Seminarium 2

Alexandra Johansson  
Sebastian Lund  
Josef Ottosson  
Johan Veeborn  
Stefan Sahlin

1

Man bör hantera indata på två sätt, dels på klientsidan med javascript för att underlätta för användaren och utesluta viss felaktig inmatning. Detta är en komplettering till den valideringen som också måste finnas på servern. Javascript kan enkelt stängas av, av klienten och ska därför inte ses som ett fullt skydd mot hackare.  
  
Vilka faror finns det?  
**SQL- injections**, När en användare genom en input tag t ex kör ett sql kommando t ex DROP Table.  
**Sessionhijacking**, och manipulation av cookies, T ex. en hackare snor session id eller kaka, eventuellt manipulerar dem och lyckas logga in med hjälp utav dem.  
**cross-site scripting**, användaren genom input lyckas lägga in script taggar eller andra taggar som påverkar koden.

2

**Emailadresser**  
filter\_var('bob@example.com', FILTER\_VALIDATE\_EMAIL)  
**Personnummer:**  
if (ereg ("([0-9]{4})-([0-9]{1,2})-([0-9]{1,2})", $date)) {..  
**Forumposter, med till exempe**lAlla taggar som inte är godkända, ska omvandlas till strängar.   
**Visning av HTML kod och javascript**  
Omvandla till strängar.  
**standardsträngar tex användarnamn och lösenord?**  
if (ereg ("([0-9]{4})-([0-9]{1,2})-([0-9]{1,2})", $date)) {..  
**Nummer**  
if (is\_numeric($element)) {..

3

Man bör vara medveten om att inte spara viktiga säkerhets uppgifter i kakor då dom lätt kan manipuleras från klienten. Man kan skydda sig till viss mån genom att kryptera kakans innehåll.

4

Inputdata ska valideras med hjälp utav javascript för att underlätta för användaren och utesluta viss felinmatning.