QUESTION PAPER TEMPLATE

Queen Mary
University of London

BSc Examination by course unit

Friday 8th May 2017 14:30 - 17:00

ECS639U Web Programming ***Duration: 2 hours 30 minutes***

YOU ARE NOT PERMITTED TO READ THE CONTENTS OF THIS QUESTION PAPER UNTIL INSTRUCTED TO DO SO BY AN INVIGILATOR

Answer ALL SIX questions

Calculators are not permitted in this examination.

Complete all rough workings in the answer book and cross through any work that is not to be assessed.

Possession of unauthorised material at any time when under examination conditions is an assessment offence and can lead to expulsion from QMUL. Check now to ensure you do not have any notes, mobile phones, smartwatches or unauthorised electronic devices on your person. If you do, raise your hand and give them to an invigilator immediately. It is also an offence to have any writing of any kind on your person, including on your body. If you are found to have hidden unauthorised material elsewhere, including toilets and cloakrooms it will be treated as being found in your possession. Unauthorised material found on your mobile phone or other electronic device will be considered the same as being in possession of paper notes. A mobile phone that causes a disruption in the exam is also an assessment offence.

EXAM PAPERS MUST NOT BE REMOVED FROM THE EXAM ROOM

Examiners:

Question 1 (HTTP, 15 marks)

a) Name one HTTP header (either request or response) which is relevant for web application *performance*, and explain its performance relevancy.
'Expires' response header. Setting an appropriate expire date for the resource representation enables the client to maximise the use of cache. Future requests to the resource will be avoided and the client will experience a faster rendering time.

[5 marks]

b) Name one HTTP header (either request or response) which is relevant for web application *security*, and explain its security relevancy.
'Set-Cookie' response header is used to pass the CSRF-token back to the server. In this way the server can verify that the request is coming from the correct client, avoiding cross-site request forgery attacks.

[5 marks]

c) Find the appropriate terms to correctly complete the following paragraph from the RFC 2616:

"The HTTP method _____ requests that the enclosed entity be stored under the supplied Request-URI. If the Request-URI refers to an already existing _____, the enclosed entity SHOULD be considered as a modified version of the one residing on the origin _____. If an existing _____ is modified, either the 200 (OK) or 204 (No Content) response codes SHOULD be sent to indicate successful completion of the _____."
Missing words are PUT, resource, server, resource, and request

[5 marks]

Question 2 (Frontend Development, 20 marks)

a) You are programming the website www.site1.com and wish to perform an Ajax request to www.site2.com. The Ajax request fails even though you are requesting access to a resource you know is available on www.site2.com. What could be the problem and how can you fix it? For security reasons browsers do not allow cross-domain Ajax requests. Either site2 needs to enable cross-site access by setting the 'Access-Control-Allow-Origin' on the response header, or the Ajax request should be made to site1's backend, and the backend can then make a request to site2.com.

[5 marks]

b) For each of the statements below state whether it is **True** or **False**:

i) Cookies are stored in a clients computer, so any browser on that computer would have access to the client's pool of cookies. False
ii) Sessions in Django use cookies, hence a session can only be established if the client's browser has enabled the creation of cookies. True
iii) Setting *HttpOnly=True* when creating a cookie is a standard way of increasing the efficiency of the frontend. False
iv) Session and cookie values are available in Django's request object. True
v) Sessions always expire when a client closes the browser. False

[5 marks]

c) An important aspect of any web technology is extensibility, i.e. a technology should provide support for the application developer to extend the given tool. Outline how the jQuery library supports extensibility. The jQuery library is based on the use of the jQuery object. The programmer can make use of javascript prototypes and extend the jQuery prototype with extra attributes and methods. Any jQuery object will immediately have access to the new attributes and methods.

[5 marks]

d) Can a web developer make use of AngularJS in conjunction with Django? Explain your answer. Yes, AngularJS extends HTML with dynamic features, and hence it can be used when defining Django templates. This is orthogonal to the business logic that is included in the view functions or the UI logic included in the template language.

[5 marks]

Question 3 (Backend Development, 15 marks)

a) Outline how the Django template language supports extensibility. Programmers can define new template tags and filters by describing them as Python functions. These need first to be registered and can then included and used in templates.

[5 marks]

b) Consider the following snippet of models.py. Describe in general terms which SQL tables would be created by the ORM, and which extra fields will be added to each of the models apart from the ones explicitly defined in the model. The ORM would add primary key fields to Coursework and Student, and create three tables: coursework, students, and an extra table to model the ManyToMany relationship between Cousework and Student.

```
class Coursework(models.Model):
   title = models.CharField(max_length=200)
   deadline = models.DateTimeField()

class Student(models.Model):
   name = models.CharField(max_length=200)
   std_id = models.CharField(max_length=200)
   email = models.EmailField()
   cws = models.ManyToManyField(Coursework,blank=True)
```

[5 marks]

c) Consider the following view function. Write a decorator that encapsulates the checking that 'username' is in the request.session dictionary. The decorator should apply the view function it is given in case the check is successful, or return the 'myapp/index.html' template with the signupForm in the context when the check fails.

```
def index(request):
   if 'username' in request.session:
      un = request.session['username']
      try:
```

```
            user = User.objects.get(username=un)
            context = { 'user' : user }
         except User.DoesNotExist:
            context = { 'error' : 'User does not exist.' }
      else:
         signupForm = SignupForm()
         context = { 'signupForm' : signupForm }
      return render(request, 'myapp/index.html', context)
```

```
def decorator(f):
   def check(request):
      if 'username' in request.session:
         f(request)
      else:
         signupForm = SignupForm()
         context = { 'signupForm' : signupForm }
         return render(request, 'myapp/index.html', context)
```

[5 marks]

Question 4 (Architecture and Testing, 20 marks)

Consider the following abstraction of three pages of a web application. cssN denotes a block of CSS code, htmlN describes a block of HTML code, and javascriptN describes a block of javascript code.

page1.html	page2.html	page3.html
css1 css2 html1 html2 javascript1	css1 html1 html3 javascript2	css1 css3 html1 javascript3

a) Outline how a developer can make use of Django's **template hierarchy** in order to avoid duplication of code in these pages. Make use of the following template tags:
{% extends <template_name> %}
{% block <block_name> %} … {% endblock %}
{% include <template_name> %}

A base template should be created with the code that is repeated in all three pages, i.e. css1 and html1. Each page should then extend this base template including the code that is particular to that page.

[5 marks]

b) For each of the following application logics, choose whether it would be more appropriately done in Python on a view function, or in a template using the Django template language:

i) Check that a user's input does not contains malicious code. view
ii) Display a user's profile image if available. template
iii) List only the user's public messages. template
iv) Return a warning if request.POST contains missing input. view
v) Round a bank account balance to the nearest integer. template

[5 marks]

c) Describe Django's support for carrying out the testing of web applications. Django provides a TestCase class (extending Python's UnitTest) and a Test client which simulates a web browser. The tool manage.py can be used to run the unit tests using the Test client provided.

[5 marks]

d) You must turn 'Debug' off when your code is deployed to the live server. Explain how one can programmatically identify whether the python code is running on 'localhost' or on the live server. This test can be done by looking at the server's environment variables. The set of environment variables on the live server is normally different, or will hold different values than the ones on the development server.

[5 marks]

Question 5 (Security and Performance, 20 marks)

a) The Django User model contains a password field. Its description says "*A hash of, and metadata about, the password. (Django doesn't store the raw password)*" Explain why raw passwords are not stored, and how users are later able to login using their raw passwords even if raw passwords are not stored on the server. Plain text user's password should never be stored on the application database, in case an attacker gains access to the DB. When a user logins in, the input password is again hashed, and the two hashes are compared.

[5 marks]

b) Regular expressions are useful to detect malicious input. Should the regular expressions describe the valid inputs, or the invalid ones? Explain your answer. Regular expressions should describe valid inputs. Describing invalid inputs raises the possibility that the application developer failed to capture all possible attacks that a malicious user may come up with.

[5 marks]

c) Name three disadvantages of optimising a web application for performance. Optimisations can result in new bugs being introduced, it can make the code less readable, and obviously involves extra cost.

[5 marks]

d) Explain how the use of Content Delivery Networks (CDNs) can reduce the download time experienced by the web application's clients. When a client makes a request to a resource in a CDN, the closest point in the CDN which can serve the resource will be used. This reduces the distance and hence the download time for that resource.

[5 marks]

Question 6 (Web APIs, 10 marks)

a) Describe two drawbacks of implementing a model-based web API. Programmer cannot change relational database without breaking API clients. Exposes your apps inner structure.

[5 marks]

b) Describe how the Accept-Content request header can be used for API content negotiation. When a client makes a request to a specific resource, it can specify in the Accept-Content request header which format it wants the response to be on. The backend of the API can then serve the client in the correct format, e.g. JSON or XML.

[5 marks]

End of Paper