Cosa c'è che non va?

Viaggio verso il Nirvana del SSDLC

CODICE INSICURO

$ whoami

- 15 anni nell'industria #itsec
- Tech blogger @codiceinsicuro
- ❤️ sviluppare security source code scanners (Owasp Orizon, dawnscanner)
- ❤️ tenere talk su temi di #appsec
- Seguimi su @thesp0nge

HACK IN BO
Winter 2016 Edition

Agenda

- Mentre mi vedrete agitare il WiiMote:
  - Rideremo sui miti che non permettono alle persone del mondo IT di parlare tra di loro
  - Percorreremo un viaggio verso il SSDLC
  - Dovrete risolvere qualche quiz
- Alla fine, tornerete a casa e da Lunedì trasformerete il modo di lavorare vostro e dei vostri colleghi

Lui è peggio di me...

Security è composta da persone strane

https://flic.kr/p/bFZpyg

HACK IN BO
Winter 2016 Edition

I miei DevOps sono pigri

https://flic.kr/p/ciAMaS

HACK IN BO
Winter 2016 Edition

Gli sviluppatori scrivono software a caso

https://flic.kr/p/djnyxR

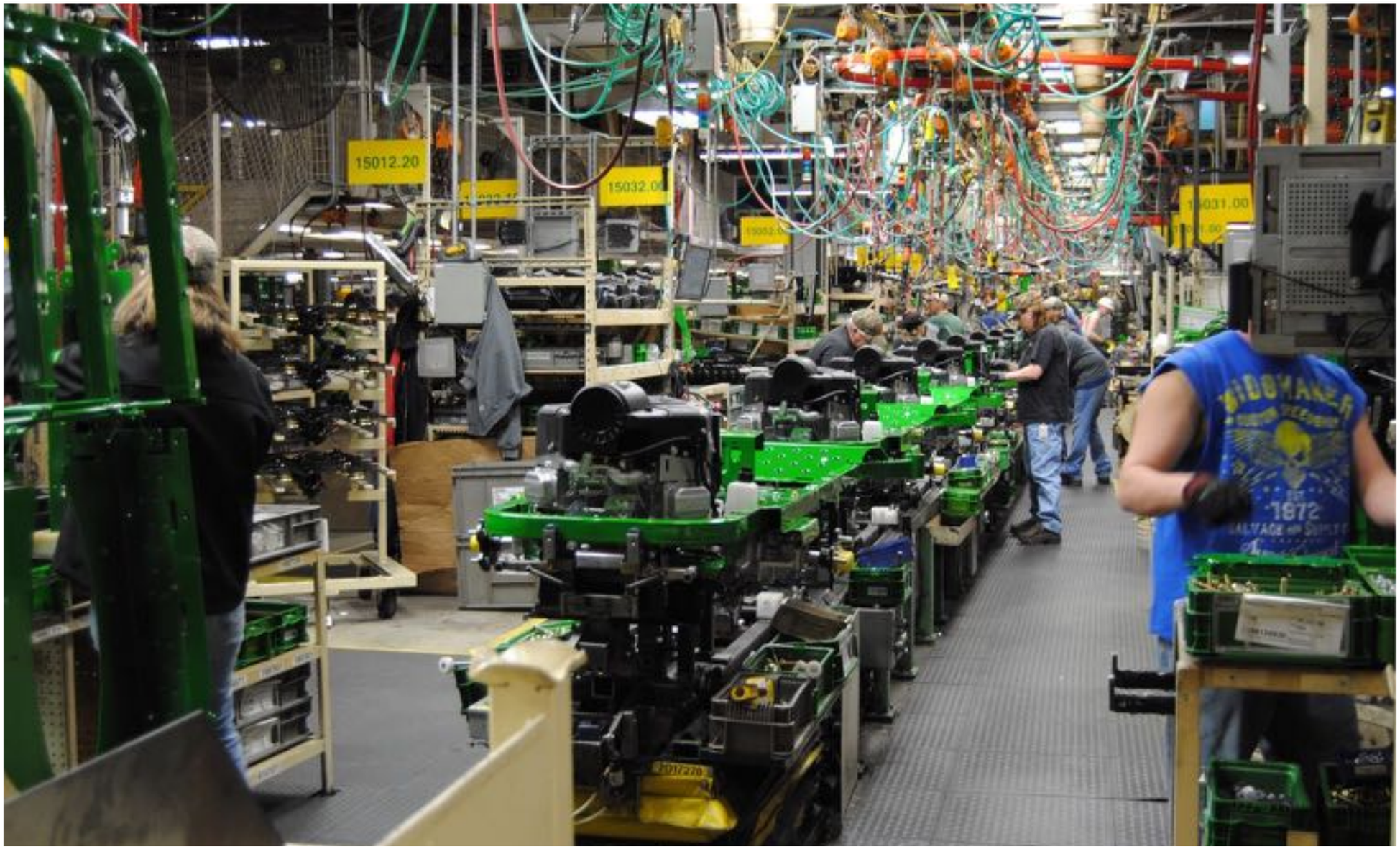
HACK IN BO
Winter 2016 Edition

Prima di partire

HACK IN BO
Winter 2016 Edition

Condividere la conoscenza

https://flic.kr/p/fKcKs2



Create e consolidate processi

https://flic.kr/p/fzBciZ

HACK IN BO
Winter 2016 Edition

Dare qualche regola base

https://flic.kr/p/mLxFGK

the_buff.c (~/Documents/1_Personal/4_Talks/2016/HackInBo) - VIM

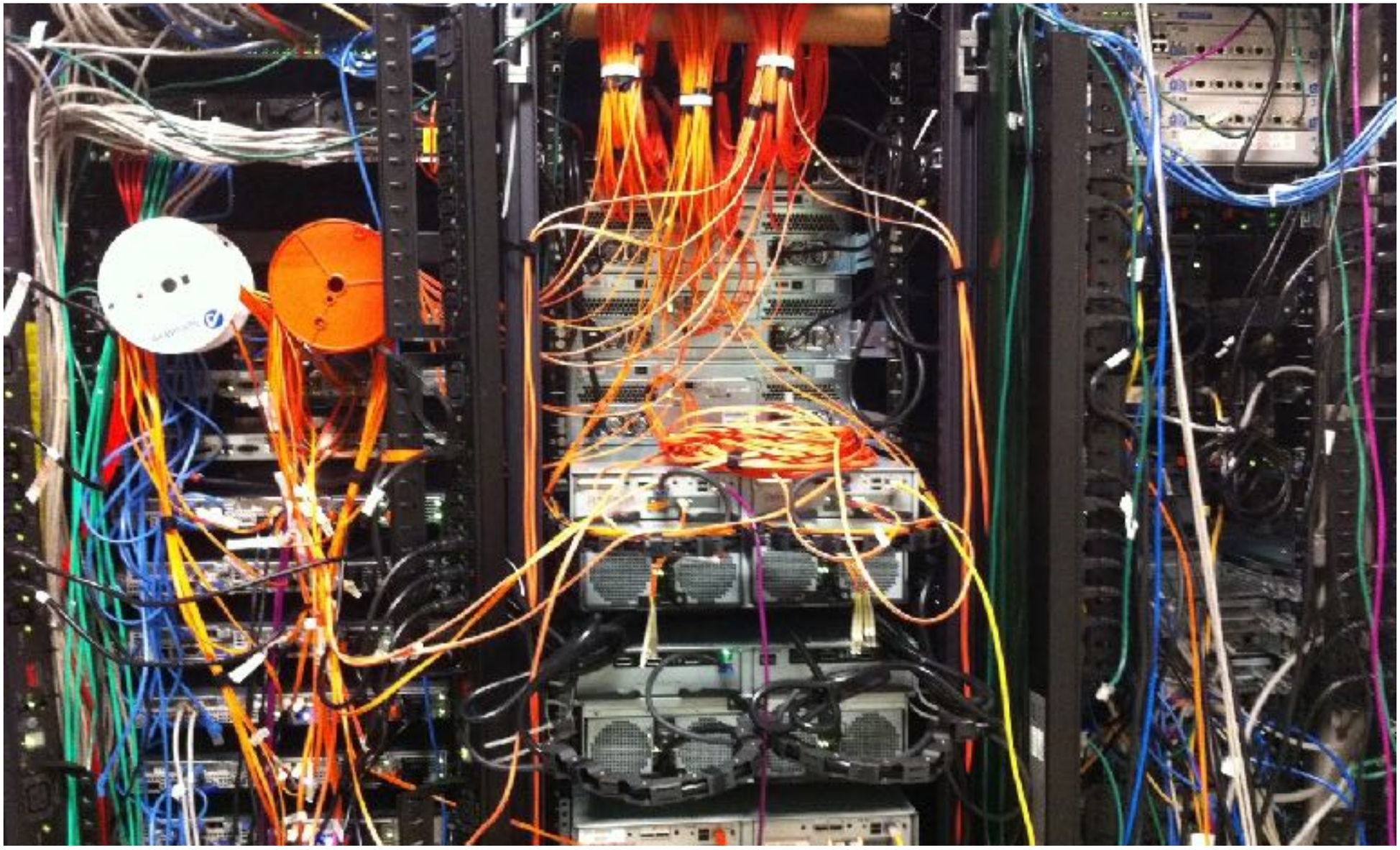
```c
#include <stdio.h>
#include <stdlib.h>
#include <strings.h>

/*
 * Familiy: CODE REVIEW
 * Level  : MEDIUM
 *
 * This great tool reads a command stored in an environment variable and
 * execute it using system() function.
 * Allowed commands are 'ls' and 'll' and a whitelist approach is in place.
 */
int main(int argc, char **argv) {
  char *envy;


  envy = malloc(20 * sizeof(char));
  bzero(envy, 20 * sizeof(char));

  envy = getenv("HACKINBO");
  if (envy == NULL) {
    fprintf(stderr, "Please set HACKINBO env variable for more fun\n");
    return -1;
  }

  printf("HACKINBO variable found with value %s\n", envy);
  /*
   * export HACKINBO="ls"
   */
  if ((strstr(envy, "ls") != NULL) || (strstr(envy, "ll") != NULL)) {
    printf("Executing HACKINBO fun");
    system(envy);
  } else {
    fprintf(stderr, "Well, you want too much fun now");
    return -2;
  }

  return 0;
}
~
~
```

NORMAL >> the_buff.c c << 33% : 13: 1 <

HACK IN BO
Winter 2016 Edition

Crea il tuo SSDLC

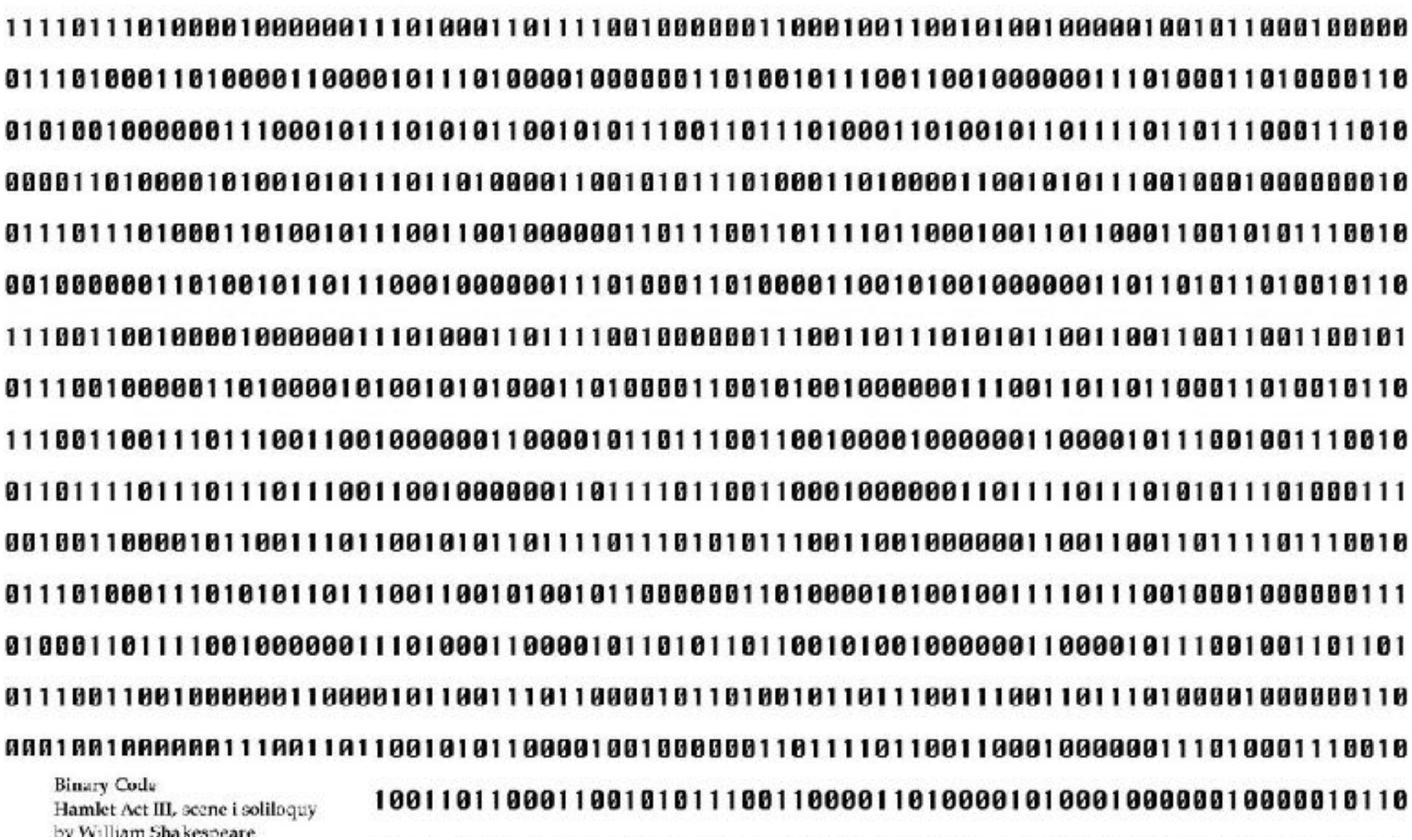
HACK IN BO
Winter 2016 Edition



Vulnerability Management

https://flic.kr/p/9v7Kgx

HACK IN BO
Winter 2016 Edition



Binary Code
Hamlet Act III, scene i soliloquy
by William Shakespeare

Code review

https://flic.kr/p/7Hs5hc

HACK IN BO
Winter 2016 Edition

Penetration test

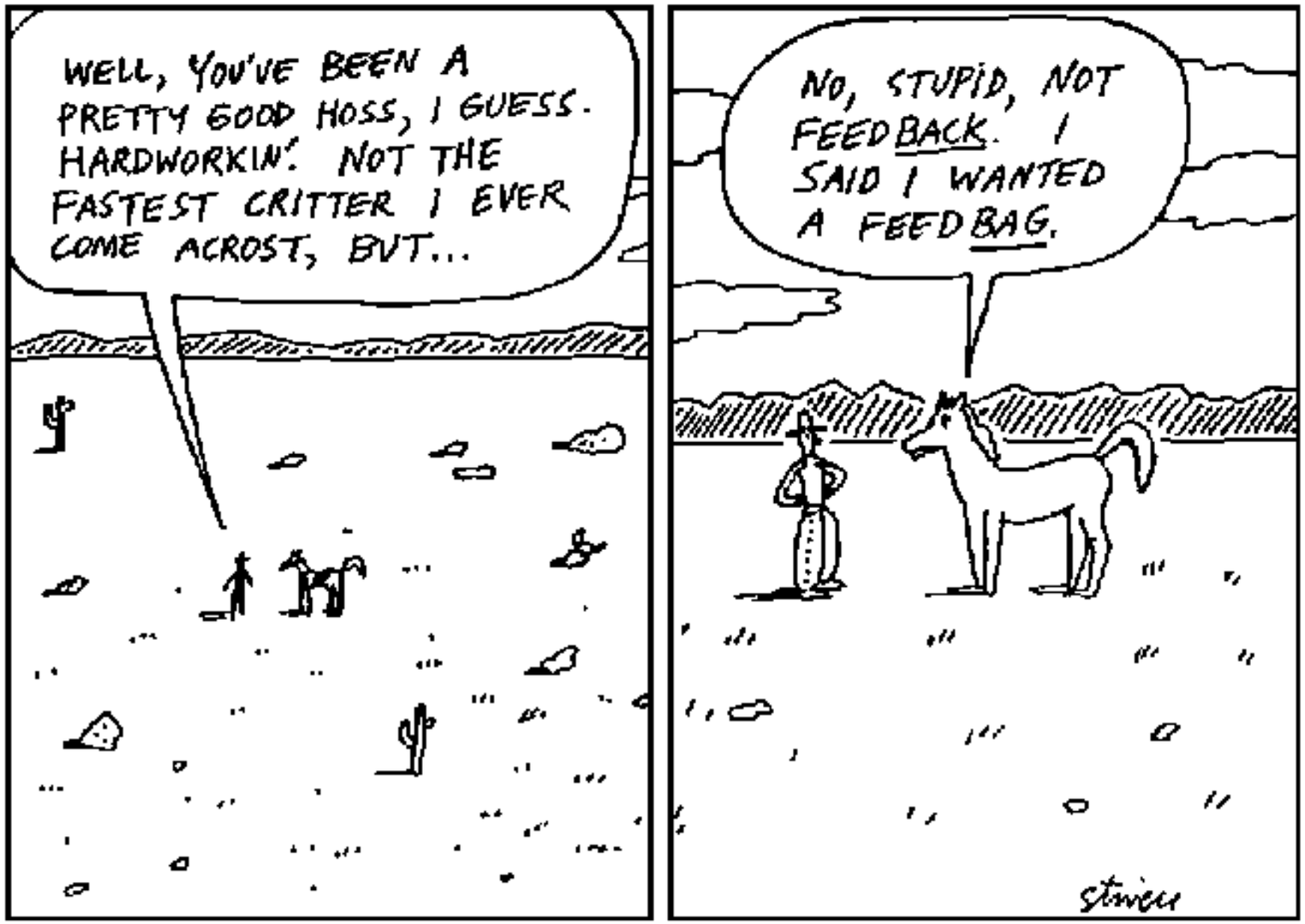
https://flic.kr/p/6Ry49m

CrackInBo.java (~/Documents/1_Personal/4_Talks/2016/HackInBo) - VIM1

```java
/**
 * Familiy: CODE REVIEW
 * Level  : MEDIUM
 *
 * This java class exposes 2 vulnerabilities. Spot them.
 */
class CrackInBo {
  public int a;
  private String b;

  public CrackInBo() {
    b = null;
    a = 42;
  }

  public boolean crack(){

    int c=(int)(40+Math.random() * 11);

    if ((c - a) <= 0) {
      System.out.println("lazyness is caused by " + b.toLowerCase());
      if (b == null) {
        System.err.println("AIEEE, nobody give a value to b");
        return false;
      }
      return false;
    }
    System.out.println("Lazyness is safe. Have fun");
    return true;
  }

  public static final void main(String[] args) {

    CrackInBo c = new CrackInBo();

    System.out.println("The fun is friend with lazyness");
    c.crack();
  }
}
```

```
NORMAL >> CrackInBo.java                    java < utf-8[unix] <   2% :
```

HACK IN BO
Winter 2016 Edition



Preoccupati di avere dei feedback

https://flic.kr/p/3UaCt1

Riassumendo

- Abbiamo creato awareness
- Abbiamo creato policy e processi
- Abbiamo istituito momenti di test formali
- Gestiamo i feedback a fronte delle nostre vulnerabilità

Chi pensa che siamo arrivati al SSDLC?

https://flic.kr/p/91eDQQ

L'SSDLC è il viaggio stesso

https://flic.kr/p/oxmVct

HACK IN BO
Winter 2016 Edition

Consigli bonus

Siate creativi

https://flic.kr/p/8Fmmcs

Non abbiate pregiudizi

https://flic.kr/p/5AzKUs

HACK IN BO
Winter 2016 Edition

Siate competitivi

https://flic.kr/p/cNAZUL

HACK IN BO
Winter 2016 Edition

Domande?

Grazie!