Team „Security"

- Sten Aus

- Matis Palm

- Sandra Suviste

- Markus Rintamäki

- Tomas Lepistö

- Mika Salmela

- Kęstutis Tautvydas

- Jurij Lukjančikov

- https://wiki.itcollege.ee/index.php/Security

What we did today

✓Divided SIS(Study Information System) modules (as-is) between ourselves

✓Tried SQL injection (manual and SQL InjectMe, TamperData) on forms and URL, including contact information – all secure so far

✓Tested changing student ID-s in the URL – nothing new

✓Tried changing https in study material links to http - secure

✓SIS is vulnerable to BEAST attack (QUALYS SSL Labs)

✓https://itcollege.test.ois.ee/- clicking Declaration results in error message

What we did today

✓Documentation: test results uploaded to Googledocs and updated Wiki

✓Upload lecturer profile picture with malicious code – not displayed

✓My data section for students

    ✓All forms are secured (characters are escaped)

    ✓Photo cannot be updated by student (only via student department)

Security threats of the day

✓ Some developer's notes are left in the systems

✓ No limit or input validation – if numbers are required, even characters are rendered back to users

✓ No limit for characters in inputs (possible DOS attack – multiple long requests which are greater than URL max capacity)

What we shall do tomorrow

➔ Complete Application Security Verification Standard Project review

➔ Start testing new parts of SIS (hopefully we can get access from developers)

   ➔ new declaration

   ➔ survey

   ➔ scholarship application

   ➔ VÕTA

➔ Continue testing