COURSEWORK OVERVIEW

Module	**CMM523 Database and Web Security**
Coursework Part	All coursework for this module will be detailed in this brief (100% coursework).
Submission Method	Coursework (Word or PDF document) must be submitted electronically via the designated coursework Dropbox on CampusMoodle.
Deadline	12 April 2022 **The submission deadline is 4pm** – whilst a 30-minute grace period has been added for technical issues, you should aim to submit by 4pm.
Module Co-ordinator	Hatem Ahriz h.ahriz@rgu.ac.uk For Staff Office Hours, visit: http://campusmoodle.rgu.ac.uk/course/view.php?id=96625
LOs Assessed	1. Identify, analyse and discuss the main threats to databases and web applications. 2. Analyse and appraise the necessary countermeasures to secure databases and web applications. 3. Apply the methods and techniques used in designing secure databases and web applications. 4. Discuss the legal and ethical considerations related to data and web privacy and security.

AUXILIARY INFORMATION

Please refer to the coursework brief below for detailed information on your submission, including any software packages/versions that should be used, word counts and limits.
Coursework received after the submission deadline indicated above will be regarded as a non-submission (NS) and one of your assessment opportunities will be lost. Coursework extended due to extenuating circumstances shall be assessed in the normal way.
If the **word count** of an assessment is considered critical, then this will be reflected in the assessment criteria for that assessment together with any consequent penalties.
In line with the RGU Assessment Policy, **this coursework has been moderated** by the School of Computing Moderation Panel, which comprised a detailed technical review and panel overview to schedule staggered submissions.

ACADEMIC INTEGRITY

All work is expected to be completed by yourself, unless you have been clearly instructed to work as part of a team or group. Before submitting assignments, you should check your submission to ensure that it complies with Academic Regulation A3-2 Student Conduct Procedure and Academic Integrity, including but not limited to:

- *all material identified as originally from a previously published source has been properly attributed by the inclusion of an appropriate citation at the point of use in the text;*
- *direct quotations are marked as such (using "quotation marks" at the beginning and end of the selected text), and*
- *full details of the reference citations have been included in the list of references.*

EXTENSIONS AND DEFERRALS

The University operates a Fit to Sit Policy which means that if you undertake an assessment then you are declaring yourself well enough to do so. For information about extensions and deferrals, please familiarise yourself with the extenuating circumstances defined therein.

The aim of this coursework is to analyse, exploit and discuss the security vulnerabilities of a website. Please see Appendix A for detailed instructions on how to access this website.

Your coursework report (max 3500 words, excluding screenshots) should include the following sections:

1. **Fingerprinting/Mapping of the website**: you should investigate the web site to determine the following:
   (a) the name and version of (i) the Operating System; (ii) the Web Server; and (iii) the server-side web technology used.
   (b) the list of all the first-level directories of the website, including any hidden directories.

2. **Identifying and exploiting the website vulnerabilities**: you should identify and exploit the following four vulnerabilities:

   (a) **Stealing users' credentials** using SQL injection: Identify a place on the website that is vulnerable to SQL injection and exploit it to list the emails and (hashed) passwords of all users, using two different approaches: (i) a manual approach, by injecting code and (ii) an automatic approach, using sqlmap.

   (b) **Authentication bypass** using SQL injection: Register a new user (author) on the website, then try to sign-in that user. You will get a message saying that you need to get approved by an administrator first (before you could start posting your adventures to the website). Identify a place within the web site where you could authenticate as an admin user then "Approve" your registered user.

   (c) **File Upload**: An approved user (author) is able to post images of their adventures. However, instead of uploading an image, show that you can upload the script available from this link[1] and that you are able to successfully access that script once uploaded into the website.

   (d) **Stored XSS**: Find a place on the website that is vulnerable to Stored XSS and exploit it by injecting a pop-up box that displays your name.

For each exploited vulnerability, your report should include screenshots to evidence the steps and results of your exploits.

3. **Discussing security risks**: Assume that the website belongs to a fictional company TravelAdventures.co.uk which plans to further develop the website to provide a platform which allows registered authors to post their adventures for a fee, and receive a fee for each image bought by a customer. The architecture of such web application is shown in Figure 1.

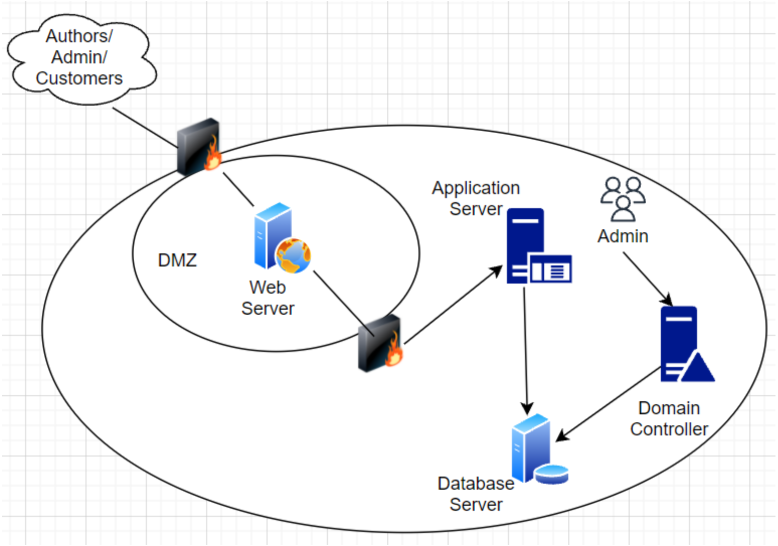


Figure 1: Architecture Diagram

[1] https://github.com/tennc/webshell/blob/master/php/b374k/source/b374k-2.8.source.php

The diagram shows that the application is accessed from both (i) the Internet (authors, customers and admin) through the web server located in the Demilitarised Zone (DMZ) and (ii) the company's internal network trough Active Directory (Domain Controller).
The company's "admin" team consists of the following staff:

- system/network administrator: manages the Windows server and the network
- database administrator (DBA) and web master: manages the database server and databases
- a sales/marketing admin: in charge of customers' orders, general marketing/sales tasks
- a web developer/webmaster: in charge of maintaining the website/web application

To allow working from home all staff can access the database server remotely. However, when in the office, staff access the database server through their Windows accounts.

Discuss potential risks to the company to be able to assess and score risks.

To help you with this task, consider the following:

- The architecture depicted in figure 1
- The way various users interact with the web application
- The various systems/technologies identified in task 1. You may want to use online resources that document publicly known vulnerabilities (e.g., the CVE database, CWE).
- The various vulnerabilities exploited in task 2.
- The webserver configuration (conf folder available on Moodle). Analyse it for any security weaknesses (5 max), compared to best practice from the literature.
- Any relevant regulations that the company needs to comply with, in particular GDPR and PCI-DSS.

4. **Discussing/Implementing security measures**: Having analysed risks in section 3, discuss the security measures that can be implemented in order to harden the security of the web application and database. As part of this task, research best practice in web server security, and describe any changes that need to be implemented in the webserver configuration (conf folder) in order to strengthen the five weaknesses identified in task 3.

Note: For task 3 and 4, please cite any resources used in your answers (See RGU Library for help with citations/referencing).

5. **Forensics of web attacks**: You are given a sample of the entries found in the webserver log file (available on Moodle) to analyse indicators of security attacks. In particular, you are expected to:
    a. Look for the following
        (i) TWO SQL Injection attacks,
        (ii) ONE Directory Traversal attacks, and
        (iii) ONE Login Brute Force Attack.
    For each attack indicate the full log entry (origin IP address; Date/Time; HTTP request made) and a description of any data that was breached.
    b. Discuss the legal and ethical implications for a company when discovering the above attacks.

Grading Grid: The following grid outlines the requirements for each grade/task:

Criteria/Grade	A Excellent	B Very Good	C Good	D Satisfactory	E Borderline Fail	F Fail
Task 1 **Fingerprinting/ Mapping**	A complete fingerprinting of the website as required. A full list of first-order directories.	As grade A but with weakness in documentation of evidence.	Mostly complete fingerprinting of the website bar one. An almost complete list of first-order directories bar one.	Mostly complete fingerprinting of the website bar one. The majority of directories is listed.	Minimal fingerprinting. Minimal enumeration of directories.	No progress with the task.
Task 2 **Exploitation**	All vulnerabilities exploited and fully documented.	As grade A but with weakness in documentation of evidence.	Three (out of 4) of vulnerabilities exploited and suitably documented.	Two (out of 4) vulnerabilities exploited and suitably documented.	Only one vulnerability exploited and documented.	No progress with the task.
Task 3 **Security Risks**	Thorough discussion of the security risks addressing all of the requirements.	Almost complete discussion of risks but with a few minor flaws.	Good discussion of risks but with several minor flaws.	Some basic discussion of risks.	A limited discussion of risks.	No progress with this task.
Task 4 **Security Measures**	A strong set of security measures fully discussed and justified. Background research evident and references well cited. Full and correct implementation of the webserver configuration security.	Strong set of security measures discussed but with very minor omissions. Background research evident. Four correct security controls correctly implemented in the webserver configuration.	Fair set of security measures proposed. Some background research evident but limited references. Three security controls correctly implemented in the webserver configuration.	Adequate set of security measures proposed. Adequate research. Two security controls correctly implemented in the webserver configuration.	Minimal set of security measures proposed. Minimal background reading is evident. Only one security control correctly implemented in the webserver configuration.	No progress with this task.
Task 5 **Forensics**	All four attacks suitably identified and documented. Full discussion of the legal and ethical implications of the attacks.	As grade A but with some weakness in documentation.	3 out of 4 attacks identified and described. Good discussion of the legal and ethical implications of the attacks.	2 out of 4 attacks identified and described. Adequate discussion of the legal and ethical implications of the attacks.	Only 1 attack identified and described. Minimal discussion of the legal and ethical implications of the attacks.	No progress with this task.

Your **overall grade** will be worked out from the 5 sub-grades obtained from the above 5 tasks.
The minimum requirement for each overall grade is as follows:

- Grade A: 4 As + 1 B
- Grade B: 4 Bs + 1 C
- Grade C: 4 Cs + 1D
- Grade D: 4 Ds + 1E
- Grade E: 5 Es
- Grade F: the set of subgrades does not qualify for any higher grade.

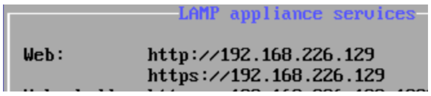
Appendix A: Instructions on accessing the Coursework Virtual Machine

A web application called TravelBlog has been set up for you as a VMWare Virtual Machine (VM). You have two options for accessing this VM:

(i) work from a School PC (the one you use for your labs), where you can find the VM under C:\VmwareVMs\CMM523\ (if in N530) or D:\VMs\CMM523\ (if in N424 or N523); **or**

(ii) download, and unzip, the VM to your own laptop from this SharePoint link. (Scroll down the page to find it). After unzipping, you should obtain a file with **ova** extension.

In VMWare Workstation Pro, open the VM file (click Retry if you get a message stating that the import has failed), then make sure that the network setting of the VM is set to “Host Only”. Once you run the VM, it will display its IP address (see below for example):



```
LAMP appliance services

Web:        http://192.168.226.129
            https://192.168.226.129
```

You can now access it using the following URL: http://192.168.226.129/TravelBlog
(simply add /TravelBlog to whatever IP address your VM displays, instead of the one shown in the example above).
You do not need to go inside the VM, so leave it alone after you have started it.