Memory cheat(AOS)

Unknown macro: 'html'

Excuse the ads! We need some help to keep our site up. Unknown macro: 'html'

List

- Memory cheat(AOS)
  - Structure of Memory Cheat
  - Process attach
    - ptrace()
    - ptrace synopsis
    - ptrace request
  - Check the process memory area
    - /proc/pid/maps
    - Filter the mapping area
  - Memory read
    - ptrace()
    - /proc/pid/mem
  - Memory write
    - ptrace()
    - /proc/pid/mem
  - Memory fuzzing
  - Memory lock
  - Related site

Memory cheat(AOS)

- 2016 Cheat tool .
  - https://github.com/Lazenca/Lazenca-A-Andoird
- Tool Memory cheat .
- Tool , .

Structure of Memory Cheat

- **Memory cheats tool .**

The default behavior of the memory cheat tool.

1	**Process attach**	ptrace() .
2	**Check the process memory area**	Memory Memory (Memory map) .
3	**Memory access**	Memory ptrace .

Process attach

ptrace()

- **ptrace() , , .**
  - ptrace() gdb, strace, ltrace .
  - ptrace() GOT .

ptrace synopsis

- **ptrace .**

ptrace()

```
#include <sys/ptrace.h>
long ptrace(enum __ptrace_request request, pit_t pid, void *addr, void *data);
```

ptrace request

- **ptrace .**

PTRACE_ATTACH	• pid .
	  ○ SIGSTOP .
	  ○ waitpid(2) .

PTRACE_TRACEME	• . ○ .

PTRACE_PEEKTEXT
PTRACE_PEEKDATA
PTRACE_PEEKUSER
	• .
	  ○ .
	  ○ PEEKTEXT,PEEKDATA,PEEKUSER .

PTRACE_POKTEXT PTRACE_POKEDATA PTRACE_POKEUSER	• .
PTRACE_GETREGS	• . ○ .
PTRACE_SETREGS	• . ○ .
PTRECE_CONT	• .
PTRACE_DETACH	• .

PTRACE_SYSCALL	• , .
	  ○ .
	  ○ strace .

PTRACE_SINGLESTEP	• , . ○ .
PTRACE_GETSIGINFO	• . ○ siginfo_t .

PTRACE_SETSIGINFO	• .
	  ○ siginfo_t .
	  ○ , .

PTRACE_SETOPTIONS	• ptrace .
	  ○ .
	  ○ ptrace(2)

man page - ptrace(process trace)

- http://man7.org/linux/man-pages/man2/ptrace.2.html

Check the process memory area

/proc/pid/maps

- **maps .**

/proc/self/maps

```
root@angler:/ # cat /proc/self/maps

address                           perms        offset  dev   inode      pathname

b6c00000-b6e00000 rw-p 00000000 00:00 0          [anon:libc_malloc]
b6eeb000-b6eed000 r-xp 00000000 b3:17 2482       /system/lib/libnetd_client.so
b6eed000-b6eee000 r--p 00001000 b3:17 2482       /system/lib/libnetd_client.so
b6eee000-b6eef000 rw-p 00002000 b3:17 2482       /system/lib/libnetd_client.so
b6eef000-b6f0f000 r--s 00000000 00:0b 7141       /dev/__properties__
b6f0f000-b6f11000 r-xp 00000000 b3:17 2727       /system/lib/libstdc++.so
b6f11000-b6f12000 r--p 00001000 b3:17 2727       /system/lib/libstdc++.so
b6f12000-b6f13000 rw-p 00002000 b3:17 2727       /system/lib/libstdc++.so

...
```

Fields in the maps file

address	• address .
perms	• perms . ○ r : read ○ w : write ○ x : execute ○ s : shared ○ p : private
offset	• .
dev	• dev . (major:minor)
inode	• inode inode . ○ inode 0 inode .
pathname	• pathname .

Filter the mapping area

- **, .**
  - .
  - .

/proc/pid/maps

```
root@angler:/ # cat /proc/8913/maps
00008000-0000d000 rw-s 00174000 00:0c 5431                               /dev/kgsl-3d0
0000d000-0002e000 rw-s 0023b000 00:0c 5431                               /dev/kgsl-3d0
12c00000-12e16000 rw-p 00000000 00:04 22331                              /dev/ashmem/dalvik-main space (deleted)
```

```
12e16000-13d6d000 rw-p 00216000 00:04 22331                              /dev/ashmem/dalvik-main space (deleted)
13d6d000-32c00000 ---p 0116d000 00:04 22331                              /dev/ashmem/dalvik-main space (deleted)
32c00000-32c01000 rw-p 00000000 00:04 22332                              /dev/ashmem/dalvik-main space 1
(deleted)
32c01000-52c00000 ---p 00001000 00:04 22332                              /dev/ashmem/dalvik-main space 1
(deleted)
70ee7000-718df000 rw-p 00000000 fd:00 318872                             /data/dalvik-cache/arm
/system@framework@boot.art
718df000-737c0000 r--p 00000000 fd:00 318869                             /data/dalvik-cache/arm
/system@framework@boot.oat
737c0000-74f63000 r-xp 01ee1000 fd:00 318869                             /data/dalvik-cache/arm
/system@framework@boot.oat
74f63000-74f64000 rw-p 03684000 fd:00 318869                             /data/dalvik-cache/arm
/system@framework@boot.oat
74f64000-75093000 rw-p 00000000 00:04 22330                              /dev/ashmem/dalvik-zygote space
(deleted)
75093000-75094000 rw-p 00000000 00:04 25095                              /dev/ashmem/dalvik-non moving space
(deleted)
75094000-7509d000 rw-p 00001000 00:04 25095                              /dev/ashmem/dalvik-non moving space
(deleted)
7509d000-78765000 ---p 0000a000 00:04 25095                              /dev/ashmem/dalvik-non moving space
(deleted)
78765000-78f64000 rw-p 036d2000 00:04 25095                              /dev/ashmem/dalvik-non moving space
(deleted)
ab1dd000-ab1e9000 r-xp 00000000 103:0b 65025                             /system/bin/app_process32_xposed
ab1e9000-ab1eb000 r--p 0000b000 103:0b 65025                             /system/bin/app_process32_xposed
ab1eb000-ab1ec000 rw-p 0000d000 103:0b 65025                             /system/bin/app_process32_xposed
bb907000-bba08000 rw-s 00160000 00:0c 5431                               /dev/kgsl-3d0
...  ...
ce683000-ce781000 rw-p 00000000 00:00 0                                  [stack:9328]
ce781000-ce782000 ---p 00000000 00:00 0
ce782000-ce880000 rw-p 00000000 00:00 0                                  [stack:9327]
ce880000-ceb80000 rw-p 00000000 00:00 0                                  [anon:libc_malloc]
ceb88000-ceb89000 ---p 00000000 00:00 0
ceb89000-ceb8b000 rw-p 00000000 00:00 0                                  [anon:thread signal stack]
ceb8b000-ceb8d000 rw-p 00000000 00:04 61129                              /dev/ashmem/dalvik-indirect ref table
(deleted)
ceb8d000-cebad000 rw-p 00000000 00:04 73001                              /dev/ashmem/dalvik-LinearAlloc
(deleted)
cebad000-cee00000 r--s 0002a000 fd:00 1062997                            /data/app/com.********.*******/base.apk
cee00000-cee40000 rw-p 00000000 00:00 0                                  [anon:libc_malloc]
cee4f000-cee50000 ---p 00000000 00:00 0
cee50000-cee52000 rw-p 00000000 00:00 0                                  [anon:thread signal stack]
cee52000-cee54000 rw-p 00000000 00:04 61127                              /dev/ashmem/dalvik-indirect ref table
(deleted)
cee54000-cee57000 r-xp 00000000 fd:00 1063087                            /data/app/com.********.*******/lib/arm
/lib*****.so
cee57000-cee58000 r--p 00002000 fd:00 1063087                            /data/app/com.********.*******/lib/arm
/lib*****.so
cee58000-cee59000 rw-p 00003000 fd:00 1063087                            /data/app/com.********.*******/lib/arm
/lib*****.so
cee63000-cee73000 rwxp 00000000 00:00 0
cee73000-cef80000 rw-p 00000000 00:00 0
cef80000-cf680000 rw-p 00000000 00:00 0                                  [anon:libc_malloc]
cf686000-cf6b6000 rwxp 00000000 00:00 0
cf6b6000-cf6b9000 r-xp 00000000 fd:00 1063085                            /data/app/com.********.*******/lib/arm
/libkeystore.so
cf6b9000-cf6ba000 r--p 00002000 fd:00 1063085                            /data/app/com.********.*******/lib/arm
/libkeystore.so
cf6ba000-cf6bb000 rw-p 00003000 fd:00 1063085                            /data/app/com.********.*******/lib/arm
/libkeystore.so
...  ...
d1bd2000-d1cf3000 r-xp 00000000 fd:00 1063088                            /data/app/com.********.*******/lib/arm
/lib*****.so
d1cf3000-d1cf4000 ---p 00000000 00:00 0
d1cf4000-d1cf7000 r--p 00121000 fd:00 1063088                            /data/app/com.********.*******/lib/arm
/lib*****.so
d1cf7000-d1cf9000 rw-p 00124000 fd:00 1063088                            /data/app/com.********.*******/lib/arm
/lib*****.so
d1cf9000-d1d40000 rw-p 00000000 00:00 0
d1d40000-d1f40000 rw-p 00000000 00:00 0                                  [anon:libc_malloc]
```

```
d1f40000-d2f80000 rw-s 00000000 00:08 9640                              anon_inode:dmabuf
d2f80000-d3fc0000 rw-s 00000000 00:08 9640                              anon_inode:dmabuf
d3fc0000-d5000000 rw-s 00000000 00:08 9640                              anon_inode:dmabuf
d5000000-d7f80000 rw-p 00000000 00:00 0                                 [anon:libc_malloc]
d7f85000-d7f86000 ---p 00000000 00:00 0
d7f86000-d8084000 rw-p 00000000 00:00 0                                 [stack:9012]
d8084000-d8085000 ---p 00000000 00:00 0
d8085000-d8183000 rw-p 00000000 00:00 0                                 [stack:9011]
d8183000-d8185000 rw-p 00000000 00:04 61044                             /dev/ashmem/dalvik-indirect ref table
(deleted)
d818b000-d818d000 rw-p 00000000 00:04 68195                             /dev/ashmem/dalvik-indirect ref table
(deleted)
d818d000-d818e000 ---p 00000000 00:00 0
d818e000-d8190000 rw-p 00000000 00:00 0                                 [anon:thread signal stack]
d8190000-d8191000 ---p 00000000 00:00 0
......
d830a000-d830c000 rw-p 00000000 00:04 68191                             /dev/ashmem/dalvik-indirect ref table
(deleted)
d830c000-d831c000 rwxp 00000000 00:00 0
d831c000-d8339000 r-xp 00000000 fd:00 1063080                           /data/app/com.********.*******/lib/arm
/lib*****.so
d8339000-d833a000 ---p 00000000 00:00 0
d833a000-d833b000 r--p 0001d000 fd:00 1063080                           /data/app/com.********.*******/lib/arm
/lib*****.so
d833b000-d833c000 rw-p 0001e000 fd:00 1063080                           /data/app/com.********.*******/lib/arm
/lib*****.so
d833c000-d8340000 rw-p 00000000 00:00 0
d8340000-d83c0000 rw-p 00000000 00:00 0                                 [anon:libc_malloc]
d83c1000-d83c3000 rw-p 00000000 00:04 57117                             /dev/ashmem/dalvik-indirect ref table
(deleted)
d83c6000-d83c7000 ---p 00000000 00:00 0
d83c7000-d84c5000 rw-p 00000000 00:00 0                                 [stack:9009]
d84c5000-d84c6000 ---p 00000000 00:00 0
...  ...
da580000-da582000 rw-p 00000000 00:04 65885                             /dev/ashmem/dalvik-indirect ref table
(deleted)
da582000-da584000 rw-p 00000000 00:04 57110                             /dev/ashmem/dalvik-indirect ref table
(deleted)
da584000-da586000 r-xp 00000000 fd:00 1063081                           /data/app/com.********.*******/lib/arm
/********.so
da586000-da587000 r--p 00001000 fd:00 1063081                           /data/app/com.********.*******/lib/arm
/********.so
da587000-da588000 rw-p 00002000 fd:00 1063081                           /data/app/com.********.*******/lib/arm
/********.so
da58d000-da58f000 rw-p 00000000 00:04 65876                             /dev/ashmem/dalvik-indirect ref table
(deleted)
da58f000-da590000 ---p 00000000 00:00 0
da590000-da592000 rw-p 00000000 00:00 0                                 [anon:thread signal stack]
da592000-da5ba000 r-xp 00000000 103:0b 1438                             /system/lib/libwilhelm.so
da5ba000-da5bb000 ---p 00000000 00:00 0
da5bb000-da5be000 r--p 00028000 103:0b 1438                             /system/lib/libwilhelm.so
da5be000-da5bf000 rw-p 0002b000 103:0b 1438                             /system/lib/libwilhelm.so
......
dcf37000-dddbb000 r-xp 00000000 fd:00 1063091                           /data/app/com.********.*******/lib/arm
/libunity.so
dddbb000-dddee000 rw-p 00e83000 fd:00 1063091                           /data/app/com.********.*******/lib/arm
/libunity.so
dddee000-ddfbd000 rw-p 00000000 00:00 0
ddfbd000-de34c000 r-xp 00000000 fd:00 1063052                           /data/app/com.********.*******/lib/arm
/libmono.so
de34c000-de34d000 ---p 00000000 00:00 0
de34d000-de34f000 r--p 0038f000 fd:00 1063052                           /data/app/com.********.*******/lib/arm
/libmono.so
de34f000-de354000 rw-p 00391000 fd:00 1063052                           /data/app/com.********.*******/lib/arm
/libmono.so
de354000-de371000 rw-p 00000000 00:00 0
de371000-de804000 r--p 00000000 fd:00 451502                            /data/data/com.linecorp.LGSDG/files/.
tomb/.D45AC878/.O/D45AC878.dex (deleted)
de804000-deb90000 r-xp 00493000 fd:00 451502                            /data/data/com.linecorp.LGSDG/files/.
tomb/.D45AC878/.O/D45AC878.dex (deleted)
deb90000-deb91000 rw-p 0081f000 fd:00 451502                            /data/data/com.linecorp.LGSDG/files/.
```

```
tomb/.D45AC878/.O/D45AC878.dex (deleted)
deb91000-df1d4000 r--p 00000000 fd:00 1063266                            /data/app/com.********.*******/oat/arm
/base.odex
df1d4000-df713000 r-xp 00643000 fd:00 1063266                            /data/app/com.********.*******/oat/arm
/base.odex
df713000-df714000 rw-p 00b82000 fd:00 1063266                            /data/app/com.********.*******/oat/arm
/base.odex
df714000-dff14000 rw-p 00000000 00:04 25094                              /dev/ashmem/dalvik-allocspace main
rosalloc space mark-bitmap 3 (deleted)
dff14000-e0714000 rw-p 00000000 00:04 25093                              /dev/ashmem/dalvik-allocspace main
rosalloc space live-bitmap 3 (deleted)
e0714000-e8040000 ---p 00000000 00:00 0
e8040000-e82c0000 rw-p 00000000 00:00 0                                  [anon:libc_malloc]
e82c0000-e82c2000 rw-p 00000000 00:04 65872                              /dev/ashmem/dalvik-indirect ref table
(deleted)
e82c2000-e82c3000 ---p 00000000 00:00 0
e82c3000-e82c5000 rw-p 00000000 00:00 0                                  [anon:thread signal stack]
e82c5000-e82c6000 ---p 00000000 00:00 0
e82c6000-e82c8000 rw-p 00000000 00:00 0                                  [anon:thread signal stack]
e82c8000-e82cd000 r-xp 00000000 103:0b 1282                              /system/lib/libeffects.so
e82cd000-e82ce000 r--p 00004000 103:0b 1282                              /system/lib/libeffects.so
e82ce000-e82cf000 rw-p 00005000 103:0b 1282                              /system/lib/libeffects.so
e82cf000-e82d2000 r-xp 00000000 103:0b 1393                              /system/lib
/libstagefright_http_support.so
e82d2000-e82d3000 ---p 00000000 00:00 0
e82d3000-e82d4000 r--p 00003000 103:0b 1393                              /system/lib
/libstagefright_http_support.so
e82d4000-e82d5000 rw-p 00004000 103:0b 1393                              /system/lib
/libstagefright_http_support.so
e82d5000-e82d9000 r-xp 00000000 103:0b 1233                              /system/lib/libOpenSLES.so
e82d9000-e82da000 r--p 00003000 103:0b 1233                              /system/lib/libOpenSLES.so
e82da000-e82db000 rw-p 00004000 103:0b 1233                              /system/lib/libOpenSLES.so
...  ...
e8e51000-e904d000 r-xp 00000000 fd:00 1063070                            /data/app/com.********.*******/lib/arm
/libglf.so
e904d000-e904e000 rwxp 001fc000 fd:00 1063070                            /data/app/com.********.*******/lib/arm
/libglf.so
e904e000-e90b5000 r-xp 001fd000 fd:00 1063070                            /data/app/com.********.*******/lib/arm
/libglf.so
e90b5000-e90cb000 rwxp 00264000 fd:00 1063070                            /data/app/com.********.*******/lib/arm
/libglf.so
e90cb000-e9109000 r-xp 0027a000 fd:00 1063070                            /data/app/com.********.*******/lib/arm
/libglf.so
e9109000-e9127000 rw-p 002b7000 fd:00 1063070                            /data/app/com.********.*******/lib/arm
/libglf.so
e9127000-e9130000 rw-p 00000000 00:00 0
e9130000-e9150000 rwxp 002d5000 fd:00 1063070                            /data/app/com.********.*******/lib/arm
/libglf.so
e9150000-e9151000 rwxp 00000000 00:00 0
......
f76aa000-f76cf000 r-xp 00000000 103:0b 1260                              /system/lib/libbinder.so
f76cf000-f76d0000 ---p 00000000 00:00 0
f76d0000-f76d7000 r--p 00025000 103:0b 1260                              /system/lib/libbinder.so
f76d7000-f76d8000 rw-p 0002c000 103:0b 1260                              /system/lib/libbinder.so
f76d8000-f76e0000 r-xp 00000000 103:0b 1319                              /system/lib/liblog.so
f76e0000-f76e1000 r--p 00007000 103:0b 1319                              /system/lib/liblog.so
f76e1000-f76e2000 rw-p 00008000 103:0b 1319                              /system/lib/liblog.so
f76e2000-f76fa000 r-xp 00000000 103:0b 1431                              /system/lib/libutils.so
f76fa000-f76fb000 ---p 00000000 00:00 0
f76fb000-f76fc000 r--p 00018000 103:0b 1431                              /system/lib/libutils.so
f76fc000-f76fd000 rw-p 00019000 103:0b 1431                              /system/lib/libutils.so
f76fd000-f770b000 r-xp 00000000 103:0b 1275                              /system/lib/libcutils.so
f770b000-f770c000 ---p 00000000 00:00 0
f770c000-f770d000 r--p 0000e000 103:0b 1275                              /system/lib/libcutils.so
f770d000-f770e000 rw-p 0000f000 103:0b 1275                              /system/lib/libcutils.so
f770e000-f770f000 rw-p 00000000 00:00 0                                  [anon:linker_alloc_vector]
f770f000-f7710000 rw-p 00000000 00:00 0                                  [anon:linker_alloc_64]
f7710000-f7711000 r--p 00000000 00:00 0                                  [anon:linker_alloc]
f7711000-f7712000 rw-p 00000000 00:00 0                                  [anon:linker_alloc]
f7712000-f7713000 rw-p 00000000 00:00 0                                  [anon:linker_alloc_vector]
f7713000-f7714000 rw-p 00000000 00:00 0                                  [anon:linker_alloc_32]
```

```
f7714000-f7715000 r--p 00000000 00:00 0                                  [anon:linker_alloc]
f7715000-f7735000 r--s 00000000 00:0c 5396                               /dev/__properties__
f7735000-f7736000 r--p 00000000 00:00 0
f7736000-f7737000 ---p 00000000 00:00 0
f7737000-f7739000 rw-p 00000000 00:00 0                                  [anon:thread signal stack]
f7739000-f7756000 r-xp 00000000 103:0b 436                               /system/bin/linker
f7756000-f7757000 r--p 0001c000 103:0b 436                               /system/bin/linker
f7757000-f7759000 rw-p 0001d000 103:0b 436                               /system/bin/linker
f7759000-f775b000 rw-p 00000000 00:00 0
ff246000-ff246000 rw-p 00000000 00:00 0
ff246000-ff247000 ---p 00000000 00:00 0
ff247000-ffa46000 rw-p 00000000 00:00 0                                  [stack]
ffff0000-ffff1000 r-xp 00000000 00:00 0                                  [vectors]
root@angler:/ #
```

- **"Lazenca-A-Android"** .
  -

void MapsListFiltering()

```
void MapsListFiltering(){
        for(int i = 0;i < mapsList.size();i++){
                maps = mapsList.at(i);

                if(!strstr(maps.strPerms,"rw-p")){
                        continue;
                }else if(strstr(maps.strPath,"/system/bin")){
                        continue;
                }else if(strstr(maps.strPath,"/system/lib")){
                        continue;
                }else if(strstr(maps.strPath,"/system/vendor")){
                        continue;
                }else if(strstr(maps.strPath,"/dev/ashmem")){
                        if(!strstr(maps.strPath,"/dev/ashmem/dalvik-heap")){
                                continue;
                        }
                }else if(strstr(maps.strPath,"")){
                        continue;
                }
                memReadAreaList.push_back(maps);
        }
}
```

Filter list

perms	• "rw-p"
pathname	• "/system/bin" • "/system/lib" • "/system/bin" • "/dev/ashmem" ○ "/dev/ashmem/dalvik-heap" • "[anon:libc_malloc]"

Memory read

ptrace()

- **ptrace()** .
  - "PTRACE_ATTACH" .
  - "PTRACE_PEEKDATA" .

    - "PTRACE_ATTACH" .

void readData(int pid, void* address)

```
void readData(int pid, void* address){
        ptrace(PTRACE_ATTACH, pid, NULL, NULL);
        long value = ptrace(PTRACE_PEEKDATA, pid,(void *) address,NULL);
        ptrace(PTRACE_DETACH, pid, NULL, NULL);
}
```

/proc/pid/mem

- .
    -
    -
- **"/proc/pid/mem" .**
    - open() .("/proc/pid/mem")
    - , .
        - ,
    - .

void getValue(int mem_fd,long staMemAddr,long endMemAddr,void *buf)

```
void getValue(int mem_fd,long staMemAddr,long endMemAddr,void *buf){
        void* address;
        void* value;

        printf("staMemAddr : %#lx, endMemAddr : %#lx\n",staMemAddr,endMemAddr);

        for (; staMemAddr < endMemAddr; staMemAddr += 4096) {
                printf("fd : %d, staMemAddr : %#lx, endMemAddr : %#lx\n",mem_fd,staMemAddr,endMemAddr);
                lseek(mem_fd, staMemAddr, SEEK_SET);
                read(mem_fd, buf, MEMREADSIZE);
                for (int j = 0; j < MEMREADSIZE / 4; j++) {
                        address = (void*) (staMemAddr + (j * 4));
                        value = ((long**) buf)[j];
                        printf("address : %#lx, Value : %ld\n",(long)address,(long)value);
                }
        }
}
```

waitpid(2) - Linux man page

- lseek() .
    - http://man7.org/linux/man-pages/man2/lseek.2.html

Memory write

ptrace()

- **ptrace() .**
    - "PTRACE_ATTACH" .
    - "PTRACE_POKEDATA" .
    - "PTRACE_ATTACH" .

void readData(int pid, void* address, void* address)

```
void readData(int pid, void* address, void* address){
        ptrace(PTRACE_ATTACH, pid, NULL, NULL);
        ptrace(PTRACE_POKEDATA, pid, (void *) address,(void *) value);
        ptrace(PTRACE_DETACH, pid, NULL, NULL);
}
```

/proc/pid/mem

- **write() "/proc/pid/mem" .**
  - .
  - .

void MemoryWrite(char *cAddress, char *cValue)

```
void MemoryWrite(char *cAddress, char *cValue) {
        if(cmdSizeCheck(cAddress)){
                if(cmdSizeCheck(cValue)){
                        int status;
                        long tmpValue;
                        long address;
                        char memFileName[30];
                        int mem_fd;

                        address = strtoul(cAddress, NULL, 16);
                        sscanf(cValue, "%ld", &tmpValue);
                        sprintf(memFileName, "/proc/%d/mem", privatePid);

                        ptrace(PTRACE_ATTACH, privatePid, NULL, NULL);
                        waitpid(privatePid, &status, WUNTRACED);

                        if (0 < (mem_fd = open(memFileName, O_WRONLY | O_LARGEFILE))) {
                                lseek(mem_fd, address, SEEK_SET);
                                write(mem_fd, &tmpValue, sizeof(tmpValue));
                                close(mem_fd);
                        } else {
                                printf("%s\n", errorMsgPid);
                        }
                        ptrace(PTRACE_DETACH, privatePid, NULL, NULL);
                        renewal();
                }
        }
}
```

Memory fuzzing

- **Memory fuzz .**
  -
  -
  -
  -
- **.**
  - Fuzz .
  - , .
    - .
    - .

Memory lock

- **Memory lock .**
  - .
  - ptrace() .

Related site

- https://github.com/Lazenca/Lazenca-A-Andoird
- http://man7.org/linux/man-pages/man5/proc.5.html

Unknown macro: 'html'