University of Glasgow | School of Computing Science

Assessed Coursework

Course Name	**Cyber Security Fundamentals (M)**			
Coursework Number	**Capture the Flag**			
Deadline	**Time:**	**00:00**	**Date:**	**See submission section**
% Contribution to final course mark	**20 %**			
Solo or Group ✓	**Solo**		**Group**	**✓**
Anticipated Hours	**20h per person**			
Submission Instructions	**See submission section**			
Please Note: This Coursework cannot be Re-Assessed				

Code of Assessment Rules for Coursework Submission

Deadlines for the submission of coursework which is to be formally assessed will be published in course documentation, and work which is submitted later than the deadline will be subject to penalty as set out below.

The primary grade and secondary band awarded for coursework which is submitted after the published deadline will be calculated as follows:

(i) in respect of work submitted not more than five working days after the deadline
   a. the work will be assessed in the usual way;
   b. the primary grade and secondary band so determined will then be reduced by two secondary bands for each working day (or part of a working day) the work was submitted late.

(ii) work submitted more than five working days after the deadline will be awarded Grade H.

Penalties for late submission of coursework will not be imposed if good cause is established for the late submission. You should submit documents supporting good cause via MyCampus.

Penalty for non-adherence to Submission Instructions is 2 bands

You must complete an "Own Work" form via https://studentltc.dcs.gla.ac.uk/ for all coursework

Capture the Flag Assessment

Assessment Overview

This assessment involves using the OWASP Vulnerable Web Application Project to formulate and execute attacks against the BodgeIt web application. The assessment includes two stages, identification of vulnerabilities and attacks, the "attack" stage, and a report describing defence mechanisms that could be employed to defend against the vulnerabilities identified.

The assessment should be completed in teams of 4 to 6 people. You should self-organise your team, details will be provided in class regarding notifying the course co-ordinator.

The vulnerabilities and corresponding attacks in the attack stage should be written in a report (described below). This stage is worth a maximum of 5% of your course grade. The defence report is worth a maximum of 15% of your course grade. Your final report and ONLY ONE submission will be the combination of your attack stage report and defence report (20%) *assessment.*

Setup

You can complete the assessment on your own machine.

Running on your own machine you will first need to install VirtualBox, software which allows you to create and run virtual machines which emulate computer systems, from the link: https://www.virtualbox.org/wiki/Downloads?replytocom=98578 From VirtualBox 5.1.12 platform packages select Windows hosts if you intend on running it on Windows and so forth. Run the installer and follow the installation instructions.

The next step is to download a Virtual Machine from the OWASP Vulnerable Web Apps project https://sourceforge.net/projects/owaspbwa/files/1.2/ Download the latest version (1.2 at the time of writing) OWASP_Broken_Web_Apps_VM_1.2.zip or OWASP_Broken_Web_Apps_VM_1.2.7z both have the same virtual machine. Unzip the contents of the file.

Follow the instructions from the lecture on creating a new VM in VirtualBox and loading the vulnerable web app VM you downloaded. Recall there is a range of VM hard disk files in the zip which you can use, select OWASP Broken Web Apps-cl1.

Configure your VM by highlighting the VM and selecting ‘settings’ then following the instructions provided in the lecture.

Select the VM and then hit ‘start’ which starts an emulation of the machine, after discarding any messages, it may take a short while to get to a screen which says, ‘Welcome to the OWASP VM’ from there you can log in using root and owaspbwa as indicated. You will then be provided with a web address which you can access from a browser and then select the web app you wish to attack (BodgeIt). You must leave the VM running in the background.

Assessment

The assessment is comprised of two stages as follows:

1. Attack Stage – BodgeIt –Vulnerabilities and Attacks Report
2. Defence Report

The vulnerabilities and attacks report result in a maximum of 5% of the course grade.
The final report contributes a maximum of 15% to your final grade.

Attack Stage

In the attack stage you should access the BodgeIt application using the setup previously described. You should then use the material taught in the course (up to and including web application security) to attempt to penetrate the vulnerable web application.

On the web site under ‘About Us’ then ‘Scoring Page’ you will find a list of challenges which you can complete. You should try all challenges as these will help you identify vulnerabilities and attacks. However, it is recognised that you may not yet be technically adept enough to complete some challenges. So you are requested to complete the first 11 challenges. Also note that challenge 'Change your password via a GET request' doesn’t necessarily correspond to a direct attack but does open a vulnerability which can be exploited by an attack not explicitly listed on the challenges. At the end of the attack stage, you should submit an attack check point report (to be included in your final report).

Defence Report

In the week commencing 31st of January, the instructions on how to install the OWASP assessment was presented. This report will give you the chance to investigate and present vulnerabilities you have identified.

This report should be **a maximum of 5 pages (exclusive of any references) using 12-point Times New Roman** and should be submitted **in pdf format** using the name final_report_<team_name>.pdf where <team_name> is replaced by your team name.
In this report the following points should be addressed:

- Briefly summarise the vulnerabilities your team discovered in the practical part of this assessment.
- What mechanisms could be employed to secure BodgeIt?
- How these mechanisms changed through the years? Are these vulnerabilities a danger?
- Why do you believe these mechanisms would prevent the vulnerabilities identified specifically for the BodgeIt application?
- Provide a brief reflection as a conclusion, describing any challenges in completing the exercise which your team faced and your team's overall experience of completing the assignment.

You must combine what you have discovered with different defence mechanisms and find solutions that can be employed.

The final report should not exceed 8 pages excluding graphs and appendices.

Marking Scheme

The marking scheme is provided below. Note that some attacks will be more difficult to locate and identifying and exploiting these attacks can result in a higher grade than identifying and exploiting lot of easily identifiable vulnerabilities. Also note that failing to adequately explain the steps taken to exploit the vulnerability will also limit the grade you can potentially achieve.

Grade	Attack Stage (5%)	Depth of understanding (10%)	Quality of Writing (5%)
A (Excellent)	A wide range of vulnerabilities were identified and corresponding attacks were successfully executed	Demonstrates deep understanding and excellent critical thought applied to establish appropriate technical solutions for an excellent range of vulnerabilities identified in the attack stage.	An excellently reasoned, coherent and logically structured report. Highly literate.
B (Very Good)	A very good range of vulnerabilities were identified and corresponding attacks were successfully executed.	Demonstrates very good understanding and critical thought applied to establish appropriate technical solutions for a very good range of vulnerabilities identified in the attack stage. There may be some instances of flaws in understanding or critical thought exist but these are minimal.	A very well-reasoned, coherent and logically structured report. Literate.
C (Good)	A good range of vulnerabilities were identified and corresponding	Demonstrates good understanding and critical thought applied to establish appropriate technical solutions for a good range of vulnerabilities identified in the attack stage. There are instances of flaws in	Moderately well organised and mostly coherent with some literacy issues.

Grade	Attack Stage (5%)	Depth of understanding (10%)	Quality of Writing (5%)
	attacks were successfully executed.	understanding or critical thought exist.	
D (Satisfactory)	Some vulnerabilities were identified and corresponding attacks were successfully executed.	Demonstrates some understanding and critical thought applied to establish appropriate technical solutions for the limited range of vulnerabilities identified in the attack stage. There may be understanding demonstrated but little critical thought or vice versa, or some combination of the two.	Adequately organised and somewhat coherent with frequent literacy issues.
E (Weak)	Very few vulnerabilities were identified and corresponding attacks were successfully executed.	Very little understanding and critical thought applied to establish appropriate technical solutions for the very limited range of vulnerabilities identified in the attack stage	Poorly organised and often incoherent with very frequent literacy issues.
F-G (Poor)	No significant attempt.	No significant attempt.	Very poor and mostly incomprehensible, no significant attempt.

Note that if the writing is poor in terms of coherence and grammar it could be very difficult to convey your understanding. It is advisable for all students to get others to read your work, even an uninformed reader – their feedback will help you identify where any issues might be. If you find yourself saying 'I meant this...' then it is likely you have not written it clearly enough.

Peer Evaluation

The overall team grade will be adjusted by deltas to represent individual contributions to the work. This will be established using a peer evaluation form. Each member of the team must submit a completed peer evaluation form (template available on Moodle). This involves allocating a total of 60 marks amongst your team. If you fail to submit this then it will be assumed, you distribute points equally between all team members

Submissions

A person should be chosen per team that will ensure the successful upload of your work. One file needs to be uploaded per team: 1) the final report including a group policy document. The group policy should state what work has been achieved per person and this should be agreed between all team members. The deltas would be uploaded individually per student as they are confidential (ONLY WHEN NECESSARY).

All submissions should be .pdf files and have the format attack_report_<team name>.pdf or final_report_<team_name>.pdf as appropriate and the documents should have the names and student numbers of the team members. Submission slots will be available on Moodle.

A summary of submissions due is shown below:

1. Final Report
2. Group policy form (attached to final report)
3. Individual peer evaluation form (only when needed)

All documents should be uploaded by 00:00 7th of March.