

# HANDS-ON E-LEARNING COURSE ON CYBER DEFENCE FOR SYSTEM ADMINISTRATORS

PRAKTIILISE KÜBERKAITSE E-KURSUS  
SÜSTEEMIADMINISTRAATORITELE

Master's thesis  
Author: Margus Ernits  
Supervisor: Rain Ottis, Ph.D  
Tallinn, 16. May 2013

# PRESENTATION OUTLINE

- Introduction and current situation
- The Problem
- The Objectives
- Methodology and the ADDIE Model
- Analysis
- Solution
- Developed Hands-On Practical Classes
- Evaluation of the E-learning Course
- Future Research
- Conclusions

# INTRODUCTION

- Estonian IT College (EITC) focuses on applied higher education with curricula
  - IT System Administration
  - IT Development
  - IT System Analysis
- Curricula development being held with help of universities, private companies, graduates and students

# THE MAIN PROBLEM

- The main problem is deficiency of the skilled and security aware system administrators
  - EITC courses do not cover needs of industry on practical security field
  - Many system administrators are self studied and do not have required qualification
  - Amount of practical word is not sufficient to gain security skills for configuring IT infrastructure services

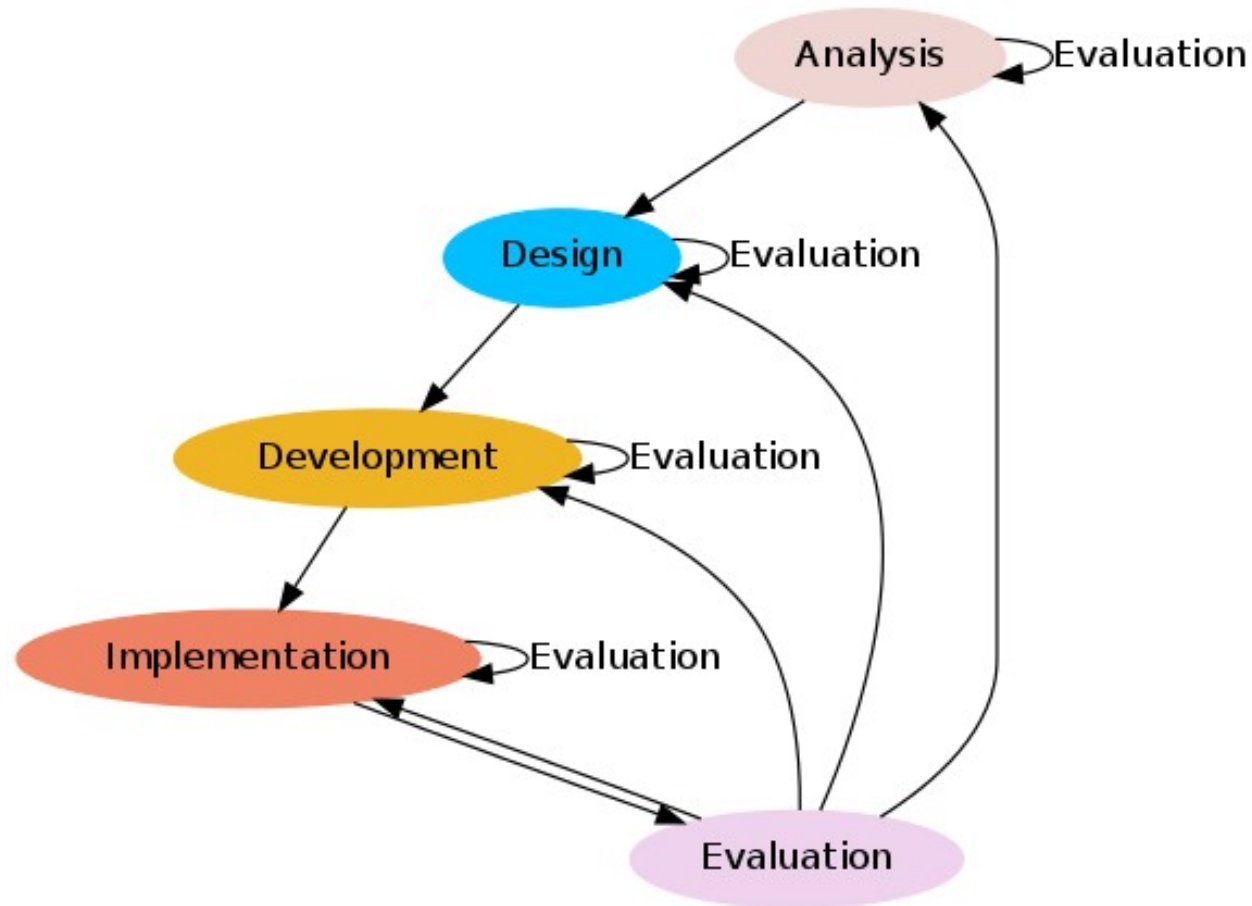
# MAIN OBJECTIVES

- Developing new hands-on e-learning course
  - Dedicated to defense of the IT systems
  - Securing services is part of configuring them
  - Lab intensive, command dojo (follow the master)
  - Playful, motivating (badges, competition)
  - Suitable for students and for continuous education
- Not for teaching offense or cyber security specialist

# METHODOLOGY

- Investigate the problem and similar research (Kasak, HyneSim, defensive and offensive courses/trainings/exercises)
- Instructional Design Models
  - Behaviorist, suitable for trainings
  - Cognitivist, suitable for exploring, group-works
  - Prescriptive Models
    - ADDIE model (more than 100 variants)

# CHOSEN METHOD – THE ADDIE MODEL



# ANALYSIS

- Goals for course
- Learning outcomes
- Learner analysis
- Course module list
- How to make course playful?
- What environment is needed?



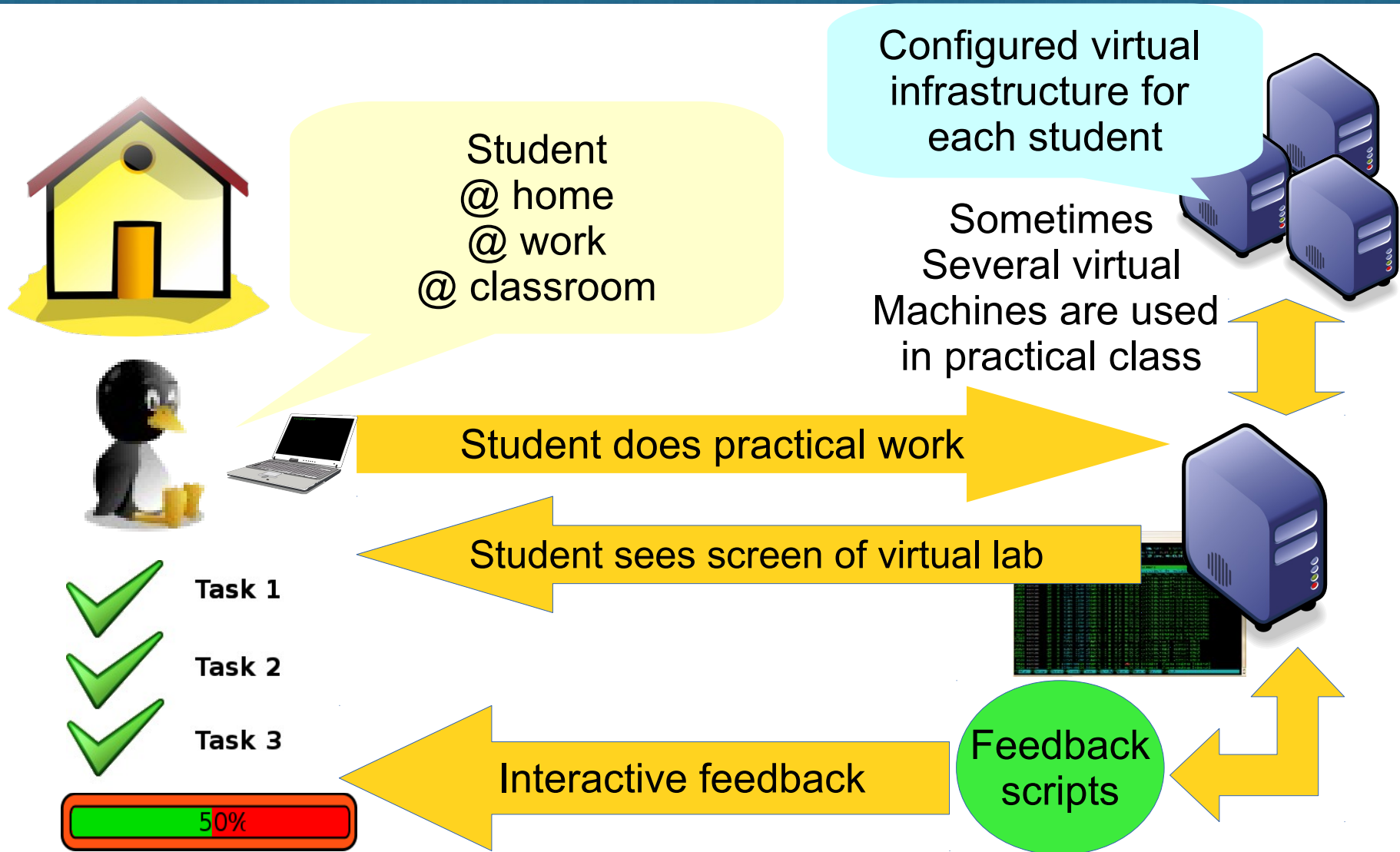
# SOLUTION

- To develop courses
  - Learning outcomes
  - Hands-on laboratory materials and learning material
  - Virtual Machine (templates) and interactive scripts for feedback
- To develop virtual environment
  - Existing environment do not cover all expectations
  - Development can take place in summer (Live system in use during semester)

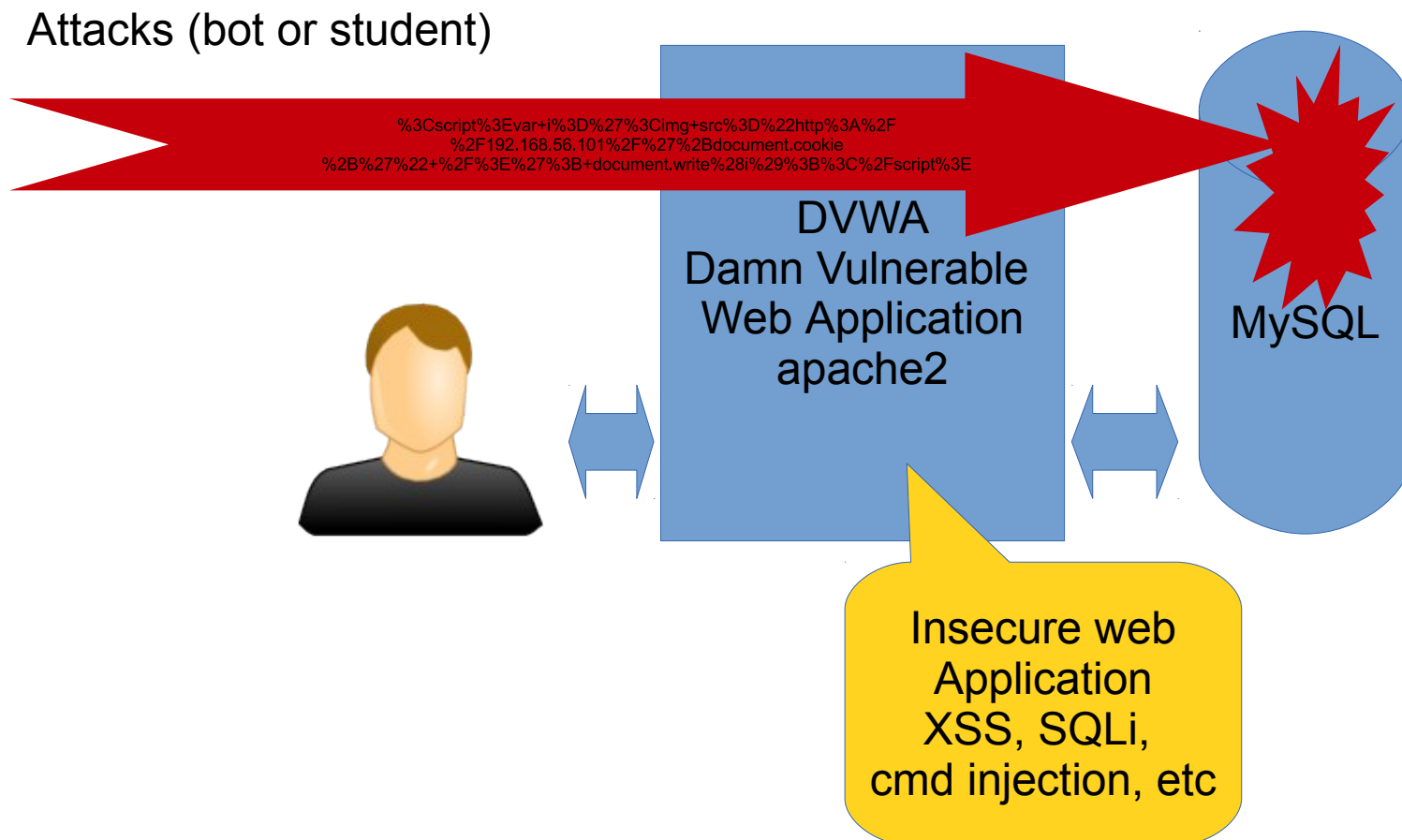
# DEVELOPED HANDS-ON PRACTICAL CLASSES

- Pre requirement course (GNU/Linux, Bash, Python and PowerShell scripting)
- Hands-on labs and materials
  - NTP/DNS/DHCP
  - Securing web application
    - Caching – varnish
    - Application firewalls
      - Hardening web server installation
      - SQL firewall (GreenSQL)
      - Mod Security firewall
      - Offload HTTPS using nginx
    - Coming shortly (Kerberos/LDAP Samba4, logging, firewalling)

# THE DISTANCE LABORATORY USED FOR HANDS-ON PRACTICAL CLASSES

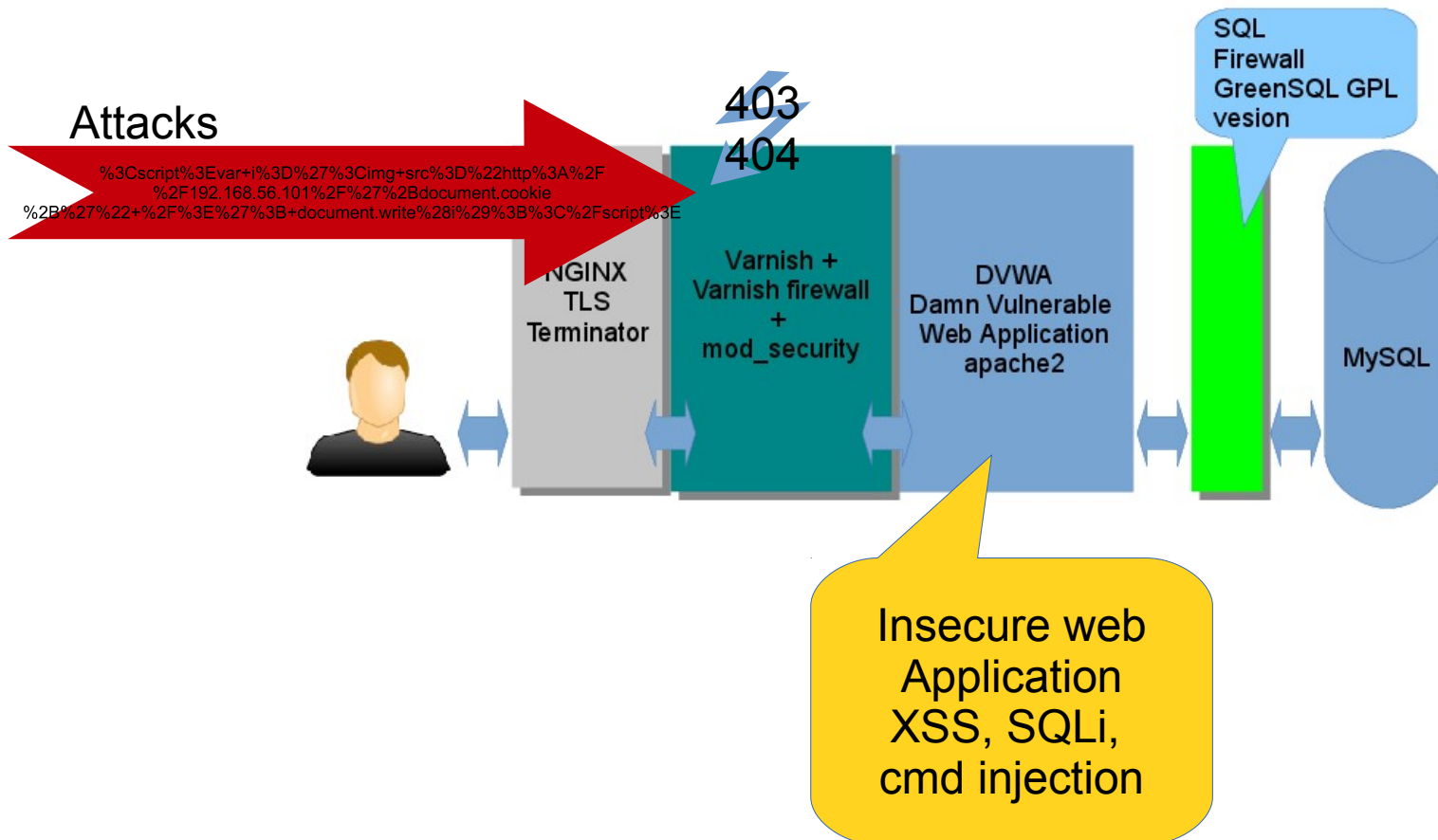


# SAMPLE LAB - SECURING INSECURE WEB APPLICATION THE BEGINNING



# SAMPLE LAB – END

## SECURING INSECURE WEB APPLICATION



# • EVALUATION OF THE E-LEARNING COURSE

- Feedback from students (feedback from Study Information System)
  - Grade for course (4.858 – distance learners, 4.6 – students, max is 5)
  - Grade for lecturer (4.88 – distance learners, 4.8 – students)
- Feedback from continuous education students
  - Grade for course (2.9 max is 3)
  - Grade for lecturer (2.9 max is 3)
- Feedback from lecturers
  - Too intensive to so limited time
  - Too much work (preparing for lab needs work before every course)

# FUTURE RESEARCH

- Evaluate new course and get more feedback
- Design interactive module (expert system) to give real-time feedback to the student (suggest what went wrong etc)
- Develop distance laboratory system to support new methodology (rewarding, badges, instant feedback and different network setups)
- Redesign some learning materials to follow new text material standards (For DNS/DHCP/NTP)
- Integrate and test new learning materials and lab scenarios (logging, fire-walling, central management)

# CONCLUSIONS

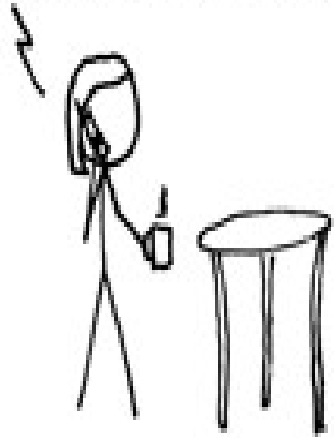
- The quality of studies will improve (improved) due to increased amount of practical hands-on classes
- System administrators are more security aware due to continuous education
  - More than 70 attendees on courses during 2012-2013
- The new E-learning course Protecting IT Infrastructure is developed and piloted



# THANK YOU

EXPLOITS OF A MOM...CAN BE STOPPED

HI, THIS IS  
YOUR SON'S SCHOOL.  
WE'RE HAVING SOME  
COMPUTER TROUBLE.



OH, DEAR - DID HE  
BREAK SOMETHING?  
IN A WAY -

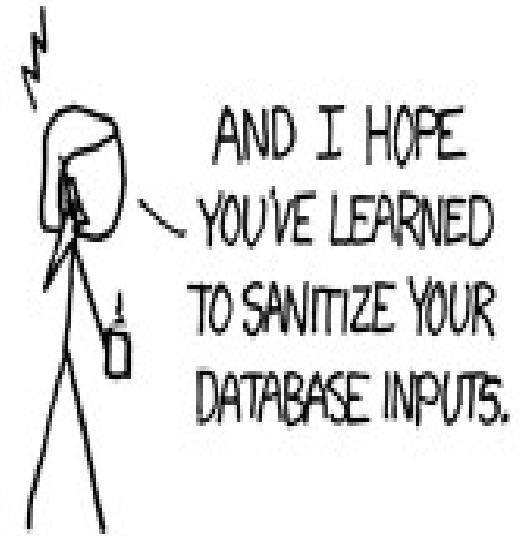


DID YOU REALLY  
NAME YOUR SON  
Robert'); DROP  
TABLE Students; -- ?



OH, YES. LITTLE  
BOBBY TABLES,  
WE CALL HIM.

WELL, WE'VE LOST THIS  
YEAR'S STUDENT RECORDS.  
I HOPE YOU'RE HAPPY.



AND I HOPE  
YOU'VE LEARNED  
TO SANITIZE YOUR  
DATABASE INPUTS.

Source: Exploits of a Mom <http://xkcd.com/327/>