Ten Commandments of IT-Security for WEB 2.0 Startups

Claus R. F. Overbeck
RedTeam Pentesting GmbH
claus.overbeck@redteam-pentesting.de
http://www.redteam-pentesting.de

HackFWD Build 0.4
09. - 12. December 2010

RedTeam Pentesting, Dates and Facts

- ★ Founded in 2004
- ★ Specialisation exclusively on penetration tests
- ★ 8 penetration testers

I : Kiss: **K**eep **i**t **s**imple and **s**ecure

- Know your interfaces, e.g.
  - GET/POST-data
  - SOAP, Java RMI, etc.
  - Management interfaces?
  - ...
- Keep the exposed attack surface small.
- Know where your really important data is. Keep it in one place!

II : Filtering: Always use whitelisting

- ★ Blacklisting can be circumvented.
- ★ Better approach: Deny all, then allow few.

III : Think about security early

- ★ It will be difficult to add security later.

IV : Have someone on your team who has experience and knowledge

- ★ For web applications at least OWASP Top 10.
- ★ This is nothing that you can learn in a few weeks.
- ★ IT-security needs experience.

V : For complex things rely on the work of experts

- ★ Don't do cryptography and similarly complex things yourself!
- ★ Use well-tested software where possible.

VI : Have multiple lines of defence

- ★ Don't have your admin login open to the Internet, even though it asks for a password.
- ★ Separate things that can be separated!
- ★ Do not mistake segmentation for separation!

VII : Do not underestimate the risk that stems from "minor" flaws

Examples:

- Cross Site Scripting
- Error Messages
- ...

VIII : Think about the case of emergency before it happens

- ★ Who is allowed to pull the plug? When?
- ★ When will customers be informed? How?
- ★ How can we get back to normal operation quickly?
- ★ Do we call the police?
- ★ Do we do forensics? How do we avoid destroying traces?
- ★ ...

IV : (Pen)Test your IT-security

- ★ Attackers are creative. They do things that you have not thought of.
- ★ Don't rely on checklists only!

X : Know your risks, learn to live with them

- ★ Some risks are hard to avoid. Reduce these to an acceptable minimum!
- ★ Don't get caught up with fixing things that are not fixable!
- ★ There will always be a few people that you just have to trust.
- ★ 100% security does not exist!

Most of these seem pretty obvious:

I	Kiss: **K**eep **i**t **s**imple and **s**ecure
II	Filtering: Always use whitelisting
III	Think about security early
IV	Have someone on your team who has experience and knowledge
V	For complex things rely on the work of experts
VI	Have multiple lines of defence
VII	Do not underestimate the risk that stems from "minor" flaws
VIII	Think about the case of emergency before it happens
IV	(Pen)Test your IT-security
X	Know your risks, learn to live with them

But how many of these have you violated in the past?