**5Coursework Assignment Brief**

|  |  |
| --- | --- |
| **Academic year and term:** | 2021/22 – Semester-1, Year 2 |
| **Module title:** | Web Application Security |
| **Module code:** | QAC020N256S |
| **Module Convener:** | **Masum Billah** |
| **Learning outcomes assessed within this piece of work as agreed at the programme level meeting** | *On successful completion of this module students will be able to*   1. Develop dynamic web pages for practical business purposes using server-side technologies. 2. Critically evaluate and compare web server-side technologies and their deployment. 3. Identify and test common security threats associated with PHP. 4. Demonstrate implementation of usability and accessibility standards in designing of dynamic website. 5. Design and test web database systems with clear justification of the design route taken. |
| **Type of assessment:** | Design and develop Source Code, Evaluation report |
| **Assessment deadline:** | Both Design and Develop Source Code and Evaluation report should be submitted via Turnitin.  Part A submission on **29/03/2022 (no later than 4pm)**.  Part B submission on **29/04/2022** **(no later than 4pm)**.  **Specific submission requirements:** MS Word document format |
| **Kind reminder:** *it is student’s full responsibility to ensure that all assignments are submitted on the correct link and on time (before 2pm). Failure to do so may result in CAPPED Resit and/or failure of the module.* | |

**Assignment Tasks**

**Expectations:** This assignment comprises of two components: *Part A* is the design and development of a database driven website for a company (worth *60%* of the total marks of the Module), and *Part* B is an evaluation report of 1500 words consisting of reflective commentary on Part A (worth *40%* of the total marks of the Module). Both components are one piece of work and will assess all the module learning outcomes.

**Rationale:** We trust more and more inputting our personal information to websites. Although this makes our everyday lives more convenient, it also engenders more vulnerabilities because this will increase the frequency of hacking attacks and security breaches. These attacks can range from serious, large scale attacks to simple ones and from simple ones to the ridiculous and life changing incidents. *(Note: web links to most prominent web application security incidents and attacks will be posted on Moodle*). In light of those incidents and vulnerabilities, this assignment will encourage you to apply the web application security concepts and identify the web application vulnerabilities by analysing web application components such as PHP and MySQL.

**How will your work be assessed?**

Your work will be assessed by a subject expert who will use the marking grid provided in this assessment brief. When you access your marked coursework, it is important that you reflect on the feedback so that you can use it to improve future assignments.

**How will feedback be provided?**

Students will have access to formative feedback on each task set in workshops, thereby helping them to refine their approach to the summative tasks that have been set. However, please note that this feedback is limited to recommendations on improving your work. Lecturers will not confirm any grades or marks.  The feedback can be one-to-one or in-group sessions.

**Assignment support:**

Although you will be guided throughout the module by your lecturer, you can get extra support for your assignment, just make an appointment with the ACE team for any language, research and study skills issues and/or talk, email the Computing ACE expert for any advice on how to approach your assignment. *REMEMBER: they are not here to give you the answers!*

**Specific requirements for the assignment**: Adobe brackets or Sublime text-2 and HTML, CSS, JavaScript on the client-side and PHP, MySQL, Mutillidae. Alternatively, you can use a complete server-side technology (e.g –Xampp/Lampp) which includes Apache web server, PHP and MySQL.

|  |
| --- |
| **Submission instructions:**  A digital version of all assignment submissions. These must be submitted via Turnitin on the module’s Moodle site. They must be submitted as a Word file… and must not include scanned in text or text boxes. They must be submitted before 2pm on the given date  For further general details on coursework preparation refer to the online information  <https://library.roehampton.ac.uk/studytoolkit>    For further details on how to submit your work, please click on the link below.  <https://roehamptonlearning.com/eLearningServices/?p=3654> |

**Scenario**:

*Background:* The COVID-19 pandemic has changed the reality of life and has directed young generation, amongst others, to use the Internet more than ever. They view the Internet as a positive aspect in our society and a robust and effective systems of communication which play a crucial role in our daily activities and development of identities. On the other hand, the advent of the Internet and its uses are also often used negatively. Many people, as well as organisations, are the targets of cyber bullying resulting in confusion on the part of the “target”. Very often, most people are unaware that what they are going through is a form of bullying. As a result, the previously safe environment of the Internet is now becoming a source of confusion and anxiety. This rapid development has increased the cybersecurity breaches with one in four businesses detecting a breach during their last few months of operations. The nature of these attacks means that many businesses may not know their IT systems have been breached and how to handle/avoid these attacks.

***ProHunt*** is a real estate company based in London. The company deals with renting, buying and selling residential and commercial properties in the area. They are committed to providing the highest levels of customer care. The company employs two directors, two receptionists, four office administrators, two consultants, and seven field workers. To be competitive and remain at cutting edge, *ProHunt* intends to launch its business online offering one stop estate services. This new website aims to offer their customers convenience, more control and speedy signup for their services to avoid manual administrative tasks. Although the claim is to improve customer services, securing customer data and eliminating the security risks, it is obvious that it will also help the club save costs and remain financially robust.

**Task A**

Now “ProHunt” has contacted BuildTech (Leading IT Company) to go through a security check for the website to project their online presence and services. The client will also use the website as a contact tool with its customers.

You have been assigned to carry out a security analysis of your client website and backend SQL database attached to a website containing possible security vulnerabilities; your answer can make reasonable assumptions.

**Deliverables**

*The web/application security testing must include the following components:*

**Note:**

Task A is worth 60% of the overall module. The marking criteria are outlined below.

**Setup Fully Functional Vulnerable Web Application**:

* PHP
* MySQL
* Apache Server

Setup Mutillidae with all the above services enabled on XAMMP. Please provide step-by-step walk through of your implementation including setup of your backend SQL database using screen shots and appropriate description of each step.

**Web Application Security Testing:**

* Nmap scanning

Perform port scanning of web application target (Mutillidae) and elaborate each step clearly mentioning the details of open ports and its relevance to identify the running protocol.

* Wireshark Sniffing

Perform data/traffic capture on target web application (Mutillidae). Please provide the detailed analysis of captured data (Protocol identified at different TCP/IP layers).

* SQL Injection using SQLMAP

Perform SQL injection attack on Mutillidae using SQLMAP. Elaborate the findings of your attack and include the name of detected database version, database names, database compromised data etc.

**Web Application Security Model:**

* Firewalls
* IDS/IPS
* Encryption

Elaborate the use of above technology to strengthen the security of web applications and discuss integration of these as effective security mechanism.

**Marking Criteria Task A**

|  |  |
| --- | --- |
| **Description** | **Marks** |
| Develop a plan to make a fully functional website. | 10 |
| Setup a server side (PHP) vulnerable web/application connected to backend database (MySQL) for security testing in local environment either using XAMPP/WAMP or Virtual Box. Provide step-by-step configuration details of environment setup (XAMPP/WAMP, Virtual Box etc), web/application and back-end database. | 15 |
| Scanning: You must use a network scanner like Nmap to perform a scan on target web/application and include your findings, open ports, applications, operating systems, etc. | 15 |
| Sniffing: You must demonstrate the use of Wireshark sniffer to perform capture of web application session data. This will require to capture session data between your browser and website/server either remote or local. | 20 |
| Use SQLMAP to identify and exploit the SQL injection vulnerabilities based on the findings from the above steps. You must elaborate the steps of SQL Injection vulnerability exploited. | 25 |
| Design and implement an appropriate web security model for the given scenario by provisioning and utilising appropriate web security standards/technology. | 15 |
| **Total** | **100** |

**Part B: Reflection and Evaluation Report**

**Tasks:**

**Your second task is to write a self-reflective commentary about your journey from looking at website design, development, testing to deployment of techniques.**

Having created your website project, you should now write a self-reflective commentary (1500 words) *critically reflecting on* your project. Your commentary should critically explore the work you have done to produce your project using relevant literature.

Task B is worth 40% of the overall module.

**Deliverables**

Your commentary should show evidence of your reading and research and use Harvard referencing. Your reflection is a chance to look back on what you have down and to revisit key design and technical decisions you have made. In other words, were they the right decisions or would you have done something differently? Your focus should primarily be on the critical aspect of what you have done in assignment 1.

Produce a 1500-word reflective report on your project and submit it via Turnitin.

**Marking Criteria Task B**

|  |  |
| --- | --- |
| **Description** | **Marks** |
| Report Structure, Introduction, Critical appraisal and Conclusion/action plan | 20 |
| Critical evaluation and comparison of web server-side technologies | 25 |
| Critically appraise web application security threats and evaluate their impact on business operations. | 25 |
| Future enhancements with the benefit of your experience on the project. What else could you have been done to evaluate/identify web application vulnerabilities? Critical discussion on web application security tools used during the security testing. | 25 |
| Referencing and references | 5 |
| **Total** | **100** |

|  |
| --- |
| **Word count**  **Don’t exceed the word count**    You need to state the word count at the end of their assignment. 10% over the stated word count is permitted without penalty.  If students go beyond this, then there is a penalty of 5 marks for every additional 10% beyond the word count with a maximum of a 15-mark penalty reduction.    There is no specific penalty for submitting a piece which is below the word count, but please note that shorter submissions are likely to attract poorer grades, particularly where they lack the necessary depth of analysis.    Tables and figures (e.g. diagrams, graphs, photographs, etc) may be used as evidence to support academic argument. They are mostly used in report writing. However, it is important that tables and figures are used purposefully (i.e. with good reasons) and when appropriate. They should also be referenced correctly.    **How do you calculate the word count?**    The word count includes the Abstract or Executive Summary and all in-text citations. The word count does not include the Bibliography and Appendices.    *Please note that Appendices should only include supplementary information, not information critical to your work.* |

**Use of pictures/images:**

It is **mandatory** that you add the following statement to your assignment: ‘disclosure: diagrams, pictures or any other images used in this assignment are for educational purposes only’.

Although images, diagrams and photographs etc..can be used in assignments, they MUST be referenced. However, you can access the following websites (copyright-friendly):

* [Pixabay](http://pixabay.com/)

Free photos for commercial and private use - no attribution necessary. Some photos may come from other websites, such as Shutterstock, which may not fall under public domain - check each photo to ensure that it is public domain.

* [Photos Public Domain](http://www.photos-public-domain.com/)

Search public domain clip art and photos by category. All photos on this site were taken by the author and released as public domain.

* [Picdrome](http://picdrome.com/)

The Picdrome gallery is divided by categories (e.g. Abstract, Food & Drink, Nature, Technology, etc.). You may also search for specific images, but the search will take you to a custom Google search of Picdrome, which makes viewing the photos a bit more difficult.

* [Ars Publik](http://www.arspublik.com/)

Browse images under categories such as medical, advertisements, people, sports, space, etc.

* [Public Domain Images](http://www.public-domain-image.com/)

Browse by category or search for images. Varied categories; the site also includes vintage photography and space images.

* [Unsplash](https://unsplash.com/)

"All photos published on Unsplash are licensed under Creative Commons Zero which means you can copy, modify, distribute and use the photos for free, including commercial purposes, without asking permission from or providing attribution to the photographer or Unsplash."

* [Shutterography](https://www.shutterography.com/)

Free images for personal and commercial use.

*(adapted from the University of Pennsylvania:* [*https://guides.library.upenn.edu/c.php?g=475958&p=3255323*](https://guides.library.upenn.edu/c.php?g=475958&p=3255323)*)*

***Assignment Preparation and Guidelines***

* All components of the assignment (text, diagrams. code etc.) must be submitted in ….**one-word file** (hand-written text or hand drawn diagrams are not acceptable), any other accompanied materials such as simulation file, code, etc. should be attached in appendices.
* Standard and commonly used fonts such as Arial or Calibri should be used, font size must be within the range of 10 to 15 points including the headings, body text and any texts within diagrams,
* Spacing should not be less than 1.5
* Pay attention to the Assessment criteria / Marking scheme, the work is to be concise and technical. Try to analyse, compare and evaluate rather than simply describe.
* All figures, screenshots, graphs and tables must be numbered and labelled.
* Tables and figures (e.g. diagrams, graphs, photographs, etc) may be used as evidence to support academic argument. They are mostly used in report writing. However, it is important that tables and figures are used purposefully (i.e. with good reasons) and when appropriate. They should also be referenced correctly.
* Screenshots without description / discussion does not constitute understanding and maybe assumed irrelevant.
* The assignment should be logically structured, the core of the report may start by defining the problem / requirements, followed by the proposed solution including a detailed discussion, analysis and evaluation, leading to implementation and testing stage, finally a conclusion and/or personal reflection on learning.
* Please access your Turnitin Test Page via Dashboard or My modules to learn more about Turnitin and to make a test submission and to check your similarity score before uploading your final version
* You will have opportunity to submit as many times to your module pages as you want up until the deadline.
* Make sure to make backup of your work to avoid distress for loss or damage of your original work, use multiple storage media (memory stick, cloud and personal computer).
* Please note file size limitation might apply. You work must be under 50MB.

***Assignment support:***

* During the delivery of the module, you will have several opportunities to get formative feedback on your assessment during tutorials.
* Although you will be guided throughout the module by your lecturer, you can get extra support for your assignment, just make an appointment with the ACE team for any language, research and study skills issues and/or talk, email the Computing ACE expert for any advice on how to approach your assignment. REMEMBER: they are not here to give you the answers!
* Students will have access to formative feedback on each task set in workshops, thereby helping them to refine their approach to the summative tasks that have been set.
* However, please note that this feedback is limited to recommendations on improving your work. Lecturers will not confirm any grades or marks.
* The feedback can be one-to-one or in-group sessions.

***Marking and feedback process***

Between you handing in your work and then receiving your feedback and marks within 20 working days, there are a number of quality assurance processes that we go through to ensure that students receive marks which reflects their work. Please note that the summative feedback and the grades remain provisional until approval from the exam board.

A brief summary is provided below.

* **Step One** – The module and marking team meet to agree standards, expectations and how feedback will be provided.
* **Step Two** – A subject expert will mark your work using the criteria provided in the assessment brief.
* **Step Three** – A moderation meeting takes place where all members of the teaching and marking team will review the marking of others to confirm whether they agree with the mark and feedback
* **Step Four** – Work at Levels 5 and 6 then goes to an external examiner who will review a sample of work to confirm that the marking between different staff is consistent and fair
* **Step Five** – Your mark and feedback is processed by the Office and made available to you.

***Plagiarism and Collusion***

* **Academic Integrity** is a matter that is taken very seriously at the university and student should endeavour to enforce it to all their assignments. In other words, plagiarism, collusion (working and copying from another student) and ghost writing will not be tolerated and will result in sanctions eg: capped resit, suspension and/or withdrawal. Correct referencing demonstrates your academic and professional skill. It also reflects your academic honesty and thus to some degree protects you from cases of plagiarism.
* You must write your assignment in your own words to demonstrate your understanding of the subject.
* Material from external sources must be properly referenced and cited within the text using the Harvard referencing system,
* You are required to follow the**Roehampton Harvard referencing System**. Please refer to Moodle for the latest version of the **Roehampton Harvard referencing System** or ask the library.
* An accompanying list of references (on a **separate page and in alphabetical order**) must also be provided as part of your work.
* It is mandatory that you add the following statement to your assignment: ‘disclosure: diagrams, pictures or any other images used in this assignment are for educational purposes only’.
* Plagiarism: occurs when you present somebody else’s work as your own, whether that work is an idea, graphs, figure, illustration or a pure text. Be it available in web, textbooks, reports or otherwise.
* Wholesale use of text and diagrams from websites is considered as plagiarism when not acknowledged.
* Plagiarism will be dealt with firmly and can lead to serious consequences and disciplinary procedures.
* Collusion: occurs when copying another student’s report (Text, Figures, Illustration etc..) and submitting it as your own.

***Submission and Late submission***

* Students must ensure that their work is satisfactory and fit for purpose, both academically and free from any plagiarism.
* Students must use an appropriate coversheet, which must include the subject, assignment title, student ID and date-time.
* Tutors, lecturers and module convenors do not have the authority to extend the submission deadlines nor the exam time/date. In case of any mitigating circumstances, students should fill in the relevant mitigating circumstances form(s) available at qahe.uormitigatingcircumstances@qa.com
* The marking of the assignment will be capped at 40 if the assignment is submitted within first seven (7) days after the deadline, any submission late than 7 days will be ignored.
* The Submission File should be appropriate to the topic/title of the assignment and contain the Student ID, (Student ID-Assignment title)
* All coursework related material must be attached as an appendix in the final coursework/assignment document, including any computer-generated document, software/ code, simulation file etc..

***Resit submission date: TBC***

For students, who are offered a resit, you are required to improve and resubmit your original work. You must resubmit your work using the specific resit Turnitin link on Moodle. Please check the Moodle page and your emails for more information.

You should:

1. Review your previously submitted work and read carefully the feedback given by the marker.
2. Use this feedback to help you revisit and rewrite your work, improving it in the areas identified as weak in the original marking process.

If you did not submit work at the first opportunity you cannot reflect on your feedback. However, you are still required to submit your work. Please note that a non-submission will result in a Qualified-Fail. The original marking criteria will still apply, please refer to the marking criteria.

***Mitigating circumstances/what to do if you cannot submit a piece of work or attend your presentation***

The University Mitigating Circumstances Policy can be found on the University website [-](http://www.roehampton.ac.uk/uploadedFiles/Pages_Assets/PDFs_and_Word_Docs/Quality_and_Standards/Mitigat) [Mitigating Circumstances Policy](https://www.roehampton.ac.uk/globalassets/documents/corporate-information/policies/mitigating-circumstances-policy-2019.pdf). Please contact the MITIGATING CIRCUMSTANCES TEAM ON: [QAHE.uormitigatingcircumstances@qa.com](mailto:QAHE.uormitigatingcircumstances@qa.com)