GUJARAT TECHNOLOGICAL UNIVERSITY

Subject Name: Application Security
Subject Code: 3725101

Semester: II

Type of course: M.E. Computer Engineering (IT systems and Network Security)

Prerequisite: Knowledge of web application development and database

Rationale: NA

Teaching and Examination Scheme:

Teaching Scheme			Credits	Examination Marks				Total Marks
L	T	P	C	Theory Marks		Practical Marks		
				ESE (E)	PA (M)	ESE (V)	PA (I)	
3	2#	0	4	70	30	30	20	150

L- Lectures; T- Tutorial/Teacher Guided Student Activity; P- Practical; C- Credit; ESE- End Semester Examination; PA- Progressive Assessment;

Content:

Sr. No.	Content	Total Hrs	% Weightage
1	**Part 1**: **MySQL** Introduction to MySQL, Installing and Configuring MySQL, Creating and Dropping Database, Queries in MySQL, Overview of Regular Expression,	11	25
2	**Part 2**: **Web Application Security** Web application Security Risks, Identifying the Application Security Risks, Threat Risk ,Modelling, OWASP Top 10	10	20
3	**Part 3: Python** Concepts of scripting language, Documenting Functions, object, Indenting Code, Testing Modules, Native Datatypes, Introducing Dictionaries , Defining Dictionaries, Modifying Dictionaries, Deleting Items From Dictionaries, Introducing Lists, Defining Lists, Adding Elements to Lists, Searching Lists, Deleting List Elements, Using List Operators, Introducing Tuples, Declaring variables, Referencing Variables, Assigning Multiple Values at Once, Formatting Strings, Mapping Lists, Joining Lists and Splitting Strings , Historical Note on String Methods, Using Optional and Named Arguments, Using type, str, dir, and Other Built-In Functions, Object References, Filtering Lists, objects and Object -Orientation, Exceptions and File Handling	11	25

Reference Books: - Dive into Python by Mark Pilgrim/ Apress
- Network Security Essentials Stallings, Stallings William.
- Head First Python by Paul Barry, Packt

Course Outcome:

After learning the course the students should be able to:

- Understand how to secure web application from intruders.
- Leak points of web application programing
- Top vulnerabilities of Web Application and Database
- Python Programing for application security testing

List of Experiments: (with Open Ended Problems)

1. Write a function translate() that will translate a text into "rövarspråket" (Swedish for "robber's language"). That is, double every consonant and place an occurrence of "o" in between. For example, translate("this is fun") should return the string "tothohisos isos fofunon".

2. Define a function overlapping() that takes two lists and returns True if they have at least one member in common, False otherwise.

3. Define a procedure histogram() that takes a list of integers and prints a histogram to the screen. For example, histogram([4, 9, 7]) should print the following:

4. Write a function find_longest_word() that takes a list of words and returns the length of the longest one.

5. Write a function filter_long_words() that takes a list of words and an integer nand returns the list of words that are longer than n.

6. Write a version of a palindrome recognizer that also accepts phrase palindromes such as "Go hang a salami I'm a lasagna hog.", "Was it a rat I saw?", "Step on no pets", "Sit on a potato pan, Otis", "Lisa Bonet ate no basil", "Satan, oscillate my metallic sonatas", "I roamed under it as a tired nude Maori", "Rise to vote sir", or the exclamation "Dammit, I'm mad!". Note that punctuation, capitalization, and spacing are usually ignored.

7. A pangram is a sentence that contains all the letters of the English alphabet at least once, for example: The quick brown fox jumps over the lazy dog. Your task here is to write a function to check a sentence to see if it is a pangram or not.

8. In cryptography, a Caesar cipher is a very simple encryption techniques in which each letter in the plain text is replaced by a letter some fixed number of positions down the alphabet. For example, with a shift of 3, A would be replaced by D, B would become E, and so on. The method is named after Julius Caesar, who used it to communicate with his generals. ROT-13 ("rotate by 13 places") is a widely used example of a Caesar cipher where the shift is 13. In Python, the key for ROT-13 may be represented by means of the following dictionary:

key =

{'a':'n', 'b':'o', 'c':'p', 'd':'q', 'e':'r', 'f':'s', 'g':'t', 'h':'u', 'i':'v', 'j':'w', 'k':

'x', 'l':'y', 'm':'z', 'n':'a', 'o':'b', 'p':'c', 'q':'d', 'r':'e', 's':'f', 't':'g', 'u':'h', '

v':'i', 'w':'j', 'x':'k', 'y':'l', 'z':'m', 'A':'N', 'B':'O', 'C':'P', 'D':'Q', 'E':'R'

, 'F':'S', 'G':'T', 'H':'U', 'I':'V', 'J':'W', 'K':'X', 'L':'Y', 'M':'Z', 'N':'A',

'O':'B', 'P':'C', 'Q':'D', 'R':'E', 'S':'F', 'T':'G', 'U':'H', 'V':'I', 'W':'J', 'X':'K

', 'Y':'L', 'Z':'M'}

Your task in this exercise is to implement an encoder/decoder of ROT-13. Once you're done, you will be able to read the following secret message: Pnrfne pvcure? V zhpu cersre Pnrfne fnynq! Note that since English has 26 characters, your ROT-13 program will be able to both encode and decode texts written in English.

9. Define a simple "spelling correction" function correct() that takes a string and sees to it that

1) two or more occurrences of the space character is compressed into one, and

2) inserts an extra space after a period if the period is directly followed by a letter.

E.g. correct("This is very funny and cool.Indeed!") should return "This is very funny and cool. Indeed!"

10. In English, the present participle is formed by adding the suffix -ing to the infinite form: go -> going. A simple set of heuristic rules can be given as follows:

• If the verb ends in e, drop the e and add ing (if not exception: be, see, flee, knee, etc.)

• If the verb ends in ie, change ie to y and add ing

• For words consisting of consonant-vowel-consonant, double the final letter before adding ing

• By default just add ing

Your task in this exercise is to define a function make_ing_form() which given a verb in infinitive form returns its present participle form. Test your function with words such as lie, see, move and hug. However, you must not expect such simple rules to work for all cases.

Major Equipment:

- VMWare-Workstation
- Linux (Kali/Fedora)
- Windows Server 2008

List of Open Source Software/learning website:

- Linux
- Apache web server
- MySql
- PHP
- HTML
- www.owasp.org

Review Presentation (RP): The concerned faculty member shall provide the list of peer reviewed Journals and Tier-I and Tier-II Conferences relating to the subject (or relating to the area of thesis for seminar) to the students in the beginning of the semester. The same list will be uploaded on GTU website during the first two weeks of the start of the semester. Every student or a group of students shall critically study 2 papers, integrate the details and make presentation in the last two weeks of the semester. The GTU marks entry portal will allow entry of marks only after uploading of the best 3 presentations. A unique id number will be generated only after uploading the presentations. Thereafter the entry of marks will be allowed. The best 3 presentations of each college will be uploaded on GTU website