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

![WebSlayer interface](image)

### Analyzed URLs

<table>
<thead>
<tr>
<th>URL</th>
<th>Attack type</th>
<th>Dictionary</th>
</tr>
</thead>
</table>

### Fuzzing Results

<table>
<thead>
<tr>
<th>Timer</th>
<th>Code</th>
<th>Lines</th>
<th>Words</th>
<th>Chars</th>
<th>MDS</th>
<th>Payload</th>
<th>Cookie</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.004266</td>
<td>301</td>
<td>9</td>
<td>27</td>
<td>298</td>
<td>03d24e25d053f19e28b861468ee1</td>
<td>admin</td>
<td><a href="http://192.168.1.100/admin/">http://192.168.1.100/admin/</a></td>
<td></td>
</tr>
<tr>
<td>0.006392</td>
<td>301</td>
<td>9</td>
<td>27</td>
<td>300</td>
<td>17208ac3e6525d49516533357300a6</td>
<td>cgi-bin</td>
<td><a href="http://192.168.1.100/cgi-bin/">http://192.168.1.100/cgi-bin/</a></td>
<td></td>
</tr>
<tr>
<td>0.010655</td>
<td>301</td>
<td>9</td>
<td>27</td>
<td>299</td>
<td>6409de2f0804bb26663d99121e4c4a</td>
<td>images</td>
<td><a href="http://192.168.1.100/images/">http://192.168.1.100/images/</a></td>
<td></td>
</tr>
<tr>
<td>0.012686</td>
<td>200</td>
<td>1</td>
<td>2</td>
<td>23</td>
<td>6f9d8df5e9143e0d9baacdb7f14e2af6</td>
<td>index</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Index of /images

<table>
<thead>
<tr>
<th>Name</th>
<th>Last_modified</th>
<th>Size</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>parent Directory</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>cgi-bin/</td>
<td>01-Dec-2007 22:02</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

_Apache Server at 192.168.1.100 Port 80_
A taste of WebSlayer – Payload Generator
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:

- Beta testers please contact me!

- Any idea is welcome

- Thank you for your time