M183
Insecure Direct Object Reference

Timo Bonomelli, Patrick Günthard

February 19, 2016

1 About *Indirect Object Reference*

1.1 What is *Indirect Object Reference*?

*Indirect Object Reference*are references to objects on a system (e.g. Database Keys) which are accesible by the user.

1.2 Who can attack?

Everyone who alerady has access to certain parts of the application but not to all data

1.3 How does the attack work?

The attacker manipulates the parameter that refers to a *direct object*.

2 Example

See Presentation

- Java-Snippet
- Web Page
- Database example

3 Prevent attack

- Use Sessions
- Authenticate on every access

3.1 Sessions

- No direct references are necessery beacause they can be saved on the server side.
- Other references can be mapped
  - Example: A dropdown can have own Ids which are mapped to direct object references on the server

3.2 Authentication

- check authentication on every *Indirect Object Reference*access
  - Example: A random token can be generated and sent to the user. The user can only access the authorized data with this token