Hacking like in the movies

Insomni'hack 2015 CTF

writeups

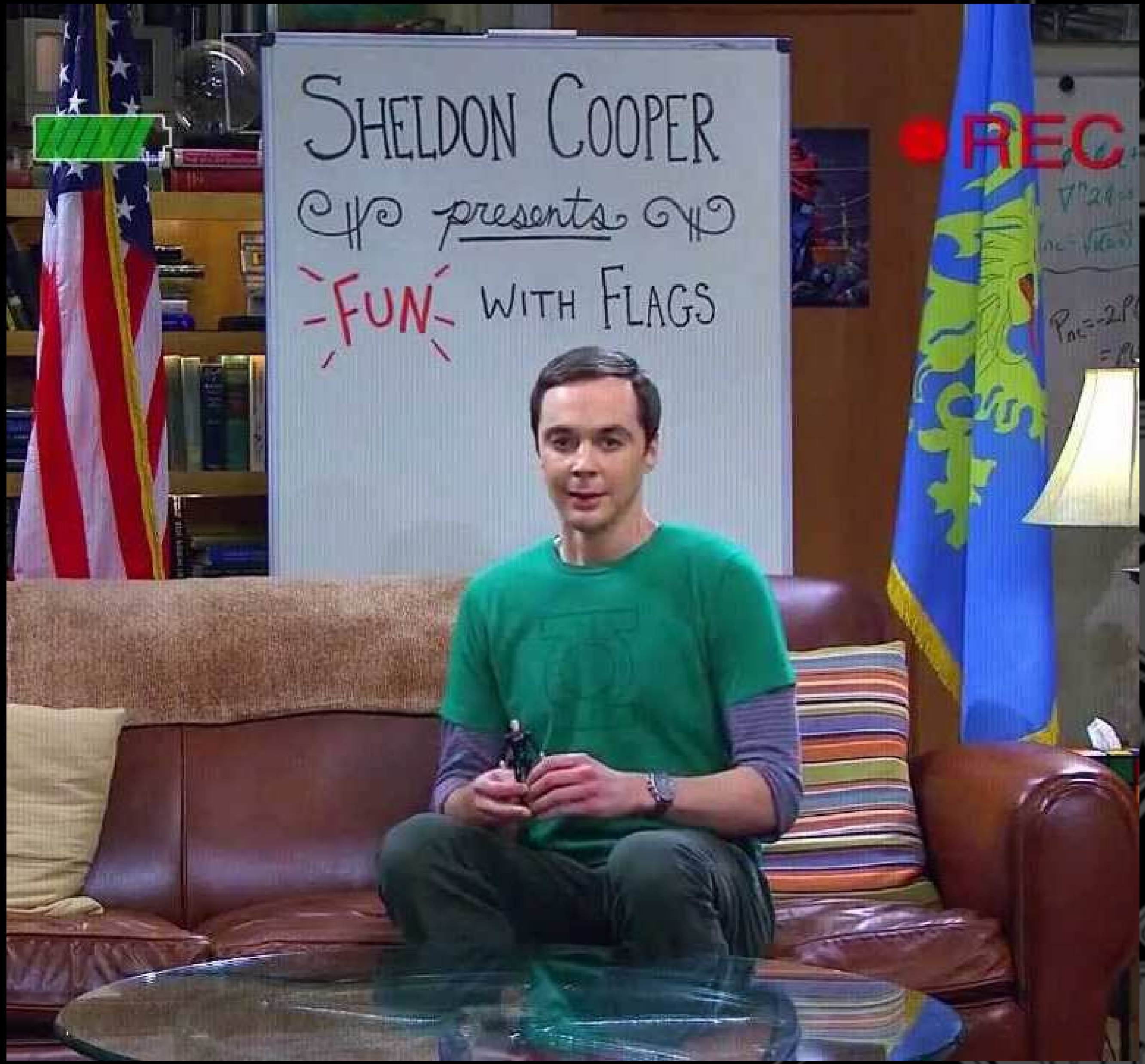
INSOMNI'HACK

Intro|Insomni’hack ?

- Organized by SCRT
- First edition in 2008
- Security talks since 2011
- Official CTF teaser since 2014
- Next edition :
  - Teaser January 16
  - CTF March 18 2016

Intro | CTF ?

- Capture The Flag
- Security challenges
- Time limited
- Jeopardy or attack/defense
- https://ctftime.org/



Intro | CTFs are good for you

- Pros
  - Get out of your comfort zone
  - Learn new tricks
  - Fun experience
- Cons
  - Time consuming

Intro | Insomni’hack 2015 teaser

- Theme: Mocking Hollywood hacking
- Online for 36h
- ~370 teams
- 5 challenges
- Pwnable, reversing and web

INSOMNI'HACK

Intro | Insomni’hack 2015 CTF

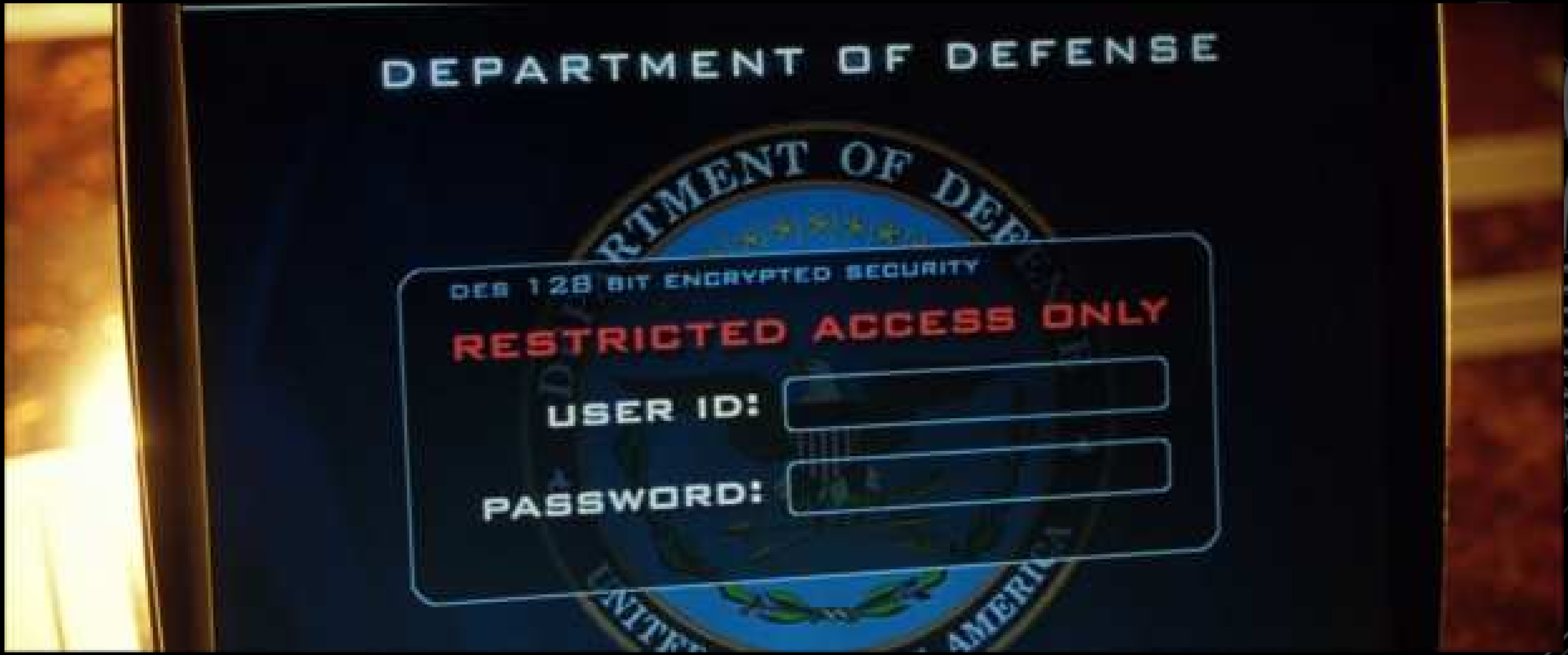
- ~350 participants (56 teams)
- Won by Dragon Sector
- Several international teams present
- 28 challenges
- Pwnable, shellcoding, reversing, web, network, forensics, hardware and mobile

Intro | Mocking Hollywood hacking

- Hollywood is terrible @hacking
- Like… really.
- Except for a very few select movies
- 3d malwares, IPv5, manual password bruteforcing, progress bars, image zooming, etc.

Intro | Mocking Hollywood hacking

Intro | Mocking Hollywood hacking



DEPARTMENT OF DEFENSE

DES 128 BIT ENCRYPTED SECURITY

RESTRICTED ACCESS ONLY

USER ID:

PASSWORD:

Intro | Mocking Hollywood hacking

Tools

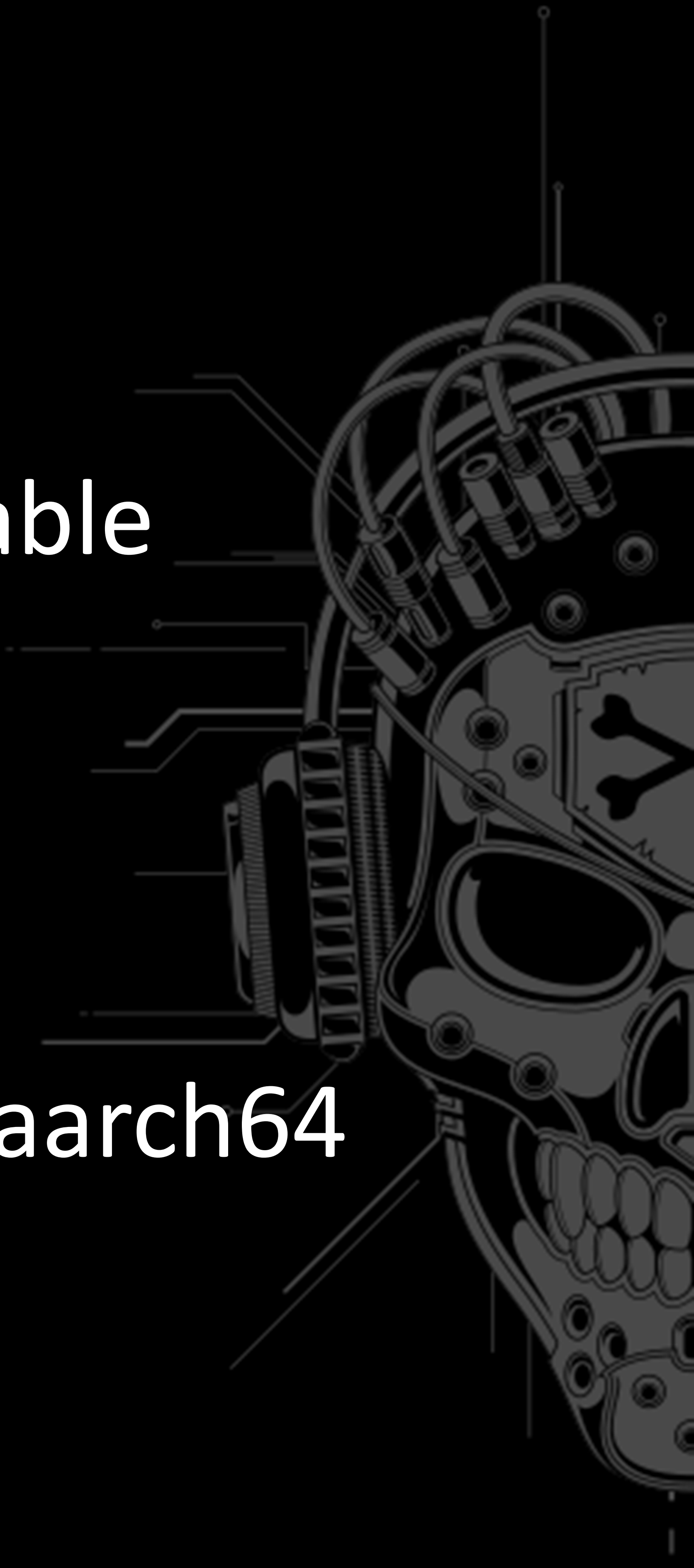
Web,reverse,exploit,forensic

Tools | web

- Burpsuite / Webscarab
- LiveHTTPHeaders / Firebug / Tamper Data / Hackbar
- Python requests
- curl

Tools | reverse

- IDA Pro
  - Expensive but the most powerful available
  - Supports many architectures
  - Hex-Rays decompiler
- Hopper
  - Cheap but supports x86, x64, arm and aarch64
  - Decompiler for x86, x64 and arm



Tools | reverse

- Snowman
  - IDA pro decompiler plugin
  - Also a standalone version
  - ARM, x86 and x64
- Radare : r2
  - Open source disassembler with console or web interface

Tools | reverse

You're planning to do this ctf only with r2 ?

Tools | reverse/exploit

- gdb & peda
  - The Linux pwner’s toolbag
  - searchmem
  - telescope
  - pretty print of changed regs
  - branching indications

Tools|exploit

- checksec.sh

```
RELRO           STACK CANARY      NX            PIE
Partial RELRO   Canary found      NX enabled    No PIE
```

- rp++
  - One of the best gadget finders for x86 / x64
  - Supports Linux, Windows, FreeBSD and Mac OSX
- ROPgadget Tool

Tools | forensics

- Volatility
  - Powerful for process reconstruction (net connections, process image, etc.)
  - Easy to use
- Wireshark
  - Network analysis swiss army knife

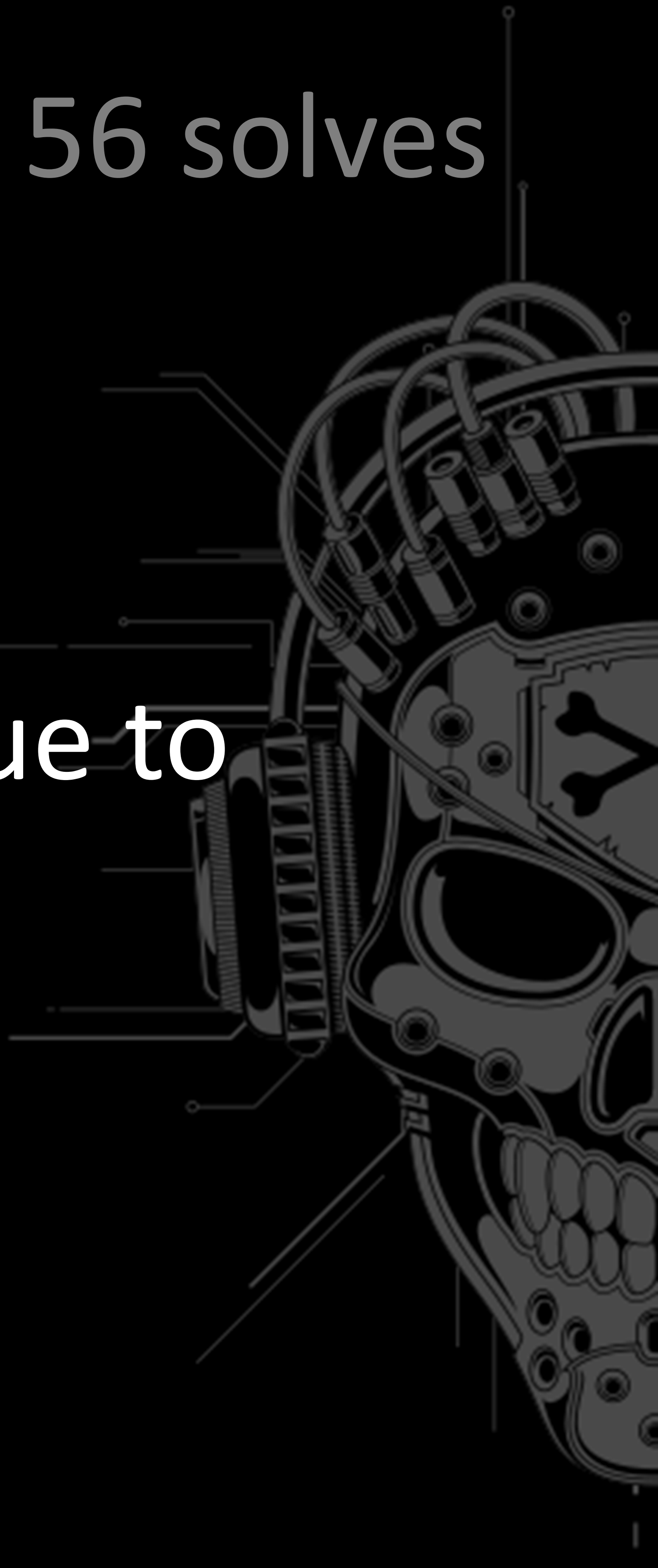
The challenges

Web, hardware, reversing, network, exploits, shellcoding, forensics, mobile

Web|n00bs gonna win!

56 solves

- Easy challenge that anyone can solve
- What is the best hacking movie
- Read the HTML source, edit form value to submit hidden field value Matrix
- Obvious bad choices : «Swordfish», «Hackers», etc.



Web | Smell of the lamp

32 solves

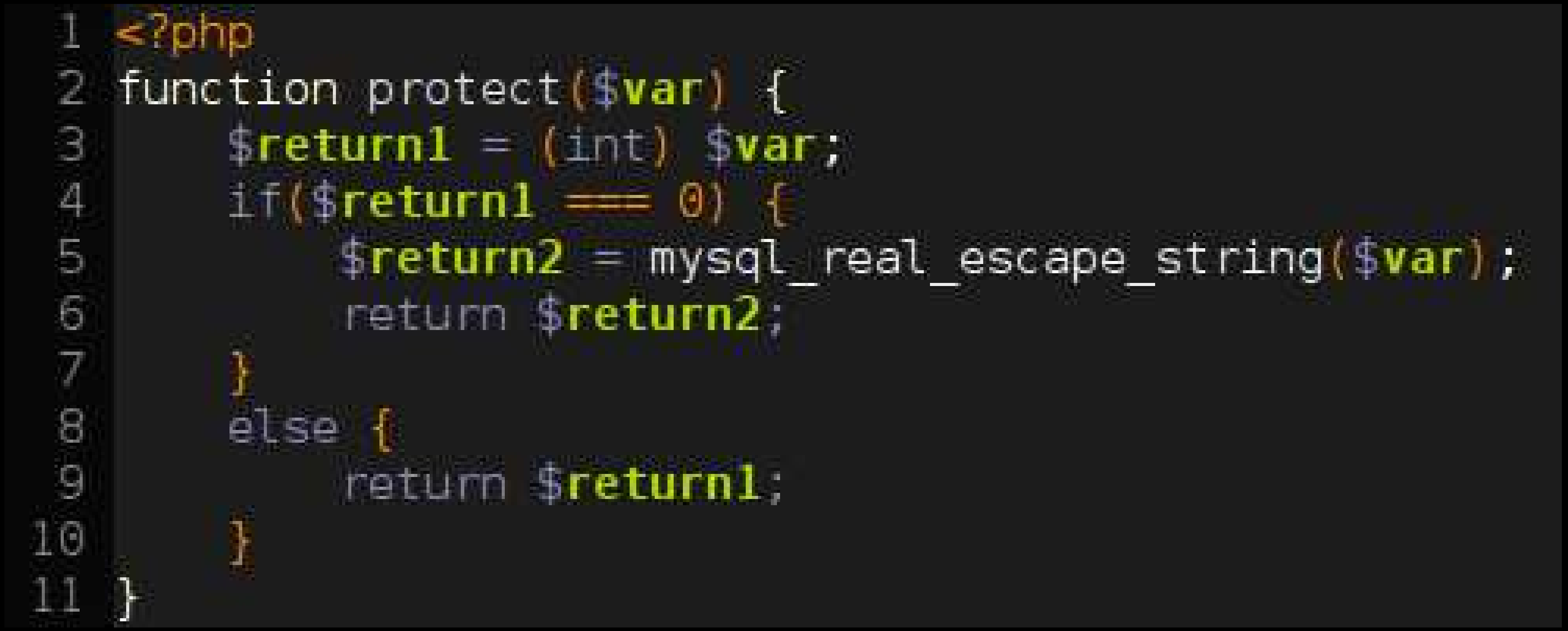
- Hint: edited with vim
- Get the source from `index.php~`
- SQL Injections everywhere
- Query results not printed
- Error-based SQL Injection

INSOMNI'HACK

Web|Hacker News

30 solves

- SQL Injection in an integer field

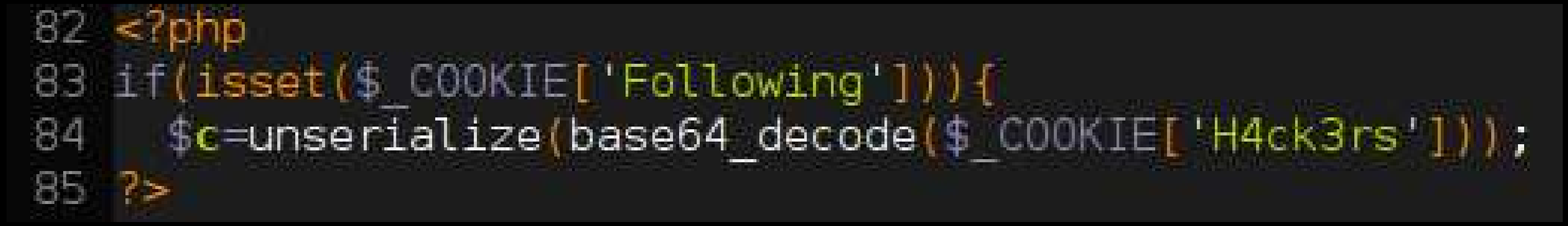


```php
<?php
function protect($var) {
    $return1 = (int) $var;
    if($return1 === 0) {
        $return2 = mysql_real_escape_string($var);
        return $return2;
    }
    else {
        return $return1;
    }
}
```

Web|Serial Hackers

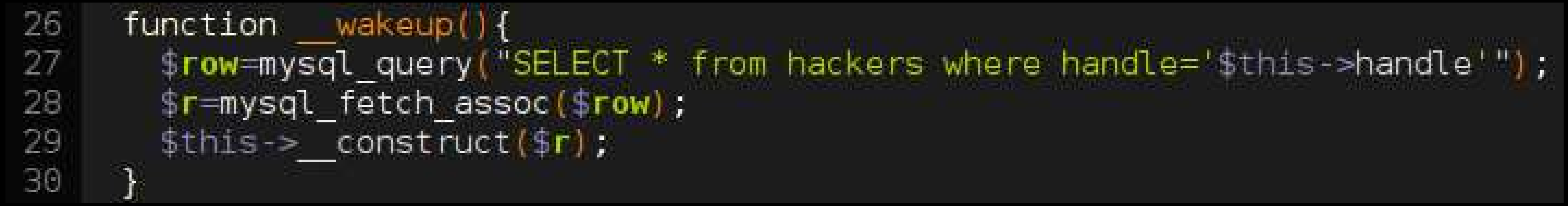
19 solves

- Unsafe unserialize



```php
<?php
if(isset($_COOKIE['Following'])){
  $c=unserialize(base64_decode($_COOKIE['H4ck3rs']));
?>
```

- Modify handle attribute ⇨ SQL Injection



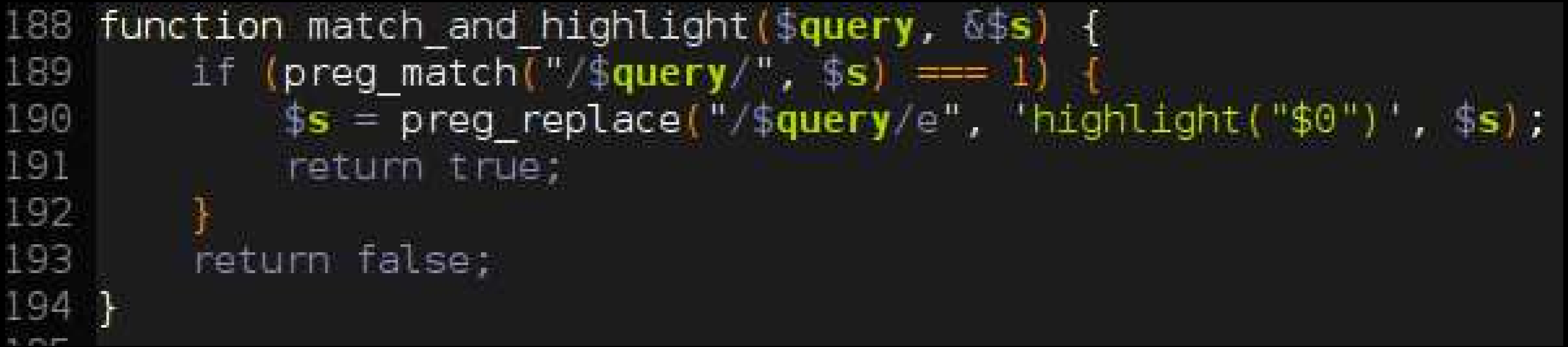
```php
  function __wakeup(){
    $row=mysql_query("SELECT * from hackers where handle='$this->handle'");
    $r=mysql_fetch_assoc($row);
    $this->__construct($r);
  }
```

- Find and dump secret table

Web | Smelly lamp got makeup

4 solves

- Forum about hacking movies
- Vuln in comments / search



```php
function match_and_highlight($query, &$s) {
    if (preg_match("/$query/", $s) === 1) {
        $s = preg_replace("/$query/e", 'highlight("$0")', $s);
        return true;
    }
    return false;
}
```

- `$query = '\$\{system\(\$_REQUEST\[code\]\)\}';`
- `$s = '${system($_REQUEST[code])}';`

Web|Hacker Idol

2 solves

- Neo4j graph database
- Traversal REST endpoint
- SSJI in `return_filter`
- sandboxed context
- Create direct relations to actors get the flag
  - Bypass the huge agency commission!

INSOMNI'HACK

Web | Jack the clicker

1 solve

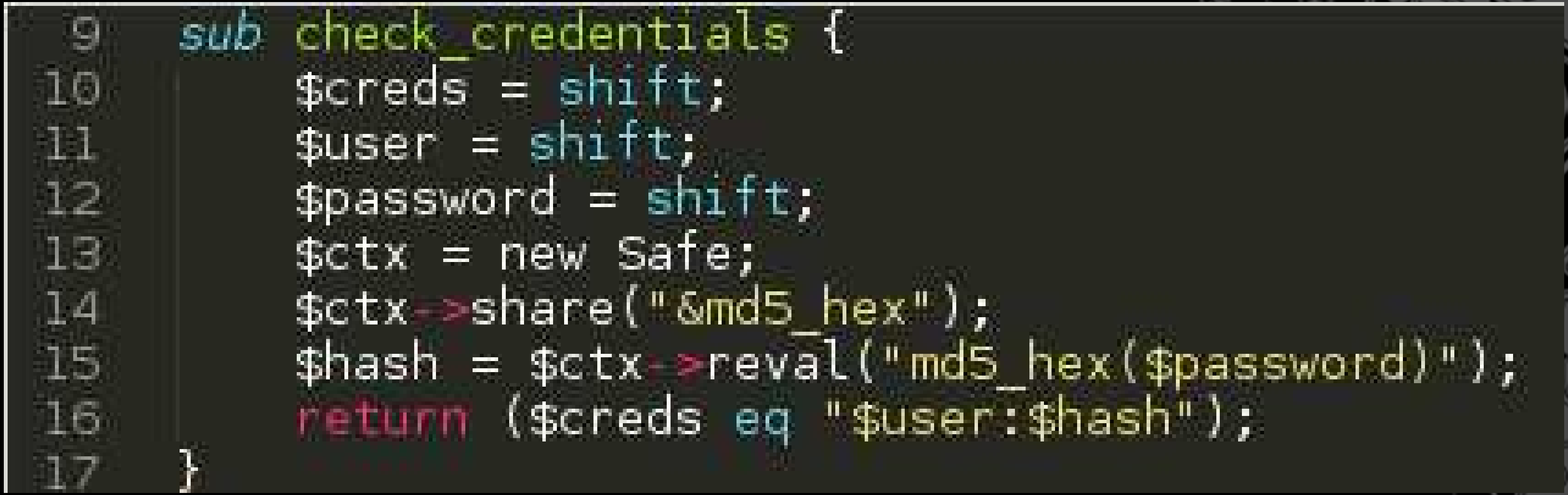
- Clickjacking!
- PhantomJS bot visits the link and clicks at random locations
- Include the application in an iframe, put the target button under the cursor with Javascript

INSOMNI'HACK

Web|Hack like it’s 1999!

0 solve

- PERL… Need to login to server
- LFI to get file source
- reval in `download.pl`
- No imports allowed



```perl
sub check_credentials {
        $creds = shift;
        $user = shift;
        $password = shift;
        $ctx = new Safe;
        $ctx->share("&md5_hex");
        $hash = $ctx->reval("md5_hex($password)");
        return ($creds eq "$user:$hash");
}
```

Web|Hack like it’s 1999!

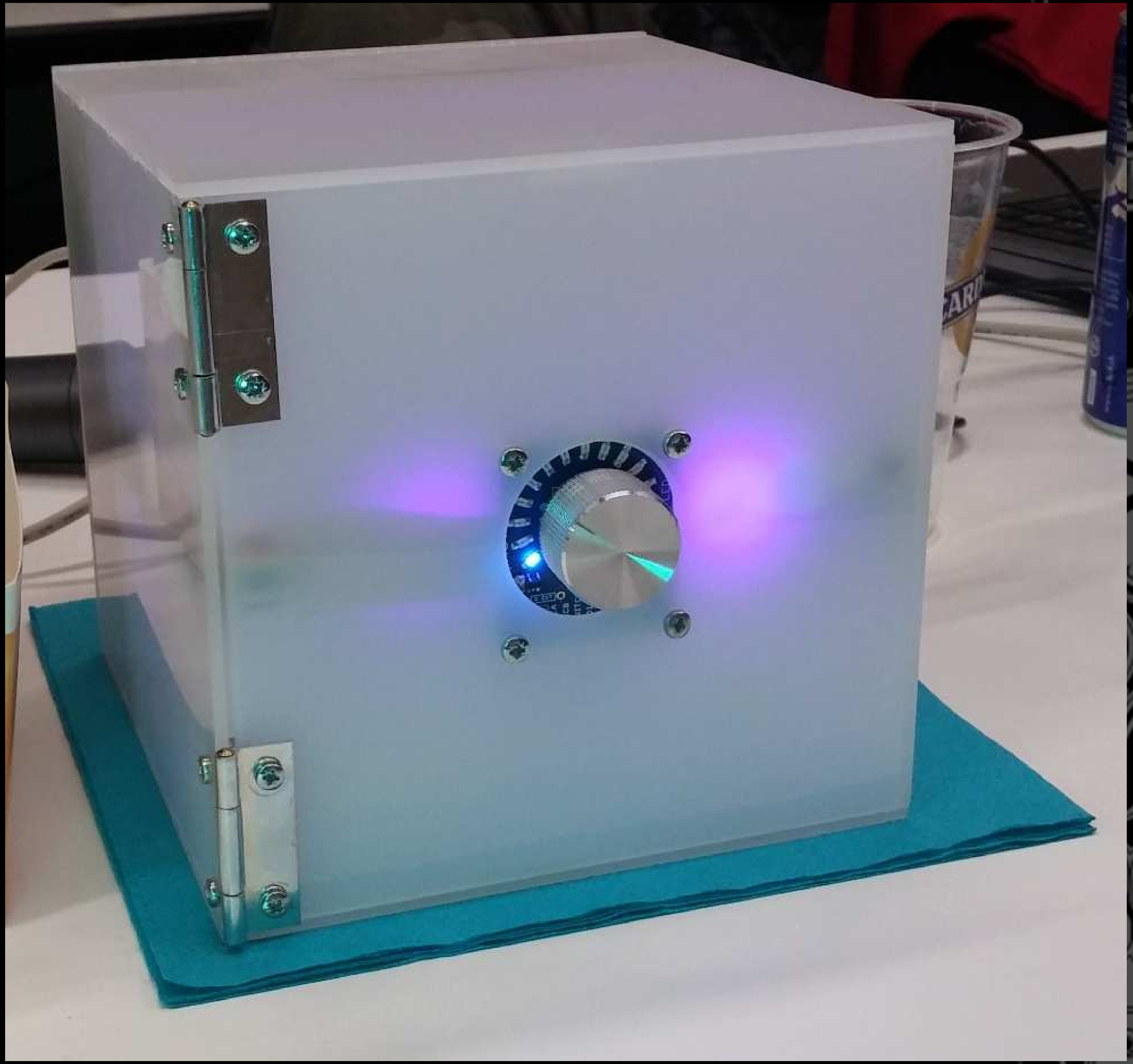
0 solve

- $_ contains hash and username
- Can close the parenthesis in order to run arbitrary perl code
- Leak the username and hash char by char using loop function to "sleep"
- use tricks of `reval("md5_hex($password), hex_value")` so it actually returns `hex_value`

Hardware | 1-2-3-4

3 solves

- What’s inside the box ?
- AVR (arduino) binary
- Reverse the logic
- Find the combination



INSOMNI'HACK

PARENTAL

ADVISORY

EXPLICIT CONTENT

Reversing | Swordfish

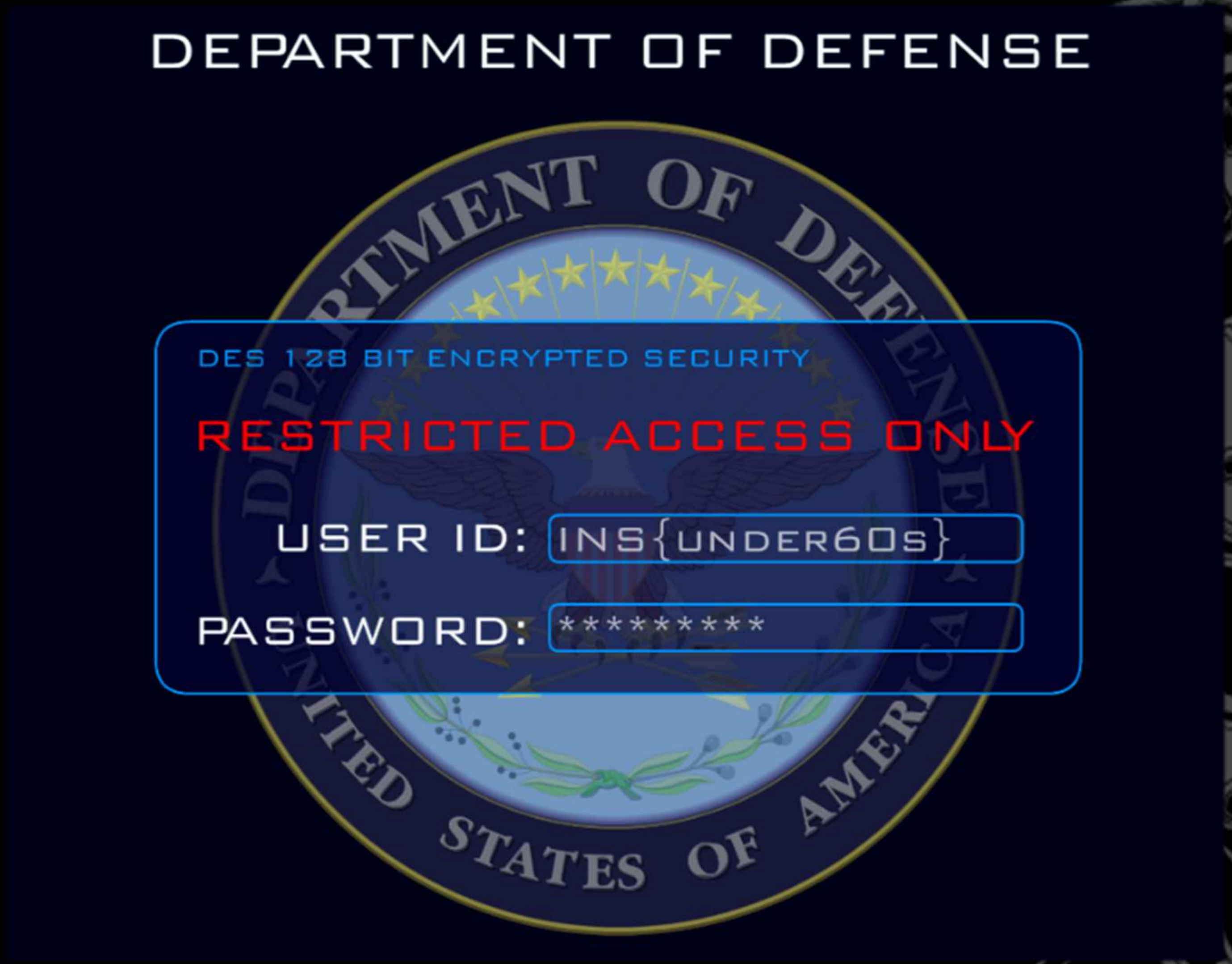
43 solves

https://www.youtube.com/watch?v=zfy5dFhw3ik

Reversing | Swordfish

43 solves

- Flash with hardcoded password
- Decompile with JPEXS (or other)



DEPARTMENT OF DEFENSE

DES 128 BIT ENCRYPTED SECURITY

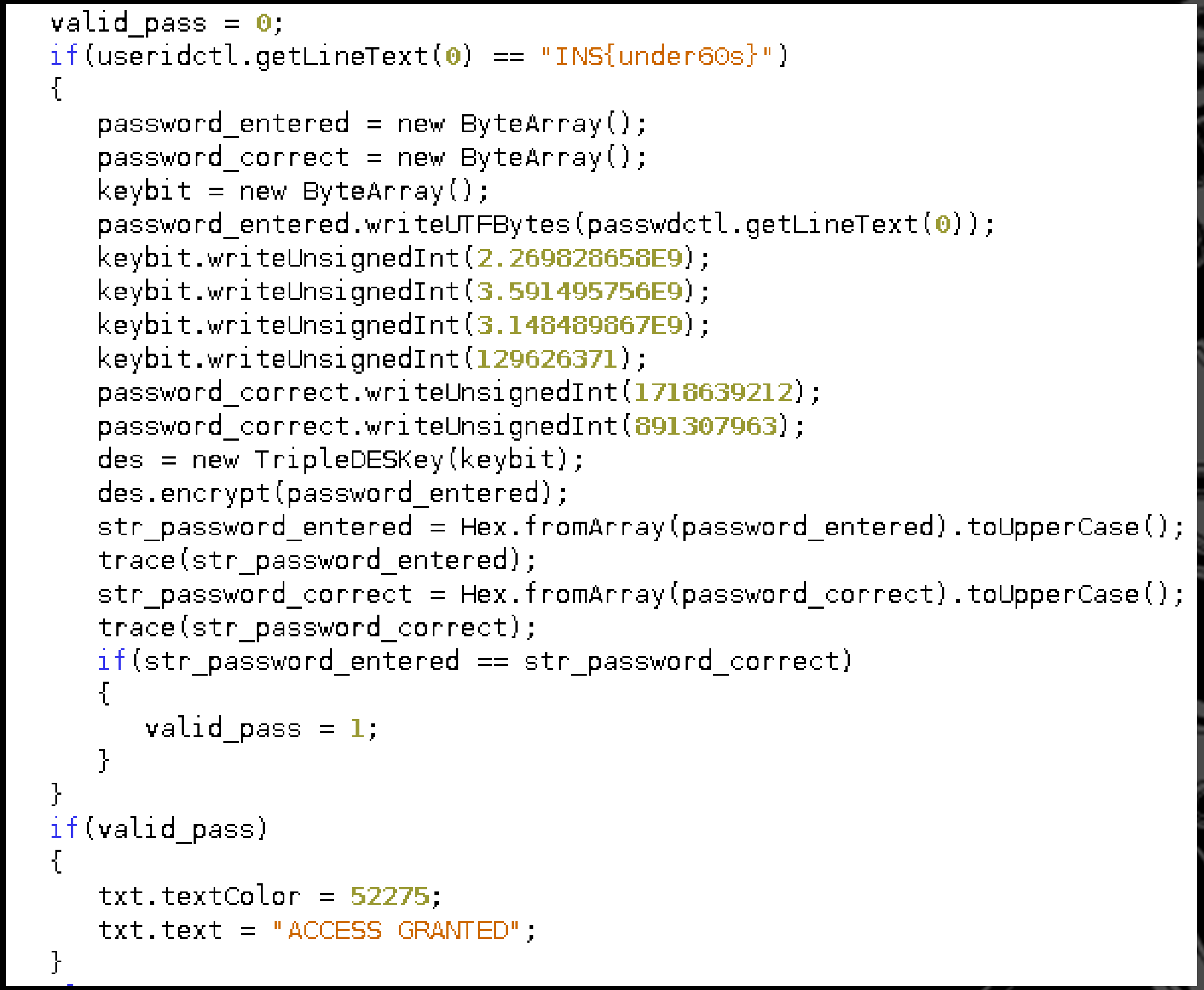
RESTRICTED ACCESS ONLY

USER ID: INS{UNDER60s}

PASSWORD: *********

Reversing | Swordfish password 12 solves

- Password stored in DES 128
- Hardcoded key
- Patch bytecode to invert the DES mode
- Patch bytecode to change the argument
- Launch Flash in debug mode
- Read the log

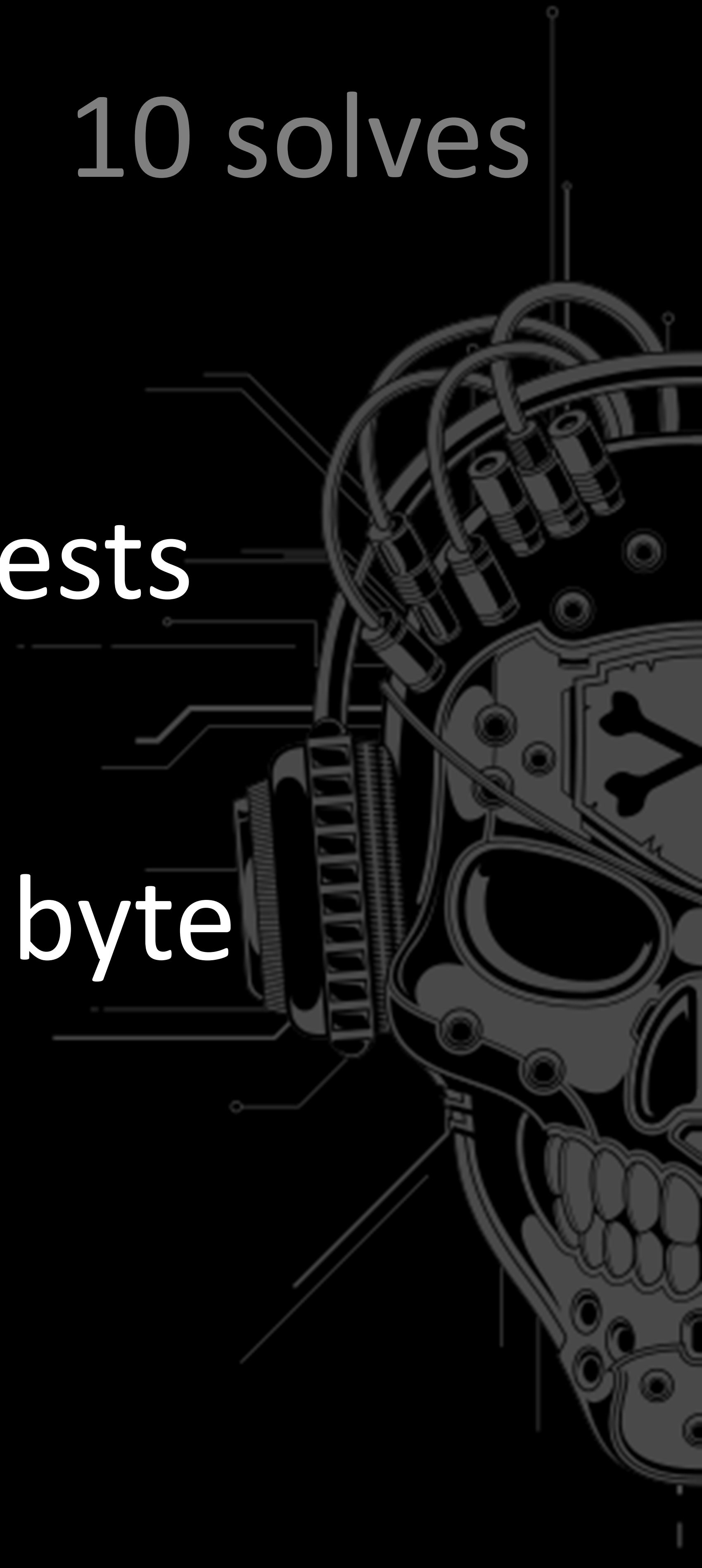


```
valid_pass = 0;
if(useridctl.getLineText(0) == "INS{under60s}")
{
   password_entered = new ByteArray();
   password_correct = new ByteArray();
   keybit = new ByteArray();
   password_entered.writeUTFBytes(passwdctl.getLineText(0));
   keybit.writeUnsignedInt(2.269828658E9);
   keybit.writeUnsignedInt(3.591495756E9);
   keybit.writeUnsignedInt(3.148489867E9);
   keybit.writeUnsignedInt(129626371);
   password_correct.writeUnsignedInt(1718639212);
   password_correct.writeUnsignedInt(891307963);
   des = new TripleDESKey(keybit);
   des.encrypt(password_entered);
   str_password_entered = Hex.fromArray(password_entered).toUpperCase();
   trace(str_password_entered);
   str_password_correct = Hex.fromArray(password_correct).toUpperCase();
   trace(str_password_correct);
   if(str_password_entered == str_password_correct)
   {
      valid_pass = 1;
   }
}
if(valid_pass)
{
   txt.textColor = 52275;
   txt.text = "ACCESS GRANTED";
}
```

Network | TimeToLeak

10 solves

- Pcap with ICMP traffic
- Host selectively replies to echo requests
- TTL "port knocking"
- Use raw sockets, guess the flag byte byte



Network|Hollywood network

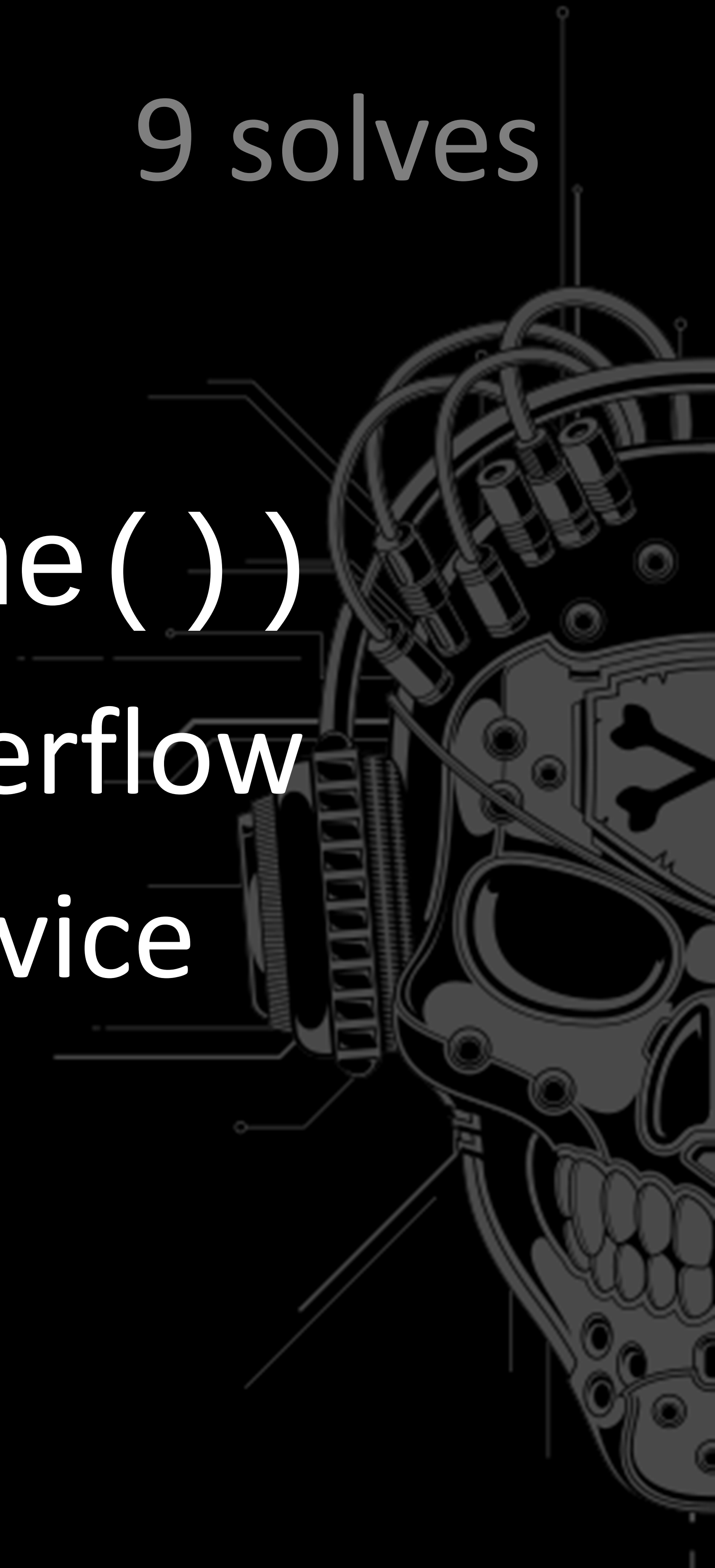
0 solve

- Connect to a fake z/OS IBM server
- FLAG command sends flag
- Running on IPv5, ex: `312.5.125.833`
- Sniff with Wireshark and notice ARPv5 packets
- Craft reply ARPv5 packet using raw sockets
- Server will send IPv5 packet with the flag in cleartext

Exploit | mastermind

9 solves

- Mastermind game
- Combination based on `srand(time())`
- Win in one attempt to be able to overflow
- Trick is to connect 2 times to the service
- Fail in one of the sessions to get the combination



Exploit | smtpwn

5 solves

- SSH challenge. Creates an unreadable temporary mail file with a random token, some constants, the flag, and your input
- `ulimit` tricks
  - limit number of open fds ⇨ file descriptor exhaustion ⇨ cannot open `/dev/urandom`
  - limit file size ⇨ use the checksum to guess the flag byte by byte

Exploit|Sql inject flow

2 solves

- Forking service using MySQL to store data
- Stack: [buffer][pointer]…
- sscanf off-by-one
- Stack: [AAAAAAAAAAAAAAAAAAAAA][\x00pointer]…
- Function pointer gets fixed
- Stack: [AAAAAAAAAAAAAAAAAAAAA][pointer]…
- Buffer is inserted in MySQL: leak!

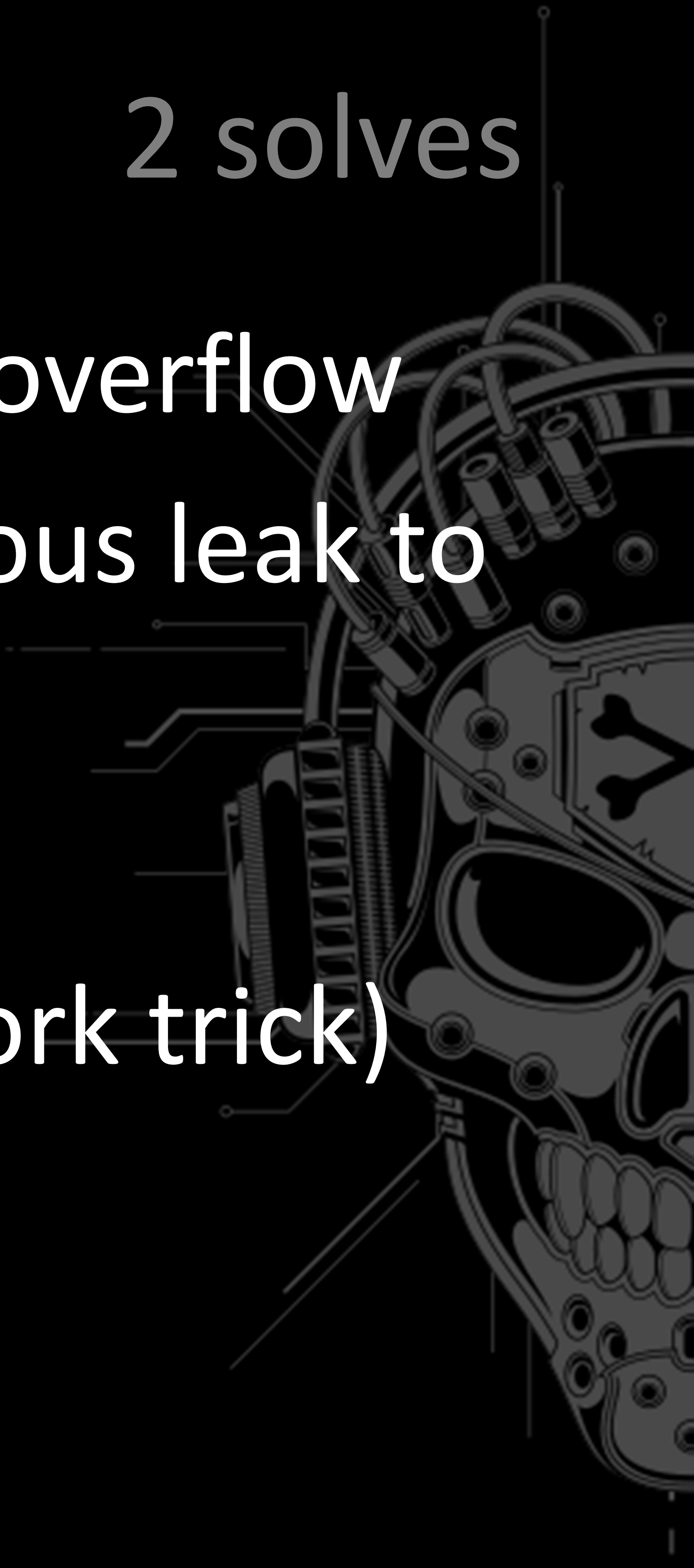
INSOMNI'HACK

Exploit | Sql inject flow

2 solves

- SQL Injection, output leads to a buffer overflow
- Build a ropchain in SQL using the previous leak to bypass PIE

- Alternative: brute ASLR byte by byte (fork trick)



Exploit | The Firm(ware)

0 solve

- Small MIPS firmware to reverse
- Obvious overflow in the HTTP `lang` parameter
- Jump directly to a nopsled + shellcode like old times (No ASLR, No NX)

Exploit | Jurassic Sparc

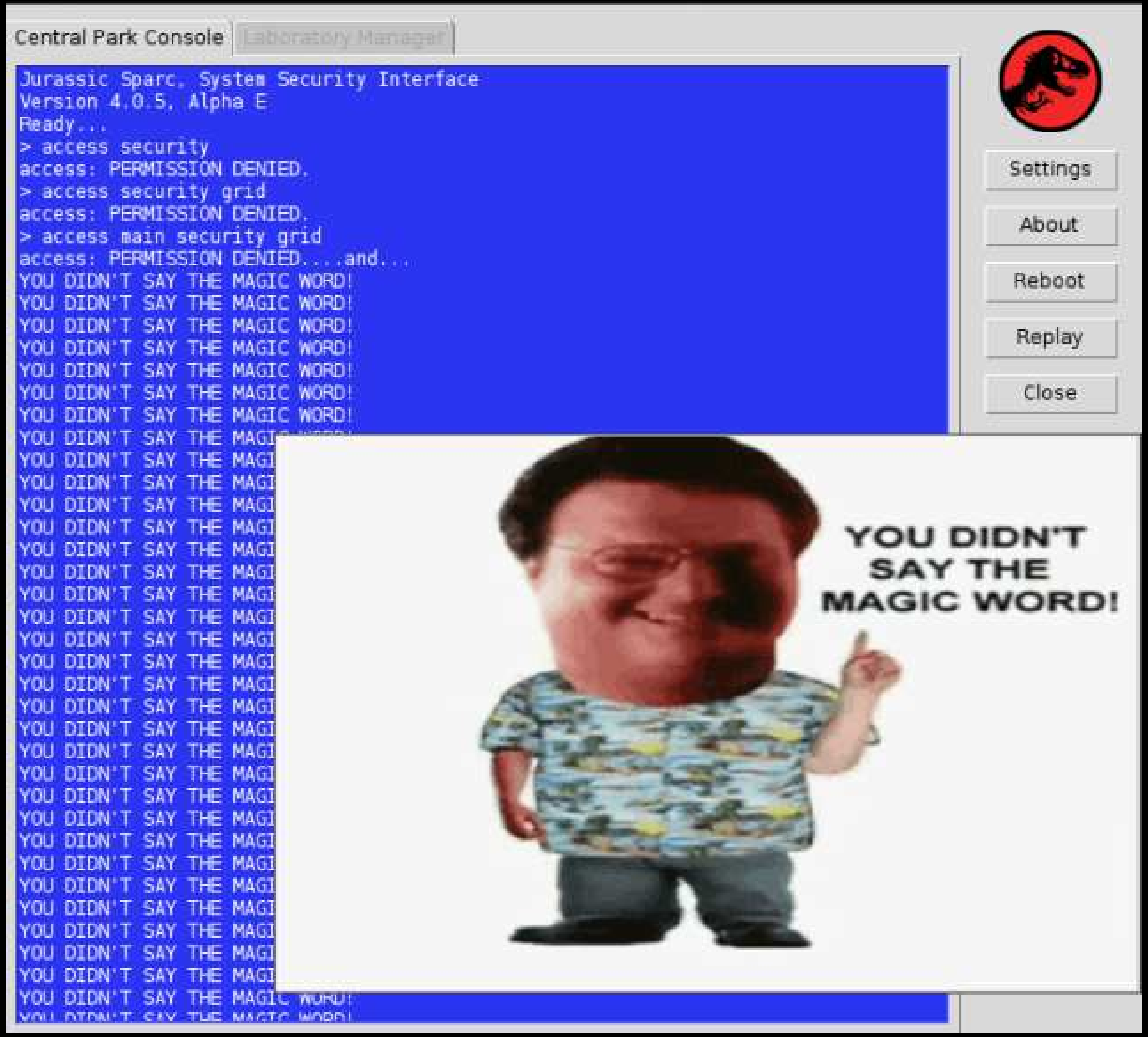
0 solve

- Sparc64 service, custom protocol
- Provided python client
- Credentials + magic word = flag

- 8 byte stack buffer overflow in the reboot feature
- Overwrite file descriptors ⇨ leak database during backup operation
- `strcmp` of a raw hash ⇨ easy collision

Exploit | Jurassic Sparc

0 solve



```
Jurassic Sparc, System Security Interface
Version 4.0.5, Alpha E
Ready...
> access security
access: PERMISSION DENIED.
> access security grid
access: PERMISSION DENIED.
> access main security grid
access: PERMISSION DENIED....and...
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGI
YOU DIDN'T SAY THE MAGI
YOU DIDN'T SAY THE MAGI
YOU DIDN'T SAY THE MAGI
YOU DIDN'T SAY THE MAGI
YOU DIDN'T SAY THE MAGI
YOU DIDN'T SAY THE MAGI
YOU DIDN'T SAY THE MAGI
YOU DIDN'T SAY THE MAGI
YOU DIDN'T SAY THE MAGI
YOU DIDN'T SAY THE MAGI
YOU DIDN'T SAY THE MAGI
YOU DIDN'T SAY THE MAGI
YOU DIDN'T SAY THE MAGI
YOU DIDN'T SAY THE MAGI
YOU DIDN'T SAY THE MAGI
YOU DIDN'T SAY THE MAGI
YOU DIDN'T SAY THE MAGI
YOU DIDN'T SAY THE MAGI
YOU DIDN'T SAY THE MAGI
YOU DIDN'T SAY THE MAGI
YOU DIDN'T SAY THE MAGI
YOU DIDN'T SAY THE MAGI
YOU DIDN'T SAY THE MAGI
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
```

Exploit|SH1TTY

0 solve

- TTY keylogger, kernel module
- Special feature to log only passwords
- Linux kernel stack buffer overflow

- More details tomorrow!

Shellcoding | blue pill

8 solves

- `read(0, buf, 4); jmp buf;`
- 4 bytes shellcode, chrooted
- Return Oriented Shellcoding
  - Stager, « enlarge your shellcode »

Shellcoding | tldr

6 solves

- Chroot and sandboxed environment (seccomp-bpf)
- Blocked syscalls include open and read
- RTFM!

-
  ```
  int openat(int dirfd, const char *pathname, int flags);
  """If pathname is relative and dirfd is the special
  value AT_FDCWD, then pathname is interpreted relative to
  the current working directory of the calling process."""
  ```
-
  ```
  ssize_t sendfile(int out_fd, int in_fd, off_t *offset,
  size_t count);
  ```

Forensic|ZoomIn

43 solves

- Use exif tools to extract a thumbnail
- Thumbnail in the thumbnail
- We need to zoom deeper

YO DAWG, I HEARD U LIKE THUMBNAILS
SO I PUT A THUMBNAIL IN YO THUMBNAIL, SO U CAN ZOOM WHILE U ZOOM
imgflip.com

INSOMNI'HACK

Forensic|Lost In Memories

26 solves

- Memory dump of an infected Windows machine communicating with a C&C.
- Use your favorite forensic tool to find the C&C address (requires creds) and get the flag:
    - volatility
    - … or strings|grep ☺

Forensic | Elysium ropchain analysis 1 solve

- Provided: PCAP + binary + libc
- Exploitation of the teaser « Elysium » task
- Mix exploit/forensics

- Exploit leaks `/proc/self/maps`
- First ropchain is a stager and pivots to stage 2

Forensic | Elysium ropchain analysis 1 solve

- Stage 2:
  - `memfrob()` to decrypt structure and filename (/flag)
  - Read flag and `cbc_crypt()` it in DES
  - `cbc_decrypt()` stage 3 ropchain

Forensic | Elysium ropchain analysis 1 solve

- Stage 3:
  - Sends the encrypted flag hidden in the TTL (byte by byte)

Conclusions | Hack the planet!

- 8 hours is short, one must pwn fast
- CTFs don't teach PowerPoint ☹
  - But are great to keep your other skills sharp!

- Challenge sources on https://github.com/Insomnihack/Insomnihack-2015

INSOMNI'HACK

Conclusions|Questions/Contact

- Questions ?

- Twitter:
  - @0xGrimmlin
  - @__awe