Mosca

Just another Simple static analysis tool to find bugs like a

grep unix command

Antonio Costa - CoolerVoid - coolerlair[aT]gmail[DOt]com

February 8, 2015

Whoami

Author:

- Antonio Costa ”CoolerVoid” is a Computer Programmer who loves the Hacker culture, he work as system analyst at CONVISO for three years. Nowadays, Antonio working with code review, pentest and security research with focus on Secure Web Applications and Reverse Engineering and he has speaking in some Brazilian Security Conferences such as YSTS, OWASP Florianopolis and Bsides Sao Paulo.

Introduction

Software Information:

- Mosca is a Open Source Tool to find bugs
- Mosca held by GPL v3 license: https://github.com/CoolerVoid/Mosca/blob/master/LICENSE.txt

Introduction

Why this tool is made in C language ?

- C have a high delay time for writing and debugging, but no pain no gain, have a fast performance, addition of this point, the C language is run at any architecture like Mips,ARM and others... at the future can follow mobile implementations. other benefits of C, have good and high profile to write optimizations, if you think write some lines in ASSEMBLY code with AES-NI or SiMD instructions, i think is good choice.
- Why you not use POO ? in this project i follow ”KISS” principe: http://pt.wikipedia.org/wiki/Keep_It_Simple
- C language have a lot old school dudes like a kernel hackers...

Introduction

Requirements:

- Need ”GCC” and ”make”, you need pcre library, at linux distributions like debian search package libpcre-dev at RPM distributions search libpcre-devel
- Current version tested only Unix Like systems(Linux, MacOS and *BSD).
- Current version run well, but is a BeTa version, you can report bug here: https://github.com/CoolerVoid/Mosca/issues

How you can use it

Following this to get, decompress, compile and execute:

- wget https://github.com/CoolerVoid/Mosca/archive/master.zip;
- unzip master.zip; cd Mosca-master; make; ./mosca

The Overview

```
[cooler@obiwan Mosca] $ ./mosca

        (^\'=='/^)
         \ \=/ /
       '--\_Y_/--'
        .'(_I_)`.
           "

    Static analysis tool to find bugs like a grep unix command  v0.02
+-----------------------------------------------------------------+
Options:
--egg = Load module to make analysis '--egg egg/php_top_fails.php'
--path = Path to open and make recursive search
--ext = File extension to search example; get only C files '\.c$'
--log = File to save results
Example:
$ ./mosca --egg egg/php_fails.egg --path home/user/blog_php --ext "\\.php$" --l
```

Explain

Mosca use Egg Modules

- Each egg is a simple config to find bug at especific language like PHP,Ruby etc...
- example of egg config at directory ”egg”
- If Mosca read a line with vunerability of egg in source code, mosca have alert about and save at logs.

The End

Greets

- IAK, Sigsegv, M0nad, Slyfunky , LaunJampa, Pr0teus, RaphaelSC, pl4nkton, gustavoRobertux, Muzgo, Otacon...
- HB, F-117, Eremita, Clandestine, Loganbr, Geyslan, Clodonil Trigo...
- my parents and friends...
- https://conviso.com.br/index.php/EN

at construction...