3 Days Training Module
CDAC-MOHALI

Advanced Web Application Security

Introduction

- ✓ Introduction to Web Applications
- ✓ Overview of Server-Client Architecture
- ✓ Overview of IoT and IoT Cyber Attacks
- ✓ Five Phases of Penetration Testing
- ✓ Active and Passive Scanning (Against Windows/Linux)
- ✓ HTTP/S Protocol Basics
- ✓ Exploring the HTTP Request and Response
- ✓ System Reconnaissance (Windows/Linux)
- ✓ Exploring Various Web Architectures
- ✓ WHOIS and DNS Reconnaissance
- ✓ Port Scanning - Techniques and Defence Against Them
- ✓ Metasploit for Web Application Testers
- ✓ Information Gathering with Metasploit Framework
- ✓ Improper Exception Handling – For PHP, ASP.NET and Java

Pre and Post Exploitation

- ✓ Top 10 Web Application Attacks and its Remedies
- ✓ Building Your Own Hacking Environment with VirtualBox and VMWare
- ✓ Overview of SSL Related Vulnerabilities
- ✓ Authentication and Session related Vulnerabilities
- ✓ Exploitation of DVR Cameras Online – Remote Code Execution
- ✓ Remote Code Execution of OpenDreamBox Console
- ✓ Drupal 7 Exploitation with Metasploit Framework
- ✓ Joomla SQL Injection – Exploitation and Security
- ✓ WordPress XML-RPC Detection and Exploitation
- ✓ File Upload Exploitation & Security Best Practices
- ✓ Apache Tomcat – Java Struts2 – Remote Code Execution
- ✓ Practical Demonstration on Apache Struts OGNL Code Execution
- ✓ Breaking into Databases with SQL Injection and XML Injection
- ✓ Node.js Deserialization Attack
- ✓ Practical Demonstration of Host Header Attack
- ✓ Develop Secure PHP Applications with PDO Statements
- ✓ Detection and Exploitation of OpenSSL Heartbleed with Metasploit Framework
- ✓ LFI/RFI Source Code Injection Attacks
- ✓ Practical Exploitation of XSS (Reflected/Stored) in real time
- ✓ PHP CGI Argument Injection with MSF
- ✓ HTTP Put Method Exploitation with 8 Different Ways

Vulnerability Assessment and Reporting

- ✓ Introduction to Security Assessment, Analysis and Assurance
- ✓ Overview of Comprehensive Web Application Scanning
- ✓ Vulnerability Detection Methods
- ✓ Perform Enterprise Threat Modelling
- ✓ Active & Passive Reconnaissance
- ✓ Catching Input Validation and Business Logic Flaws

3 Days Training Module
CDAC-MOHALI

- ✓ Overview of Enhanced Vulnerability Scanning with Nikto and W3AF
- ✓ Creating and Navigating Vulnerability Prioritization Schemes
- ✓ Calculating Vulnerability Frequency and Severity
- ✓ Handling False Positive Results
- ✓ Introduction to Open-source and Commercial Tools
- ✓ Common Vulnerabilities and Exposure (CVE) list
- ✓ Deploying Exploit Frameworks
- ✓ Creating a Vulnerability Report
- ✓ Secure Programming Practices