BCS THE CHARTERED INSTITUTE FOR IT

BCS HIGHER EDUCATION QUALIFICATIONS
BCS Level 6 Professional Graduate Diploma in IT

March 2017

WEB ENGINEERING

EXAMINERS' REPORT

General Comments

There was a large disparity between well-prepared candidates and those who were not ready to sit this examination.

As with previous years, one comment from previous examiners' reports warrants repeating, since the Examiners continue to see answer pointers from old papers quoted verbatim in a small number of answer scripts:

"It is important for candidates to know that whilst on occasion questions may look similar to those in past papers, the context and approach is often significantly different, which means that previous answers cannot simply be restated. It is not appropriate to memorise and restate past paper answers. Additionally, the answer pointers provided here are only guidelines and should not be merely quoted by candidates but applied to the topic of the question."

Candidates should be aware that at Professional Graduate Diploma level, questions require application of knowledge rather than just restating knowledge for sake of knowledge.

Section A
Answer Section A questions in Answer Book A

A1. a) i) For each of the following three common security attacks, **briefly describe the attack**, and **outline a suitable countermeasure** that could be used to minimise risk or impact:

- *Man in the middle attack*;
- *Buffer overrun*; and
- *SQL Injection;*

(6 marks)

ii) Another risk to network security is *packet sniffing*. **Briefly describe the attack** and explain why this is a particularly important risk to **wireless networks.**

(2 marks)

iii) Users often access Internet services using other devices such as mobile phones and home video games consoles (e.g. mobile phones, tablets).

State **ONE** risk specific to accessing Internet services using *mobile phones*, and **ONE** risk specific to Internet services using *home video games consoles*.

(2 marks)

b) Some people believe that web services should not require users to log in or authenticate in any way and should instead be open for all to use.

i) With a suitable example, briefly explain why authentication may be necessary.

(1 mark)

ii) One traditional method of restricting user access to web pages is the use of `htaccess` and `htpasswd`. State **TWO** features that `htaccess` offers for restricting access to pages.

(2 marks)

iii) A company is currently using `htaccess` files to restrict access to sensitive pages, but a recent visit from an IT consultant has suggested this technique is old fashioned and insecure. Your manager would like to understand some alternatives.

Briefly explain the following three methods of authentication and provide a **drawback** of using each method.

a. Biometric data alone;
b. 2-factor authentication (not using biometric data); and
c. Personal digital certificates using public key infrastructure.

(6 marks)

c) Following a number of UK High Court judgements since 2014, large UK Internet Service Providers are obliged to restrict access to a "blacklist" of Torrent and Streaming Media sites, as well as those that may deal in counterfeit products.

Considering the above and using any other real-life examples that may support your argument, **discuss** the statement *"It is ethical for Courts of Law to restrict access to websites."* You should ensure that you present a balanced argument (considering situations when blocking access might have positive and negative consequences) and come to a clear conclusion.

(6 marks)

A1. Answer Pointers

a) i)

Man in the middle	Where a third party intercepts and relays communication between two parties (possibly altering the information), whilst the two parties believe they are communicating directly with each other.	One example is use of public key cryptography (using public certificates stored by a trusted certificate authority) that can be used to establish a secure channel between the two parties.
Buffer overrun	When a program overruns the buffer's boundary when writing data and overwrites adjacent memory locations.	Use a programming language that provides automatic protection at the language level, or perform manual bounds checking before writing data to memory.
SQL Injection	Where an attacker executes malicious SQL statements that control a web application's database, by embedding these statements in a web form's data entry fields.	Using appropriate cleansing/validation of user input to ensure input cannot be interpreted as SQL commands.

[1 mark for each based on accuracy of explanation].
Candidates should provide a credible and effective countermeasure for each [up to 1 mark for each].

ii) Packet sniffing involves examining the data being transmitted across the network, in order to compromise the confidentiality [1 mark]. This is particularly important to wireless networks because an attacker does not have to physically make a connection to the network (which might be noticeable), but can do so discreetly and from a distance, and normal physical security such as walls/doors is not necessarily an effective protection [1 mark].

iii) One example risk for mobile phones:

- These are portable devices, and so can be lost in a public area where others can find them. If the user is logged into the service when this happens, a third party could access the service using their credentials [1 mark].

One example risk for games consoles:

- Home video games consoles are often shared devices with other people in the same household, who might then have access [1 mark].

b) i) Authentication may be required when storing sensitive information, or personal settings that the service may rely on, but that you would not want other's accessing (e.g. financial or medical data), or for the use of administration functions.
[1 mark for an appropriate reason]

ii) There are many relevant features that can be used within an htaccess file. Some include:

- Restricting access via a username and password (AuthUserFile)
- Redirection to an error page upon incorrect login
- Allowing/denying access based on hostname, IP address, or referrer.
- Disabling directory listing

[1 mark for each of the two points provided. Two similar answers will not attract full marks]

iii)

Biometric data alone	A method of authentication by measuring some physical aspect of the user, and comparing it to previously known data.	Requires storage of personal data, and if compromised biometrics cannot be changed.
2-factor authentication (<u>not</u> using biometric data)	A method of authentication requiring not only a username/password, but something that the user has on them that other people cannot have access to (e.g. a key-generating device).	There may be a cost attached to issuing a physical device (unless it is something the user already has), and the system would not be usable if the item is not present.
Personal digital certificates using a public key infrastructure	A method of authentication using certificates that are issued by a certificate authority, who assure a link between the certificate and the person it is issued to. These rely on having a public certificate which is available for cryptographically verifying some data that has been signed by the private key (which only the holder should have access to).	Requires the users to have digital certificates set up in advance, which may cost money or require technical skill to set up, restricting access to the site.

[1 mark for each description and 1 mark for a relevant drawback]

c) This is a discussion question. Marks will be allocated for:

- The depth of discussion on <u>each</u> of the two sides of the discussion to be considered (i.e. positive and negative aspects) [2 marks for each aspect, based on quality of argument and supporting examples]
- The structure and completeness of the discussion overall [1 mark]
- Stating a definite answer to the question [1 mark]; this is marked on the quality of this conclusion and degree to which is supported by the main argument.

A1. Examiners' Guidance Notes

a)

i)

- Man-in-the-middle – generally well answered. Stronger Candidates drew diagrams to assist their explanation.
- Buffer overrun – generally mistaken for Denial of Service, these are not the same attack.
- SQL Injection – often omitted, and for those that answered it was generally vaguely described and missed the key aspect of malicious data input.

ii) Generally poorly described – many Candidates believed that Packet Sniffing involved modification of data.

iii) Typically omitted. Of those that answered, many could identify a risk for mobile phones, but very few candidates could identify a distinct risk for home video games consoles.

b)

i) Generally well answered, but a suitable example was often omitted.

ii) Generally omitted. Very few Candidates could provide one feature that htaccess can provide to help with restricting access to web pages.

iii)

- Biometrics – generally well answered.
- 2-factor authentication – mixed; there was a strong dichotomy between those that understood the concept and could provide a real life example, strong benefits and a drawback, but those with a poorer understanding typically could not explain any benefits or drawbacks.
- PKI – omitted by almost all candidates, and those that answered generally confused these with Website SSL certificates, when the question was asking about *personal* certificates.

c) Typically omitted, or answered very briefly. Answers tended to talk about general web content restriction, and ethical support for blocking material, but not specifically about those <u>imposed by Court Order</u> as the question asked – these did not attract much credit. There were some good identifications of cultural differences that may make for inconsistencies between jurisdictions. The evidence suggests that very few candidates appreciated that Internet services tend to cross multiple jurisdictions and there would be difficulty deciding which jurisdiction the provider and user may fall under.

A2. **a)** i) What does CSS stand for? Explain the **acronym**, and the general **purpose** of this technology.

(1 mark)

ii) List (along with a brief explanation**) THREE** distinct benefits brought by using CSS, as well as **ONE** limitation.

(4 marks)

b) Analyse the code sample in the following figure. Describe what **colour** each of the **TEN** following words will show up as, and briefly explain **why**: Australia, Bolivia, China, Denmark, Ethiopia, Finland, Germany, Honduras, India, Japan.

(5 marks)

File mystyle.css

```
 1  body > h1 { color: grey; }
```

File cssdemo.html

```
 1  <!DOCTYPE html>
 2  <html>
 3    <head>
 4      <title>My CSS Demo</title>
 5      <link rel="stylesheet" type="text/css"
href="mystyle.css">
 6      <style>
 7        h2 { color: green; }
 8        .myselector { color: blue; }
 9        div h1 { color: orange; }
10        div * { color: red; }
11        #myselector { color: yellow; }
12      </style>
13    </head>
14    <body>
15      <div style="color:purple;">
16        Australia
17        <span style="color:pink;">Bolivia</span>
18        <span>China</span>
19      </div>
20      <div>
21        <div>
22          <h3>Denmark</h3>
23          <h2 id="myselector">Ethiopia</h2>
24          <h2 class="myselector">Finland</h2>
25        </div>
26        <h1>Germany</h1>
27        <p>Honduras</p>
28      </div>
29      <h1>India</h1>
30      <h2>Japan</h2>
31    </body>
32  </html>
```

c) The British **Equality Act 2010** mandates that **reasonable adjustments** should be made (free of charge) to ensure disabled individuals can access:

- education
- employment
- housing
- goods and services (a.g. shops, banks, cinemas, hospitals, council offices, leisure centres)
- associations and private clubs

Failure to make such adjustments constitutes **unlawful discrimination**.

i) In **which circumstances** does this law apply to **websites**?

(1 mark)

ii) What **kind of adjustments** can be made?

(2 marks)

iii) How can you ensure these **requirements are met**?

(1 mark)

iv) In countries where similar laws don't exist, what could **motivate** (or discourage) web developers (and their clients) to make **similar adjustments**?

(2 marks)

d) "**Bounce rate**" is a metric used in **web traffic analysis**. It represents the percentage of visitors who enter a site and then leave ("bounce") rather than continuing on to view other pages within the same site.

An e-commerce website has recently been upgraded. Following the upgrade, the following bounce rates have been observed (broken down by web browsers):

- Chrome: 38%
- Internet Explorer: 100%
- Firefox: 29%
- Safari: 31%
- Opera: 36%
- Others: 34%

i) What do these numbers suggest?

(1 mark)

ii) How can this hypothesis be verified?

(1 mark)

iii) How could this situation have been avoided?

(1 mark)

e) Some users have been complaining your website is "too slow". What can be done to improve the situation?

(6 marks)

A2. Answer Pointers

a) i) CSS stands for Cascading Style Sheets. It can be used to describe the layout and formatting of a document written in a markup language such as HTML. [1 mark]

ii) Benefits include: (any three of the following – not an exhaustive list)
- websites are easier to maintain and update (due to the separation between content and presentation)
- Greater consistency in design (the same stylesheet can be reused on every page of a website)
- Lightweight code means faster download times (same as above)
- The same content can easily be presented differently to different viewers, e.g. PC and mobile users (separation between content and presentation)
- Greater accessibility (layout is managed without HTML tables. The resulting page can be interpreted more easily by the screen readers of visually impaired users)

[1 mark per benefit + explanation, up to 3 marks]

One of the main limitations remains differences between web browsers in term of CSS support: the same CSS may be displayed differently; some features of the language may not be supported.

Other limitations (e.g. in term of language features) are also accepted (with a concrete explanation)

[1 mark]

b)

Australia: purple	
Bolivia: pink	
China: purple	
Denmark: red	div * { color: red; }
Ethiopia: yellow	#myselector { color: yellow; }
Finland: blue	myselector { color: blue; }
Germany: orange	div h1 { color: orange; }
Honduras: black (default)	[no selector applies]
India: grey	body > h1 { color: grey; }
Japan: green	h2 { color: green; }

[0.5 mark per answer, 5 marks total]

c) i) This law applies to websites which provide access to physical goods and services (e.g. an online shop or a hotel booking system). But it also applies to websites which, in themselves, constitute a service (e.g. when they are delivering information or entertainment to the public) [1 mark]

ii) Reasonable adjustments to improve accessibility for disabled users can include:
- Providing text (e.g. through “alt” tag) to accompany non-text element (such as pictures content or graphical navigation buttons)
- Organising the content of each HTML page in a sensible order in term of readability (independently of the layout encoded in any accompanying stylesheet)

- Making sure information conveyed through colour can be inferred (or is available) without colour
- Etc. (see W3C guidelines on accessibility)

[2 marks]

iii) Whether these requirements are met can be verified through testing (e.g. against the W3C's recommendations). Automated testing tools are available (e.g. to verify standard compliance). More thorough audits can be completed by involving a wide range of actual disabled users (a number of charities and commercial firms offer such services) [1 mark]

iv) Cons: there is a cost (in term of testing and development effort) involved in following accessibility guidelines. It also requires specific expertise (which may be financially costly or unavailable). [1 marks]

Pros: it may be economically beneficial to reach a wider user base. Accessibility improvement for disabled users may also benefit other users (e.g. web crawlers), and, for instance, improve the site's ranking in search engines. It's also generally perceived as "the right thing to do" from an ethical perspective (therefore, not catering for disabled users could have negative consequences in term of business image, if the fact became widely known) [1 mark]

d) i) A bounce rate of 100% suggests the website is no longer compatible with Internet Explorer (for instance it is impossible to navigate due to a layout error or a broken menu) [1 mark]

ii) To verify this hypothesis, thorough testing should be performed using this web browser: e.g. check that all the navigation links are functional and clearly visible. [1 mark]

iii) This situation could have been avoided by testing the website internally (e.g. on a test server) before the upgrade was rolled out on the production server. [1 mark]

e) This open-ended question assesses the candidate's knowledge and problem solving skills.

To obtain full marks [up to 6 marks in total], the answer should:

- consider at least TWO hypothesis [1 mark each]
- propose a way to test each hypothesis [1 mark each]
- recommend one or more solutions in case the hypothesis is validated [1 mark each]

Candidates should try to narrow down the problem (by talking to users, or performing relevant testing) before considering a solution. E.g.:

- Are some particular pages (or other resources, e.g. images, videos) slow to load? (Check their size. Could the size be reduced, e.g. by using better compression algorithms, and/or by displaying less multimedia resources per page?)
- Do some forms take a long time to process on the server end? (check the server's processing power, and the quality of the code doing the server side processing. Could the code be optimized in term of speed, or should perhaps the server be upgraded in term of memory or CPU?)

- Is the problem more prevalent at certain times, and does this correlate with spikes in visitor numbers? (Consider load testing, and load balancing between different servers. Check if the server could be upgraded, e.g. in term of connection bandwidth)
- What is the client configuration? (type of machine and web client, type of internet connection) If the client is limited in term of memory (e.g. mobile device) or connection bandwidth, should the user be advised to upgrade their set up, or should an alternative version of our website be provided? (less computationally intensive on the client side, and requiring less bandwidth: smaller files, less frequent data transfers, etc.)

A2. Examiners' Guidance Notes

a)

i) Generally well answered.

ii) Benefit were typically well articulated, but very few were able to provide any drawbacks.

b) Generally well answered; well prepared candidates typically scored full marks, and less able candidates were typically able to understand around half the effects.

c)

i) Most candidates answered in generalities about all disabled users in all contexts and failed to make the connection with the five categories provided in the question.

ii) Generally well answered.

iii) Generally omitted or poorly answered. Some candidates made reference to legal penalties which was not the purpose of this question.

iv) Generally omitted. Of those that answered, very few were able to give convincing arguments of how these adjustments can be encouraged.

d)

i) Generally well answered, in that there is a critical problem with the web page under IE.

ii) Generally omitted.

iii) Generally omitted, or answered with a blanket statement of "use another browser", this does not solve the problem of IE users having a 100% bounce rate.

e) Candidates typically outlined one or two potential causes of slowness, but there was not generally any attempt at methodically identifying a hypothesis, proposing how this might be tested, and offering a solution. Without this (or similar) structure, the analysis is likely to be very shallow, and focus too much on factors entirely outside the control of the developers (e.g. "upgrade

browsers/internet connection"), or on broad brush solutions that may not be cost-effective and my not fix the problem (e.g. "buy more servers/bandwidth").

Section B

Answer Section B questions in Answer Book B

B3. **a)** Explain, with reference to XML, the purpose of the Document Type Definition and the Document Type Declaration.

(3 marks)

b) Explain how an XML document would call:

- an internal DTD
- an external DTD
- an XML schema

(3 marks)

c) The XML document in figure 4.2 contains precisely **FOUR** errors when validated against the DTD in figure 4.1. Identify all the errors, and provide a solution for each one.
[Note: the line numbers are for your benefit and are not part of the XML code.]

(4 marks)

d) Write an external DTD for the XML file in figure 4.3:

- The element `trainlog` may contain, in any order, one or more `session` and `progress_report` elements.
- A `session` element must first contain a `duration` element, followed by `distance` element, followed by a `location` element, followed optionally by a `comment` element, followed by zero or more `photo` elements.
- The `date` and `heartrate` attributes in `session` are optional.
- The `type` attribute in `session` must be present but allow only 3 values – running, swimming, cycling - with default set to running.
- A `photo` element must contain a `url` attribute, but may not contain any text.
- A `progress_report` element must contain one or more `comment` elements.

(15 marks)

B3. Answer pointers

a) The document type (DOCTYPE) declaration consists of an internal, or references an external Document Type Definition (DTD). It can also have a combination of both internal and external DTDs. The DTD defines the constraints on the structure of an XML document.

b) Inline Definition:

```
<?xml version="1.0"?>

<!DOCTYPE documentelement [definition]>
```

External Definition:

```
<?xml version="1.0"?>

<!DOCTYPE documentelement SYSTEM "documentelement.dtd">
```

XML schema:

```
<?xml version="1.0>

<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema">
```

c)

```
Line 5: Attribute undefined (IBSN should be ISBN)
Line 6: Undefined element type (Journal_Title should be Journal_title)
Line 7: No end tag for Journal_url
Line 7: Required attribute not specified (Jounal_url)
```

d)

```
<!DOCTYPE trainlog [
  <!ELEMENT trainlog (session | progress_report)+>
  <!ELEMENT session (duration, distance, location, comment?, photo*)>
  <!ATTLIST session
    date CDATA #IMPLIED
    type (running | swimming | cycling) "running"
    heartrate CDATA #IMPLIED>
  <!ELEMENT duration (#PCDATA)>
  <!ATTLIST duration
    units (seconds | minutes | hours) "minutes">
  <!ELEMENT distance (#PCDATA)>
  <!ATTLIST distance
    units (miles | kilometers | lengths | laps) "miles">
  <!ELEMENT location (#PCDATA)>
  <!ELEMENT comment (#PCDATA)>
  <!ELEMENT photo EMPTY>
  <!ATTLIST photo url CDATA #REQUIRED
  <!ELEMENT progress_report (comment)+>
]>
```

B3. Examiners' Guidance Notes

Most candidates were well prepared for this question and ably demonstrated the knowledge regarding the topic. There was a minority who did not know the syntax for internal and external DTD.

Most candidates had a good attempt at writing the DTD, however for some, nesting of elements and use of optional and required attributes caused problems.

B4.

a) CSS, XSLT and JavaScript can transform XML documents into HTML documents.
Briefly explain how each of the technologies achieves this.

(5 marks)

b) Textbooks for a computing course are to be stored in an XML document as shown in Figure 5.1 and an XSLT style sheet will render this as a web page as shown in Figure 5.2. Using the HTML template provided in Figure 5.3, in your answer book provide the missing code (the section marked <!-- TO BE COMPLETED -->) to accomplish this. You can assume that the textbook.css file exists and that no style code needs to be written.

(12 marks)

c) Modify the HTML template so that the book image is a link to book's website. Write in your answer book **ONLY** the code to accomplish this.

(4 marks)

d) Modify the HTML template so that the book title is a link to book's website. Write in your answer book **ONLY** the code to accomplish this.

(2marks)

e) Modify the HTML template so that the author name is an email link to author. Write in your answer book **ONLY** the code to accomplish this.

(2marks)

B4. Answer pointers

a. Identify limitations of using CSS to transform XML. Similarly for JavaScript. XSLT is more flexible. ~https://www.quora.com/How-and-why-did-CSS-beat-XML+XSLT-in-Web-UI-presentation-layers

b-d).

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<xsl:stylesheet xmlns:xsl="http://www.w3.org/1999/XSL/Transform" version="1.0">
    <xsl:template match="/">
        <html>
            <head>
                <title> Text Books</title>
                <link rel="stylesheet" type="text/css" href="textbook.css"/>
            </head>
            <body>

                <h2>Text Books by Modules </h2>
                <table border="1">
                    <xsl:for-each select="textbook/subject">
                        <tr>
                            <th colspan="3" align="center">
                                <div class="alttd">
                                    <xsl:value-of select="field"/>
                                </div>
                            </th>
                        </tr>
                        <tr bgcolor="#ffefef">
                            <th align="left">Image</th>
                            <th align="left">Book Details</th>
                            <th align="left">Tutor Comments</th>
                        </tr>
                        <xsl:for-each select="book">
                            <tr>
                                <td>
                                    <a href="{book_url/@page}" target="_self">
                                        <img>
                                            <xsl:attribute name="src">
                                                <xsl:value-of select="image/@src" />
                                            </xsl:attribute>
                                            <xsl:attribute name="width">
                                                <xsl:value-of select="image/@width" />
                                            </xsl:attribute>
                                            <xsl:attribute name="height">
                                                <xsl:value-of select="image/@height" />
                                            </xsl:attribute>
                                        </img>
                                    </a>
                                </td>
                                <td>
                                    <xsl:text>Title:</xsl:text>
                                    <br />
                                    <a href="{book_url/@page}" target="_blank">
                                        <xsl:value-of select="title"/>
                                        <br />
                                    </a>
                                    <xsl:text>Authors:</xsl:text>
                                    <br />
                                    <xsl:for-each select="author">
                                        <a href="mailto:{email}">
                                            <xsl:value-of select="name/First_name"/> 
                                            <xsl:value-of select="name/Last_name"/>
                                            <br/>
                                        </a>
                                    </xsl:for-each>
                                </td>
                                <td>
                                    <xsl:value-of select="comments"/>
                                </td>
                            </tr>
                        </xsl:for-each>
                    </xsl:for-each>
                </table>
            </body>
        </html>
    </xsl:template>
</xsl:stylesheet>
```

B4. Examiners' Guidance Notes
Some candidates were unaware that CSS and Javascript can be used to transform XML documents though in practice it is XSLT that is used.

Each part of the question was built on the previous part to better render the XML data as a web page using the images to extract the relevant information.
The use of nested for loops was at the heart of the problem with the knowledge of how to render images, email addresses and urls.

Some candidates rewrote the entire stylesheet for each and every part, when it would have been sufficient to simply write the new lines code for each part from the previous part.

There were a minority of candidates who simply wrote HTML scripts for each part using the images as a guide and did not get any marks for it – the question clearly stated this was about XSLT.

B5.

a) Internet of things (IoT) is defined as "the infrastructure of the information society." Briefly explain what this means using appropriate examples.

(5 marks)

b) What key issues will need to be addressed for IoT to be fully accepted?

(5 marks)

c) Briefly explain **virtualisation**, citing suitable examples.

(5marks)

d) A Small Medium Enterprise company is reviewing its IT requirements and is considering using a Cloud solution as opposed to investing in existing infrastructure.

You are required to make a presentation to company board outlining the potential benefits and drawbacks of both approaches.

Your answer should be in the form of a power point presentation to the client (6 slides with bullet points, no need for introductory slides, focus on the key issues). The presentation should differentiate between IaaS, PaaS and SaaS.

(10 marks)

B5. Answer pointers

a) The Internet of Things extends internet connectivity beyond traditional devices like desktop and laptop computers, smartphones and tablets to a diverse range of devices and everyday things that utilize embedded technology to communicate and interact with the external environment, all via the Internet.

b) Security and privacy – vulnerability to hacking (CIA – confidentiality, Integrity, Accessibility).

c) Virtualization software makes it possible to run multiple operating systems and multiple applications on the same server at the same time

d) Cloud computing – storing of data and applications on remote servers, and accessing them via the Internet. Inexpensive, efficient, flexible (Haas, Paas, Saas). Security and privacy. Authentication policy. In house – infrastructures costs including, hardware, software, personnel, risk mitigation, etc.

B5. Examiners' Guidance Notes

This was the least popular question. Most candidates had some knowledge of IoT but did not fully articulate and explain it.

Very few candidates were able to identify the key issues of security, privacy, etc.

Most candidates knew virtualisation to some extent but the examples cited could have been more concrete.

The final part was mainly about cloud computing and virtual hosting. Very few candidates recognised this and the quality of answers was poor.