Payload mask

Tool designed for bypass waf

Antonio Costa - CoolerVoid - c00f3r[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:

- Payload mask is a Open Source Tool to generate payload list to try bypass Web Application Firewall, you can use a lot list of encodes and techniques to convert your payload list.
- Payload mask held by GPL v3 license: https://github.com/CoolerVoid/payloadmask/blob/master/LICENSI

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:

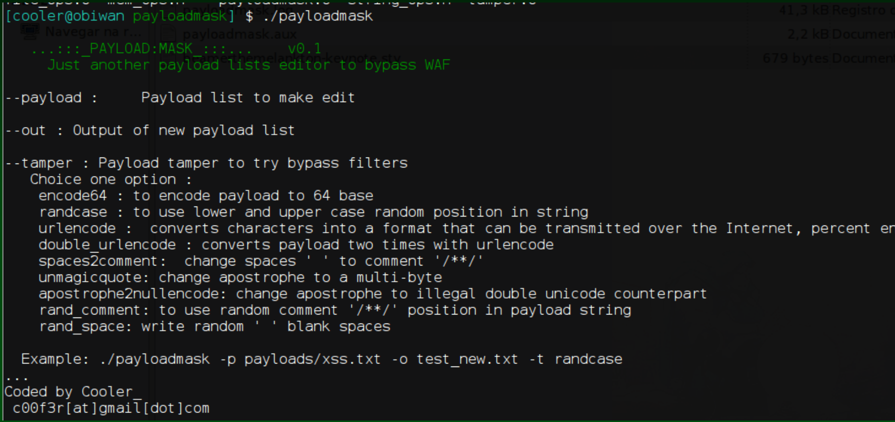
- Need ”GCC” and ”make”
- Current version tested only Unix Like systems(Linux, MacOS and *BSD).
- Current version run well, but is a BeTa version, you can report bug here: https://github.com/CoolerVoid/payloadmask/issues

How you can use it

Following this to get, decompress, compile and execute:

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

The Overview



```
file_ops.c  mem_ops.h   payloadmask.c  string_ops.h  tamper.c
[cooler@obiwan payloadmask] $ ./payloadmask

   ...:::_PAYLOAD:MASK_:::...    v0.1
     Just another payload lists editor to bypass WAF

--payload :     Payload list to make edit

--out : Output of new payload list

--tamper : Payload tamper to try bypass filters
   Choice one option :
    encode64 : to encode payload to 64 base
    randcase : to use lower and upper case random position in string
    urlencode :  converts characters into a format that can be transmitted over the Internet, percent en
    double_urlencode : converts payload two times with urlencode
    spaces2comment:  change spaces ' ' to comment '/**/'
    unmagicquote: change apostrophe to a multi-byte
    apostrophe2nullencode: change apostrophe to illegal double unicode counterpart
    rand_comment: to use random comment '/**/' position in payload string
    rand_space: write random ' ' blank spaces

  Example: ./payloadmask -p payloads/xss.txt -o test_new.txt -t randcase
...
Coded by Cooler_
 c00f3r[at]gmail[dot]com
```

Explain

WAF stands for Web Application Firewall. It is widely used nowadays to detect and defend SQL Injections and XSS...

- You can use comments to bypass WAF: http://www.site.com/index.php?page_id=-15 /*!UNION*/ /*!SELECT*/ 0,1,2,3...
- You can also change the Case of the Command: http://www.site.com/index.php?page_id=-15 UnIoN sELecT 0,1,2,3...
- You can combine methods: http://www.site.com/index.php?page_id=-15 /*!uNIOn*/ /*!sElECt*/ 0,1,2,3.

The End

Greets

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

at construction...