abc - acb - bac - bca - cab - cba

Temporal Generators: PPerm00

PAYLOAD:

```
aeio-SUMMIT
aeiu-SUMMIT
aei1-SUMMIT
aei2-SUMMIT
aei3-SUMMIT
aeoi-SUMMIT
aeou-SUMMIT
aeo1-SUMMIT
aeo2-SUMMIT
aeo3-SUMMIT
aeui-SUMMIT
aeuo-SUMMIT
aeu1-SUMMIT
aeu2-SUMMIT
aeu3-SUMMIT
ae1i-SUMMIT
ae1o-SUMMIT
ae1u-SUMMIT
ae12-SUMMIT
ae13-SUMMIT
ae2i-SUMMIT
ae2o-SUMMIT
ae2u-SUMMIT
ae21-SUMMIT
ae23-SUMMIT
ae3i-SUMMIT
ae3o-SUMMIT
ae3u-SUMMIT
ae31-SUMMIT
ae32-SUMMIT
aieo-SUMMIT
aieu-SUMMIT
aie1-SUMMIT
aie2-SUMMIT
aie3-SUMMIT
aioe-SUMMIT
```

Pattern: [@PPerm00@]-SUMMIT

Attack finished OK

Status and Future Steps

- The status for the project is beta, this version is 100% usable, but minor bugs could rise. The tool is developed in python and QT, and the version available runs on Windows (installable package)

- The next version will have a redesign of the interface and the engine, to provide better features and improve performance

- Multiple OS, Linux and OSX coming on next version

Status and Future Steps

- 2) Work in some features and bug fixes
- 3) Release stable version for win32, linux and OSX
- 4) Start working in the branch 2.0:
  - Engine and GUI redesign
  - And many more features (more info in the OWASP project page)

Closing

- Information about the project:
    - https://www.owasp.org/index.php/Category:OWASP_Webslayer_Project
- Beta testers please contact me!
- Any idea is welcome
- Thank you for your time