Get Free Fluent Tutorial Injection File Read Pdf Free

Some Examples Related to Ethical Computer Networking Hacking Some Tutorials In Computer Hacking Some Tutorials in Computer Networking Hacking The Java EE 6 Tutorial Servlet and JSP Spring MVC: A Tutorial (Second Edition) The Java EE 7 Tutorial Some Tutorial In Hacking Servlet & JSP: A Tutorial, Second Edition Web Security Testing Cookbook *The Java EE 5 Tutorial* Some Tutorials in Computer Networking Hacking **Penetration Testing of Computer Networks Using BurpSuite and Various Penetration Testing Tools** *Penetration Testing of Computer Networks Using BurpSuite and Various Penetration Testing Tools* Securing Social Networks in Cyberspace **Struts 2 Design and Programming SQL Injection Attacks and Defense Software Fault Injection** PREscore Software Users Manual & Tutorial **The Ruby on Rails 3 Tutorial and Reference Collection** *SolidWorks 2014 Tutorial with Video Instruction* The Java EE 7 Tutorial **Bug Bounty Bootcamp The Book of GENESIS Proceedings of the 1st International Congress on Engineering Technologies CompTIA PenTest+ Certification All-in-One Exam Guide, Second Edition (Exam PT0-002)** *Building Next-Generation Converged Networks* **VSC-FACTS-HVDC Embedded Device Security Mastering NetBeans Introduction to Security and Network Forensics Cyberspace and Cybersecurity Mold Design Using NX 11.0: A Tutorial Approach** *The Most In-depth Hacker's Guide* Learning Website Development with Django **Learn AngularJS in 24 Hours** *Practical Poser 7* **A Tutorial on Java Socket Programming and Source Code Analysis Process Modeling in Composites Manufacturing Trace Environmental Quantitative Analysis**

This fully-updated guide delivers complete coverage of every topic on the current version of the CompTIA PenTest+ certification exam. Get complete coverage of all the objectives included on the CompTIA PenTest+ certification exam PT0-002 from this comprehensive resource. Written by expert penetration testers, the book provides learning objectives at the beginning of each chapter, hands-on exercises, exam tips, and practice questions with in-depth explanations. Designed to help you pass the exam with ease, this definitive volume also serves as an essential on-the-job reference. Covers all exam topics, including: Planning and engagement Information gathering Vulnerability scanning Network-based attacks Wireless and radio frequency attacks Web and database attacks Cloud attacks Specialized and fragile systems Social Engineering and physical attacks Post-exploitation tools and techniques Post-engagement activities Tools and code analysis And more Online content includes: 170 practice exam questions Interactive performance-based questions Test engine that provides full-length practice exams or customizable quizzes by chapter or exam objective Angular JS is responsible for making the website interactive and responsive. It helps designer and developers to eliminate much of the code usually needed for websites development. Angular JS is based upon MVC model. To learn and harness more power of the Angular JS framework, it takes a continuous intervention from an expert. But if you like to learn by yourself without spending big bucks behind expensive courses. This e-book could be your ultimate guide to AngularJS or AngularJS 2 Programming. The book covers all basic fundamentals of Angular JS like Routes, Modules, Directives, Dependency Injection and so on. The images and examples are well-illustrated addressing each and every glitch of Angular JS. The book purpose is to make Angular JS easier, simpler and interesting such that even beginners will feel like a pro at the end of the book. This edition promises your eventual mastery of AngularJS. The best thing about the book is that it is small and can be completed in a day. It will not only save your time but also accomplish our goal to save your effort in learning all needless jargons of Angular JS. With this e-book, you will be ready to create angular UI development as well as large scale applications effortlessly. Table Of Content Chapter 1: What is AngularJS? AngularJS Features AngularJS Architecture AngularJS Advantages Chapter 2: Hello World Chapter 3: Controller What Controller does from Angular's perspective How to build a basic Controller How to define Methods in Controller Using ng-controller in External Files Chapter 4: What is $Scope in AngularJS? Chapter 5: ng-repeat Directive Chapter 6: How to use ""ng-model"" The ng-model Attribute How to use ng-model Chapter 7: ng-view What is a View? ng-view Directive in AngularJS ng-view Example Chapter 8: Expressions Explain Angular.js Expressions with an example Angular.JS Numbers AngularJS Strings Angular.JS Objects AngularJS Arrays AngularJS Expression capabilities and Limitations Difference between expression and $eval Chapter 9: Filter Lowercase Uppercase Number Currency JSON Chapter 10: Custom Filter Chapter 11: Directive Chapter 12: CUSTOM Directive How to Create a Custom Directive? AngularJs Directives and Scopes Using controllers with directives How to create reusable directives AngularJS Directives and components - ng-transclude Nested directives Handling events in a directive Chapter 13: Module How to Create a module in AngularJS Modules and Controllers Chapter 14: Events The ng-click directive Showing HTML Elements using ng-show Hiding HTML Elements using ng-hide AngularJS Event Listener Directives Chapter 15: Routing with Parameters Adding Angular Route ($routeProvider) Creating a default route Accessing parameters from the route Using Angular $route service Enabling HTML5 Routing Chapter 16: AJAX Call High-level interactions with servers using $resource Low-level server interactions with $http Fetching data from a server running SQL and MySQL Chapter 17: Table Populate & Display Data in a Table AngularJS in-built Filter Sort Table with OrderBy Filter Display Table with Uppercase Filter Display the Table Index ($index) Chapter 18: Form Validation Form validation using HTML5 Form validation using $dirty, $valid, $invalid, $pristine Form validation using AngularJS Auto Validate User feedbacks with Ladda buttons Chapter 19: Form Submit Chapter 20: ng-include Client Side includes Server Side Includes How to include HTML file in AngularJS Chapter 21: Dependency Injection Which Component can be Injected as a Dependency In AngularJS Example of Dependency Injection Chapter 22: Karma Jasmine Introduction & Installation of Karma framework Testing AngularJS Controllers Testing AngularJS Directives End to End Testing AngularJS JS applications Chapter 23: Protractor Testing Why Do We Need Protractor Framework? Protractor Installation Sample AngularJS application testing using Protractor Execution of the Code Generate Reports using Jasmine Reporters SolidWorks 2014 Tutorial with video instruction is targeted towards a technical school, two year college, four year university or industry professional that is a beginner or intermediate CAD user. The text provides a student who is looking for a step-by-step project based approach to learning SolidWorks with video instruction, SolidWorks model files, and preparation for the Certified Associate - Mechanical Design (CSWA) exam. The book is divided into two sections. Chapters 1 - 5 explore the SolidWorks User Interface and CommandManager, Document and System properties, simple machine parts, simple and complex assemblies, proper design intent, design tables, configurations, multi-sheet, multi-view drawings, BOMs, Revision tables using basic and advanced features. Chapters 6 - 9 prepare you for the Certified Associate - Mechanical Design (CSWA) exam. The certification indicates a foundation in and apprentice knowledge of 3D CAD and engineering practices and principles. Follow the step-by-step instructions and develop multiple assemblies that combine over 100 extruded machined parts and components. Formulate the skills to create, modify and edit sketches and solid features. Learn the techniques to reuse features, parts and assemblies through symmetry, patterns, copied components, apply proper design intent, design tables and configurations. Learn by doing, not just by reading. Desired outcomes and usage competencies are listed for each chapter. Know your objective up front. Follow the steps in each chapter to achieve your design goals. Work between multiple documents, features, commands, custom properties and document properties that represent how engineers and designers utilize SolidWorks in industry. This first volume in the Mosharaka for Research and Studies International Conference Proceedings series (P-MIC) contains peer-reviewed papers presented at the 1st International Congress on Engineering Technologies (EngiTek 2020). This event was held remotely on 16-18 June 2020, and hosted by the Faculty of Engineering, Jordan University of Science & Technology (Irbid, Jordan). The conference represented a major forum for professors, students, and professionals from all over the world to present their latest research results, and to exchange new ideas and practical experiences in the most cutting-edge areas of the field of engineering technologies. Topics covered include electrical engineering, computer science and electronics. Burp Suite is an integrated platform/graphical tool for performing security testing of web applications. Burp suite is a java application that can be used to secure or crack web applications. The suite consists of different tools, like a proxy server, a web spider an intruder and a so-called repeater, with which requests can be automated. You can use Burp's automated and manual tools to obtain detailed information about your target applications. Damn Vulnerable Web App (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goals are to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and aid teachers/students to teach/learn web application security in a class room environment. In this report I am using a combination of Burp tools to detect and exploit vulnerabilities in Damn Vulnerable Web App (DVWA) with low security. By default, Burp Scanner scans all requests and responses that pass through the proxy. Burp lists any issues that it identifies under Issue activity on the Dashboard. You can also use Burp Scanner to actively audit for vulnerabilities. Scanner sends additional requests and analyzes the application's traffic and behavior to identify issues. Various examples are outlined in this report for different types of vulnerabilities such as: SQL injection, Cross Site Request Forgery (CSRF), Cross-site scripting, File upload, Local and Remote File Inclusion. I tested various types of penetration testing tools in order to exploit different types of vulnerabilities. The report consists from the following parts: 1. Installing and Configuring BurpSuite 2. BurpSuite Intruder. 3. Installing XMAPP and DVWA App in Windows System. 4. Installing PHP, MySQL, Apache2, Python and DVWA App in Kali Linux. 5. Scanning Kali-Linux and Windows Using . 6. Understanding Netcat, Reverse Shells and Bind Shells. 7. Adding Burps Certificate to Browser. 8. Setting up Target Scope in BurpSuite. 9. Scanning Using BurpSuite. 10. Scan results for SQL Injection Vulnerability with BurpSuite and Using SQLMAP to Exploit the SQL injection. 11. Scan Results for Operating System Command Injection Vulnerability with BurpSuite and Using Commix to Exploit the OS Command Injection. 12. Scan Results for Cross Side Scripting (XSS) Vulnerability with BurpSuite, Using Xserve to exploit XSS Injection and Stealing Web Login Session Cookies through the XSS Injection. 13. Exploiting File Upload Vulnerability. 14: Exploiting Cross Site Request Forgery (CSRF) Vulnerability. 15. Exploiting File Inclusion Vulnerability. 16. References. Servlet and JavaServer Pages (JSP) are the underlying technologies for developing web applications in Java. They are essential for any programmer to master in order to effectively use frameworks such as JavaServer Faces, Struts 2 or Spring MVC. Covering Servlet 3.1 and JSP 2.3, this book explains the important programming concepts and design models in Java web development as well as related technologies and new features in the latest versions of Servlet and JSP. With comprehensive coverage and a lot of examples, this book is a guide to building real-world applications. There is a wealth of literature on modeling and simulation of polymer composite manufacturing processes. However, existing books neglect to provide a systematic explanation of how to formulate and apply science-based models in polymer composite manufacturing processes. Process Modeling in Composites Manufacturing, Second Edition provides tangible m The objective of this work is to provide some quick tutorials in computer networking hacking. The work includes the following tutorials: Tutorial 1: Setting Up Penetrating Tutorial in Linux. Tutorial 2: Setting Up Penetrating Tutorial in Windows. Tutorial 3: OS Command Injection: Tutorial 4: Basic SQL Injection Commands. Tutorial 5: Manual SQL injection using order by and union select technique. Tutorial 6: Damping SQL Tables and Columns Using the SQL Injection. Tutorial 7: Uploading Shell in the Site having LFI. Tutorial 8: Advanced Way for Uploading Shell Tutorial 9: Uploading shell Using Sqli Command. Tutorial 10: Uploading Shell Using SQLmap Tutorial 11: Post Based SQL Injection Tutorial 12: Cracking the Hashes Using Hashcat. Tutorial 13: Hacking windows 7 and 8 through Metasploite Tutorial 14: Tutorial on Cross Site Scripting Tutorial 15: Hacking Android Mobile Using Metasploit Tutorial 16: Man of the middle attack: Tutorial 17: Using SQLmap for SQL injection Tutorial 18: Hide Your Ip Tutorial 19: Uploading Shell and Payloads Using SQLmap Tutorial 20: Using Sql Shell in SQLmap Tutorial 21: Blind SQL Injection Tutorial 22: Jack Hridoy SQL Injection Solution Tutorial 23: Using Hydra to Get the PasswordTutorial 24: Finding the phpmyadmin page using websploit. Tutorial 25: How to root the server using back connect Tutorial 25: How to root the server using back connect Tutorial 26: HTML Injection Tutorial 27: Tutuorial in manual SQl Injection Tutorial 28: Venom psh-cmd-exe payload Tutorial 29: Cross site Request Forgery (CSRF) Tutorial 30: Disable Victim Computer Tutorial 31: Exploit any firefox by xpi_bootstrapped addon Tutorial 32: Hack android mobile with metasploit Tutorial 33: PHP Code Injection to Meterpreter Session Tutorial 34: Basic google operators Tutorial 35: Hacking Credit Cards with google Tutorial 36: Finding Vulnerable Websites in Google Tutorial 37: Using the httrack to download website Tutorial 38: Getting the credit cards using sql injection and the SQLi dumper Tutorial 39: Using burp suite to brute force password Supplying a comprehensive introduction to next-generation networks, Building Next-Generation Converged Networks: Theory and Practice strikes a balance between how and why things work and how to make them work. It compiles recent advancements along with basic issues from the wide range of fields related to next generation networks. Containing the contributions of 56 industry experts and researchers from 16 different countries, the book presents relevant theoretical frameworks and the latest research. It investigates new technologies such as IPv6 over Low Power Wireless Personal Area Network (6LoWPAN) architectures, standards, mobility, and security. Presenting the material in a manner that entry-level readers can easily grasp the fundamentals, the book is organized into five parts: Multimedia Streaming—deals with multimedia streaming in networks of the future—from basics to more in-depth information for the experts Safety and Security in Networks—addresses the issues related to security, including fundamental Internet and cyber-security concepts that will be relevant in any future network Network Management and Traffic Engineering—includes coverage of mathematical modeling-based works Information Infrastructure and Cloud Computing—integrates information about past achievements, present conditions, and future expectations in information infrastructure-related areas Wireless Networking—touches on the various aspects of wireless networks and technologies The text includes coverage of Internet architectures and protocols, embedded systems and sensor networks, web services, Cloud technologies, and next-generation wireless networking. Reporting on the latest advancements in the field, it provides you with the understanding required to contribute towards the materialization of future networks. This book is suitable for graduate students, researchers, academics, industry practitioners working in the area of wired or wireless networking, and basically anyone who wants to improve his or her understanding of the topics related to next-generation networks. An authoritative reference on the new generation of VSC-FACTS and VSC-HVDC systems and their applicability within current and future power systems VSC-FACTS-HVDC and PMU: Analysis, Modelling and Simulation in Power Grids provides comprehensive coverage of VSC-FACTS and VSC-HVDC systems within the context of high-voltage Smart Grids modelling and simulation. Readers are presented with an examination of the advanced computer modelling of the VSC-FACTS and VSC-HVDC systems for steady-state, optimal solutions, state estimation and transient stability analyses, including numerous case studies for the reader to gain hands-on experience in the use of models and concepts. Key features: Wide-ranging treatment of the VSC achieved by assessing basic operating principles, topology structures, control algorithms and utility-level applications. Detailed advanced models of VSC-FACTS and VSC-HVDC equipment, suitable for a wide range of power network-wide studies, such as power flows, optimal power flows, state estimation and dynamic simulations. Contains numerous case studies and practical examples, including cases of multi-terminal VSC-HVDC systems. Includes a companion website featuring MATLAB software and Power System Computer Aided Design (PSCAD) scripts which are provided to enable the reader to gain hands-on experience. Detailed coverage of electromagnetic transient studies of VSC-FACTS and VSC-HVDC systems using the de-facto industry standard PSCAD/EMTDC simulation package. An essential guide for utility engineers, academics, and research students as well as industry managers, engineers in equipment design and manufacturing, and consultants. The objective of this work is to provide some quick tutorials in computer networking hacking. The work includes the following tutorials: · Tutorial 1: Setting Up Penetrating Tutorial in Linux. · Tutorial 2: Setting Up Penetrating Tutorial in Windows. · Tutorial 3: OS Command Injection: · Tutorial 4: Basic SQL Injection Commands. · Tutorial 5: Manual SQL injection using order by and union

select technique. · Tutorial 6: Damping SQL Tables and Columns Using the SQL Injection. · Tutorial 7: Uploading Shell in the Site having LFI. · Tutorial 8: Advanced Way for Uploading Shell · Tutorial 9: Uploading shell Using Sqli Command. · Tutorial 10: Uploading Shell Using SQLmap · Tutorial 11: Post Based SQL Injection · Tutorial 12: Cracking the Hashes Using Hashcat. · Tutorial 13: Hacking windows 7 and 8 through Metasploite · Tutorial 14: Tutorial on Cross Site Scripting · Tutorial 15: Hacking Android Mobile Using Metasploit · Tutorial 16: Man of the middle attack: · Tutorial 17: Using SQLmap for SQL injection · Tutorial 18: Hide Your Ip · Tutorial 19: Uploading Shell and Payloads Using SQLmap · Tutorial 20: Using Sql Shell in SQLmap · Tutorial 21: Blind SQL Injection · Tutorial 22: Jack Hridoy SQL Injection Solution · Tutorial 23: Using Hydra to Get the PasswordTutorial 24: Finding the phpmyadmin page using websploit. · Tutorial 25: How to root the server using back connect · Tutorial 25: How to root the server using back connect · Tutorial 26: HTML Injection · Tutorial 27: Tutuorial in manual SQl Injection · Tutorial 28: Venom psh-cmd-exe payload · Tutorial 29: Cross site Request Forgery (CSRF) · Tutorial 30: Disable Victim Computer · Tutorial 31: Exploit any firefox by xpi_bootstrapped addon · Tutorial 32: Hack android mobile with metasploit · Tutorial 33: PHP Code Injection to Meterpreter Session · Tutorial 34: Basic google operators · Tutorial 35: Hacking Credit Cards with google · Tutorial 36: Finding Vulnerable Websites in Google · Tutorial 37: Using the httrack to download website · Tutorial 38: Getting the credit cards using sql injection and the SQLi dumper · Tutorial 39: Using burp suite to brute force password This book collates the key security and privacy concerns faced by individuals and organizations who use various social networking sites. This includes activities such as connecting with friends, colleagues, and family; sharing and posting information; managing audio, video, and photos; and all other aspects of using social media sites both professionally and personally. In the setting of the Internet of Things (IoT) that can connect millions of devices at any one time, the security of such actions is paramount. Securing Social Networks in Cyberspace discusses user privacy and trust, location privacy, protecting children, managing multimedia content, cyberbullying, and much more. Current state-of-the-art defense mechanisms that can bring long-term solutions to tackling these threats are considered in the book. This book can be used as a reference for an easy understanding of complex cybersecurity issues in social networking platforms and services. It is beneficial for academicians and graduate-level researchers. General readers may find it beneficial in protecting their social-media-related profiles. Providing comprehensive coverage of cyberspace and cybersecurity, this textbook not only focuses on technologies but also explores human factors and organizational perspectives and emphasizes why asset identification should be the cornerstone of any information security strategy. Topics include addressing vulnerabilities, building a secure enterprise, blocking intrusions, ethical and legal issues, and business continuity. Updates include topics such as cyber risks in mobile telephony, steganography, cybersecurity as an added value, ransomware defense, review of recent cyber laws, new types of cybercrime, plus new chapters on digital currencies and encryption key management. This introduction to the fastest growing part of Java platform, gives clear explanations and examples of the essential topics - JSP's, servlets, JDBC and EJB. The objective of this work is to provide some quick tutorials in computer networking hacking. The work includes the following tutorials: Tutorial 1: Setting Up Penetrating Tutorial in Linux. Tutorial 2: Setting Up Penetrating Tutorial in Windows. Tutorial 3: OS Command Injection: Tutorial 4: Basic SQL Injection Commands. Tutorial 5: Manual SQL injection using order by and union select technique. Tutorial 6: Damping SQL Tables and Columns Using the SQL Injection. Tutorial 7: Uploading Shell in the Site having LFI. Tutorial 8: Advanced Way for Uploading Shell Tutorial 9: Uploading shell Using Sqli Command. Tutorial 10: Uploading Shell Using SQLmap Tutorial 11: Post Based SQL Injection Tutorial 12: Cracking the Hashes Using Tutorial 13: Hacking windows 7 and 8 through Metasploite Tutorial 14: Tutorial on Cross Site Scripting Tutorial 15: Hacking Android Mobile Using Metasploit Tutorial 16: Man of the middle attack: Tutorial 17: Using SQLmap for SQL injection Tutorial 18: Hide Your Ip Tutorial 19: Uploading Shell and Payloads Using SQLmap Tutorial 20: Using Sql Shell in SQLmap Tutorial 21: Blind SQL Injection Tutorial 22: Jack Hridoy SQL Injection Solution Tutorial 23: Using Hydra to Get the PasswordTutorial 24: Finding the phpmyadmin page using websploit. Tutorial 25: How to root the server using back connect Tutorial 25: How to root the server using back connect Tutorial 26: HTML Injection Tutorial 27: Tutuorial in manual SQl Injection Tutorial 28: Venom psh-cmd-exe payload Tutorial 29: Cross site Request Forgery (CSRF) Tutorial 30: Disable Victim Computer Tutorial 31: Exploit any firefox by xpi_bootstrapped addon Tutorial 32: Hack android mobile with metasploit Tutorial 33: PHP Code Injection to Meterpreter Session Tutorial 34: Basic google operators Tutorial 35: Hacking Credit Cards with google Tutorial 36: Finding Vulnerable Websites in Google Tutorial 37: Using the httrack to download website Tutorial 38: Getting the credit cards using sql injection and the SQLi dumper Tutorial 39: Using burp suite to brute force password This is a tutorial on Spring MVC, a module in the Spring Framework for rapidly developing web applications. The MVC in Spring MVC stands for Model-View-Controller, a design pattern widely used in Graphical User Interface (GUI) development. This pattern is not only common in web development, but is also used in desktop technology like Java Swing. Sometimes called Spring Web MVC, Spring MVC is one of the most popular web frameworks today and a most sought-after skill. This book is for anyone wishing to learn to develop Java-based web applications with Spring MVC. Sample applications come as Spring Tool Suite and Eclipse projects. Master building complex applications with NetBeans to become more proficient programmers About This Book Customize NetBeans to fit your unique needs Excel in NetBeans IDE, learning the shortcuts and hidden features to become more productive A comprehensive guide to become more productive at application development using NetBeans IDE Who This Book Is For If you are a competent developer who wants to fast-track your application development with NetBeans IDE, then this book is for you. Reasonable knowledge and an understanding of Java programming and NetBeans IDE is assumed. What You Will Learn Install NetBeans either from a distribution package or from source code Test, debug, and run production code using the NetBeans IDE Use external services such as PaaS environments and web services Create desktop applications using Swing tools Manage and configure relational databases Build a Java business model and web tiers using Java EE and Spring technologies Explore web services both with XML and RESTful approaches Handle external services such as databases , Maven repositories, and cloud providers Extend NetBeans for those situations where you require more from your IDE In Detail With the increasing complexity of software development and the abundance of tools available, learning your IDE in-depth will instantly increase your developer productivity. NetBeans is the only IDE that can be downloaded with Java itself and provides you with many cutting edge features not readily available with many IDEs. The IDE also provides a great set of tools for PHP and C/C++ developers. It is free and open source and has a large community of users and developers around the world. This book will teach you to ace NetBeans IDE and make use of it in creating Java business and web services. It will help you to become a proficient developer and use NetBeans for software development. You will learn effective third-party interaction and enable yourself for productive database development. Moving on, you will see how to create EJB projects and write effective and efficient web applications. Then you will learn how to use Swing and manage and configure a relational database. By the end of the book, you will be able to handle external services such as databases, Maven repositories, and cloud providers, and extend your NetBeans when you require more from your IDE. Style and approach An easy-to-follow yet comprehensive guide to help you master the exhaustive range of NetBeans features in order to become more efficient at Java programing. More advanced topics are covered in each chapter, with subjects grouped according to their complexity as well as their utility. Covering Servlet 3.1 and JSP 2.3, this book explains the important proogramming concepts and design models in Java web development as well as related technologies and new features in the latest versions of Servlet and JSP. Topics include: Servlet API - JSP syntax and scripting elements; session management; expression Language 3.0 - JSTL; custom tags and tag files; filters and listeners; application design; dependency injection; file upload and programming file download; asynchronous processing; security; deployment and the deployment descriptor; dynamic registration; Servlet container initializers; WebSocket and JPA. -- The objective of this work is to provide some quick tutorials in computer networking hacking. The work includes the following tutorials: · Tutorial 1: Setting Up Penetrating Tutorial in Linux. · Tutorial 2: Setting Up Penetrating Tutorial in Windows. · Tutorial 3: OS Command Injection: · Tutorial 4: Basic SQL Injection Commands. · Tutorial 5: Manual SQL injection using order by and union select technique. · Tutorial 6: Damping SQL Tables and Columns Using the SQL Injection. · Tutorial 7: Uploading Shell in the Site having LFI. · Tutorial 8: Advanced Way for Uploading Shell · Tutorial 9: Uploading shell Using Sqli Command. · Tutorial 10: Uploading Shell Using SQLmap · Tutorial 11: Post Based SQL Injection · Tutorial 12: Cracking the Hashes Using Hashcat. · Tutorial 13: Hacking windows 7 and 8 through Metasploite · Tutorial 14: Tutorial on Cross Site Scripting · Tutorial 15: Hacking Android Mobile Using Metasploit · Tutorial 16: Man of the middle attack: · Tutorial 17: Using SQLmap for SQL injection · Tutorial 18: Hide Your Ip · Tutorial 19: Uploading Shell and Payloads Using SQLmap · Tutorial 20: Using Sql Shell in SQLmap · Tutorial 21: Blind SQL Injection · Tutorial 22: Jack Hridoy SQL Injection Solution · Tutorial 23: Using Hydra to Get the PasswordTutorial 24: Finding the phpmyadmin page using websploit. · Tutorial 25: How to root the server using back connect · Tutorial 25: How to root the server using back connect · Tutorial 26: HTML Injection · Tutorial 27: Tutuorial in manual SQl Injection · Tutorial 28: Venom psh-cmd-exe payload · Tutorial 29: Cross site Request Forgery (CSRF) · Tutorial 30: Disable Victim Computer · Tutorial 31: Exploit any firefox by xpi_bootstrapped addon · Tutorial 32: Hack android mobile with metasploit · Tutorial 33: PHP Code Injection to Meterpreter Session · Tutorial 34: Basic google operators · Tutorial 35: Hacking Credit Cards with google · Tutorial 36: Finding Vulnerable Websites in Google · Tutorial 37: Using the httrack to download website · Tutorial 38: Getting the credit cards using sql injection and the SQLi dumper · Tutorial 39: Using burp suite to brute force password The Java EE 7 Tutorial: Volume 2, Fifth Edition, is a task-oriented, example-driven guide to developing enterprise applications for the Java Platform, Enterprise Edition 7 (Java EE 7). Written by members of the Java EE documentation team at Oracle, this book provides new and intermediate Java programmers with a deep understanding of the platform. This guide includes descriptions of platform features and provides instructions for using the latest versions of NetBeans IDE and GlassFish Server Open Source Edition. The book introduces Enterprise JavaBeans components, the Java Persistence API, the Java Message Service (JMS) API, Java EE security, transactions, resource adapters, Java EE Interceptors, Batch Applications for the Java Platform, and Concurrency Utilities for Java EE. The book culminates with three case studies that illustrate the use of multiple Java EE 7 APIs. Offering both theoretical explanations and real-world applications, this in-depth guide covers the 2.0 version of Struts, revealing how to design, build, and improve Java-based Web applications within the Struts development framework. Feature functionality is explained in detail to help programmers choose the most appropriate feature to accomplish their objectives, while other chapters are devoted to file uploading, paging, and object caching. The book is organized into two modules: In the first module, we present a tutorial on socket programming in Java, illustrating complete examples for simplex and duplex communications with both connectionless datagram and connection-oriented stream-mode sockets. In addition, this module explains in detail, with examples, the differences between a concurrent server and iterative server and the use of the Multicast socket API. In the second module, we present the source code analysis of a file reader connection-oriented server socket Java program, to illustrate the identification, impact analysis and solutions to remove the following important software security vulnerabilities: (1) Resource Injection, (2) Path Manipulation, (3) System Information Leak, (4) Denial of Service and (5) Unreleased Resource vulnerabilities. We analyze the reason for these vulnerabilities to occur in the program, discuss the impact of leaving them unattended, and propose solutions to remove each of these vulnerabilities from the program. The proposed solutions are very generic in nature, and can be suitably modified to correct any such vulnerabilities in software developed in any other programming language. "The Ruby on Rails 3 Tutorial and Reference Collection" consists of two bestselling Rails eBooks: "Ruby on Rails 3 Tutorial: Learn Rails by Example" by Michael Hartl"The Rails 3 Way" by Obie Fernandez In "Ruby on Rails 3 Tutorial" leading Rails developer Michael Hartl teaches Rails 3 by guiding you through the development of your own complete sample application using the latest techniques in Rails Web development. Drawing on his experience building RailsSpace, Insoshi, and other sophisticated Rails applications, Hartl illuminates all facets of design and implementation-including powerful new techniques that simplify and accelerate development. Hartl explains how each new technique solves a real-world problem and demonstrates this with bite-sized code that's simple enough to understand, yet novel enough to be useful. "The Rails 3 Way" is the only comprehensive, authoritative guide to delivering production-quality code with Rails 3. Pioneering Rails expert Obie Fernandez and a team of leading experts illuminate the entire Rails 3 API, along with the idioms, design approaches, and libraries that make developing applications with Rails so powerful. You learn advanced Rails programming techniques that have been proven effective in day-to-day usage on dozens of production Rails systems. Dive deep into the Rails 3 codebase and discover why Rails is designed the way it is-and how to make it do what you want it to do. This collection helps youInstall and set up your Rails development environmentGo beyond generated code to truly understand how to build Rails applications from scratchLearn Test Driven Development (TDD) with RSpecEffectively use the Model-View-Controller (MVC) pattern Structure applications using the REST architectureBuild static pages and transform them into dynamic onesMaster the Ruby programming skills all Rails developers needDefine high-quality site layouts and data modelsImplement registration and authentication systems, including validation and secure passwordsUpdate, display, and delete users Add social features and microblogging, including an introduction to AjaxRecord version changes with Git and share code at GitHubSimplify application deployment with HerokuLearn what's new in Rails 3Increase your productivity as a Web application developerRealize the overall joy in programming with RailsLeverage Rails' powerful capabilities for building REST-compliant APIsDrive implementation and protect long-term maintainability using RSpecDesign and manipulate your domain layer using Active RecordUnderstand and program complex program flows using Action ControllerMaster sophisticated URL routing conceptsUse Ajax techniques via Rails 3 support for unobtrusive JavaScriptLearn to extend Rails with popular gems and plugins and how to write your own Extend Rails with the best third-party plug-ins and write your ownIntegrate email services into your applications with Action MailerImprove application responsiveness with background processingCreate your own non-Active Record domain classes using Active ModelMaster Rails' utility classes and extensions in Active Support Mold Design Using NX 11.0: A Tutorial Approach book is written with the intention of helping the readers effectively design molds and its parts such as gate, runner, and various other standard parts using Mold Wizard of NX. After going through this book, the users will be able to design molds easily and effectively through processes such as analysis and documentation which have been dealt in detail. Also, the chapters in this book are arranged in a pedagogical sequence that makes this book very effective in learning the features and capabilities of the software. Keeping in mind the requirements of the users, the book at first introduces basic terms and analyses and gradually progresses to cover sequential method to create mold and documentation. Written with the tutorial point of view and the learn by doing a theme, the book caters to the needs of both novice and advanced users and is ideally suited for learning at your convenience and pace. Salient Features Consists of 10 chapters that are organized in a pedagogical sequence. Cover mold design concepts using NX 11.0. Tutorial approach to explain the concepts of Mold Design using NX 11.0. Summarized content on the first page of the topics that are covered in the chapter. Hundreds of illustrations for easy understanding of concepts. Step-by-step instructions to guide the users through the learning process. Additional information throughout the book in the form of notes and tips. Self-Evaluation Tests and Review Questions at the end of each chapter to help the users assess their knowledge. Technical support by contacting 'techsupport@cadcim.com' Additional learning resources at 'allaboutcadcam.blogspot.com' Table of Contents Chapter 1: Introduction to Mold Design and NX Mold Wizard Chapter 2: Part Analysis Chapter 3: Creating Parting Surface Chapter 4: Creating Core and Cavity Chapter 5: Adding Mold Base and Standard Parts Chapter 6: Creating Gate, Runner, and Layout Chapter 7: Creating Sliders and Lifters Chapter 8: Creating Ejection and Cooling Systems Chapter 9: Creating Electrodes Chapter 10: Documentation Index Trace Environmental Quantitative Analysis: Principles, Techniques, and Applications, Second Edition offers clear and relevant explanations of the principles and practice of selected analytical instrumentation involved in trace environmental quantitative analysis (TEQA). The author updates each chapter to reflect the latest improvements in TEQA that This book is an introduction for the reader into the wonderful world of embedded device exploitation. The book is supposed to be a tutorial guide that helps a reader understand the various skills required for hacking an embedded device. As the world is getting more and more into the phenomenon of "Internet of Things", such skill sets can be useful to hack from a simple intelligent light bulb to hacking into a car. The Java EE 6 Tutorial: Advanced Topics, Fourth Edition, is a task-oriented, example-driven guide to developing enterprise applications for the Java Platform, Enterprise Edition 6 (Java EE 6). Written by members of the Java EE 6 documentation team at Oracle, this book provides new and intermediate Java programmers with a deep understanding of the platform. This guide–which builds on the concepts introduced in The Java EE 6 Tutorial: Basic Concepts, Fourth Edition–contains advanced material, including detailed introductions to more complex platform features and instructions for using the latest version of the NetBeans IDE and the GlassFish Server, Open Source Edition. This book introduces the Java Message Service (JMS) API and Java EE Interceptors. It also describes advanced features of JavaServer Faces, Servlets, JAX-RS, Enterprise JavaBeans components, the Java Persistence API, Contexts and Dependency Injection for the Java EE Platform, web and enterprise application security, and Bean Validation. The book culminates with three new case studies that illustrate the use of multiple Java

EE 6 APIs. Being a beginner's guide this book has a very simple and clear approach. It is a practical guide that will help you learn the features of Django and help you build a dynamic website using those features. This book is for web developers who want to see how to build a complete site with Web 2.0 features, using the power of a proven and popular development system, but do not necessarily want to learn how a complete framework functions in order to do this. Basic knowledge of Python development is required for this book, but no knowledge of Django is expected. This book is the first to describe the unique benefits and challenges associated with fault injection methods. Using real world case-studies and applications data, the authors explain fault injection to the programmer and the developer. CD-ROM includes demo versions of fault injection tools and some basic algorithms for the reader to customize. The Java EE 7 Tutorial: Volume 1, Fifth Edition, is a task-oriented, example-driven guide to developing enterprise applications for the Java Platform, Enterprise Edition 7 (Java EE 7). Written by members of the Java EE documentation team at Oracle, this book provides new and intermediate Java programmers with a deep understanding of the platform. This guide includes descriptions of platform features and provides instructions for using the latest versions of NetBeans IDE and GlassFish Server Open Source Edition. The book introduces platform basics, including resource creation, resource injection, and packaging. It covers JavaServer Faces, Java Servlets, the Java API for WebSocket, the Java API for JSON Processing (JSON-P), internationalization and localization, Bean Validation, Contexts and Dependency Injection for Java EE (CDI), and web services (JAX-WS and JAX-RS). Bug Bounty Bootcamp teaches you how to hack web applications. You will learn how to perform reconnaissance on a target, how to identify vulnerabilities, and how to exploit them. You'll also learn how to navigate bug bounty programs set up by companies to reward security professionals for finding bugs in their web applications. Bug bounty programs are company-sponsored programs that invite researchers to search for vulnerabilities on their applications and reward them for their findings. This book is designed to help beginners with little to no security experience learn web hacking, find bugs, and stay competitive in this booming and lucrative industry. You'll start by learning how to choose a program, write quality bug reports, and maintain professional relationships in the industry. Then you'll learn how to set up a web hacking lab and use a proxy to capture traffic. In Part 3 of the book, you'll explore the mechanisms of common web vulnerabilities, like XSS, SQL injection, and template injection, and receive detailed advice on how to find them and bypass common protections. You'll also learn how to chain multiple bugs to maximize the impact of your vulnerabilities. Finally, the book touches on advanced techniques rarely covered in introductory hacking books but that are crucial to understand to hack web applications. You'll learn how to hack mobile apps, review an application's source code for security issues, find vulnerabilities in APIs, and automate your hacking process. By the end of the book, you'll have learned the tools and techniques necessary to be a competent web hacker and find bugs on a bug bounty program. Winner of the Best Book Bejtlich Read in 2009 award! "SQL injection is probably the number one problem for any server-side application, and this book is unequaled in its coverage." Richard Bejtlich, http://taosecurity.blogspot.com/ SQL injection represents one of the most dangerous and well-known, yet misunderstood, security vulnerabilities on the Internet, largely because there is no central repository of information to turn to for help. This is the only book devoted exclusively to this long-established but recently growing threat. It includes all the currently known information about these attacks and significant insight from its contributing team of SQL injection experts. What is SQL injection?-Understand what it is and how it works Find, confirm, and automate SQL injection discovery Discover tips and tricks for finding SQL injection within the code Create exploits using SQL injection Design to avoid the dangers of these attacks Burp Suite is an integrated platform/graphical tool for performing security testing of web applications. Burp suite is a java application that can be used to secure or crack web applications. The suite consists of different tools, like a proxy server, a web spider an intruder and a so-called repeater, with which requests can be automated. You can use Burp's automated and manual tools to obtain detailed information about your target applications. Damn Vulnerable Web App (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goals are to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and aid teachers/students to teach/learn web application security in a class room environment. In this report I am using a combination of Burp tools to detect and exploit vulnerabilities in Damn Vulnerable Web App (DVWA) with low security. By default, Burp Scanner scans all requests and responses that pass through the proxy. Burp lists any issues that it identifies under Issue activity on the Dashboard. You can also use Burp Scanner to actively audit for vulnerabilities. Scanner sends additional requests and analyzes the application's traffic and behavior to identify issues. Various examples are outlined in this report for different types of vulnerabilities such as: SQL injection, Cross Site Request Forgery (CSRF), Cross-site scripting, File upload, Local and Remote File Inclusion. I tested various types of penetration testing tools in order to exploit different types of vulnerabilities. The report consists from the following parts: 1. Installing and Configuring BurpSuite 2. BurpSuite Intruder. 3. Installing XMAPP and DVWA App in Windows System. 4. Installing PHP, MySQL, Apache2, Python and DVWA App in Kali Linux. 5. Scanning Kali-Linux and Windows Using . 6. Understanding Netcat, Reverse Shells and Bind Shells. 7. Adding Burps Certificate to Browser. 8. Setting up Target Scope in BurpSuite. 9. Scanning Using BurpSuite. 10. Scan results for SQL Injection Vulnerability with BurpSuite and Using SQLMAP to Exploit the SQL injection. 11. Scan Results for Operating System Command Injection Vulnerability with BurpSuite and Using Commix to Exploit the OS Command Injection. 12. Scan Results for Cross Side Scripting (XSS) Vulnerability with BurpSuite, Using Xserve to exploit XSS Injection and Stealing Web Login Session Cookies through the XSS Injection. 13. Exploiting File Upload Vulnerability. 14: Exploiting Cross Site Request Forgery (CSRF) Vulnerability. 15. Exploiting File Inclusion Vulnerability. 16. References. "The Book of GENESIS" is in two parts. Firstly, a collection of contributed articles describes projects created using the GENESIS system, and then a step-by-step tutorial explains how the software works and how best to manipulate it so as to achieve maximum use. As a result, this publication may be seen as a reference guide, a textbook for course use, and as a resource to which readers can turn for ideas on how to devise their own models and applications. The accompanying cross-platform CD-ROM contains the full source code for GENESIS and its graphical interface, XODUS; the GENESIS Reference Manual in hypertext, plain text and Postscript formats; numerous tutorial simulations and example simulation scripts, including all of those used in the book. As a bonus, also included on the CD are a number of items which are not part of the standard distribution of GENESIS. The GENESIS system will continue to be made available through the Cal Tech World Wide Web site, as well, at: www.bbb.caltech.edu/GENESIS. Keeping up with the latest developments in cyber security requires ongoing commitment, but without a firm foundation in the principles of computer security and digital forensics, those tasked with safeguarding private information can get lost in a turbulent and shifting sea. Providing such a foundation, Introduction to Security and Network Forensics covers the basic principles of intrusion detection systems, encryption, and authentication, as well as the key academic principles related to digital forensics. Starting with an overview of general security concepts, it addresses hashing, digital certificates, enhanced software security, and network security. The text introduces the concepts of risk, threat analysis, and network forensics, and includes online access to an abundance of ancillary materials, including labs, Cisco challenges, test questions, and web-based videos. The author provides readers with access to a complete set of simulators for routers, switches, wireless access points (Cisco Aironet 1200), PIX/ASA firewalls (Version 6.x, 7.x and 8.x), Wireless LAN Controllers (WLC), Wireless ADUs, ASDMs, SDMs, Juniper, and much more, including: More than 3,700 unique Cisco challenges and 48,000 Cisco Configuration Challenge Elements 60,000 test questions, including for Certified Ethical Hacking and CISSP® 350 router labs, 180 switch labs, 160 PIX/ASA labs, and 80 Wireless labs Rounding out coverage with a look into more advanced topics, including data hiding, obfuscation, web infrastructures, and cloud and grid computing, this book provides the fundamental understanding in computer security and digital forensics required to develop and implement effective safeguards against ever-evolving cyber security threats. Along with this, the text includes a range of online lectures and related material, available at: http://asecuritybook.com. For hacking you need to have a basic knowledge of programming. The information provided in this eBook is to be used for educational purposes only. My soul purpose of this book was not to sell it but to raise awareness of the danger we face today, and yes, to help teach people about the hackers tradition. I am sure this will book make creative and constructive role to build your life more secure and alert than ever before. Do you want to take your Poser skills beyond the basics and put the new features of Poser 7 into practice right away? If so, you've come to the right place. Practical Poser 7 is an updated edition of this best-selling reference for intermediate to advanced Poser users. It teaches the tasks you want and need to know to get the most out of Poser 7 for achieving professional, commercial-quality work. This edition covers new Poser features, including new animation functionality, morphing tools, and more. Learn texturing and material techniques from a master texture artist, and explore the work of Poser pros in the beautiful color section! Among the tests you perform on web applications, security testing is perhaps the most important, yet it's often the most neglected. The recipes in the Web Security Testing Cookbook demonstrate how developers and testers can check for the most common web security issues, while conducting unit tests, regression tests, or exploratory tests. Unlike ad hoc security assessments, these recipes are repeatable, concise, and systematic-perfect for integrating into your regular test suite. Recipes cover the basics from observing messages between clients and servers to multi-phase tests that script the login and execution of web application features. By the end of the book, you'll be able to build tests pinpointed at Ajax functions, as well as large multi-step tests for the usual suspects: cross-site scripting and injection attacks. This book helps you: Obtain, install, and configure useful-and free-security testing tools Understand how your application communicates with users, so you can better simulate attacks in your tests Choose from many different methods that simulate common attacks such as SQL injection, cross-site scripting, and manipulating hidden form fields Make your tests repeatable by using the scripts and examples in the recipes as starting points for automated tests Don't live in dread of the midnight phone call telling you that your site has been hacked. With Web Security Testing Cookbook and the free tools used in the book's examples, you can incorporate security coverage into your test suite, and sleep in peace.

- VSC FACTS HVDC
- Embedded Device Security
- Mastering NetBeans
- Introduction To Security And Network Forensics
- Cyberspace And Cybersecurity
- Mold Design Using NX 110 A Tutorial Approach
- The Most In depth Hackers Guide
- Learning Website Development With Django
- Learn AngularJS In 24 Hours
- Practical Poser 7
- A Tutorial On Java Socket Programming And Source Code Analysis
- Process Modeling In Composites Manufacturing
- Trace Environmental Quantitative Analysis