Attacking client-side controls



Reasons for client-side controls

- Many vulnerability types are caused by insufficient user input validation
 - Input validation should be done in server since client-side data can not be trusted
- Many web applications however try to force rules for client-side data with client side controls
 - This can be done f.e. with JavaScript
 - Obviously since user owns the client, he can tamper client-side data maliciously



Kimmo Sauren 2

Client-side controls

- Basically there is two broad categories for restricting user input
 - 1. Data can be transmitted via client component which is assumed to prevent data tampering
 - 2. Application can implement restrictions to user interface



Transmitting data via the client

- Basically sending data to client that should be stored only in server. Why?
 - Removes need to store information in serverside
 - Might improve the performance of website
 - Might simplify the application logic
 - Application might be divided into several servers and distributing server side data might be complicated
 - Integration of third party components might require to send data through client



Transmitting data via the client

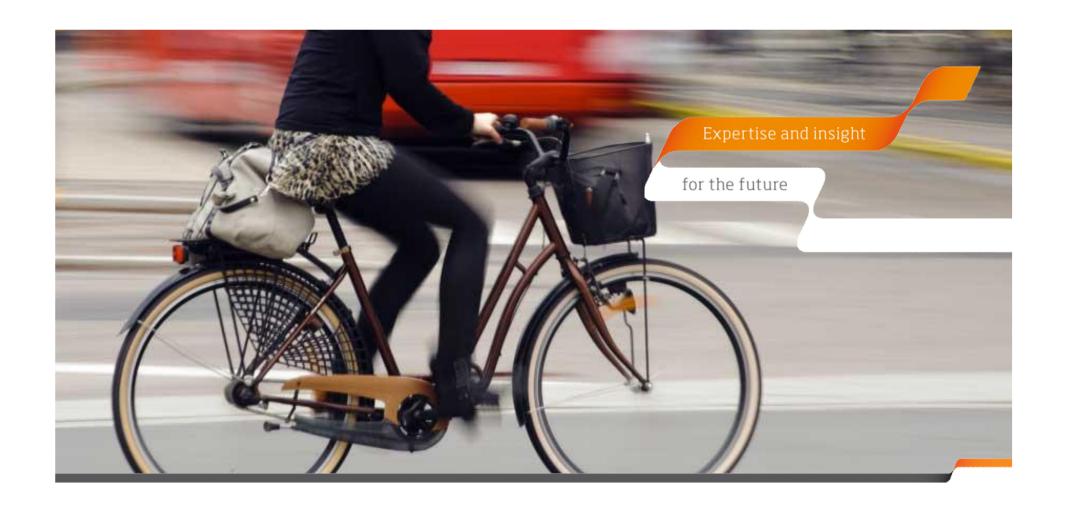
- Hidden form fields
 - Is not seen by user, but can be edited by malicious user
 - F.e. prices of webshop items could be stored hidden form fields in client-side
- HTTP Cookies
 - Some information can be stored in cookies
 - F.e. price categories
 - Remember that it can encrypted or obstructed



Transmitting data via the client

- URL parameters
 - Some of the sensitive data can be relayed via URL parameters
- HTTP referer header
 - Functionality of website can be relaying to the referer
 - F.e. some functionality can be only active if referer header points to certain webpage





THANK YOU!

www.metropolia.fi/en/ www.facebook.com/MetropoliaAMK kimmo.sauren@metropolia.fi

