Security Testing of Web Application

IP Deploying IT Infrastructure Solutions
4 April 2013

- Tomas Lepistö
- Sandra Suviste
- Jurij Lukjančikov
- Markus Rintamäki
- Kęstutis Tautvydas
- Matis Palm
- Sten Aus
- Mika Salmela

Lifelong Learning Programme

Security Testing of Web Application: Structure

- Information about SIS (Study Information System)
- Tools
- Results
- Conclusion, proposals

Security Testing of Web Application: SIS

- Study Information System
- Used by
  - 13 higher education institutes
  - 17 000 users
- Goal
  - Learn and test security threats

Security Testing: Tools and Resources

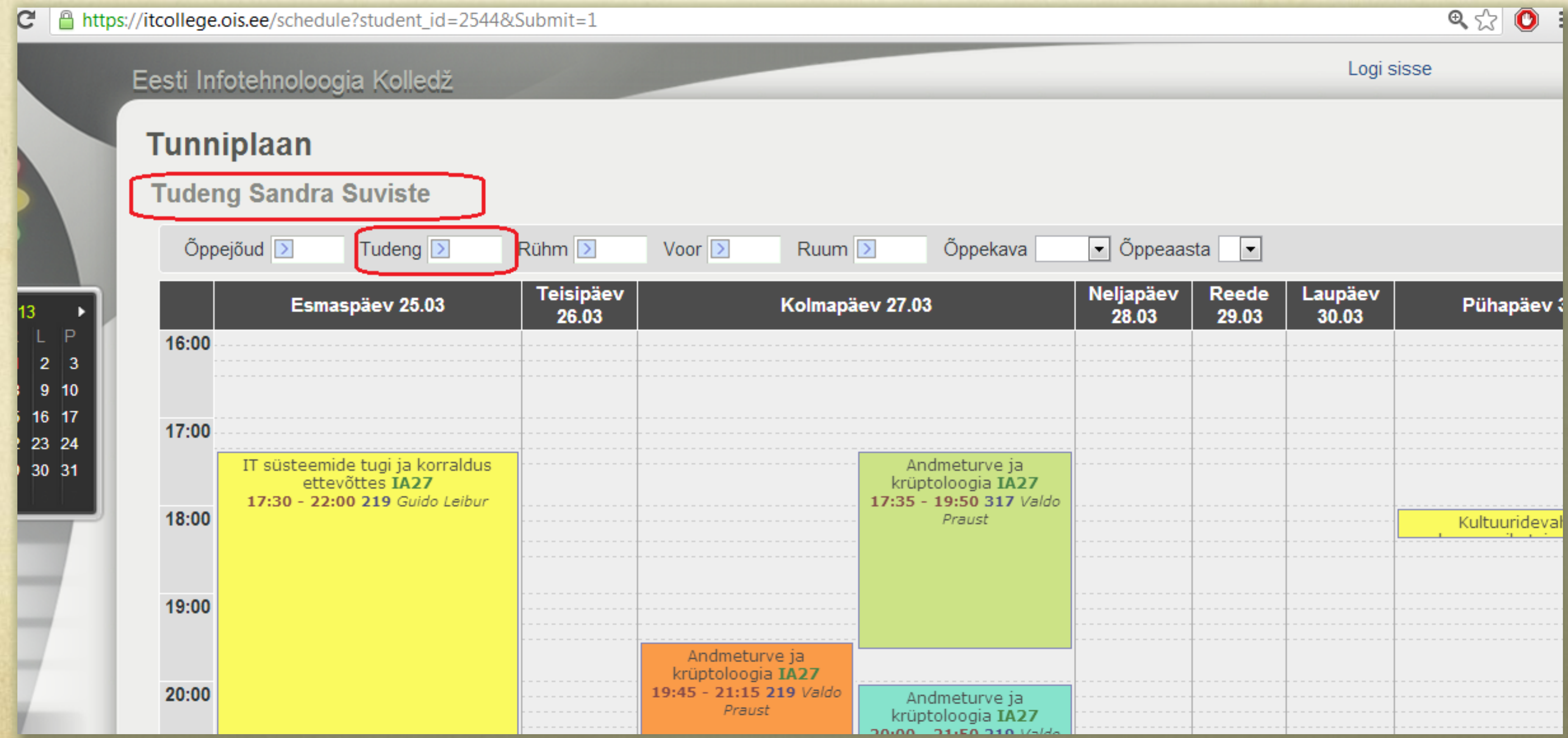
- OWASP (Open Web Application Security Project)
- OWASP ASVS (Application Security Verification Standard Project)
- Kali Linux
- Firefox Tamperdata
- Qualys SSL, SQL InjectMe, XSS InjectMe

Security Testing: Results I

- Developer’s notes
- Scanning: vulnerability to BEAST attack
- Live data (& users) in development environment

Security Testing: Results II

- Anonymous user can see student’s schedule
  - Fixed thanks to new schedule module (since 2 April)



https://itcollege.ois.ee/schedule?student_id=2544&Submit=1

Eesti Infotehnoloogia Kolledž

Logi sisse

Tunniplaan

Tudeng Sandra Suviste

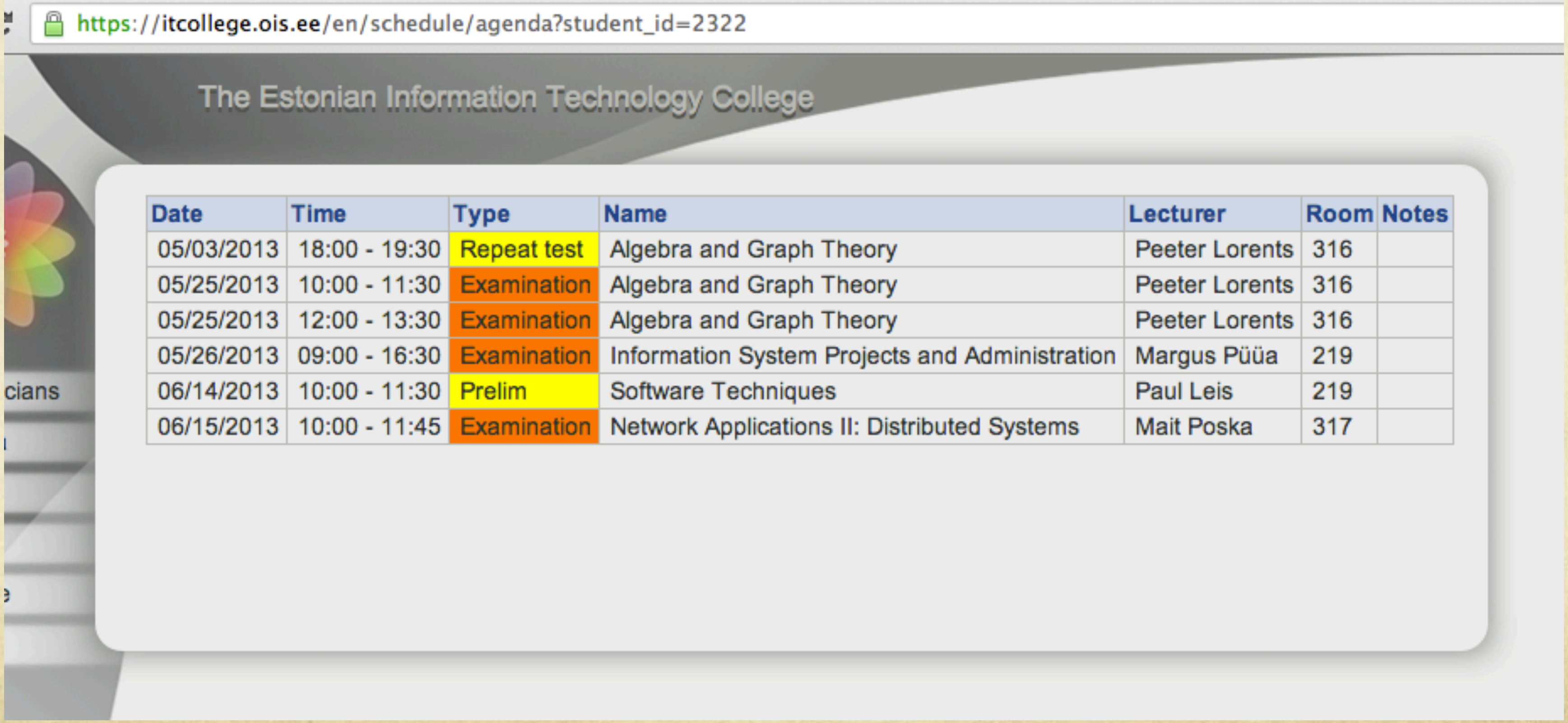
Õppejõud | Tudeng | Rühm | Voor | Ruum | Õppekava | Õppeaasta

13
L P
2 3
9 10
16 17
23 24
30 31

	Esmaspäev 25.03	Teisipäev 26.03	Kolmapäev 27.03		Neljapäev 28.03	Reede 29.03	Laupäev 30.03	Pühapäev 3
16:00								
17:00	IT süsteemide tugi ja korraldus ettevõttes **IA27** **17:30 - 22:00 219** *Guido Leibur*			Andmeturve ja krüptoloogia **IA27** **17:35 - 19:50 317** *Valdo Praust*				
18:00								Kultuurideval
19:00			Andmeturve ja krüptoloogia **IA27** **19:45 - 21:15 219** *Valdo Praust*					
20:00				Andmeturve ja krüptoloogia **IA27** **20:00 - 21:50 219** *Valdo*				

Security Testing: Results III

- Student's agenda is visible to everyone
  - Retake exams – Data Protection Law



https://itcollege.ois.ee/en/schedule/agenda?student_id=2322

The Estonian Information Technology College

Date	Time	Type	Name	Lecturer	Room	Notes
05/03/2013	18:00 - 19:30	Repeat test	Algebra and Graph Theory	Peeter Lorents	316	
05/25/2013	10:00 - 11:30	Examination	Algebra and Graph Theory	Peeter Lorents	316	
05/25/2013	12:00 - 13:30	Examination	Algebra and Graph Theory	Peeter Lorents	316	
05/26/2013	09:00 - 16:30	Examination	Information System Projects and Administration	Margus Püüa	219	
06/14/2013	10:00 - 11:30	Prelim	Software Techniques	Paul Leis	219	
06/15/2013	10:00 - 11:45	Examination	Network Applications II: Distributed Systems	Mait Poska	317	

Security Testing: Results IV

- Files in any format can be uploaded in …
  - Study materials
  - Application forms

Security Testing: Results V

- Changing user data does not require re-authentication
  - Form security token does not change
- “Few” more hours and one script
- Demo

Security Testing: Conclusion

- Summary of tests
- Areas of improvement
  - Re-authentication for changing user personal data
  - Form token algorithm
  - Live (real) data is being used in test environment
- Suggestions for future testing
- SIS is much more secure now

Security Testing of Web Application: For more information

- See our IT College Wiki page
  - https://wiki.itcollege.ee/index.php/Security