Suggested Teaching Guidelines for

Application Security & Testing–PG-DAC August 2018

Duration: 20 classroom hours + 20 lab hours **(40 hrs)**

Objective: To aware the student about issues related to web application security

Prerequisites: knowledge of web application language, MySQL and Java

Evaluation method: Theory exam– 40% weightage
Lab exam – 40% weightage
Internal exam– 20% weightage

List of Books / Other training material

Text Book: Network Security Essentials Stallings, Stallings William

Session 1:

- Web Application Security Risks
- Identifying the Application Security Risks
- Guide line for providing security for web application

Lab 1

- Different method for finding the web application vulnerability

Session 2:

- Data Extraction
- Advanced Identification/Exploitation
- Foundation of Security(Identification, Authentication, Authorization, Access Control)

Lab 2

- Email data Extraction from targeted URL
- Deleted Database data extraction
- Extracting a data from DUMP.
- Offline authentication, Mutual authentication, Message Authentication(MAC, HMAC, GMAC)

Session 3:

- Classic SDLC model
- Secure Software Development Life Cycle

Session 4:

- PKI
- Cryptographic algorithms
- Types of symmetric key and Asymmetric key algorithms
- Digital Signature, Hash function,

Suggested Teaching Guidelines for

Application Security & Testing–PG-DAC August 2018

Lab 3

- Generate certificate for SSH communication.
- Generate Digital signature for Authentication
- Deployment of Kerberos

Session 5:

- Other HTTP fields
- Injection in stored procedures
- Threat Risk Modelling
- OWASP Top 10 of 2017

Lab 4

- Broken authentication and session management
- Security Misconfiguration
- Using component with known vulnerability

Session 6:

- Threat, vulnerability and attack identification
- Injection and Inclusion

Session 7:

- Buffer Overflows and Input Validation
- Access Control

Lab 5 & 6 :

- Broken Access Control
- Sensitive Data Exposer
- Insufficient attack protection

Session 8:

- SQL, OS, XXE injection
- Cross site scripting
- Case Study On Web Application Framework

Lab 7:

- XSS
- SQL injection techniques
- Cross site request Forgery (CSRF)

Session 9:

- Web DOS attack
- Types of DOS attack

Suggested Teaching Guidelines for

Application Security & Testing–PG-DAC August 2018

- DOS and DDOS
- Attacker motivation

Lab 8:

- Identify the DOS attack and mitigation for DOS

Session 10:

- Web server Security
- Performance Testing

Lab 9 & 10:

- Build your secure application with removing all know vulnerability
- Build your website with all included authentication and authorization certificate.