دوره‌های آموزشی
زمستان ۱۳۹۶

معرفی دوره آموزشی تخصصی

امنیت برنامه‌های کاربردی تحت وب

کد دوره : APA 131

۲۴ ساعت

http://cert.um.ac.ir
cert@um.ac.ir
@fum_apa

مخاطبان دوره: برنامه‌نویسان و توسعه‌دهندگان برنامه‌های کاربردی تحت وب

پیش‌نیازهای دوره: آشنایی با برنامه‌نویسی تحت وب (پیاده‌سازی‌ها به زبان PHP خواهد بود)

روش ثبت‌نام: به‌صورت الکترونیکی و از طریق وب‌گاه آزمایشگاه تخصصی آپا دانشگاه فردوسی مشهد به نشانی http://cert.um.ac.ir انجام می‌گیرد.

سرفصل دوره:

Row #	Course Syllabus (Web Application Security in PHP)
1	➢ **Description of "Web Application Architecture"** ➢ **Introducing HTTP Protocol** ➢ **Web Applications ' Main Security Problem** ➢ **Introducing Some Vulnerable Web Applications** ➢ **Introducing Some Security Testing Firefox Extensions** ➢ **Scenario** : "Tampering HTTP Requests" • HTTP Requests and Responses • HTTP Methods • HTTP Proxies • Security Related HTTP Headers ➢ **Practice: Tampering Some Headers & Fields**
2,3	➢ **Data Validation** • Data Validation Strategies • Where to Include Validation ➢ **Preventing SQL Injection Attacks in PHP** • **Scenario** : " Perform SQL Injection attacks in College Library Website" • Introduction to SQL Injection Attacks • Countermeasures Of SQL Injection ➢ **Interpreter Injection** • HTTP Injection o HTTP Response Splitting ➢ **Practice : Implement 2 Simple Login Page For "PHP Test Application" :** • vulnerable to the SQL Injection • Secure to the SQL Injection
4	➢ **Strategies For Strong Authentication in PHP** ➢ **Scenario** : " Providing An Appropriate Authentication for College Library Website " • Common Web Authentication Threats • Common Attacker Testing Authentication • Common Weak Web Authentication Strategies • Strategies For Strong Authentication in php o Strategies For Preventing Brute Force Attacks o Strategies For Preventing SQL Injection Attacks o Strategies For Check strength Of Username And Password

	➢ **Authorization** ➢ **Scenario** : " Providing An Appropriate Authorization for College Library Website " • Objectives • Authorization Strategies • Principle Of Least Privilege ○ How to Determine If Application Is Vulnerable ○ How to Protect Application • Centralized Authorization Routines • Client-Side Authorization Tokens • Access Control models ○ DAC ○ MAC ○ RBAC ➢ **Practice 1 :** Complete "PHP Test Application" Login ○ Secure To Brute Force Attacks ➢ **Practice 2 :** Implement Simple RBAC Access Control in Test Application
5,6	➢ **Preventing XSS and CSRF Attacks in PHP** ➢ **Scenario 1** : " Preventing XSS in College Library Website " ➢ **Scenario 2** : " Stealing Cookies Using XSS " • Introduce XSS attacks • Strategies for Preventing of XSS ➢ **Scenario 3** : " Testing CSRF in College Library Website " • Introduce CSRF Attacks • Strategies For Preventing Of CSRF ○ Some Weak Strategies For Preventing Of CSRF ➢ **Web Browser Security Models** • Same Origin/Domain Policy • Cookie Security Model • Flash Model Security ➢ **Clickjacking** • Introduce Clickjacking Attacks • defending against Clickjacking ➢ **Practice: Implement News Management Page For "PHP Test Application" :** • Vulnerable to XSS Attacks
7	➢ **Next Generation Web Application Attacks** • Cross-Domain Attacks • Malicious JavaScript ➢ **Malicious AJAX** ➢ **Scenario**: "Intercepting And Modifying Ajax Requests"
8	➢ **AJAX Security** • AJAX Types • AJAX Parameter Manipulation
9	➢ **Protecting Sensitive Data** ➢ **Scenario : "** Protecting Sensitive Data in College Library Website **"** • Encryption • Data Protection in Storage ○ Encryption vs. Encoding

	○ Least Privilege ○ using ORM • Data Protection in Transit • Using SSL • Channel Security vs. Token Security
10	➢ **Secure Session Management** ➢ **Scenario** : " Providing Strong Session Management in College Library Website " • Description Mechanism of Sessions and Cookies • Common Attacker Testing Session Management • Introducing Session Management Attacks ○ Session Fixation ○ Session Brute-Forcing ○ Session Hijacking ○ Session Poisoning • Strategies Of Session Storage • Strategies For Providing Secure Session Management
11	➢ **Path traversal & File Inclusion** ➢ **Scenario** : " Preventing Path traversal & File Inclusion in College Library Website " • Introducing File Uploads Threats • Countermeasure Of File Uploads Threats • Strategies Of Secure File Upload ➢ **Practice: Implement Secure File Upload in Test Application:** • Data integrity must be respected
12	➢ **Application Threat Modeling** ➢ **Introducing Sample Application " College Library Website "** ➢ **Scenario** : " Producing The Threat Model For The College Library Website " • Decompose The Application • Threat Model Information ○ External Dependencies ○ Entry Points ○ Assets ○ Trust Levels • Determine And Rank Threats ○ Threat Categorization ○ Introducing STRIDE And ASF • Security Controls • Countermeasure Identification • Mitigation Strategies ➢ **Review of Other Vulnerabilities of Web Application** • Security Missconfiguration in PHP ○ When Application Vulnerable to 'Security Misconfiguration • Invalidated Redirect and Forwards • Error handling And Logging ➢ **Introducing MVC Software Architecture** ➢ **Introducing and Comparing PHP Framworks** ○ **Introducing " Yii " PHP Framework**