PES University, Bengaluru

(Established under Karnataka Act No. 16 of 2013)

December 2018: End SEMESTER ASSESSMENT
B.TECH. VII SEMESTER ELECTIVE CSE

UE15CS421: INFORMATION SECURITY

Time: 180 Mins | Answer All Questions | Max Marks: 100

		Questions	Marks
Q1	1A	Explain one security challenge for each pillar of the CIA triad. Explain how computer security is different from functional testing.	5

Q1	1B	Consider the following piece of code. What could cause a buffer overflow? Rewrite it to make it safe.
		void main(int argc, char**argv)
		{
		charbuf[256];
		sscanf(argv[0],"%s", buf);
		}
			2

Q1	1C	Consider the following piece of code. Will this cause a buffer overflow?
		
		If no, Please explain.
		
		If yes, rewrite the code to make it safe.
		
		`int check_authentication(char *password)`
		`{`
		`int auth_flag = 0;`
		`char password_buffer[16];`
		`strcpy(password_buffer, password);`
		`if(strcmp(password_buffer, "brillig") == 0)`
		`auth_flag = 1;`
		`if(strcmp(password_buffer, "outgrabe") == 0)`
		`auth_flag = 1;`
		`return auth_flag;`
		`}`
		`int main(int argc, char *argv[])`
		`{`
		`if(argc < 2)`
		`{`
		`printf("Usage: %s <password>\n", argv[0]);`
		`exit(0);`
		`}`
		`if(check_authentication(argv[1]))`
		`{`
		`printf("\n-=-=-=-=-=-=-=-=-=-=-=-=-=-\n");`
			3

```
            printf(" Access Granted.\n");
            printf("-=-=-=-=-=-=-=-=-=-=-=-=-=-=-\n");
        }
else
        {
            printf("\nAccess Denied.\n");
        }
 }
```

	1D	What are CVE and CWE, CVSS scoring, NVD? Explain with relavant examples.	8

Q1	1E	Consider the below code snippet which demonstrates an *off-by-one* error. Can you rewrite the code to prevent the *off-by-one* error?
		
		`#include <stddef.h>`
		`void copy(size_t n, char src[n], char dest[n]) {`
		`  size_t i;`
		`  for (i = 0; src[i] && (i < n); ++i) {`
		`  dest[i] = src[i];`
		`  }`
		`  dest[i] = '\0';`
		`}`
			2

Q 2	2A	Consider the following code
		
		`1 #include <stdio.h>`
		`2 #include <stdlib.h>`
		`3`
		`4 int main(int argc, char *argv[]) {`
		`5  unsigned int i;`
		`6  unsigned int k = atoi(argv[1]);`
		`7  char *buf = malloc(k); /* 1 */`
		`8  if(buf == 0) {`
		`9  return -1;`
		`10  }`
		`11`
		`12 for(i = 0; i < k; i++) {`
		`13  buf[i] = argv[2][i]; /* 2 */`
		`14  }`
		`15`
		`16 printf("%s\n", buf); /* 3 */`
		`17`
		`18 return -1;`
		`19 }`
			5

		What is the output when this code is executed? Please explain your answer	

Q2	2B	Look at the following code snippet.
		
		You may assume that escape () argument is always non-null and points to a '\0'- terminated string.
		/*Escapes all newlines in the input string, replacing them with"\n".*/
		/* Requires: p != NULL; p is a valid '\0'-terminated string */
		
		`void escape(char *p)`
		`{`
		`  while (*p != '\0')`
		`  switch (*p)`
		`  {`
		`  case '\n':`
		`  memcpy(p+2, p+1, strlen(p));`
		`  *p++ = '\\'; *p++ = 'n';`
		`  break;`
		`  default:`
		`  p++;`
		`  }`
		`}`
		
		Name the major problem and explain three issues with this code from a security point of view?
			7

Q2	2C	Write in the secure code snippet in C langauage to perform addition of signed integer operands si_a and si_b without causing overflow regardless of their representation.	8

Q3	3A	You are hired in a software company as a software Architect /designer and you have a team of developers. Your company has won an order to develop a web application and you have asked to design the internet facing web log in page. The web log in page has to authenticate the users by their user ID and password. The system must allow legitimate uses in to the system and prevent malicious users from entering. What guidelines will you provide your developers regarding the authentication rules to meet the above conditions. Hint: A strong password policy guidelines will help improve the security of your web application.	10

Q3	3B	Consider the below code in an application: POST http://www.example.com/public/doc HTTP/1.1 Host: www.example.com User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; it; rv:1.8.1) Gecko/20061010 FireFox/2.0 Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5 Accept-Language: it-it,it;q=0.8,en-us;q=0.5,en;q=0.3 Accept-Encoding: gzip,deflate Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7 Keep-Alive: 300 Proxy-Connection: keep-alive Referer: http://127.0.0.1/WebGoat/attack?Screen=20 Cookie: JSESSIONID=295500AD2AAEEBEDC9DB86E34F24A0A5 Authorization: Basic T2Vbc1Q9Z3V2Tc3e= Content-Type: application/x-www-form-urlencoded Content-length: 33 Doc=Doc1.pdf+|+Dir c: When the above code is executed, the following result is obtained: *Exec Results for 'cmd.exe /c type "C:\httpd\public\doc\"Doc=Doc1.pdf+|+Dir c:\'* *Output...* *Il volume nell'unità C non ha etichetta.* *Numero di serie Del volume: 8E3F-4B61* *Directory of c:* *18/10/2006 00:27 2,675 Dir_Prog.txt* *18/10/2006 00:28 3,887 Dir_ProgFile.txt* *16/11/2006 10:43* *Doc* *11/11/2006 17:25*	10

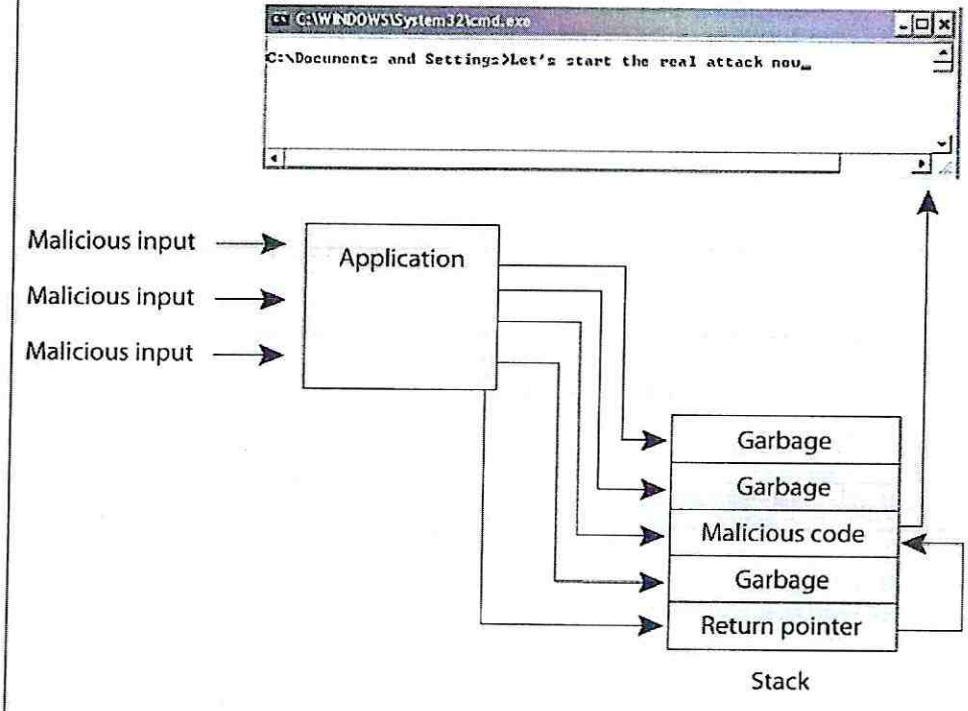
		Documents and Settings *25/10/2006 03:11* *I386* *14/11/2006 18:51* *h4ck3r* *30/09/2005 21:40 25,934* *OWASP1.JPG* *03/11/2006 18:29* *Prog* *18/11/2006 11:20* *Program Files* *16/11/2006 21:12* *Software* *24/10/2006 18:25* *Setup* *24/10/2006 23:37* *Technologies* *18/11/2006 11:14* *3 File 32,496 byte* *13 Directory* *6,921,269,248 byte disponibili* *Return code: 0* (i) What attack is the code an example of? (ii) What does the results signify? (iii) What changes, if any, would you make in the code? Explain.	

Q4	A	This question relates to Threat Modelling. For each element of the STRIDE mnemonic, • Provide the full name of the threat, • Name the property it violates E.g. Integrity • Define the threat and with an example. You may use the template below to provide your responses.	marks 6 6 8

Threat Full Name	Property Violated	Definition	Example
S			
T			
R			
I			
D			
E			

Q5		Choose the right answer	1 mark each
	1	Lisa has learned that most databases implement concurrency controls. What is concurrency, and why must it be controlled? A. Processes running at different levels, which can negatively affect the integrity of the database if not properly controlled B. The ability to deduce new information from reviewing accessible data, which can allow an inference attack to take place C. Processes running simultaneously, which can negatively affect the integrity of the database if not properly controlled D. Storing data in more than one place within a database, which can negatively affect the integrity of the database if not properly controlled	
	2	There are many types of viruses that hackers can use to damage systems. Which of the following is **NOT** a correct description of a polymorphic virus? A. Intercepts antimalware's call to the operating system for file and system information B. Varies the sequence of its instructions using noise, a mutation engine, or random-number generator C. Can use different encryption schemes requiring different decryption routines D. Produces multiple varied copies of itself	

	3	It can be very challenging for programmers to know what types of security should be built into the software that they create. The amount of vulnerabilities, threats, and risks involved with software development can seem endless. Which of the following describes the best first step for developers to take to identify the security controls that should be coded into a software project? A. Penetration testing B. Regression testing C. Threat modeling D. Attack surface analysis	
	4	Mary is creating malicious code that will steal a user's cookies by modifying the original client-side Java script. What type of cross-site scripting vulnerability is she exploiting? A. Second order B. DOM-based. Or Local cross site C. Persistent D. Non-persistent or reflected	
	5	Of the following steps that describe the development of a botnet, which best describes the step that comes first? A. Infected server sends attack commands to the botnet. B. Spammer pays a hacker for use of a botnet. C. Controller server instructs infected systems to send spam to mail servers. D. Malicious code is sent out that has bot software as its payload.	
	6	An angry former employee of the organization discovers a web form vulnerable to SQL injection. Using the injection string **SELECT * FROM Orders_Pend WHERE Location_City = 'Orlando'**, he is able to see all pending orders from Orlando. If he wanted to delete the Orders_Pend table altogether, which SQL injection string should be used? A. SELECT * FROM Orders_Pend WHERE Location_City = Orlando';DROP TABLE Orders_Pend -- B. SELECT * FROM Orders_Pend WHERE 'Orlando';DROP_TABLE -- C. DROP TABLE Orders_Pend WHERE 'Orlando = 1' -- D. WHERE Location_City = Orlando '1 = 1': DROP_TABLE --	

	7	There are several types of attacks that programmers need to be aware of. What attack does the graphic that follows illustrate? A. Traffic analysis B. Race condition C. Covert storage D. Buffer overflow 	
	8	This scenario applies for Q8 AND Q9 Trent is the new manager of his company's internal software development department. He has been told by his management that the group needs to be compliant with the international standard that provides guidance to organizations in integrating security into the processes used for managing their applications. His new boss told him that he should join and get familiar with the Open Web Application Security Project (OWASP), and Trent just received an e-mail stating that one of the company's currently deployed applications has a zero-day vulnerability. Which of the following best describes the consortium Trent's boss wants him to join?	

		A. Nonprofit organization that produces open-source software and follows widely agreed-upon best-practice security standards for the World Wide Web B. U.S. DHS group that provides best practices, tools, guidelines, rules, principles, and other resources for software developers, architects, and security practitioners to use C. Group of experts who create proprietary software tools used to help improve the security of software worldwide D. Group of experts and organizations who certify products based on an agreed-upon security criteria	
	9	Refer Scenario in Q 8. Which of the following best describes the type of vulnerability mentioned in this scenario? A. Dynamic vulnerability that is polymorphic B. Static vulnerability that is exploited by server-side injection parameters C. Vulnerability that does not currently have an associated solution D. Database vulnerability that directly affects concurrency	
	10	Cross-site scripting (XSS) is an application security vulnerability usually found in web applications. What type of XSS vulnerability occurs when a victim is tricked into opening a URL programmed with a rogue script to steal sensitive information? A. Persistent XSS vulnerability B. Nonpersistent XSS vulnerability C. Second-order vulnerability D. DOM-based vulnerability	
	11	How is interface testing different from misuse case testing? A. Interface testing is intended to determine correct function, whereas misuse case testing is intended to determine error conditions. B. Interface testing is intended to determine usability, whereas misuse case testing is intended to determine when misuse has occurred. C. Interface testing and misuse case testing are essentially the same. D. Interface testing is intended to determine correct function, whereas misuse case testing is intended to determine if an intentional misuse error condition could be problematic.	

	12	Which of the following statements is true with respect to security audits, vulnerability assessments, and penetration tests? A. Third-party security audits are only necessary when regulations require them. B. Vulnerability assessments and penetration tests are essentially the same. C. Vulnerability assessments help to prioritize weaknesses that need to be addressed. D. Internal assessments have very little value.	
	13	A web application developer is discussing security flaws discovered in a new application prior to production release. He suggests to the team that they modify the software to ensure users are not allowed to enter HTML as input into the application. Which of the following is most likely the vulnerability the developer is attempting to mitigate against? A. Cross-site scripting B. Cross-site request forgery C. Connection string parameter pollution D. Phishing	
	14	Fred is a new security officer who wants to implement a control for detecting and preventing users who attempt to exceed their authority by misusing the access rights that have been assigned to them. Which of the following best fits this need? A. Management review of existing controls B. Two-factor identification and authentication C. Capturing this data in audit logs D. Implementation of a strong security policy	
	15	John and his team are conducting a penetration test of a client's network. The team will conduct its testing armed only with knowledge it acquired from the Web. The network staff is aware that the testing will take place, but the penetration testing team will only work with publicly available data and some information from the client. What is the degree of the team's knowledge, and what type of test is the team carrying out? A. Full knowledge; blind test B. Partial knowledge; blind test C. Partial knowledge; double-blind test D. Zero knowledge; targeted test	

	16	Charlie is a new security manager at a textile company that develops its own proprietary software for internal business processes. He has found out that many of the critical applications have been developed in the C programming language and has asked for these applications to be reviewed for a specific class of security vulnerabilities. Which of the following is Charlie most likely concerned with in this situation? A. Injection attacks B. Memory block C. Buffer overflows D. Browsing attacks	
	17	Tim's development team is designing a new operating system. One of the requirements of the new product is that critical memory segments need to be categorized as nonexecutable, with the goal of reducing malicious code from being able to execute instructions in privileged mode. The team also wants to make sure that attackers will have a difficult time predicting execution target addresses. Which of the following best describes the type of technology the team should implement to increase the work effort of buffer overflow attacks? A. Address space layout randomization B. Memory induction application C. Input memory isolation D. Read-only memory integrity checks	
	18	A web application developer wishes to test a new application for security flaws. Which of the following is a method of testing input variations by using randomly generated invalid input in an attempt to crash the program? A. Insploit B. Finglonger C. Metasplation D. Fuzzing	

	19	An attacker tricks a user into visiting a malicious website via a phishing e-mail. The user clicks the e-mail link and visits the malicious website while maintaining an active, authenticated session with his bank. The attacker, through the malicious website, then instructs the user's web browser to send requests to the bank website. Which of the following best describes this attack? A. CSPP B. XSS C. CSRF D. Hidden form field	
	20	The source code of software used by your client seems to have a large number of gets() alongside sparsely used fgets(). What kind of attack is this software potentially susceptible to? A. SQL injection B. Buffer overflow C. Parameter tampering D. Cookie manipulation	