Softwarica College of IT & E-Commerce

ST5067CEM Web Security

Assignment Brief 2022

Module Title **Web Security**	**Ind/Group** Ind	**Cohort** March 2022	**Module Code** ST5067CEM
Coursework Title ST5067CEM Coursework Component			**Hand out date:** TBD
Module Leader Suyash Nepal			**Due date:** TBD
Estimated Time (hrs): ST4056CEM Expects 100 hours of self-study over the semester. **Word Limit***: N/A	**Coursework type:** One coursework- Security Assessment Report		**% of Module Mark** one coursework- Security Assessment Report : 100 %
Submission arrangement online via Softwarica Moodle: Upload through Softwarica LMS web portal **Mark and Feedback date:** Marks and written feedback will be given to students within three weeks of final submission **Mark and Feedback method:** All marks delivered by Moodle. Written feedback will be given via Softwarica LMS			

Module Learning Outcomes Assessed: 1. Understand and implement penetration testing methodology, and be able to communicate this with a detailed comprehensive report structure, demonstrating an understanding of the legal and ethical considerations in the context of offensive security. 2. Critically evaluate and discuss potential vulnerabilities in the digital system. 3. Critically review preparation, use and application of appropriate tools for attacks performed across multiple platforms. 4. Apply appropriate defences and countermeasures for vulnerabilities discovered and document findings in an appropriate fashion and report findings in accordance with industry standards.
Tasks and Mark distribution: a. Coursework 1- Security Assessment Report (100%) These make up 100% of the module mark.

1. **Coursework 1- Security Assessment Report (100%)**

100% of the final assessment will be done with a report around 2000 words on web application security audit

Instructions

You will need to perform security assessment of the provided web application and prepare a report on the assessment detailing the findings of the assessment.

The report should have the following structure:

1. Reconnaissance and target analysis
2. Process used (describing in detail the steps you have taken, tools you used)
3. Findings and remediation
4. Recommendation and Conclusions (this should contain evaluation of your work and also describe some alternative approaches you could have taken and generic suggestion on ensuring security of the application and its deployment)

You should submit your paper as a PDF file **formatted precisely as specified in the instructions for publication** (these instructions are available via Moodle)

Note:

The Individual Coursework is assessed by module leader that take place at the end of the semester by giving some configuration work in the Lab. Students should attend their allocated slot and can only take the at another time under exceptional circumstances with permission of their Course Director.

1. Students are encouraged to use their own user-defined data structure rather than built-in data structure of given language.
2. You are expected to use the Coventry University APA style for referencing. For support and advice on this, students can contact Centre for Academic Writing (CAW).
3. Please notify your academic services team and module leader for disability support.
4. The college cannot take responsibility for any coursework lost or corrupted on disks, laptops or personal computer. Students should therefore regularly back-up any work and are advised to save it on the cloud based services.
5. If there are technical or performance issues that prevent students submitting coursework through the online coursework submission system on the day of a coursework deadline, an appropriate extension to the coursework submission deadline will be agreed. This extension will normally be 24 hours or the next working day if the deadline falls on a Friday or over the weekend period. This will be communicated via your Module Leader.
6. Collusion between students (where sections of your work are similar to the work submitted by other students in this or previous module cohorts) is taken extremely

seriously and will be reported to the academic conduct panel. This applies to both coursework and exam answers.

7. A marked difference between your writing style, knowledge and skill level demonstrated in class discussion, any test conditions and that demonstrated in a coursework assignment may result in you having to undertake a Viva Voce in order to prove the coursework assignment is entirely your own work.
8. If you make use of the services of a proof reader in your work you must keep your original version and make it available as a demonstration of your written efforts.
9. You must not submit work for assessment that you have already submitted (partially or in full), either for your current course or for another qualification of this college, with the exception of resits, where for the coursework, you may be asked to rework and improve a previous attempt. This requirement will be specifically detailed in your assignment brief or specific course or module information. Where earlier work by you is citable, i.e., it has already been published/submitted, you must reference it clearly. Identical pieces of work submitted concurrently may also be considered to be self-plagiarism.

Learning Outcomes matrix:

Question No.	**Learning Outcomes Assessed**
Coursework 1 – Security Assessment Report	**1,2,3 and 4**

Mark allocation guideline to students

0-39	40-49	50-59	60-69	70+	80+
Work mainly incomplete and /or weaknesses in most areas	Most elements completed; weaknesses outweigh strengths	Most elements are strong, minor weaknesses	Strengths in all elements	Most work exceeds the standard expected	All work substantially exceeds the standard expected

Mark allocation guidelines to students: marking rubric for Coursework 1-Security Assessment Report (100%)

P Pass marks will be awarded for basic scanning of the targets, identifying a vulnerability and exploiting it. Report describing the above work will some analysis and recommendations but no critical evaluation. Shortcomings in the structure/presentation of the report. Good presentation and answers demonstrating understanding of the approach and tools used in the assignment.

Good marks will be awarded for comprehensive scanning and fingerprinting, identifying most security vulnerabilities, and exploiting more than one of them. Good conclusions with some critical evaluation and recommendations to secure the system. Good structure/presentation of the report and suitable references. Good presentation and answers demonstrating understanding of the approach and tools used in the assignment.

Excellent marks will be awarded for comprehensive scanning and fingerprinting, identifying all security vulnerabilities, and exploiting all of them. Able to maintain your presence on the target systems. Good conclusions with critical evaluation and recommendations to secure the system. Good structure/presentation of the report and suitable references. Excellent presentation and answers demonstrating understanding beyond the approach and tools used in the assignment.

Scanning (10) **Info gathering, scanning and fingerprinting**	**5** **Basic Scanning without appropriate analysis of the results**	**10** **Detailed scanning and analysis of the results**			
Client side (15) **Exploiting client-side vulnerabilities**	**5** **Successful exploitation of one client-side issue**	**10** **Successful exploitation of two client-side issues**	**15** **Successful exploitation of all three client-side issues**		
Server-side issues (15) **Exploiting server-side issues**	**5** **Successful exploitation of one server-side issue**	**10** **Successful exploitation of two server-side issues**	**15** **Successful exploitation of all three server-side issues**		
Reporting of findings (15)	**5** **Report with just basic details and**	**10** **Report with proper assessment of the finding with POC**	**15** **Report of findings with technical remediation steps in**		

	reproduction steps of the finding		**addition to proper assessment and POC**		
Conclusions (5) **Recommendations and conclusion**	**2** **Presenting sound conclusion of the assessment using proper evidence**	**5** **Appropriate recommendation to keep the web application secure**			
Arguments (20) (Viva and Report)	**2** **Limited understanding, no valid arguments**	**5** **Good overall analysis, but no clear arguments or conclusions**	**10** **Some valid arguments, but no clear critical thinking**	**15** **Some gaps in the arguments but good critical thinking**	**20** **Excellent arguments and critical thinking**