Ασφάλεια Εφαρμογών: Από την Θεωρία στη Πράξη με το Hackademic

Μια νέα κατεύθυνση στην διδασκαλία της ασφάλειας εφαρμογών στα πανεπιστήμια και τα ΤΕΙ

Δρ. Βασίλης Βλάχος
ΤΕΙ Λάρισας

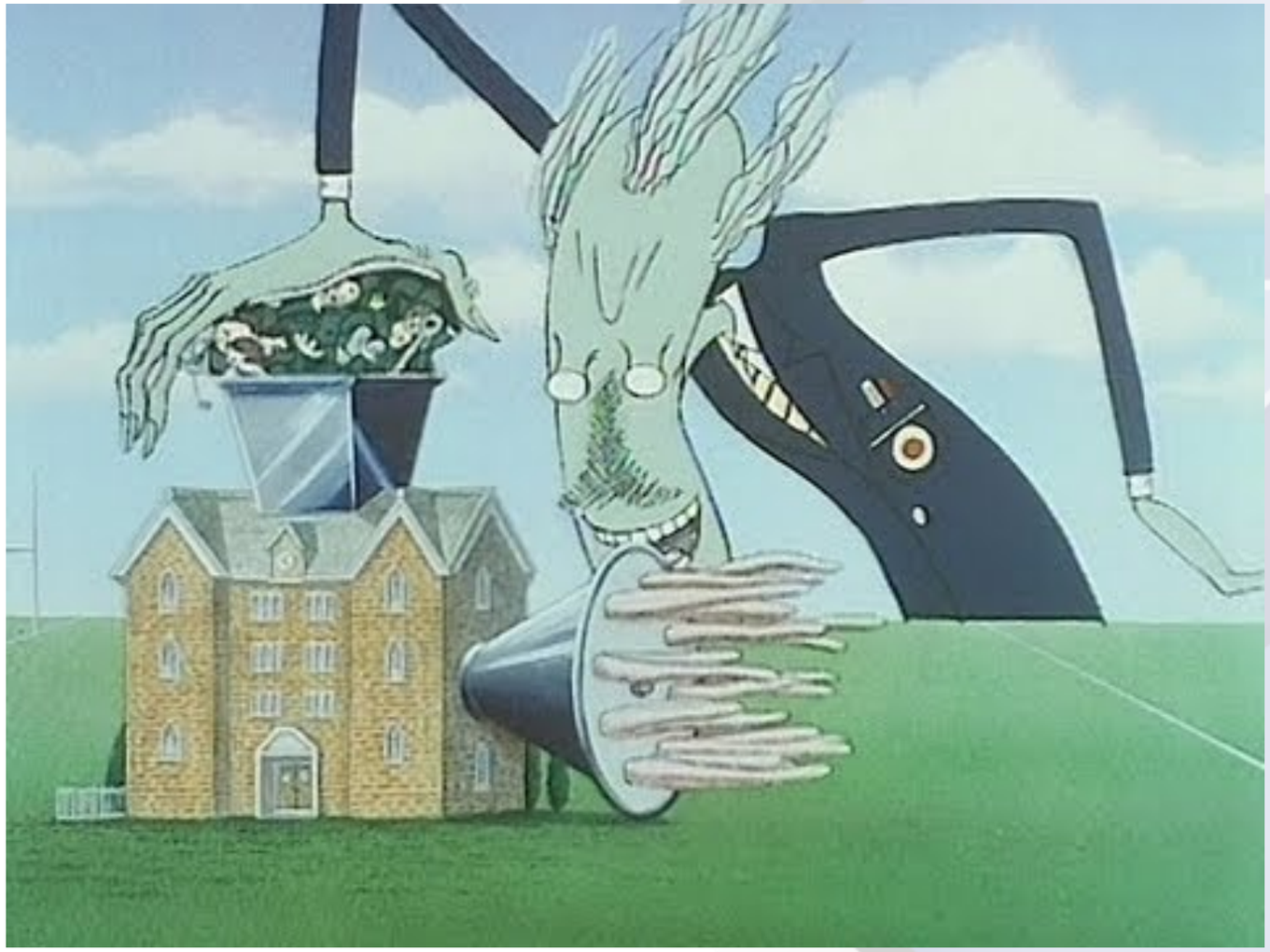
.about

Καθηγητής Εφαρμογών ΤΕΙ Λάρισας
Συντονιστής DART-NGO www.dart-ngo.gr
Μέλος της ομάδα συντονισμού του ελληνικού παραρτήματος του OWASP
Αρθρογράφος στο ελληνικό Linux{Format, Inside}
Συνιδρυτής στο projects ανοικτού λογισμικού hackademic
Συνσυγγραφέας μαζί 100+ φοιτητές της «Τεχνικής Νομοθεσίας για Μηχανικούς Πληροφορικής»

Διδάκτορας του ΟΠΑ/ΔΕΤ/Sense του Διομήδη Σπινέλλη
MSc Ολοκληρωμένα Συστήματα Υλικού και Λογισμικού – Τμήμα Ηλεκτρολόγων Μηχανικών + Τμήμα Μηχανικών Η/Υ Πανεπιστημίου Πατρών
Ηλεκτρονικός Μηχανικός και Μηχανικός Υπολογιστών, Πολυτεχνείο Κρήτης

.disclaimer

Κανένας φοιτητής δεν έπαθε το παραμικρό κατά την ανάπτυξη αυτού του project



hackademic v0.1

Δρ Κώστας Παπαπαναγιώτου και Αναστάσης Στασινόπουλος:

Challenges - Κίνητρα

- Διδασκαλία ασφάλειας σε 300+ φοιτητές κάθε εξάμηνο.
- Τα μαθήματα του Πανεπιστημίου είναι πολύ θεωρητικά.
- Οι φοιτητές διαθέτουν υπόβαθρο, δεξιότητες και γνώσεις που ποικίλουν.
- Κάθε φοιτητής (και κάθε καθηγητής) θέλει να έχει ένα "εργαστήριο δοκιμών"

Καλά είναι τα εργαστήρια αλλά...

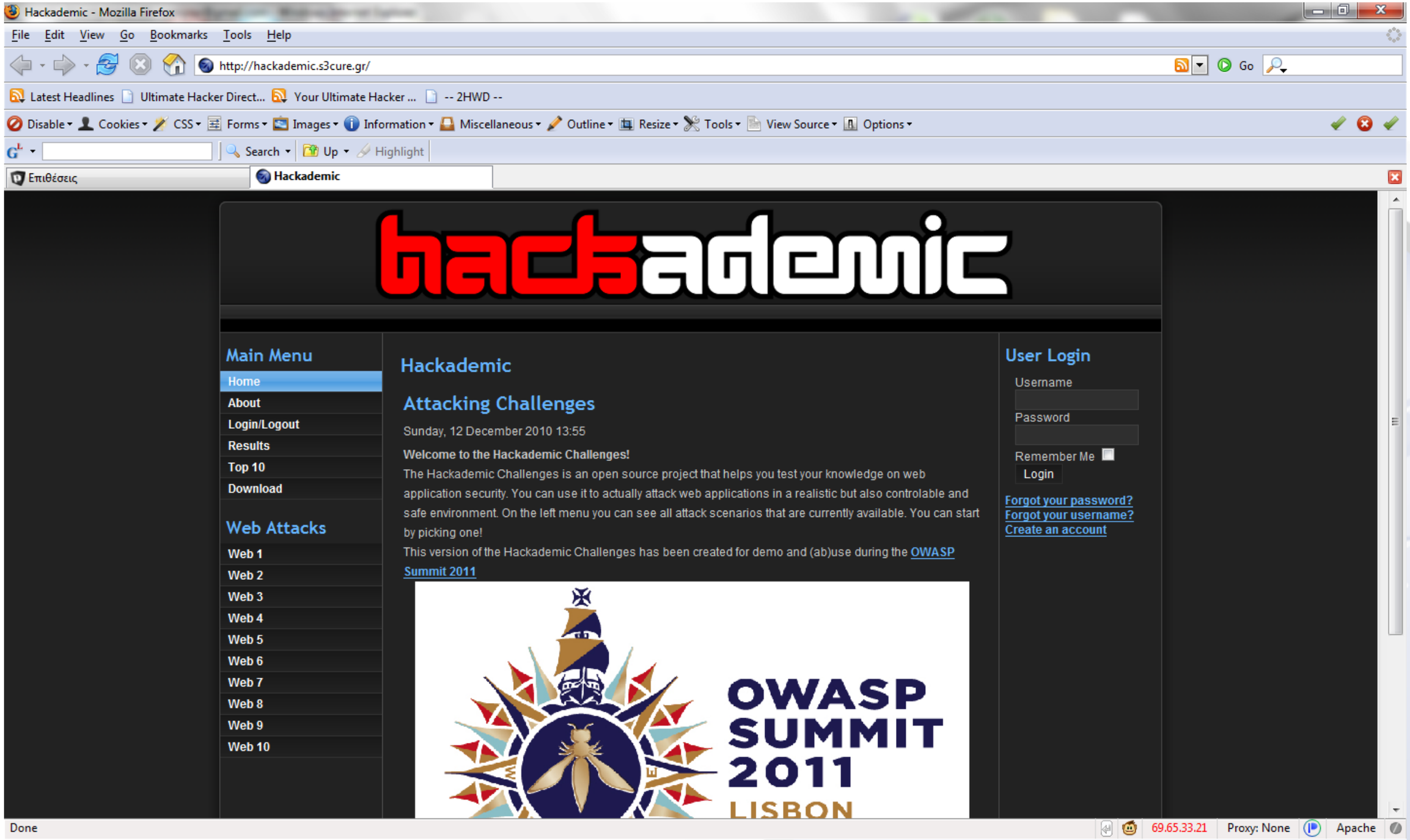
- Δυσκολία στο στήσιμο/διατήρηση (ειδικά αν οι φοιτητές δοκιμάζουν επιθέσεις σε αυτά)
- Οι περισσότερες ευάλωτες εφαρμογές (π.χ. WebGoat) είναι καλές για επίδειξη ή αυτοδιδασκαλία αλλά όχι για ένα εργαστηριακό περιβάλλον διδασκαλίας.
- Χρειάζεται η προώθηση της κουβέντας και της αλληλεπίδρασης.

hackademic v0.2

Ανδρέας Βενιέρης και Δρ. Αλέξανδρος Παπανικολάου

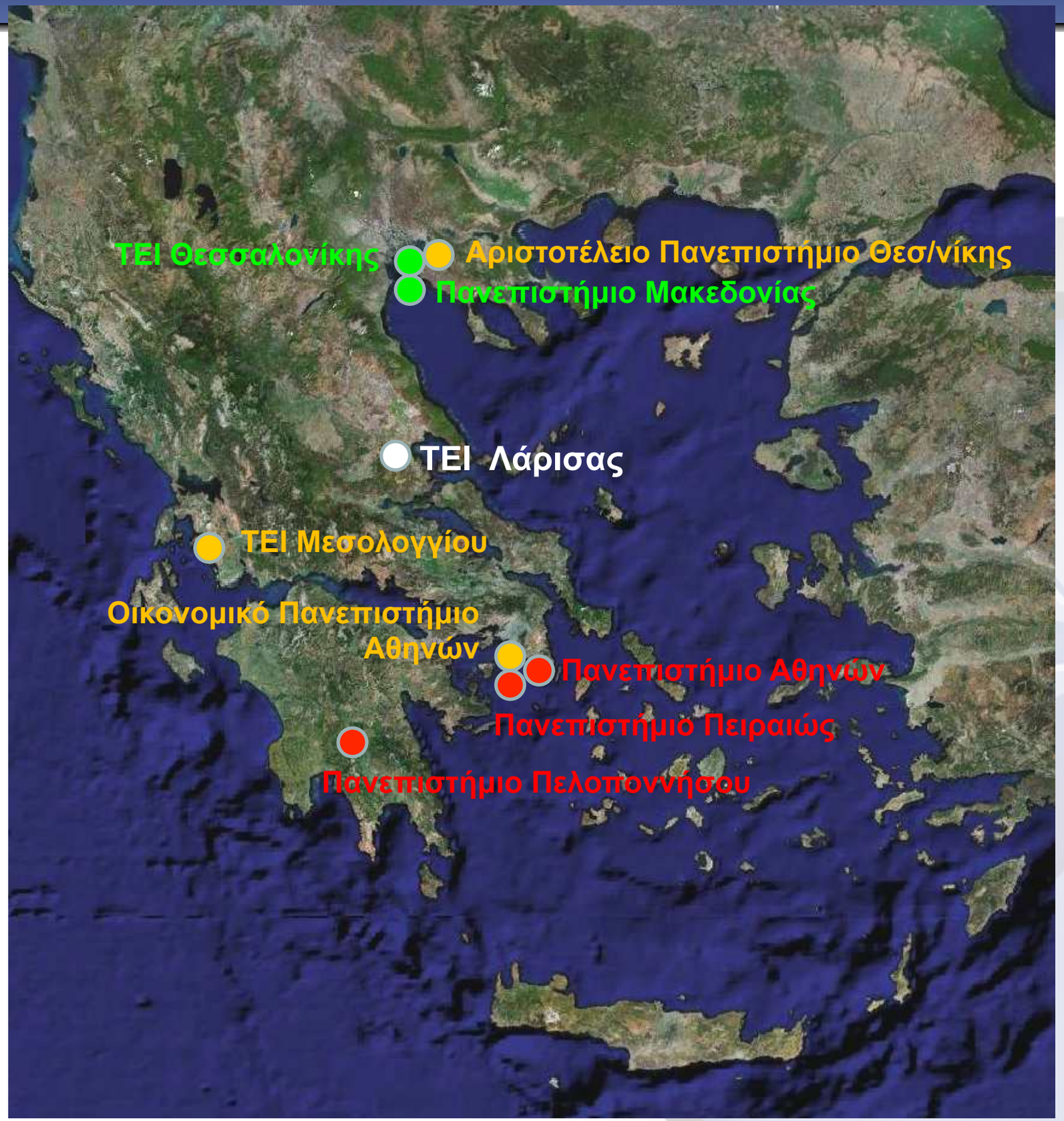
Και έτσι...

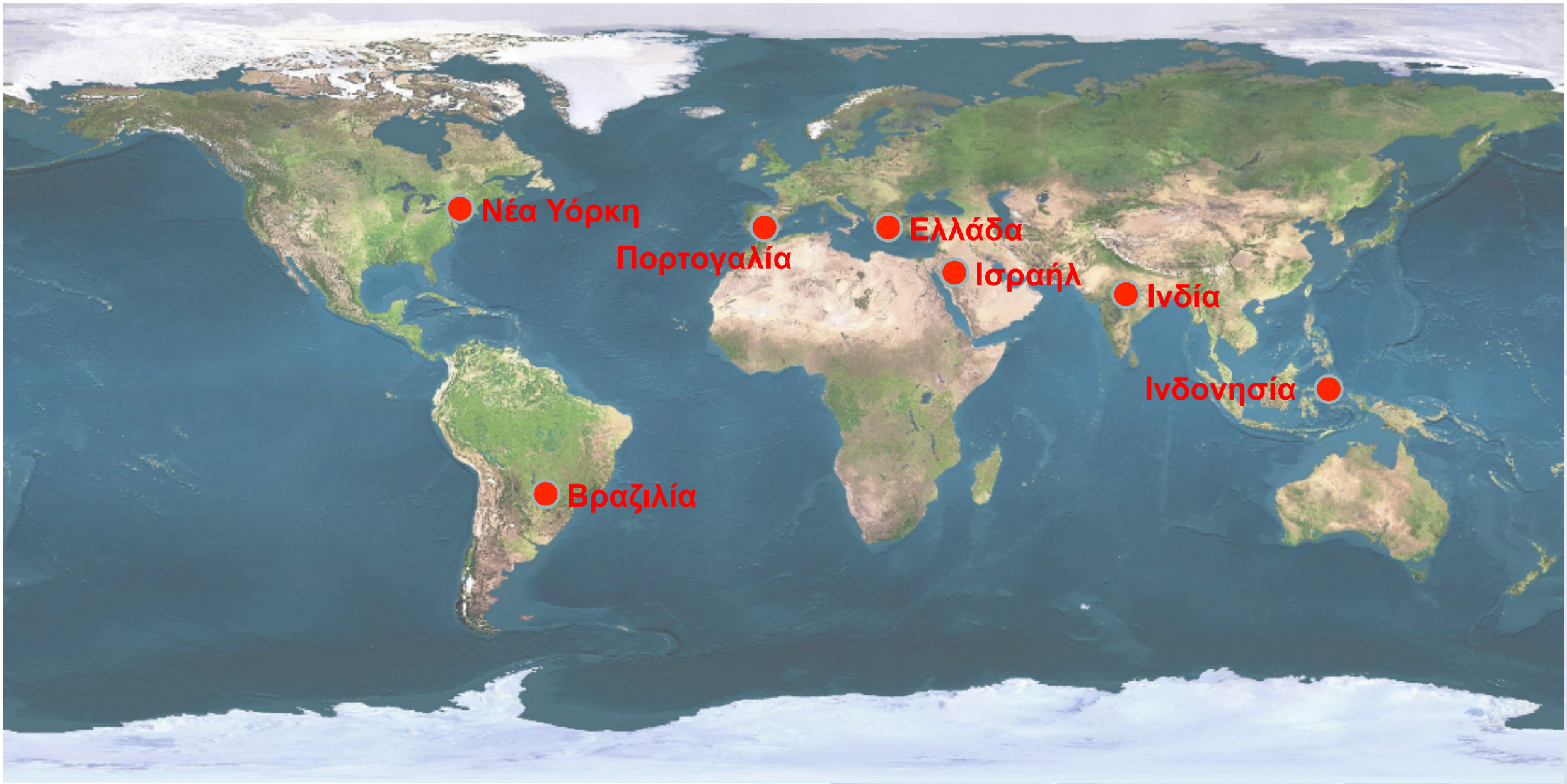
hackademic


Hackademic - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
http://hackademic.s3cure.gr/
Go
Latest Headlines
Ultimate Hacker Direct...
Your Ultimate Hacker ...
-- 2HWD --
Disable Cookies CSS Forms Images Information Miscellaneous Outline Resize Tools View Source Options
Search Up Highlight
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 controlable 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 v 02

- Βασισμένο σε περιβάλλον Joomla
- 10 δοκιμασίες ασφάλειας διαδικτυακών εφαρμογών
  - Από το απλό στο εξειδικευμένο
  - Θεματολογία: information gathering, xss, encoding, κλπ.
- Περισσότερες δοκιμασίες προστέθηκαν αργότερα
  - Crypto
  - SQLi
  - Ολοκληρωμένες Εικονικές Μηχανές (VMs)


ΤΕΙ Θεσσαλονίκης
Αριστοτέλειο Πανεπιστήμιο Θεσ/νίκης
Πανεπιστήμιο Μακεδονίας
ΤΕΙ Λάρισας
ΤΕΙ Μεσολογγίου
Οικονομικό Πανεπιστήμιο Αθηνών
Πανεπιστήμιο Αθηνών
Πανεπιστήμιο Πειραιώς
Πανεπιστήμιο Πελοποννήσου


Νέα Υόρκη
Πορτογαλία
Ελλάδα
Ισραήλ
Ινδία
Ινδονησία
Βραζιλία

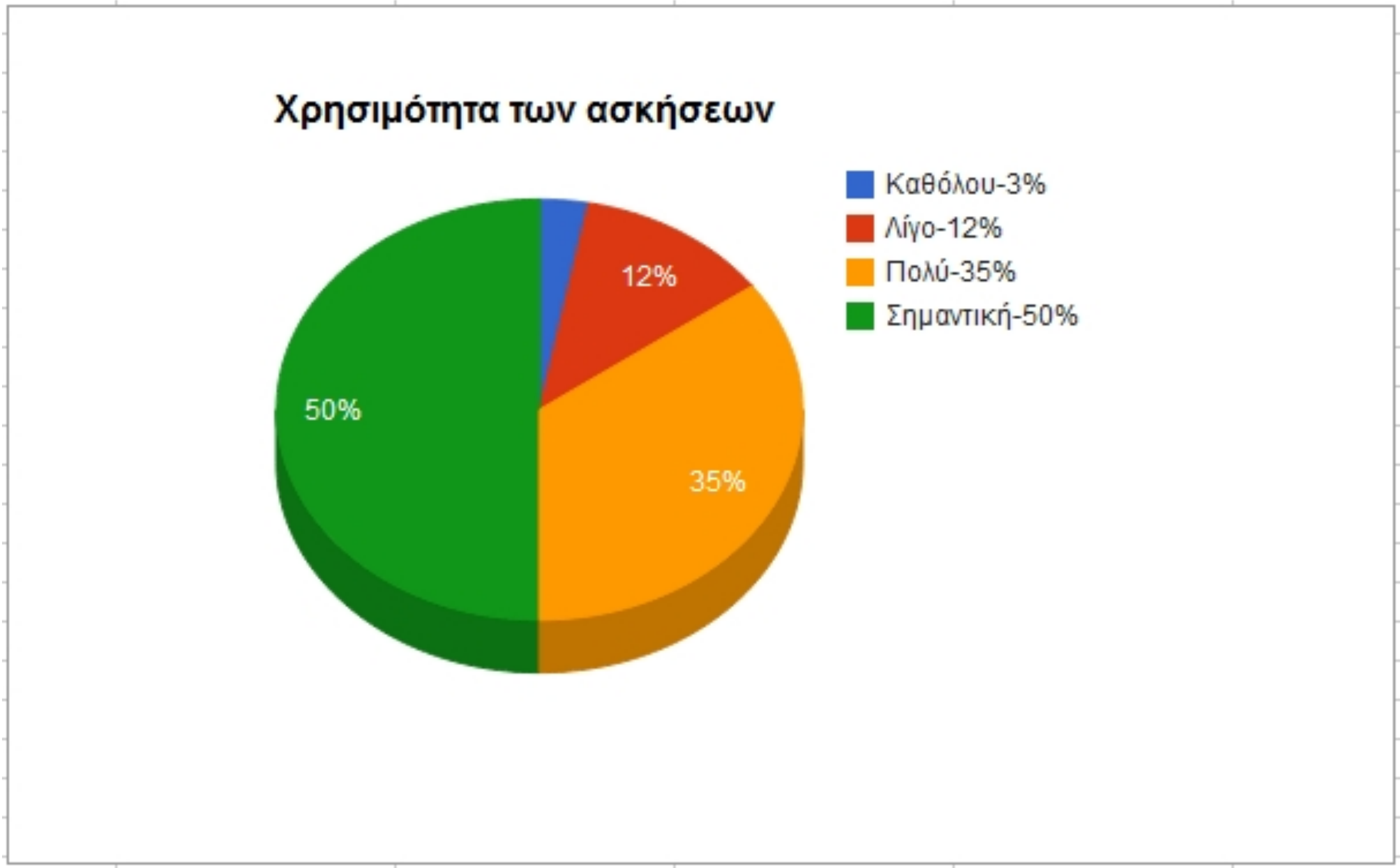
Τι είναι το hackademic;

- Σχετικά απλές δοκιμασίες, κυρίως web exploits που περιλαμβάνουν JavaScript, PHP, Λανθασμένα ρυθμισμένοι web servers, κλπ.
- Ο στόχος είναι η παρουσίαση της κεντρικής ιδέας που αφορά συγκεκριμένα θέματα ασφαλείας, αντί να δίνονται λεπτομερείς οδηγίες για το στήσιμο.
- Καλύπτεται ποικιλία θεμάτων, αντί να αναλύεται διεξοδικά κάποιο από αυτά.
- Κάποιες μπορεί να φαίνονται απλές και 'παλαιομοδίτικες' (π.χ. XSS) αλλά υπάρχουν ακόμη σελίδες ευάλωτες σε αυτές.

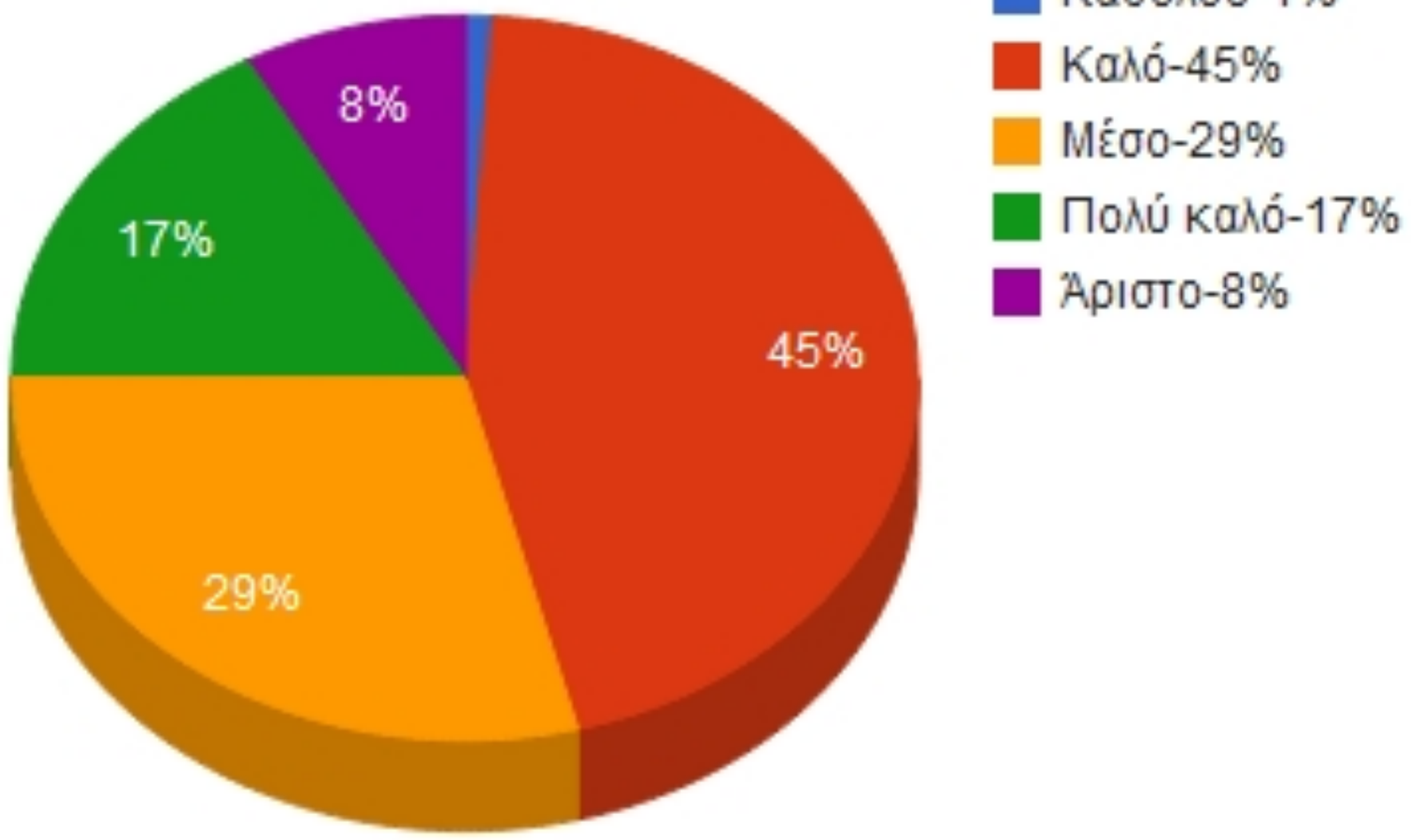
Αντιδράσεις φοιτητών

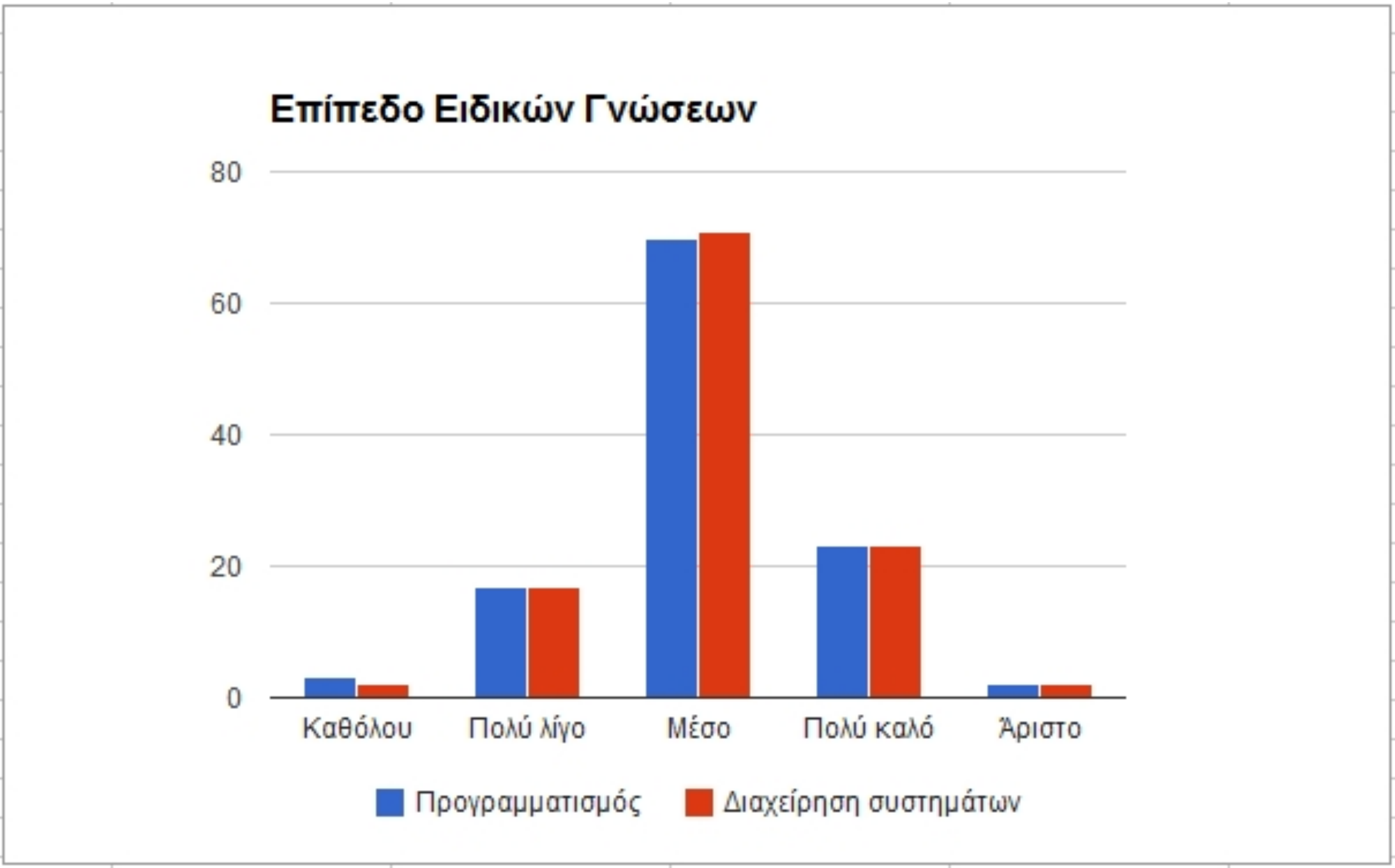
Έχει αποτέλεσμα!

- Οι φοιτητές περιμένουν "βασισμένες σε κείμενο", θεωρητικές διαλέξεις
- Αντιθέτως, για λίγο καλούνται να 'σκεφτούν ως επιτιθέμενοι'.
- Αρκετοί φοιτητές, μετά την ολοκλήρωση των ζητούμενων δοκιμασιών, προσπάθησαν να λύσουν τις επόμενες. Κάποιοι τις έκαναν από το σπίτι ⇒ Τους άρεσε!
- Μπορεί να οδηγήσει σε αρκετές συζητήσεις και προσθήκες από φοιτητές.


Χρησιμότητα των ασκήσεων
Καθόλου-3%
Λίγο-12%
Πολύ-35%
Σημαντική-50%
12%
50%
35%

Σχετικό γνωστικό επίπεδο




Επίπεδο Ειδικών Γνώσεων
80
60
40
20
0
Καθόλου
Πολύ λίγο
Μέσο
Πολύ καλό
Άριστο
Προγραμματισμός
Διαχείριση συστημάτων

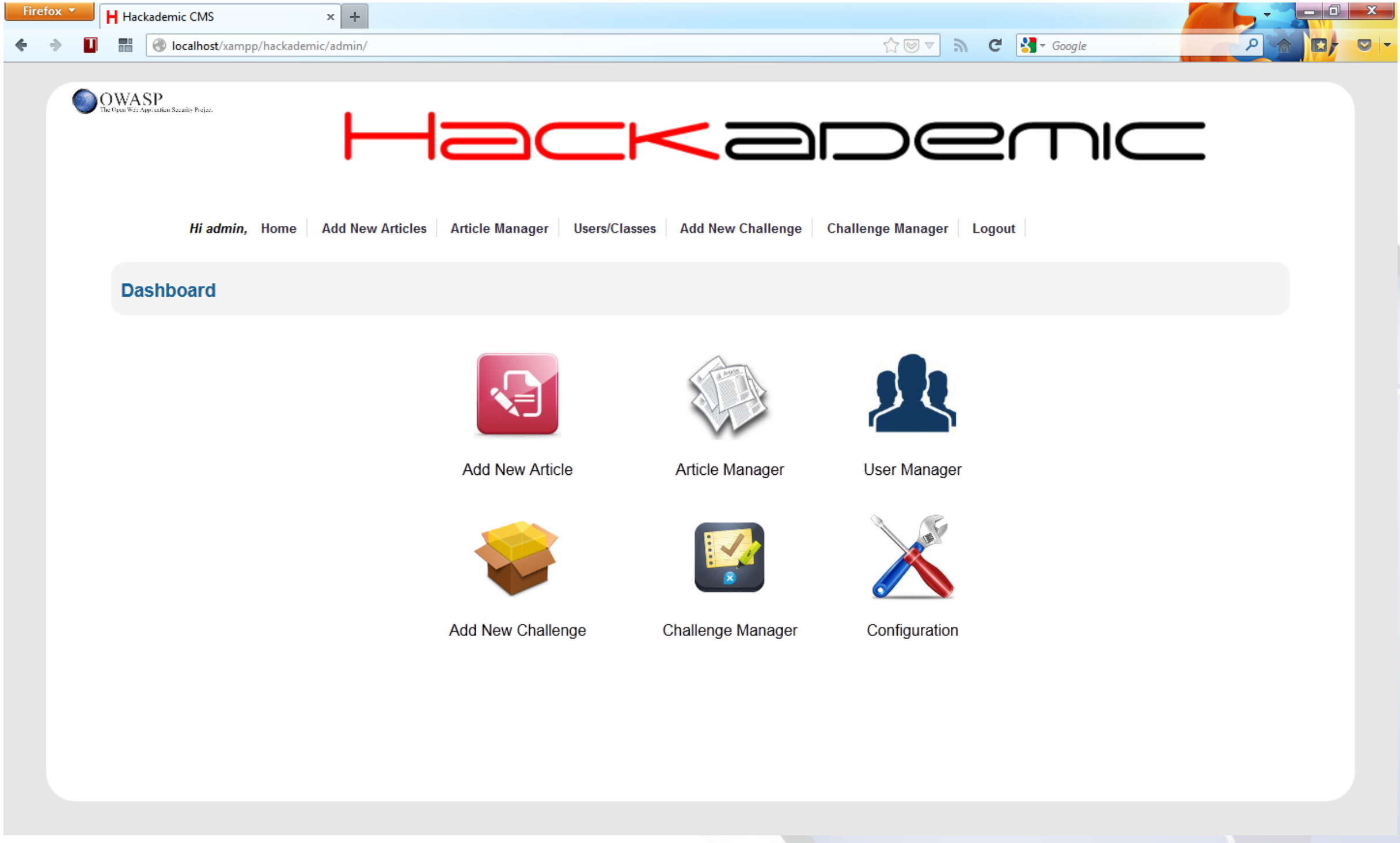
Γιατί νέο Interface;

- Αρκετό ενδιαφέρον για την ανάπτυξη νέων δοκιμασιών
- Παρομοίως ενδιαφέρον για την χρήση του hackademic σε διάφορες ημερίδες / πανεπιστήμια
- Ανάγκη για βελτίωση της χρησιμότητας και της ευκολίας της εγκατάστασης
- Ανάγκη φιλοξενίας των νέων δοκιμασιών

hackademic v0.3

Νέα χαρακτηριστικά:

- Ένα εξ' ολοκλήρου νέο interface
- Μηχανισμός Εγκατάστασης
- Ενσωματώνει/αυτοματοποιεί την εγκατάσταση
- Προϋποθέσεις: Apache/PHP/MySQL (XAMPP, LAMP, κλπ.)


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

Νέα χαρακτηριστικά

Προστέθηκε χρηστικότητα για τους καθηγητές:

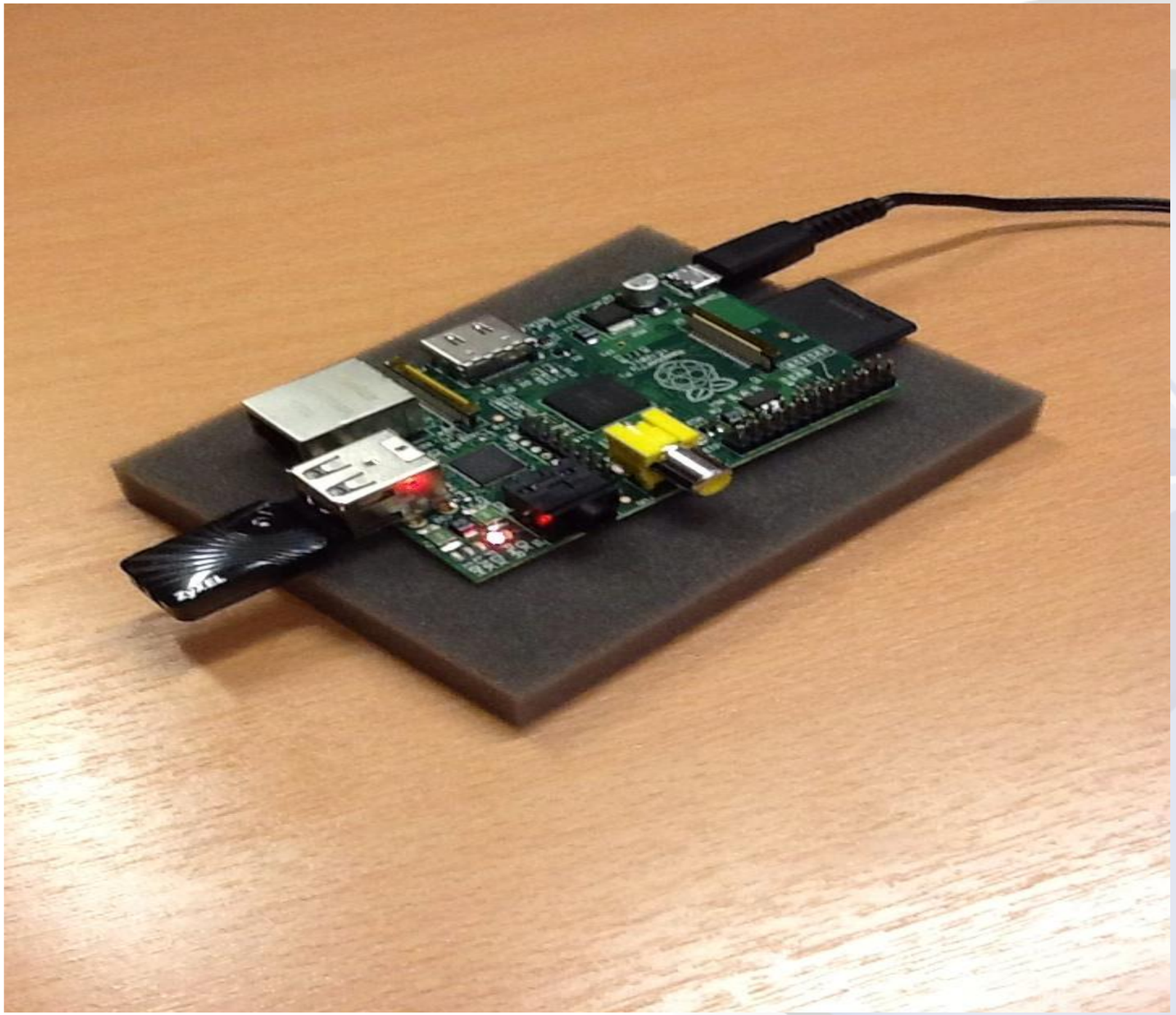
- Δημιουργία/Διαχείριση/Αρχειοθέτηση Τάξης
  - Εγγραφή φοιτητών στις τάξεις
  - Εγγραφή δοκιμασιών σε τάξεις(φοιτητές)
  - Παρακολούθηση προόδου φοιτητών/τάξης
- Προσθήκη ανακοινώσεων/άρθρων

Νέα χαρακτηριστικά

Δυνατότητα εισαγωγής νέων δοκιμασιών

- (Σχεδόν) αυτοματοποιημένη διαδικασία
- Ροή Εργασιών:
  - Ο Καθηγητής ανεβάζει την δοκιμασία σε μορφή .zip
  - Η δοκιμασία τοποθετείται αυτόματα στον σωστό κατάλογο
  - Ο διαχειριστής ελέγχει την δοκιμασία
  - Ο διαχειριστής δημοσιεύει την δοκιμασία
  - Ο Καθηγητής μπορεί να προσθέσει δοκιμασίες στην τάξη

hackademic Pi



hackademic Pi

- Το Hackademic σε Raspberry Pi
  - Apache/PHP/MySQL
- Ρύθμιση του Raspberry Pi ως Ασύρματο Σημείο Πρόσβασης
- Αποτέλεσμα:
  - Περ. 3GB απαιτούμενος χώρος
  - Κάπως αργό για κανονική χρήση
  - Αρκετά καλό για PoC ;)

Δουλειά Για το (Κοντινό) Μέλλον

- Ολοκλήρωση με το ESAPI (για να εξαληφθούν τα θέματα ασφάλειας)
- Τεκμηρίωση– νέος οδηγός καθηγητή
- Δημοσίευση σταθερής έκδοσης (καθορισμός "δοκιμαστικοού" επίπεδο)
- Δημοσίευση μιας σταθερής έκδοσης για εικονική μηχανή (VM).

Δουλειά για το Μέλλον

- Σύνθετο σύστημα βαθμολόγησης
- Πολλαπλές (τυχαιοποιημένες) λύσεις
  - (Για να εξαλειφθούν οι «αντιγραφές»)

Ομάδα Hackademic

Βασίλης Βλάχος
Κώστας Παπαπαναγιώτου
Ανδρέας Βενιέρης
Αναστάσης Στασινόπουλος
Αλέξανδρος Παπανικολάου
Pragya Gupta
Σπύρος Γαστεράτος
Πέτρος Ανδρέου

Ευχαριστούμε Πολύ!

CAMPSEC

CAMPUS SECURITY TEAM

http://www.campsec.teilar.gr

CampSec

- Ομάδα φοιτητών που ασχολείται με την ασφάλεια δικτύων & εφαρμογών
- Πρωτοβουλία φοιτητών

Δράσεις

Συμμετοχή σε ασκήσεις κυβερνοάμυνας και διαγωνισμούς
Πανόπτης 2011
Mozilla CTF 2012

Προσεχώς: Πανόπτης 2013, CyberCoallation

Συμμετοχή σε Συνέδρια και Φεστιβάλ Πληροφορικής (AthCon 2012, OWASP AppSec Research 2012, i2fest 2012)

Εκδηλώσεις

Παρουσιάσεις στα πλαίσια του μαθήματος “Ασφάλεια & Διαχείρηση Δικτύων”
Διοργάνωση ημερίδων με θέμα την “Ασφάλεια Διαδικτυακών εφαρμογών” με προσκεκλημένους επαγγελματίες του χώρου
Διοργάνωση ημερίδων σε συνεργασία με τις υπόλοιπες ομάδες στο ΤΕΙ Λάρισας

Η ομάδα

Αντώνης Μανάρας, Πέτρος Ανδρέου, Φώτης Λιάτσης, Δημήτρης Σωτηρίου, Ανδρέας Λάμπρης, Μαρία Ατζάμπου, Νίκος Ανδριόπουλος, Ζήσης Άρης, Γιώργος Μιχαήλου, Κοντοκώστας Θανάσης και Βασίλης Βλάχος

Menu

Αρχική

English

Βικιβιβλίο

Τεχνική Νομοθεσία

Τεχνική Νομοθεσία Για Μηχανικούς Πληροφορικής

Wikibook

Η ιστοσελίδα αυτή αφορά την χρήση των wikis στην εκπαιδευτική διαδικασία ενός τριτοβάθμιου ανώτατου τεχνολογικού ιδρύματος.

Ειδικότερα στο ΤΕΙ Λάρισας στο Τμήμα Τεχνολογιών Πληροφορικής και Τηλεπικοινωνιώ στα πλαίσια του μαθήματος «Τεχνική Νομοθεσ χρησιμοποιήθηκε ένα βικιβιβλίο ως το επίσημο σύγγραμμα του μαθήματος.

Το πλέον ενδιαφέρον χαρακτηριστικό αυτή τη προσπάθειας αποτελεί το γεγονός ότι οι φοιτητές συμμετείχαν ενεργά στην ανάπτυξη του και εξετάστηκαν πρακτικά στην ύλη που οι ίδιοι είχαν προσθέσει.

ΕΡΕΥΝΗΤΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΑΚΟ ΙΝΣΤΙΤΟΥΤΟ ΕΦΗΡΜΟΣΜΕΝΗΣ ΕΠΙΚΟΙΝΩΝΙΑΣ

ΕΘΝΙΚΟ ΚΑΙ ΚΑΠΟΔΙΣΤΡΙΑΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

Με χρηματοδότηση από το Ίδρυμα Νεολαίας και Δια Βίου Μάθησης – Εθνική Υπηρεσία και την Γενική Γραμματεία Νέας Γενιάς στο πλαίσιο του συγχρηματοδοτούμενου Προγράμματος 'Νέα Γενιά σε Δράση' της Ευρωπαϊκής Επιτροπής

D.a.r.T-n.g.o
Digital Awareness & Reinforcement of Trust

Κοινωνικοποιώντας δημόσιους φορείς????

http://www.dart-ngo.gr/

Έρευνα
- Διενέργεια ερευνών σε θέματα ψηφιακής ασφάλειας
- Παρουσίαση πρότυπων ερευνητικών εργασιών σε θέματα ασφάλειας πληροφοριακών συστημάτων

Επιμόρφωση
- Ενημέρωση πολιτών για την ασφαλή χρήση του Διδικτύου
- Ενημέρωση επιχειρήσεων για τους ψηφιακούς κινδύνους

Συνεργασίες

Ιδρύματα της Ελλάδας και του εξωτερικού	Οργανισμούς ιδιωτικού και δημοσίου δικαίου	Υπουργεία, Δήμους, Κοινότητες	Νομικά & Φυσικά πρόσωπα

Πρόληψη

Λιγότερα spam emails μετά την εξάρθρωση του Rustock botnet

Πέμπτη, 31 Μάρτιος 2011 16:36

Figure 1 - Chart showing global daily spam volumes (billions per day)

Πριν από λίγες ημέρες, η Microsoft και οι διωκτικές αρχές των ΗΠΑ κατάφεραν ένα σημαντικό πλήγμα κατά των spammers, με την εξάρθρωση του δικτύου Rustock. Όπως εκτιμά η Symantec, τις τελευταίες ημέρες η ανεπιθύμητη αλληλογραφία έχει μειωθεί κατά 33,6%.

Το 83,1% των spam emails που απεστάλησαν τις προηγούμενες εβδομάδες προέρχονταν από τα διάφορα botnets, με το Rustock να είναι υπεύθυνο για ένα μεγάλο ποσοστό αυτών των μηνυμάτων. Υπολογίζεται ότι οι υπολογιστές του Rustock botnet έστελναν σχεδόν 14 δισεκατομμύρια spam emails κάθε μέρα.

Παρόλο που το Rustock εξαρθρώθηκε, δεν αποκλείεται να επανέλθει στο προσεχές μέλλον. Ακόμα κι αν παραμείνει ανενεργό για πάντα, είναι δεδομένο ότι ένα νέο botnet θα πάρει τη θέση του για να καλύψει το "κενό στην αγορά"

Η Ινδία απαγορεύει τα domains .xxx

Τρίτη, 29 Μάρτιος 2011 17:32

Tags: Xxx Απαγόρευση Domain

Είναι η πρώτη από πολλές χώρες που θα απαγορεύσουν τα sites πορνογραφικού περιεχομένου.

Δεν έχουν περάσει πολλές ημέρες από τότε που η ρυθμιστική αρχή του Internet, η ICANN, όρισε επισήμως την απόδοση κατάληξης .xxx σε domain names για sites πορνογραφικου΄περιεχομένου, και έχουμε ήδη την πρώτη περίπτωση απαγόρευσής τους από μια χώρα.

Συγκεκριμένα, οι Ινδικές Αρχές θα προχωρήσουν άμεσα στην καθολική απαγόρευση των domains .xxx, δηλώνοντας ότι η χώρα ουδέποτε είχε αποδεχτεί την σχετική απόφαση της ICANN, καθώς η ύπαρξή τους αντίκειται στη νομοθεσία της χώρας. Όπως αναφέρει η έγκυρη οικονομική εφημερίδα Economic Times, η Ινδία είναι μονάχα η πρώτη από μια μακρά σειρά κρατών της Μέσης και Άπω Ανατολής οι οποίες θα μπλοκάρουν τα συγκεκριμένα domains