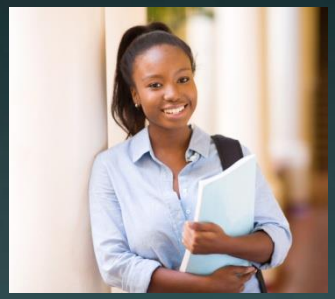
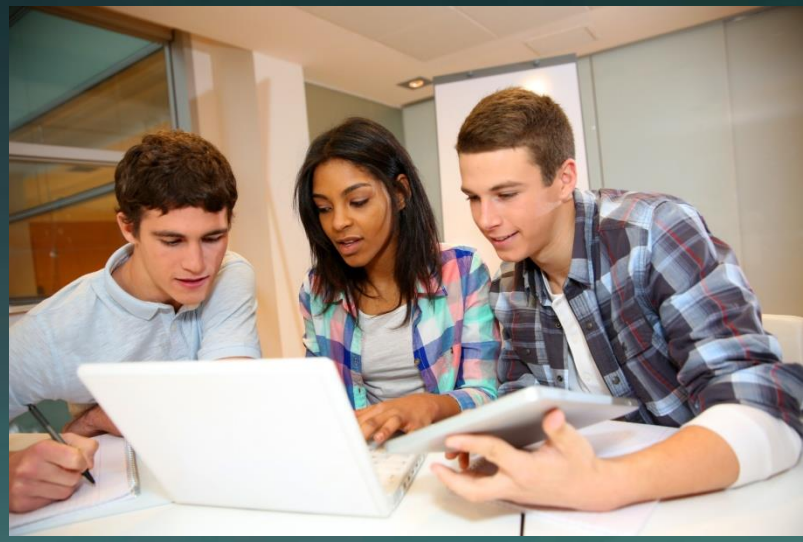
Awarding Great British Qualifications





Dynamic Websites

Topic 11:

Building A Dynamic Website

Scope and Coverage

This topic will cover:

- Building a dynamic website based on the previous lectures:
  - Analysing a real world scenario and creating a design solution
  - Integrating tools to develop a solution to the scenario
  - Consider security issues when building the solution
  - Testing the website.

Learning Outcomes

By the end of this topic students will be able to:

- Analyse a real world scenario;
- Integrate web development tools to develop a solution to the scenario (mobile website/mobile applications);
- Develop solutions to solve security issues;
- Test the website.

Introduction

- In this lecture you are provided with a real world scenario and you will practice the skills you have developed so far to bring them together to design and solve a problem for a client.
- You will integrate different web tools that we have looked at in previous lectures.
- You will understand some of the security issues with web development and test the website.

Scenario

- Stocks ’r’ Us is a stock trading site. Recently, clients have asked for a mechanism by which they can check the current value of their stock portfolios without having to call their broker. You have been commissioned to develop the site that would permit people to record their stock purchases and find their value at any given time.

Tools and Techniques

- CSS
- Semantic structure
- Responsive Design
- Mobile site
- PHP/MySQL/Ruby on Rails
- JavaScripts/jQuery/JSON
- Web development tools
- Mobile Applications
- Web services

Security Issues

- Common website vulnerabilities:
  - SQL injection
  - Malicious File Upload and Execution
  - User Authentication
  - Logging actions
- Cyber security
- SSL
- Encryption

Common Website Vulnerabilities - 1

- SQL Injection
  - User injects code into website to modify, or steal or even delete information that is stored in your database.
  - One way to overcome this is to not trust any data received from any user and validate all input.

Common Website Vulnerabilities - 2

- Malicious File Upload
  - This can occur when users are allowed to upload files.
  - Uploading a malicious file could mean that the user could gain full control of your website and maybe able to access your data.
  - One way to prevent this is to validate the files being upload

Common Website Vulnerabilities - 3

- Ensure that information is secured and whatever is displayed is restricted to users.
- Ensure that user is validated and can’t get into a protected area.
- Data can be protected through UserID and password signin or through IP address.

Common Website Vulnerabilities - 4

- Logging Actions
  - Ensure that each user has their own login details
  - Ensure that all actions are logged making users accountability of their actions
  - One way to do this is through logging the actions in a database and writing a rule which flags malicious actions for further investigation.

Cybersecurity - 1

- Cybersecurity is becoming both national and international importance.
- Cyber actors can exploit vulnerabilities to steal information and money to destroy or threaten the delivery of services eg NHS UK.
- Traditional crimes are being perpetrated through cyberspace.

Cybersecurity - 2

- Cyberspace is difficult to secure:
  - Ability of malicious actors to operate from anywhere in the world.
  - Links between cyberspace and physical systems.
  - Terrorist content and the new Global Internet Forum on Counter Terrorism.

Cybersecurity - 3

- The UK government through the National Cyber Security Strategy has identified the following measures:
  - Protected DNS
  - DMARC anti-spoofing
  - Web Check
  - Phishing and malware mitigation

Secure Socket Layer

- Secure Socket Layer protocol is technology that is used to establish a link between a server and client (web server) and browser.
- SSL allows sensitive information such as credit card information, national insurance numbers and login credentials to be transmitted securely.
- SSL secures data especially during online transactions.

Secure Socket Layer Certificate

- SSL certificates establish a secure connection.
  - SSL Certificate eg lock icon or green bar shows visitors that the connection is secure.
  - SSL Certificates have a key pair: a public and private key.
  - Keys work together to establish the encrypted connection.

Encryption

- Encryption is how a message is encoded.
- SSL encryption is essential part of ecommerce.
- RSA is the industry standard algorithm for all hardware, software and networking systems.

Adding Encryption

- If you have your own server then you can setup SSL within the server environment.
- You can use a SSL secured server provided by a web hosting company.
- The hosting company should provide a URL reference that routes the data through their secured server to a secured folder.

Scenario – Part 2

Activities to complete:

- Create a setup page for the stock portfolio.
- Create PHP to query the database.
- Create PHP for updating stock portfolio.
- Create the front-end application.
- Incorporate OpenID authentication and PHP class
- Create website for mobile devices and mobile applications
- Ensure that the website works on mobile devices.

Testing the Website

- There are different ways that the website can be tested, for example:
  - Technical Correctness;
  - Browser Compatibility;
  - Standards Compliance.

Technical Correctness

- Technical correctness is ensuring that our web applications perform the tasks they should perform correctly.
  - In this respect, it is much like creating a normal desktop application and requires formal testing.
- However, there are numerous aspects of technical correctness that are unique to web pages.
  - We must address these as part of the evalution of our web applications.

Browser Compatibility - 1

- One of the largest and most troublesome issues of ensuring a web application is technically correct is ***browser compatibility.***
  - We must be sure that it works correctly in the major browsers.
  - And ideally, some of the minor ones too.
- A web application must work correctly on at least Microsoft Edge, Firefox and Chrome, although ideally also Internet Explorer which covers 90% of the market.
  - Safari is also popular with some users.

Browser Compatibility - 2

- While most of the substance of Ajax is the same across languages, there are differences in how certain things are done.
  - There are too many to cover in this lecture, but we will talk about some of them.
- Handling of white space in XML nodes is a source of browser differences.
  - Edge/Internet Explorer ignores white space
  - Firefox and other browsers do not ignore it.

Browser Compatibilty - 3

- In addition, there are issues that are not directly related to the browser.
  - Availability of fonts
  - Monitor sizes and resolutions
  - Installed add-ones
- Different browsers render HTML with different engines.
- Different browsers handle user input differently.
  - Some automatically escape harmful input.

Browser Compatibilty - 4

- As a developer, you must be mindful of this and let your website in a range of different configurations:
  - With the major browsers
  - With different screen resolutions
  - With and without add-ons
- When you identify isssues as a result of trying a different browser, you must identify them and then correct them.
  - A subject that is worth a module of its own!

Browser Compatibilty - 5

- Some suggestions to ease this burden:
  - Use only well supported functionality.
    - Ideally functionality that is core to a particular specification.
  - Be wary of bleeding edge functionality.
    - Give it a few years to settle down.
    - A good example of this would be with the HTML 5 specifications.
  - Modularise your applications.
    - That way, finding the exact source of flaws is easier.

Standards Compliance - 1

- Good and robust communication between web applications is predicated on standards.
  - We have spoken about this already.
- However, standards are often complicated.
  - And sometimes only erractically enforced.
- We must ensure that we use set standards when creating web aplications.
  - And we must ensure that we ***comply*** with those standards.

Standards Compliance - 2

- There are many reasons why standards do not get followed properly.
  - They are ambiguous
    - Many standards have aspects that are set as being “implementation defined”.
  - They are insufficient
    - This leads to an “embrace and extend” adoption of standards which fractures the standard.
  - They are too complex
    - People end up ignoring the nuance in favour of something that is good enough.

Standards Compliance - 3

- In an effort to make standards easier for developers to work with, it is often tempting to be forviging with errors.
  - Web browsers worked like this for a long time.
- Unfortuantely, much of what makes up developing is driven by ***social proofing***.
  - We look to the prople around us to determine ow we should be acting.
  - Flawed code then becomes inspifcation for other people.

Standards Compliance - 4

- We are using many standards in our web applications.
  - It is important that we make sure that they are being used properly.
- External tools called ***validators*** can help with this.
  - They can be used to make sure that our compliance with standards is complete, and show where we are not complying with the standards.
  - http://validator.w3.org/ is one such validator that can be used to ensure compliance with standards.
  - Remember there is a one for mobile testing as well which was covered in an earlier lesson.

Ensuring Standards Compliance

- The process you go through to ensure standards compliance is as follows:
  - Use any validators you can find on your web applications.
    - Link them into the page for anyone to use.
  - Make use of DTDs or XML schemas to ensure validty of XML documents.
    - Use these to validate the XML you produce.
  - Ensure your testing browser is using the ***strict*** mode If any rendering engine it uses.
    - That way you will encounter the errors that come from sloppy syntax.

Conclusion

- Students should have created the web site linked the scenario.
- They will have gained an understanding of security vulnerabilities and how these can be overcome.
- Technical, Browser and Standards compliance testing has been introduced and students should have tested these on the website they have created.

Terminology

DNS – Domain Name Service

Secure Socket Layer – technology used to establish a secure link between a web server and browser.

Globalsign – Certificate Authorisation

References

- Validator.w3.org, 2017. [online] Available at: http://validator.w3.org/

Awarding Great British Qualifications

Topic 11 – Building a Dynamic Website

Any Questions?