**MODULE III & IV**

* **How do you reduce the impact of XSS vulnerabilities?**
* **What is phishing? Give an example.**
* **How can buffer overflow vulnerability be prevented?**
* **llustrate SQL injection with an example.**

A sample webpage code and associated SQL injection query.

* **Explain XSS or Cross Site Scripting**
* **Differentiate between polymorphic and metamorphic worm.**

Any two differences (2 each).



* **How Buffer OverFlow (BOF) vulnerability makes software insecure. Explain different ways in which BOF exploitations occur. (5)**

 **b) Explain XSS vulnerabilities. (4)**

* **Describe SQL injection vulnerability. (5)**

**b) How can a shell code be used for exploiting stack overflow? (4)**

* **Explain how can you detect and prevent SQL Injection vulnerabilities. (5)**

Server builds an sql query based on input from user- entering part of an sql command as an input parameter- changing semantics of original query –4 marks Prevention methods -1 mark

**b) Name any worm that exploited buffer overflow vulnerability. Explain its characteristics –**

Explain CodeRed or Slammer

Any one worm- 1 mark Characteristics- 3 marks eg CodeRed , Slammer etc

* **a) What are topological worms? Illustarte email and P2P worms. (5)**

**b) Explain Kermack-McKendrick Model of worm propagation. (4)**

* **a) Describe SQL injection vulnerability. (5)**

**b) How can a shell code be used for exploiting stack overflow? (4)**

* **a) Discuss cross site scripting vulnerabilities. (4)**

**b) Explain different worm characteristics. (5)**

* **a) How does buffer overflow vulnerability occur? How does a canary variable detect buffer overflow attack? (5)**

Occurrence of buffer overflow Significance of canary variable

**b) What is software vulnerability? What are the common types of software flaws that lead to vulnerability? (4)**

b) Definition-2 marks Listing -2 marks

* **a) Explain various Internet propagation models for worms. (6)**

**b) Explain about code red worms. (3)**

* **a) What are topological worms? Explain any 2 Topological worms. (5)**

**b) Differentiate between stored and reflected XSS (4)**