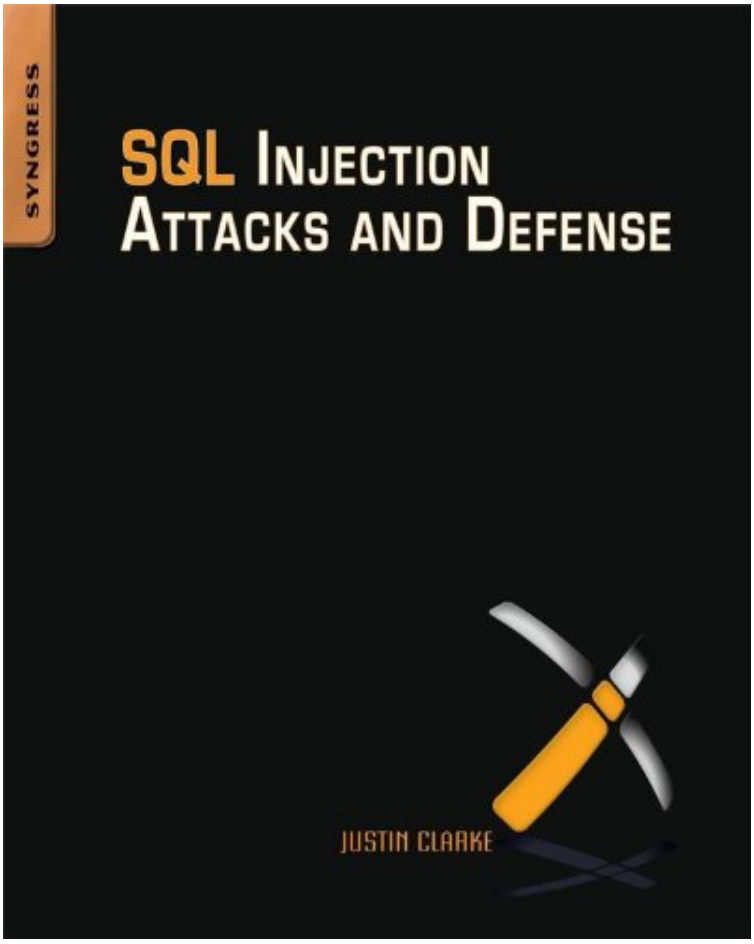
SQL Injection Attacks and Defense

Von Justin Clarke-Salt
*ebooks | Download PDF | *ePub | DOC | audiobook*



Produktinformation -Verkaufsrang: #530861 in eBooksVerffentlicht am: 2009-06-16Erscheinungsdatum: 2009-06-16File Name: B008PQESLI | File size: 29.Mb

Von Justin Clarke-Salt : SQL Injection Attacks and Defense before purchasing it in order to gage whether or not it would be worth my time, and all praised SQL Injection Attacks and Defense:

KurzbeschreibungSQL Injection Attacks and Defense, First Edition: Winner of the Best Book Bejtlich Read Award "SQL injection is probably the number one problem for any server-side application, and this book unequaled in its coverage." Richard Bejtlich, Tao Security blog 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 available for penetration testers, IT security consultants and practitioners, and web/software developers to turn to for help. SQL Injection Attacks and Defense, Second Edition is the only book devoted exclusively to this long-established

but recently growing threat. This is the definitive resource for understanding, finding, exploiting, and defending against this increasingly popular and particularly destructive type of Internet-based attack. SQL Injection Attacks and Defense, Second Edition includes all the currently known information about these attacks and significant insight from its team of SQL injection experts, who tell you about: Understanding SQL Injection Understand what it is and how it works Find, confirm and automate SQL injection discovery Tips and tricks for finding SQL injection within code Create exploits for using SQL injection Design apps to avoid the dangers these attacks SQL injection on different databases SQL injection on different technologies SQL injection testing techniques Case Studies Securing SQL Server, Second Edition is the only book to provide a complete understanding of SQL injection, from the basics of vulnerability to discovery, exploitation, prevention, and mitigation measures. Covers unique, publicly unavailable information, by technical experts in such areas as Oracle, Microsoft SQL Server, and MySQL---including new developments for Microsoft SQL Server 2012 (Denali). Written by an established expert, author, and speaker in the field, with contributions from a team of equally renowned creators of SQL injection tools, applications, and educational materials. Pressestimmen""The most stunningly impactful attacks often leverage SQL Injection vulnerabilities. This book has everything you need to fight back, from applying the core fundamentals to protecting emerging technologies against such attacks. Keep it by your bedside and distribute it within your business."--Nitesh Dhanjani, Executive Director" at Ernst Young LLP ""Securing SQL Server - Protecting Your Database from Attackers and SQL Injection Attacks and Defense are two new books out on SQL security. The first, Securing SQL Server - Protecting Your Database from Attackers, author Denny Cherry takes a high-level approach to the topic. The book explains how to secure and protect a SQL database from attack. The book details how to configure SQL against both internal and external-based attacks. This updated edition includes new chapters on analysis services, reporting services, and storage area network security. For anyone new to SQL security, Cherry does a great job of explaining what needs to be done in this valuable guide. In and SQL Injection Attacks and Defense, editor Justin Clarke enlists the help of a set of experts on how to deal with SQL injection attacks. Since SQL is so ubiquitous on corporate networks, with sites often running hundreds of SQL servers; SQL is prone to attacks. SQL injection is a technique often used to attack databases through a website and is often done by including portions of SQL statements in a web form entry field in an attempt to get the website to pass a newly formed rogue SQL command to the database. SQL injection is a code injection technique that exploits security vulnerability in a website's software. The vulnerability happens when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and unexpectedly executed. With that, the need to defend servers against such attacks is an imperative and SQL Injection Attacks and Defense should be required reading for""Lead author and technical editor Clarke has organized the volume's 11 chapters into sections on understanding, finding, exploiting, and defending SQL injection, and has also included reference materials that provide information on database platforms not covered in detail in the main body of the text."--""Reference and Research Book News, " August 2013 ""The most stunningly impactful attacks often leverage SQL Injection vulnerabilities. This book has everything you need to fight back, from applying the core fundamentals to protecting emerging technologies against such attacks. Keep it by your bedside and distribute it within your business."--Nitesh Dhanjani, Executive Director" at Ernst Young LLP ""Securing SQL Server - Protecting Your Database from Attackers and SQL Injection Attacks and Defense are two new books out on SQL security. The first, Securing SQL Server - Protecting Your Database from Attackers, author Denny Cherry takes a high-level approach to the topic. The book explains how to secure and protect a SQL database from attack. The book details how to configure SQL against both internal and external-based attacks. This updated edition includes new chapters on analysis services, reporting services, and storage area network security. For anyone new to SQL security, Cherry does a great job of explaining what needs to be done in this valuable guide. In and SQL Injection Attacks and Defense, editor Justin Clarke enlists the help of a set of experts on how to deal with SQL injection attacks. Since SQL is so ubiquitous on corporate networks, with sites often running hundreds of SQL servers; SQL is prone to attacks. SQL injection is a technique often used to attack databases through a website and is often done by including portions of SQL statements in a web form entry field in an attempt to get the website to pass a newly formed rogue SQL command to the database. SQL injection is a code injection technique that exploits security vulnerability in a website's software. The vulnerability happens when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and unexpectedly executed. With that, the need to defend servers against such attacks is an imperative and SQL Injection Attacks and Defense should be required reading for anyone tasks with securing SQL servers."--RSA Conference""Lead author and technical editor Clarke has organized the volume's 11 chapters into sections on understanding, finding, exploiting, and defending SQL injection, and has also included reference materials that provide information on database platforms not covered in detail in the main body of the text."--Reference and Research Book News, August 2013 "The most stunningly impactful attacks often leverage SQL Injection vulnerabilities. This book has everything you need to fight back, from applying the core fundamentals to protecting emerging technologies against such attacks. Keep it by your bedside and distribute it within your business."--Nitesh Dhanjani, Executive Director at Ernst Young LLP "Securing SQL Server - Protecting Your Database from Attackers and SQL Injection Attacks and Defense are two new books out on SQL security. The first,

Securing SQL Server - Protecting Your Database from Attackers, author Denny Cherry takes a high-level approach to the topic. The book explains how to secure and protect a SQL database from attack. The book details how to configure SQL against both internal and external-based attacks. This updated edition includes new chapters on analysis services, reporting services, and storage area network security. For anyone new to SQL security, Cherry does a great job of explaining what needs to be done in this valuable guide. In and SQL Injection Attacks and Defense, editor Justin Clarke enlists the help of a set of experts on how to deal with SQL injection attacks. Since SQL is so ubiquitous on corporate networks, with sites often running hundreds of SQL servers; SQL is prone to attacks. SQL injection is a technique often used to attack databases through a website and is often done by including portions of SQL statements in a web form entry field in an attempt to get the website to pass a newly formed rogue SQL command to the database. SQL injection is a code injection technique that exploits security vulnerability in a website's software. The vulnerability happens when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and unexpectedly executed. With that, the need to defend servers against such attacks is an imperative and SQL Injection Attacks and Defense should be required reading for anyone tasks with securing SQL servers."--RSA Conference-Lead author and technical editor Clarke has organized the volume's 11 chapters into sections on understanding, finding, exploiting, and defending SQL injection, and has also included reference materials that provide information on database platforms not covered in detail in the main body of the text.---Reference and Research Book News, August 2013 -The most stunningly impactful attacks often leverage SQL Injection vulnerabilities. This book has everything you need to fight back, from applying the core fundamentals to protecting emerging technologies against such attacks. Keep it by your bedside and distribute it within your business.---Nitesh Dhanjani, Executive Director at Ernst Young LLP -Securing SQL Server - Protecting Your Database from Attackers and SQL Injection Attacks and Defense are two new books out on SQL security. The first, Securing SQL Server - Protecting Your Database from Attackers, author Denny Cherry takes a high-level approach to the topic. The book explains how to secure and protect a SQL database from attack. The book details how to configure SQL against both internal and external-based attacks. This updated edition includes new chapters on analysis services, reporting services, and storage area network security. For anyone new to SQL security, Cherry does a great job of explaining what needs to be done in this valuable guide. In and SQL Injection Attacks and Defense, editor Justin Clarke enlists the help of a set of experts on how to deal with SQL injection attacks. Since SQL is so ubiquitous on corporate networks, with sites often running hundreds of SQL servers; SQL is prone to attacks. SQL injection is a technique often used to attack databases through a website and is often done by including portions of SQL statements in a web form entry field in an attempt to get the website to pass a newly formed rogue SQL command to the database. SQL injection is a code injection technique that exploits security vulnerability in a website's software. The vulnerability happens when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and unexpectedly executed. With that, the need to defend servers against such attacks is an imperative and SQL Injection Attacks and Defense should be required reading for anyone tasks with securing SQL servers.---RSA ConferenceKurzbeschreibungSQL Injection Attacks and Defense, First Edition: Winner of the Best Book Bejtlich Read Award "SQL injection is probably the number one problem for any server-side application, and this book unequaled in its coverage." Richard Bejtlich, Tao Security blog 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 available for penetration testers, IT security consultants and practitioners, and web/software developers to turn to for help. SQL Injection Attacks and Defense, Second Edition is the only book devoted exclusively to this long-established but recently growing threat. This is the definitive resource for understanding, finding, exploiting, and defending against this increasingly popular and particularly destructive type of Internet-based attack. SQL Injection Attacks and Defense, Second Edition includes all the currently known information about these attacks and significant insight from its team of SQL injection experts, who tell you about: Understanding SQL Injection Understand what it is and how it works Find, confirm and automate SQL injection discovery Tips and tricks for finding SQL injection within code Create exploits for using SQL injection Design apps to avoid the dangers these attacks SQL injection on different databases SQL injection on different technologies SQL injection testing techniques Case Studies Securing SQL Server, Second Edition is the only book to provide a complete understanding of SQL injection, from the basics of vulnerability to discovery, exploitation, prevention, and mitigation measures. Covers unique, publicly unavailable information, by technical experts in such areas as Oracle, Microsoft SQL Server, and MySQL---including new developments for Microsoft SQL Server 2012 (Denali). Written by an established expert, author, and speaker in the field, with contributions from a team of equally renowned creators of SQL injection tools, applications, and educational materials.