Moodle ~~development~~ with security in mind

Petr Škoda (skodak)

http://moodle.com/

Computer security

100 % - disconnect and turn off computers

...

...

0 % - let anybody do anything

Weakest link of chain

- Humans are part of the system
- Weakest link of a chain fails first

Web security

- Web was designed for distribution of information
- Browser trusts anything coming from the same server
- Javascript was not designed to be secure
- Browser plug-ins are not perfect
- Access control is only part of the problem

Common attacks

- XSS (Cross Site Scripting)
- CSRF (Cross Site Request Forgery)
- SQL injection
- Code execution
- Cookie stealing
- Non-validated input
- Social engineering and others

Cross Site Scripting (XSS)

- Very common problem – usually Javascript is used, could be malicious Flash, applet, etc.
- Data either stored on server or page parameters are abused
- Sometimes caused by buggy/non-standard browsers behaviour
- Attacker is able to do anything user may do with mouse or keyboard

Banking x Education

- Internet banking – as secure as possible
- Education – balanced security

Balanced security

- Education is based on interactive content
- Security often prevents collaboration
- We have to trust the teachers
- We do not usually trust students
- Trust is global for one site, can not be course only

Recommendations

- Backup often
- Keep sites up-to-date
- Set up separate sites for student projects
- Make sure admins and teachers understand capability risks

Moodle security issues

- Responsible disclosure is preferred over full disclosure
- All potential security problems should be reported to tracker – it is not recommended to use public forums at moodle.org
- Advisories are mailed to registered site administrators before each release
- Advisories are released after public release

Questions?