



The OWASP Foundation

<http://www.owasp.org>

Hack your way to a degree

A new direction in teaching
application security at universities

Dr Konstantinos Papapanagiotou

konstantinos@owasp.org

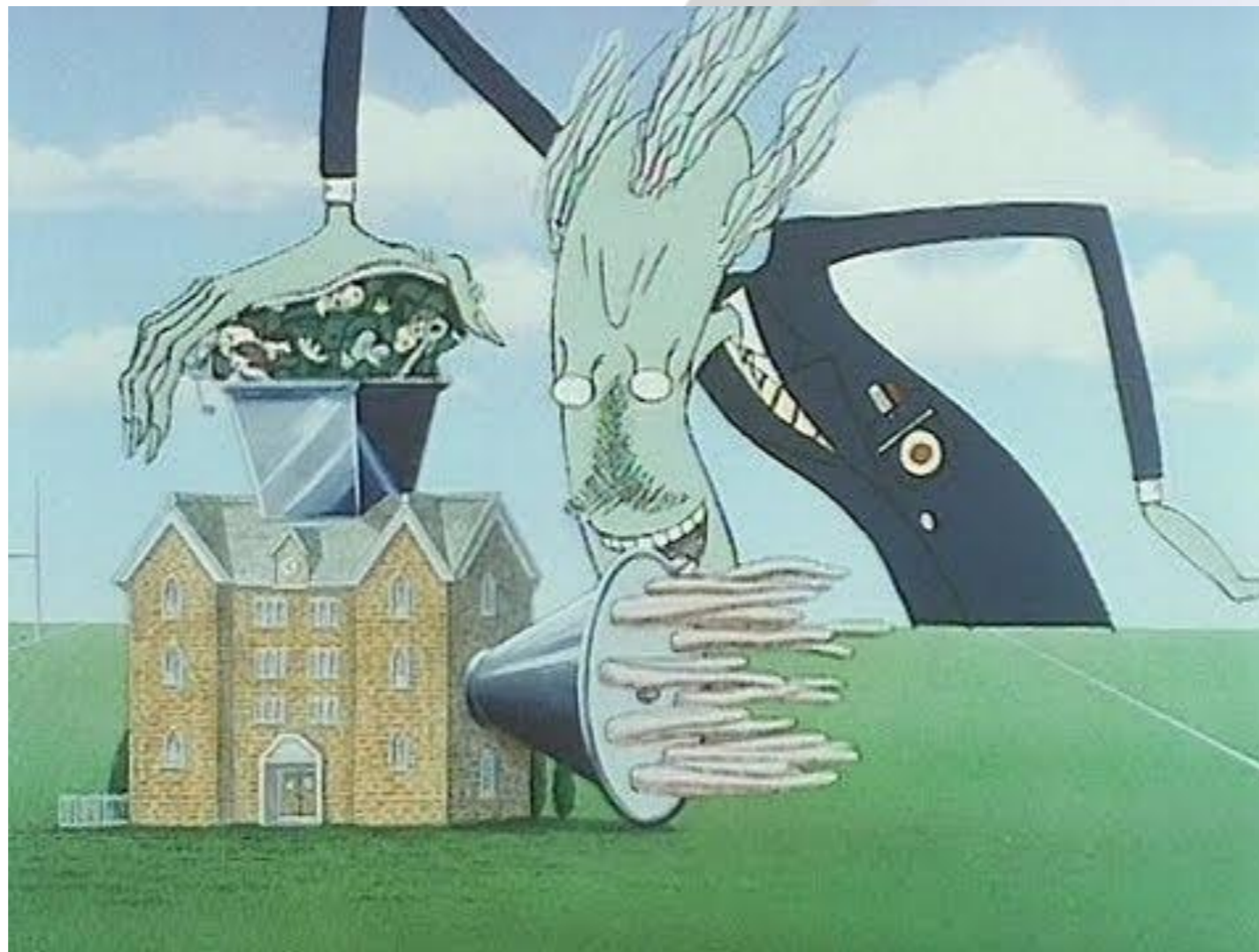
@kpapapan

.about

- 10+ years of experience in InfoSec as a consultant and researcher
- Currently: InfoSec Services Manager at Syntax IT Inc (www.syntax.gr)
- Involved with OWASP since 2005 as the Greek Chapter Leader
 - Started the Hackademic Challenges Project in 2011.
 - Organized the OWASP AppSec Research (EU) 2012 conference.
- Research
 - PhD in Trust in MANETs – Univ. of Athens, GR
 - 10+ publications and 50+ citations
 - Teaching InfoSec and AppSec at Greek universities

.disclaimer

No students were harmed in the making of this project





hackademic v0.1

Meet Dr Vassilis Vlachos and Dr Alex Papanikolaou:



Challenges - Motivation

- Teach security at 300+ students each semester.
- Students have varying background, skills and knowledge.
- University courses are too theoretical.
- Every student (and every teacher) wants to have a “pen-test lab”

labs are cool but...

- Hard to build/maintain (especially if students practice hacking on them!)
- Most existing vulnerable apps (e.g. WebGoat) are nice for demos or self-teaching but not designed for use in a class-lab environment.
- Need to promote discussion and interaction
- Need to introduce the “attacker’s perspective”

hackademic v0.2

Meet Andreas and Anastasis



hence...

hackademic

Hackademic - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

http://hackademic.s3cure.gr/

Latest Headlines Ultimate Hacker Direct... Your Ultimate Hacker ... -- 2HWD --

Disable Cookies CSS Forms Images Information Miscellaneous Outline Resize Tools View Source Options

Επιθέσεις Hackademic

hackademic

Main Menu

- Home
- About
- Login/Logout
- Results
- Top 10
- Download

Web Attacks

- Web 1
- Web 2
- Web 3
- Web 4
- Web 5
- Web 6
- Web 7
- Web 8
- Web 9
- Web 10

Hackademic

Attacking Challenges

Sunday, 12 December 2010 13:55

Welcome to the Hackademic Challenges!

The Hackademic Challenges is an open source project that helps you test your knowledge on web application security. You can use it to actually attack web applications in a realistic but also controllable and safe environment. On the left menu you can see all attack scenarios that are currently available. You can start by picking one!

This version of the Hackademic Challenges has been created for demo and (ab)use during the [OWASP Summit 2011](#)



**OWASP
SUMMIT
2011
LISBON**

User Login

Username

Password

Remember Me ☐

Login

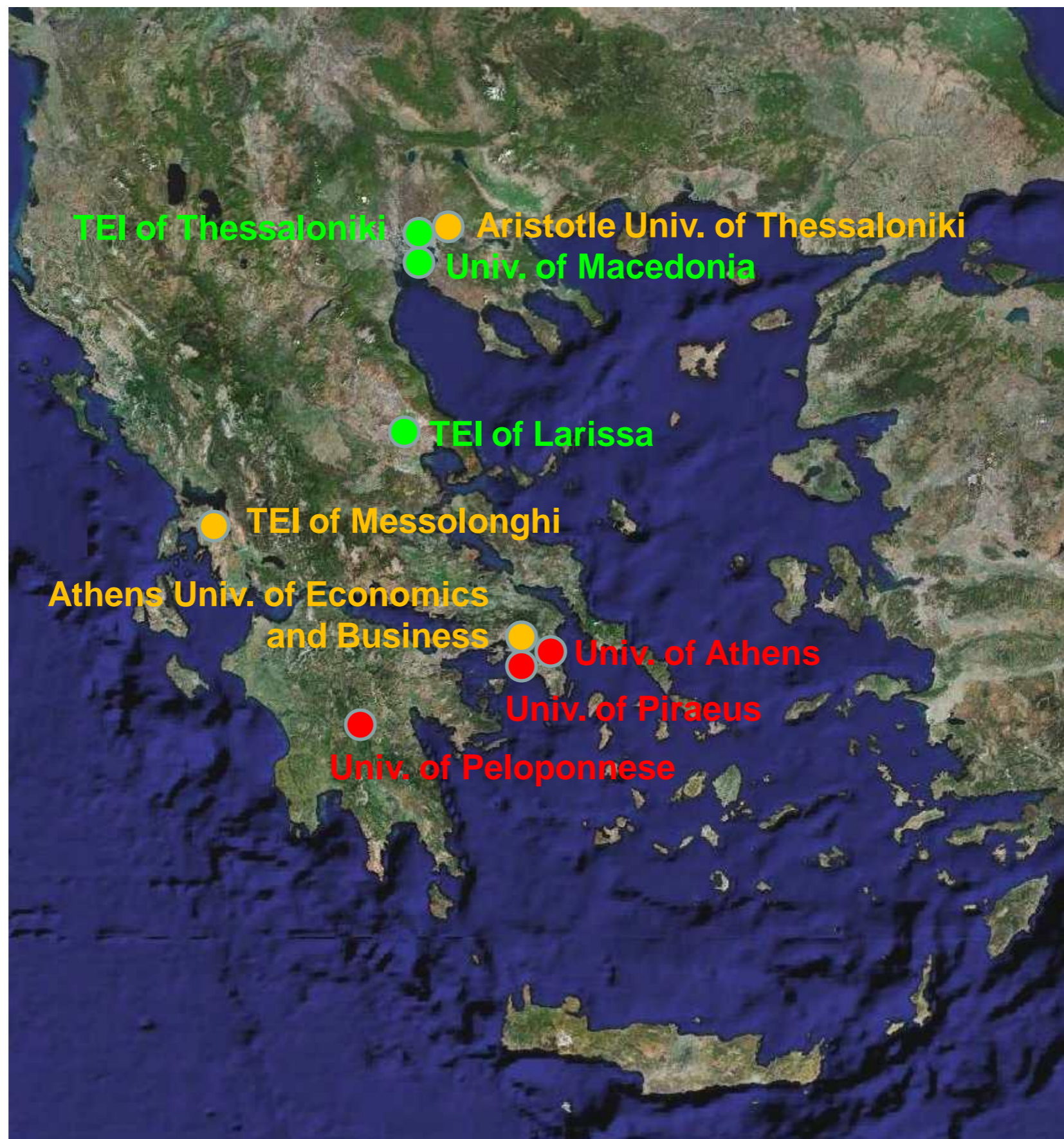
[Forgot your password?](#)
[Forgot your username?](#)
[Create an account](#)

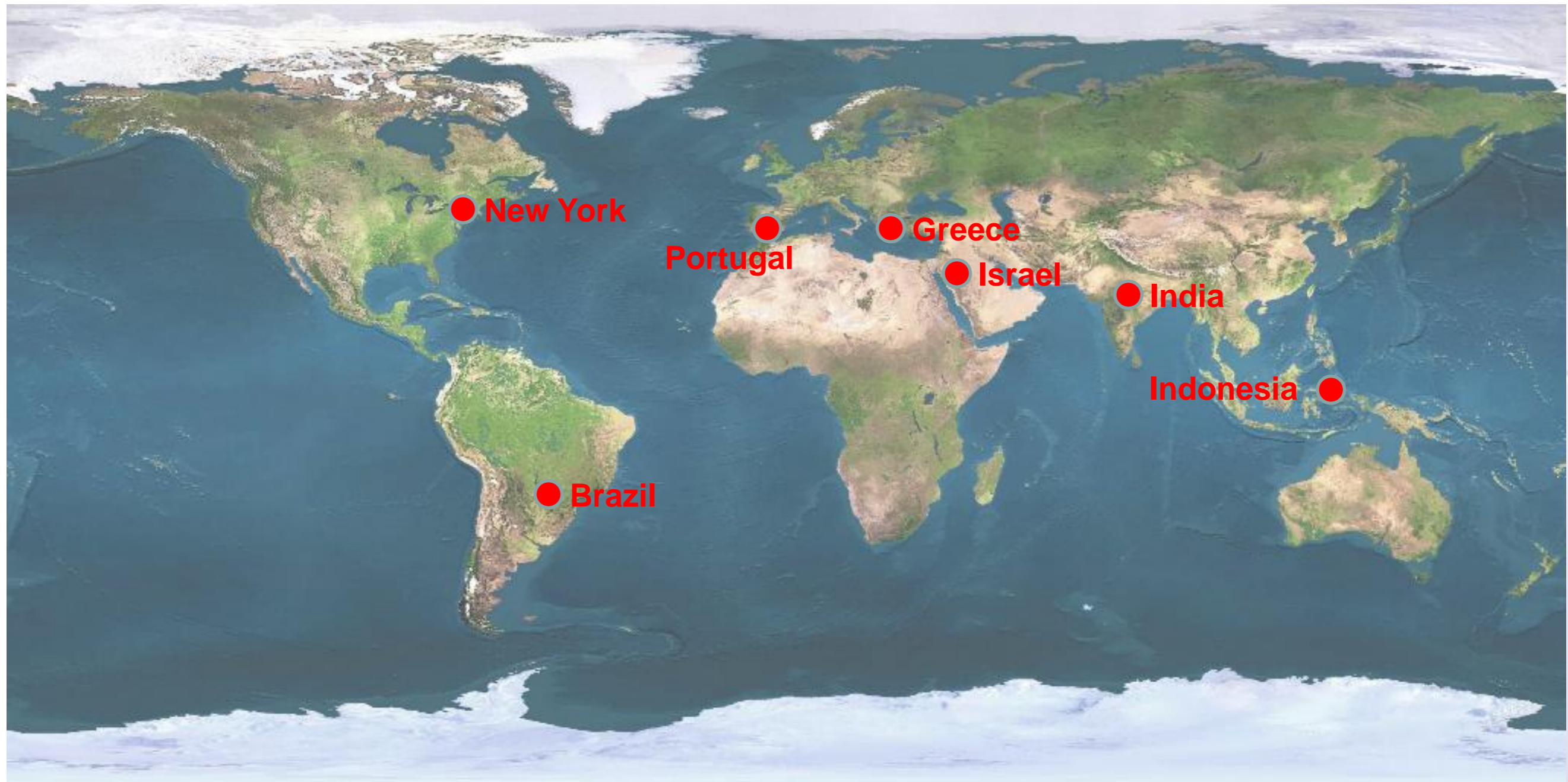
Done

69.65.33.21 Proxy: None Apache

hackademic v0.2

- Based on a Joomla frontend
- 10 web application security challenges
 - From simple to intermediate
 - Topics: information gathering, xss, encoding, etc.
- More challenges came in later
 - Crypto
 - SQLi
 - Entire VMs





What is hackademic?

- Relatively simple challenges, mainly web-based that involve JavaScript, PHP, web server mis-configuration, etc.
- The goal is to present the general idea behind certain security issues, rather than having complex, sophisticated challenges.
- Variety of topics covered, rather than going too deep into one of them.
- Some may seem simple and 'old-fashioned' (e.g. XSS) but websites vulnerable to them still exist!

Challenges

- There must be a scenario/story/myth.
- It must target a specific topic.
- The solution should be single and deterministic.
- There should be a “timeline” and a strategy for delivering the knowledge behind the set of all these exercises
- The difficulty in solving the exercises should escalate

Student's reactions



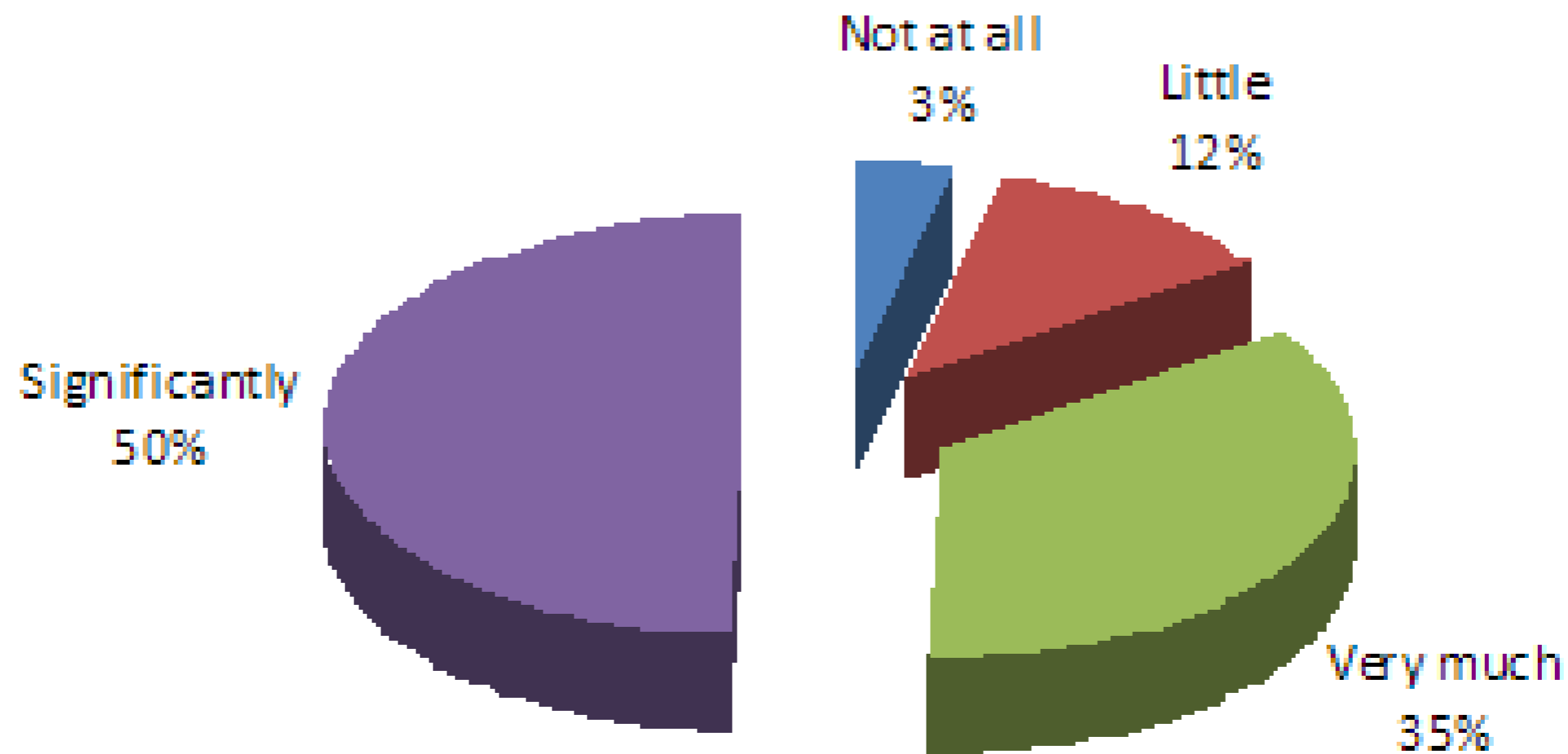
it works!

- Student expect typical “text-based”, theoretical lectures
- Instead, for a minute they get to ‘think like an attacker’.
- Several students, upon completion of the given challenges, attempted the next ones. Some did so at home ⇒ They liked it!
- Can lead to several discussions and input from students

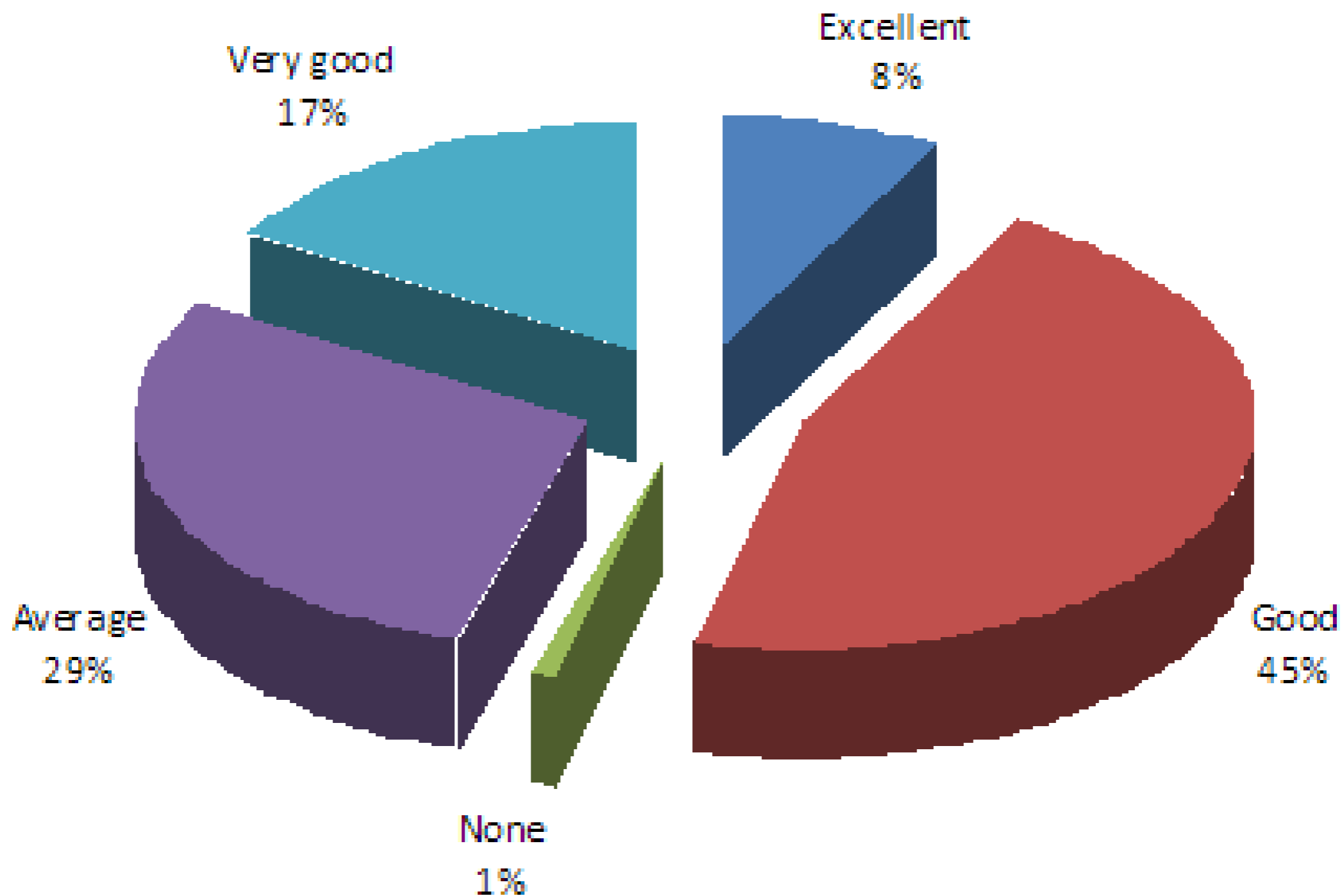
Questionnaires

- 25 questions in total
- Approx. 500 students have replied up to now
 - Looking to automate this...
- Questions on the level of skills/knowledge
- Feedback on the use of challenges

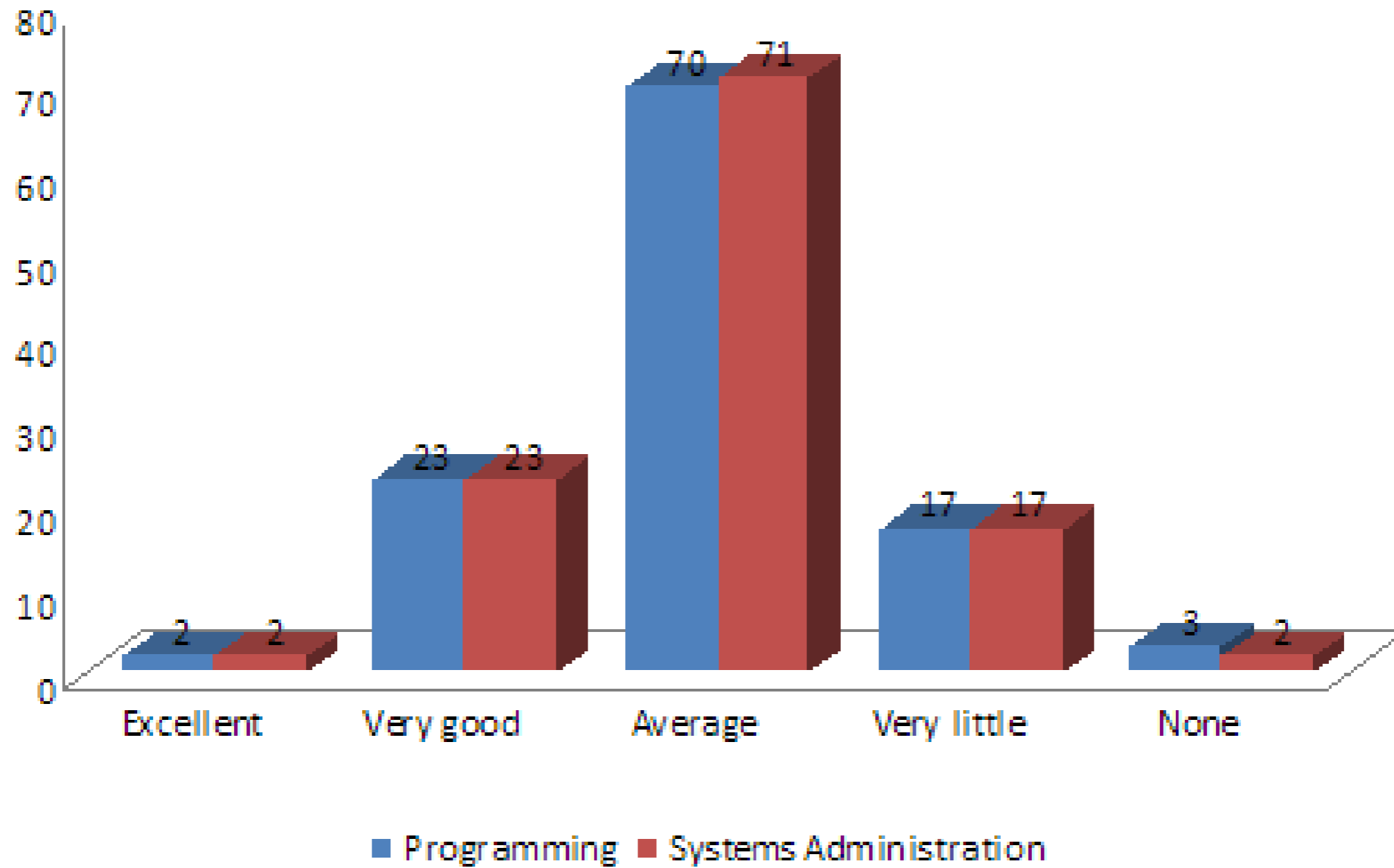
Usefulness of exercises



Related knowledge level



Level of specific knowledge



GSOC 2012

- 16 amazing proposals = 16 new interesting ideas
 - New challenges
 - New interface
 - ...
- Decided to work on new interface before building new challenges
 - With a bit of luck...

Why a new interface?

- Lots of interest to build new challenges
- Similar interest to use hackademic in various classes/universities.
- Need to work on usability and ease of installation
- Need to facilitate importing new challenges

hackademic v0.3

New features:

- An entirely new interface
- Installer
 - Facilitates/automates installation
 - Prerequisites: Apache/PHP/MySQL (XAMPP, LAMP, etc.)


Firefox Hackademic CMS localhost/xampp/hackademic/admin/ Google

OWASP The Open Web Application Security Project


HACKademic

Hi admin, Home Add New Articles Article Manager Users/Classes Add New Challenge Challenge Manager Logout


Dashboard




Add New Article




Article Manager




User Manager



Add New Challenge



Challenge Manager



Configuration

New features

Added usability for teachers:

- Create/Manage/Archive Class
- Assign students to classes
- Assign challenges to classes (students)
- Monitor student/class progress
- Add announcements/articles

New features

Ability to import new challenges

- (Nearly) automated procedure
- Workflow:
 - Teacher uploads challenge as .zip file
 - Challenge is automatically placed in the correct directory
 - Admin checks challenge
 - Admin published challenge
 - Teacher can add challenge to class

Demo

- Installer
- Admin/Teacher Interface
- User/Student Interface



hackademic Pi

- Hackademic on Raspberry Pi
 - Apache/PHP/MySQL
- Setup Raspberry Pi as a Wireless Access Point
- Result:
 - Approx. 3GB space needed
 - Kinda slow for normal use
 - Pretty cool for PoC ;)

How to access hackademicPi

- SSID: hackademic
- pass: hadkademicpi
- URL: <http://192.168.2.1/hackademic>
- You'll have to create a new user for yourself

Still in test (beta) version

Play along but **please** don't mess with it!!

(Near) Future Work

- Integration with ESAPI (to eliminate security issues)
- Documentation – new teacher's guide
- Release stable version (achieve “beta” project status)
- Release a hardened VM version.

Future Work

- Complex scoring system
- Multiple (randomized) solutions
 - (to eliminate cheating)



Thanks

Dr. Vasilis Vlachos

Andreas Venieris

Anastasis Stasinopoulos

Alex Papanikolaou

Pragya Gupta

Spiros Gasteratos

Petros Andreou





Thank You!

Visit the Hackademic Stand at the
Open Source Showcase
this afternoon to get some hands-on
experience!

Dr Konstantinos Papapanagiotou

konstantinos@owasp.org

@kpapapan

<http://hackademic1.teilar.gr> (old version, new coming soon)