GUJARAT TECHNOLOGICAL UNIVERSITY

Master of Engineering
Subject Code: 3725904
SUBJECT NAME: Web and Database Security
Semester II

Type of course: Elective

Prerequisite: Fundamentals of Web Technology & Database Management Systems

Rationale: This subject will give introduction to security aspects in web application and database systems. Students will be introduced to various types of attacks and risks to web applications and database. They will also learn how to mitigate those risks and attacks.

Teaching and Examination Scheme:

Teaching Scheme			Credits	Examination Marks						Total Marks
				Theory Marks		Practical Marks				
L	T	P	C	ESE (E)	PA (M)	ESE (V)		PA (I)		
						ESE	OEP	PA	RP	
3	0	2	4	70	30	30	0	10	10	150

Content:

Sr. No.	Content	Total Hrs	% Weightage
1	**Web Application Basics:** Introduction, HTTP Protocol, Web Functionality, Encoding Schemes, Enumerating Content and Functionality, Analyzing the Application	3	5%
2	**Authentication Security:** Authentication Techniques, Design Flaws in Authentication, Implementation Flaws in Authentication, Securing Authentication, Path Traversal Attacks	3	5%
3	**Injection Attacks:** Injecting into Interpreted Contexts, SQL Injection, NoSQL Injection, XPath Injection, LDAP Injection, XML Injection, Http Injection, Mail Service Injection	4	10%
4	**Cross Site Scripting (XSS):** Types of XSS, XSS in Real World, Finding and Exploiting XSS Vulnerabilities, Preventing XSS Attacks	4	10%
5	**User Attacks:** Inducing User Actions, Capturing Cross-Domain Data, Client-Side Injection Attacks, Local Privacy Attacks, ActiveX Control attacks, Browser Attacks	5	10%
6	**Vulnerability Analysis of Source Code:** Approaches to Code Review, Signatures of Common Vulnerabilities, Analysis of Java platform, Analysis of ASP.NET platform, Analysis of PHP, Analysis of Perl, Analysis of Javascript, Analysis of SQL	6	15%

7	**Introduction To Database Security:** Fundamental Data Security Requirements, Data Security Concerns, Compliance Mandates, Security Risks, Developing Enterprise Security Policy, Defining a Security Policy, Implementing a Security Policy, Techniques to Enforce Security	**3**	**5%**
8	**Database Access Control:** User Authentication, Protecting Passwords, Creating Fixed Database Links, Encrypting Database Link Passwords, Using Database Links Without Credentials, Using Database Links And Changing Passwords, Auditing With Database Links, Restricting A Database Link With Views, Trust Management & Negotiation	**4**	**10%**
9	**Database Security Issues:** Database Security Basics, Security Checklist, Reducing Administrative Effort, Applying Security Patches, Default Security Settings, Secure Password Support, Enforcing Password Management, Protecting The Data Dictionary, System and Object Privileges, Secure Data Outsourcing, Security in Advanced Database Systems, Managing Enterprise User Security	**6**	**15%**
10	**Framework For Database Security:** Security for Workflow Systems, Secure Semantic Web Services, Spatial Database Security, Security Reengineering, Strong Authentication, Single Sign-On, Public Key Infrastructure (PKI) Tools, Configuring SSL on the Server, Certificates, Using Kerberos for Authentication	**6**	**15%**

Reference Books:

1. "The Web Application Hacker's Handbook", Dafydd Stuttard, Wiley India Pvt. Ltd.
2. " Database Security" , S.Castano, M. Fugini, G. Martella,P. Samarati, Addision-Wesley
3. " Database Security " Alfred Basta, Melissa Zgola, Cengage Publication, 2012

Course Outcome:

Sr. No.	CO statement	Marks % weightage
CO-1	Understand the importance of security of web application and database.	15
CO-2	Launch cross site scripting attacks, forgery attack, SQL injection attack on vulnerable web application.	30
CO-3	Carry out vulnerability analysis of source code in different languages and platforms.	15
CO-4	Implement security policy for a database & Create database links.	20
CO-5	Configure SSL on Server & Use PKI tools for database security.	20

Suggested List of Experiments:

1. Reset password of Ubuntu and Cent OS (I forget the password of my machine).
2. Create the password less Authentication between 2 machines.
(a. Two Linux machine b. One window and another is Linux). Use key based authentication.

3. Set strong password policy in Linux machine for authentication perform this task in Windows machine. Prevent reusing old password. Set minimum password length. Set password complexity. Set password expiration period. Also set accounts lock out policy after 5 attempts.
4. Make a vulnerable web application
5. Launch the Cross-site Scripting Attack, Cross-Site Request Forgery Attack, and Sql injection attack on a vulnerable web application and also perform Web Tracking using web tracking technology based on Elgg based labs on Seeds lab
6. Install Game over in your VMWARE and access it through browser. Study and perform the tests given in Section 1 and 2 also prepare the report according to your understanding.
7. Install Nginx in Linux and secure it (https) by creating your own certificate. Use different keys for encryption.
8. Collect Log Events from Windows Server by using Log Parser tool.
9. How to protect WordPress from XML-RPC Attacks on Ubuntu.
10. Configure SQUID proxy server and block social websites and chat application.
11. Create on login server with 2-factor authentication. Use one pre-defined python script for this.
12. Use PSAD to detect network Intrusion on Ubuntu. And also perform Dos attack the machine by using tool (Low orbit ION Cannon/hping/slowcoris).
13. Create one WSUS server (Windows Server 2012) and fetch all the updates from this server.

Major Equipments:

The following are minimal requirements for your laptop:

- •Intel-compatible 64-bit dual-core CPU i5 or higher (a faster processor is recommended)
- •8 GB RAM (more memory is recommended)
- •60 GB of available disk space (more space is recommended)
- •USB port 2.0 or higher (USB port 3.0 is recommended)
- •Ethernet network interface card (NIC) or adapter
- •Wi-Fi card or adapter
- •Virtualization support enabled in the BIOS; this is sometimes called Intel Virtualization Technology (also known as Intel VT) or AMD-V