राष्ट्रीय प्रौद्योगिकी संस्थान पटना / NATIONAL INSTITUE OF TECHNOLOGY PATNA
संगणक विज्ञान एंव अभियांत्रिकी विभाग / DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
अशोक राजपथ, पटना-८००००५, विहार / ASHOK RAJPATH, PATNA-800005, BIHAR
Phone No.: 0612-2372715, 2370419, 2370843, 2371929 Ext- 200, 202 Fax-0612-2670631 Website: www.nitp.ac.in

No:- Date:

CSX4213 Ethical Hacking

L-T-P-Cr: 2-0-2-3

Pre-requisites: Basics of Computer Networks, Operating System and Security

Objectives/Overview:

- to introduce the concept of ethical hacking
- to introduce the vulnerabilities in web based applications
- to introduce techniques for hacking web browsers
- to introduce SQL injection

Course Outcomes:
At the end of the course, a student should:

Sl. No	Outcome	POs
1.	Describe the vulnerabilities in a system or network.	PO1, PO2
2.	Analyze and evaluate techniques used to break into an insecure web application and identify relevant countermeasures.	PO2, PO4
3.	Evaluate the potential countermeasures to advanced hacking techniques.	PO4, PO5, PO9
4.	Explain computer forensic fundamentals	PO2, PO10, PO12

UNIT I: Session Hijacking **Lectures: 4**

Introduction to Session Hijacking, Spoofing Versus Hijacking, Types of Session Hijacking, TCP/IP Hijacking, Session Hijacking Tools, Dangers Posed by Hijacking, Countermeasures.

UNIT II: Hacking Web Servers **Lectures: 8**

Introduction to Hacking Web Servers, Sources of Security Vulnerabilities in Web Servers, Webmaster's Concern, Network Administrator's Concern, End User's Concern, Risks, Web Site Defacement, Attacks against Internet Information Services, Piggybacking Privileged Command Execution on Back-End Database Queries (MDAC/RDS), Buffer Overflow Vulnerabilities, Privileged Command Execution Vulnerability, WebDAV/RPC Exploits, IIS 7 Components, Unicode Directory Traversal Vulnerability, Netcat,

Tool: IIS Xploit, Msw3prt IPP Vulnerability, RPC DCOM Vulnerability, ASP Trojan, IIS Logs, Management, Patches and Hotfixes, Vulnerability Scanners, Online Vulnerability Search Engine, Countermeasures, File System Traversal Countermeasures, Increasing Web Server Security.

UNIT III: Web Application Vulnerabilities **Lectures: 8**

Introduction to Web Application Vulnerabilities, Web Applications, Web Application, Anatomy of an Attack, Web Application Threats, Cross-Site Scripting/XSS Flaws, SQL Injection, Command Injection Flaws, Cookie/Session Poisoning, Parameter/Form Tampering,Buffer Overflow, Directory Traversal/Forceful Browsing, Cryptographic Interception, Authentication Hijacking, Log Tampering, Error Message Interception, Attack Obfuscation, Platform Exploits, DMZ Protocol Attacks, Security Management Exploits, Web Services Attacks, Zero-Day Attacks, Network Access Attacks, TCP Fragmentation, Web Application Hacking Tools.

Tool: Instant Source, Wget, WebSleuth, BlackWidow, SiteScope, Tool: WSDigger, CookieDigger, SSLDigger, WindowBomb, Burp Intruder, Burp Proxy, Burp Suite, Tool: cURL, dotDefender, Acunetix Web Vulnerability Scanner, AppScan, AccessDiver, Tool: NetBrute Scanner Suite, Emsa Web Monitor, Tool: KeepNI, Paros Proxy, WebScarab, IBM Rational AppScan, WebWatchBot,Ratproxy, Mapper.

UNIT IV: Web-Based Password Cracking Techniques **Lectures: 8**

Introduction to Web-Based Password Cracking Techniques, Authentication, Authentication Techniques, HTTP Authentication, Integrated Windows (NTLM) Authentication, Negotiate Authentication, Certificate-Based Authentication, Forms-Based Authentication, RSA SecurID Token, Biometric Authentication, Password Cracking, Password Cracking Techniques, Password Cracker Programs, Password Cracker Countermeasures,

Tools: Password-Generating Tools, Password Recovery Tools, Password Revealing Tools, Password Security Tools.

UNIT V: Hacking Web Browsers **Lectures: 8**

Introduction to Hacking Web Browsers, How Web Browsers Work, Hacking Firefox, Firefox Information Leak Vulnerability, Firefox Spoofing Vulnerability, Firefox Password Vulnerability, Concerns with Saving Forms or Login Data, Cleaning Up Browsing History, Cookies, Cookie Viewer, Cookie Blocking Options.

Tools for Cleaning Unwanted Cookies, Firefox Security, Getting Started,Privacy Settings, Security Settings, Content Settings, Clear Private Data, Firefox Security Features, Hacking Internet Explorer, Redirection Information Disclosure Vulnerability, Window Injection Vulnerability, Internet Explorer Security, Security Zones, Privacy, Specify Default Applications, Internet Explorer Security Features.

Hacking Opera, JavaScript Invalid Pointer Vulnerability, BitTorrent Header Parsing Vulnerability, BitTorrent File-Handling Buffer Overflow Vulnerability, Opera Security and Privacy Features, Hacking Safari, Safari Browser Vulnerability, iPhone Safari Browser Memory Exhaustion Remote DoS Vulnerability, Securing Safari, AutoFill, Security Features.

UNIT VI: SQL Injection **Lectures: 6**

Introduction to SQL Injection, Exploiting Web Applications, What Attackers Look For, OLE DB Errors, Database Footprinting, Getting Data from the Database Using OLE DB Errors, How to Mine All Column Names of a Table, How to Retrieve Any Data, How to Update/Insert Data into a Database, Input Validation Attack, SQL Injection Techniques, Authorization Bypass, Using the SELECT Command, Using the INSERT Command, Using SQL Server Stored Procedures, Test for an SQL Injection Vulnerability, Example: BadLogin.aspx.cs, BadProductList.aspx.cs, SQL Injection in Oracle, SQL Injection in MySQL, Attacks Against Microsoft SQL Server, SQL Server Resolution Service (SSRS), OSQL -L Probing, SC Sweeping of Services.

Tools for Automated SQL Injection:SQLDict, SQLExec, SQLbf, SQLSmack, SQL2, AppDetective, Database Scanner, SQLPoke, NGSSQLCrack, SQLPing, Sqlmap,Sqlninja, SQLier, Automagic SQL Injector, Absinthe

Blind SQL Injection, Blind SQL Injection Countermeasures, SQL Injection Countermeasures, Preventing SQL Injection Attacks, Removing Culprit Characters/Character Sequences Minimizing, Implementing Consistent Coding Standards, Firewalling the SQL Server, Tool: SQL Block, Acunetix Web Vulnerability Scanner.

UNIT VII: Hacking Database Servers

Lectures:4

Introduction to Hacking Database Servers, Attacking Oracle, Security Issues in Oracle, Types of Database Attacks, Breaking into an Oracle Database, Oracle Worm: Voyager Beta, Hacking an SQL Server, How an SQL Server Is Hacked, Security Tools,

AppRadar, DbEncrypt, AppDetective, Oracle Selective Audit, Security Checklists, Administrator Checklist, Developer Checklist.

Text/Reference Books:

1. Ethical Hacking and Countermeasures: Web Applications and Data Servers by EC-Council.