School of Information Technology and Electrical Engineering
INFS3202/7202 – Web Information Systems

Assignment Two (20 Marks)

Demo Submission due at 6 PM 30/05/2016 -3/06/2016

Overview and objectives

The goal of this assignment is carry out your proposed website in assignment one by implementing server side code and deploying with cloud technology.
The assignment can be done either in the lab or at home via VPN. However, you must present this assignment from one of the allowed cloud platforms to your lab tutor during your scheduled lab sessions in Week 13, that starts from 30/05/2016. You must also submit the code to Blackboard before 6pm on the day of your scheduled lab sessions.

This assignment has one major task:
Website (20 marks)

Note: you must deploy your work on a cloud platform (MS Azure, Google Cloud, Amazon AWS) in order to be assessed.

Website (20 Marks)

In your group of between one and three members, you must decide on an assignment one proposal from your group members to implement fully. You must implement any advanced features that were described in the proposal, and deploy your project to a cloud platform.

Preparation

Interface

Ensuring your website is usable for your target audience is vital. Your website should be accessible, usable and following common conventions and best practices. You should be able to justify your implementation decisions.

For an example of some of the areas you should consider:

- Colour scheme consistency
- Layout common conventions (navigation placement etc.)
- Responsiveness
- Contrast
- Accessibility

Useful links:

https://developer.mozilla.org/en-US/docs/Tools/Responsive_Design_Mode - Tool for testing responsiveness built into Mozilla Firefox.

https://developers.google.com/web/tools/chrome-devtools/iterate/device-mode/ - Tool for testing responsiveness built into Google Chrome/Chromium.

https://developer.mozilla.org/en-US/docs/Web/Accessibility/ARIA - Accessible Rich Internet Applications (ARIA) guidelines for making websites/web applications more accessible.

http://clrs.cc/a11y/ - Shows background/foreground pairs and their colour contrast scores.

Functionality

The website you create must functionally match the one you proposed in assignment one. Ensure you implement as much as possible of your proposal, as you will be marked on how closely your final project matches the proposal. You may add extra functionality to your website if it does not meet the requirements listed below.

Security

Your website must be reasonably secure in order to protect your users and your own website. Minimally, you must make use of HTTPS to protect your users. You should also protect your website against common attacks and vulnerabilities. Some of the attacks you should be particularly aware of include DoS and the OWASP Top 10.

DoS stands for Denial of Service, and involves typically malicious requests to your web server that take up significant resources. Either a very large number of requests all at once, or a few very resource intensive requests, which mean your service is not able to adequately serve your non-malicious users. DoS attacks are very common, and take many different forms. While DoS attacks cannot be completely prevented, there are some steps you can take to protect your websites from being easily overloaded by a DoS attack, such as rate limiting.

The OWASP Top 10 is a security project that attempts to highlight the top 10 most common vulnerabilities in web services. These vulnerabilities actively exploited frequently, and often through automated attacks. Whether you are working on a large website or a very small one, automated attacks, or indicators that your website is an easy target for a manual attack, mean that you can and likely will be attacked in some way. For a recent example of the effect this can have, in May 2016 the Commission on Elections in the Philippines was attacked through what is assumed to be an SQL Injection attack (top of the OWASP vulnerabilities list), and more than 55 million people had sensitive data leaked including names, passport numbers and addresses. Protecting against the top 10 vulnerabilities is absolutely crucial as a first step toward security.

The latest version of the OWASP Top 10 can be found here:
https://www.owasp.org/index.php/Top_10_2013-Top_10

Cloud Deployment

You must deploy your code on a cloud platform such as Microsoft Azure, Google Cloud Platform (GCP) or Amazon Web Services (AWS). Microsoft Azure is highly recommended as it provides free access to students through the Microsoft Dreamspark program. There are trials available for students on GCP and AWS, however they require you to provide credit card details.

Requirements

Module	Task	Description	Mark
Interface	UI & UX	Implementation of the interface of your website follows best practices for UI & UX including consistent colour scheme, layout etc.	2%
	Accessibility & Responsiveness	Ensure your website uses best practices for accessibility. Ensure your website works correctly on mobile and desktop browsers.	3%
Functionality	Advanced JavaScript	Include communication between the client and server using JavaScript. Make use of a Data Exchange Format such as JSON, XML or YAML. Use an external library or API. Include JavaScript advanced feature that matches proposal.	3%
	Advanced use of Server Side Language	Use of a server side language such as PHP or JSP. Include an advanced feature that matches the chosen proposal.	3%
	Database	Make use of a database that is appropriate for your dataset. Communicate with your database using the chosen server side language.	3%

Security	Security against Dos attacks	Ensure your website can be handle Dos attacks.	1%
	Security against common malicious attacks	Coverage of most vulnerabilities listed on the OWASP Top 10.	2%
Cloud Deployment	Successfully Deployed	Your project is successfully deployed and available from an instance on one of the cloud platforms.	3%

---ooo00O00ooo---