



B.TECH DEGREE EXAMINATIONS: DEC 2022

(Regulation 2018)

Seventh Semester

INFORMATION TECHNOLOGY DEPARTMENT

U18ITE005:WEB APPLICATION SECURITY

COURSE OUTCOMES

- CO1:** Explain the architecture web application architecture
CO2: Demonstrate Core Defense Mechanisms
CO3: Explain the authenticated attacking mechanism
CO4: Explain various process of attacking user
CO5: Design attacking mechanism for Native Software Vulnerabilities

Time: Three Hours

Maximum Marks: 100

**Answer all the Questions:-
 PART A (10 x 2 = 20 Marks)
 (Answer not more than 40 words)**

- | | | |
|--|-----|-------------------|
| 1. What is session management? | CO1 | [K ₂] |
| 2. What is Cross site request forgery? | CO1 | [K ₂] |
| 3. Differentiate SELECT and UPDATE statement. | CO2 | [K ₂] |
| 4. What is bypass filtering? | CO2 | [K ₂] |
| 5. What is injecting OS Commands? | CO3 | [K ₂] |
| 6. Write a short note about HTTP parameter injection. | CO3 | [K ₂] |
| 7. What is second order SQL injection? | CO4 | [K ₂] |
| 8. Write a short note about Beating signature-based filters. | CO4 | [K ₂] |
| 9. Write a short note on Test for Xpath injection. | CO5 | [K ₂] |
| 10. Give an example of the Back door passwords. | CO5 | [K ₂] |

**Answer any FIVE Questions:-
 PART B (5 x 16 = 80 Marks)
 (Answer not more than 400 words)**

- | | | |
|--|-----|-------------------|
| 11. a) Explain the following terms in detail | CO1 | [K ₂] |
| 1. Web spidering | | 8 |
| 2. User Directed spidering | | 8 |

- | | | | | | |
|-----|----|---|----|-----|------|
| 12. | a) | An application developer wants to stop an attacker from performing brute force attacks against the login function. Because the attacker may target multiple usernames, the developer decides to store the number of failed attempts in an encrypted cookie, blocking any request if the number of failed attempts exceeds five. How can this defense be bypassed? | 8 | CO2 | [K3] |
| | b) | Explain about the weakness in token generation. Also explain any two of the approaches in detail. | 8 | CO2 | [K2] |
| 13. | a) | Explain in detail about the file inclusion vulnerabilities. Also explain about the approaches used in the file inclusion with an example. | 16 | CO3 | [K3] |
| 14. | a) | With the neat diagram explain about the varieties of the XSS vulnerabilities. | 8 | CO4 | [K2] |
| | b) | When you are fuzzing a request that contains a number of different parameters, why is it important to perform requests targeting each parameter in turn and leaving the others unmodified? | 8 | CO4 | [K3] |
| 15. | a) | In detail explain about the buffer overflow technologies. Also explain about the stack and Heap overflow technologies. | 8 | CO5 | [K2] |
| | b) | The architecture components Linux, Apache, MySQL, and PHP are often found installed on the same physical server. Why can this diminish the security posture of the application's architecture? For the given case write your answer with an example. | 8 | CO5 | [K3] |
| 16. | a) | Explain the following terms with an example: | | CO3 | [K2] |
| | | a. Rolling your own insurance. | 8 | | |
| | | b. Breaking the Bank | 8 | | |
