WEBTECHNOLOGIE – TENTAMEN

16 april 2014

17.00 – 19.00

- Dit tentamen is ***gesloten boek***. Je mag geen boeken, aantekeningen, slides, etc. gebruiken tijdens dit tentamen.
- Dit tentamen bestaat uit 12 deelvragen in 5 categorieën. Elke deelvraag heeft hetzelfde gewicht en bepaalt daarmee voor 1/12e het cijfer voor dit tentamen.
- Formuleer je antwoorden duidelijk en precies. Probeer je antwoorden compact te houden (zonder de helft weg te laten :). Geef altijd een toelichting. Schrijf leesbaar, met een pen.
- Je mag je antwoorden in het Nederlands of het Engels geven.
- Dit tentamen duurt ***twee uur***. Dat is 10 minuten voor elke deelvraag.
- Succes!

1. Web programming environment, client side representation

a) Teken het centrale architectuurdiagram zoals dat binnen het vak Webtechnologie gehanteerd wordt. Benoem elk van de componenten en de gegevensstromen. Leg eveneens uit waarom er geen database component aan de client side aanwezig is, terwijl dit wel voor de hand ligt.

b) Leg uit wat de betekenis is van de term "Cascading" bij het gebruik van Cascading Style Sheets. Benoem eveneens de drie locaties waar style properties aan een HTML element gekoppeld kunnen worden.

2. Client side scripting, server side scripting

a) Leg uit hoe event propagation werkt in de huidige DOM standaard. Geef bij je uitleg duidelijk het verschil aan tussen event capturing en bubbling. Laat aan de hand van een voorbeeld eveneens zien dat dit verschil van groot belang kan zijn voor het resulterende gedrag van een webapplicatie.

b) Het object model van PHP en het object model van JavaScript verschillen aanzienlijk van elkaar. Beschrijf beide object modellen en geef daarbij duidelijk aan waarin deze van elkaar verschillen.

3. State, sessions, webdatabases, stateful web

a) Atomaire database transacties zorgen voor een consistente database bij gelijktijdige toegang door meerdere gebruikers. Leg uit waarom database consistentie d.m.v. atomaire database transacties zo moeilijk te realiseren is in de context van een webapplicatie.

b) Enkele aan HTML5 gerelateerde standaarden zijn server-sent events, cross-document messaging (ook wel web messaging genoemd) en websockets. Alhoewel deze standaarden elk een eigen doel dienen, hebben ze ook overeenkomsten. Eén overeenkomst betreft de wijze waarop berichten ontvangen en verzonden worden. Geef een voorbeeld in JavaScript van de manier waarop dit binnen deze standaarden in z'n werk gaat. Leg eveneens uit hoe binnen deze standaarden met de Same Origin Policy (SOP) wordt omgesprongen.

c) Noem twee nadelen die het gevolg zijn van het hanteren van slechts één enkele zichtbare URL binnen de browser voor de volledige webapplicatie, bij het gebruik van AJAX. Geef eveneens aan hoe vanuit een webapplicatie betekenisvolle URLs opgebouwd kunnen worden zonder een page refresh te forceren.

4. Security

a) Een web developer gebruikt de volgende PHP code om een website te personaliseren:

```
$template = 'chainsaw_theme.php';

if (isset($_COOKIE['template'])) {
  $template = $_COOKIE['template'];
}

include ('templates/' . $template);
```

Leg uit welk beveiligingsprobleem deze code kent. Geef eveneens aan hoe je dit probleem kunt oplossen.

b) Een web developer wil XSS voorkomen door de volgende controle in PHP uit te voeren:

```
if (stripos($_GET['query'], '<script>') == false) {
  echo 'Je hebt gezocht op: ' . $_GET['query'];
}
else {
  echo 'Ongeldige invoer';
}
```

stripos is een PHP functie die het tweede argument (de speld) op case insensitive wijze zoekt binnen het eerste argument (de hooiberg). De positie van het eerste voorkomen wordt teruggegeven, of false als de speld niet in de hooiberg voorkomt.

Beschrijf twee beveiligingsproblemen die deze controle kent. Geef voor elk probleem eveneens een voorbeeld van ongewenste invoer die toch geaccepteerd wordt.

c) Leg uit wat Cross-Site Request Forgery (CSRF/XSRF) is, hoe het werkt en welke gevaren hieraan verbonden zijn.

5. Odds & ends

a) Een IP adres bestaat uit vier integers in de range 0 ... 255, gescheiden door een punt. Voorloopnullen in elk van de integers worden niet genoteerd. Voorbeelden van geldige IP adressen zijn: 192.168.0.1, 0.0.0.0 en 255.255.255.255. Voorbeelden van ongeldige IP adressen zijn 000.00.01.042 en 256.256.256.256.

   Geef één Perl compatible reguliere expressie die precies matcht met de hierboven beschreven gedaante van IP adressen. Probeer een zo compact mogelijke reguliere expressie te geven. Licht je reguliere expressie toe.

b) Het is verstandig om in HTML een scheiding aan te brengen tussen layout en structuur, net zoals het verstandig is om een scheiding aan te brengen tussen code die HTML genereert en code die de "business logic" van een webapplicatie bevat. Leg uit wat de voordelen zijn van deze twee scheidingen. Geef eveneens aan op welke wijze in de meeste frameworks de scheiding gemaakt wordt tussen code die HTML genereert en code die de "business logic" implementeert.

– THE END –