# Database Security – discuss the problems involved in keeping a database secure and the possible solutions

This paper discusses database security, specifically the threats involved and how to protect against them, this is important to consider when developing a database because should you be handling sensitive data then it must be protected against attacks such as SQL Injection, malicious employees using security measures such as intrusion detection systems, encryption, auditing, privileges, authorisation and more otherwise the data will be stolen, the database damaged or even wiped completely.

One database security threat is SQL Injection a technique whereby a malicious individual injects SQL code into an application e.g. using a text box allowing the attacker access to the database in order to do untold damage to the database. This is backed up by the work of Shar, L (2013) who describes what SQL Injection is, how systems can be vulnerable to it and the security methods that can be implemented to combat it as well as how to detect SQL injection vulnerabilities in a system. The source is useful because it provides the reader with a detailed overall analysis of SQL Injection which is a starting point on the topic and helps to show what security threats there are and how to deal with them. The source is similar to the work of Kim, M (2014) as both sources deal with the issue of database security in particular SQL Injection however the first source gives a detailed description of the topic as a whole while the second source takes this further by not only informing the reader of the problem but also shows its own solution to this problem as well as the results of its testing therefore the second source is a better source of information based on this, however the first source is still useful as it can educate the reader to the point where they can easier understand the topic and be able to find better sources such as the second source.

Another source that covers SQL Injection is the work of Dorai, R (2011) which details why security is so important, the readiness of large websites to block this threat as well as how they might go about dealing with this kind of security threats such as a firewall or encryption etc. The source is useful as it gives an introduction to SQL Injection but more importantly it provides the reader with information on how to deal with security threats by describing several different solutions that can be implemented and how that will improve the security of a system. The source is similar to the work of Lee, I (2012) as both sources deal with database security specifically the threat SQL Injection, the first source gives a well rounded explanation of SQL Injection while the second source takes this further by showing off its solution designed to detect if a system is under attack by this threat therefore the second source provides a higher quality of information due to this, however the first source can still be used to build up an individual's knowledge on the topic of SQL Injection and the factors that go with it which is quite useful.

The work of Kim, M (2014) deals with the problem of most of the database security being handled at the front end of the system which is bypassed by SQL Injection attacks, therefore the source suggests a way to be able to sense these attacks at the database level with a method it has created itself. The source is useful as not only does it show how dangerous SQL Injection is but also provides the reader with a practical demonstration of how to deal with this kind of attack by creating its own solution and testing it which showed it to be quite useful for dealing with SQL Injection. The source is similar to the work of Shar, L (2013) as both sources deal with SQL Injection attacks, the first source provides information on this topic and how that relates to database security as a whole as well as its own solution to the problem, meanwhile the second source gives detailed information on SQL Injection which is important however the first sources information is of a higher quality and therefore is the better paper.

The source Pinzón, C (2013) also deals with the problem of SQL Injection attacks and proposes its own method to deal with said problem using a layered approach, this paper is useful as not only does it go into detail on SQL Injection but also provides the reader with detailed information on the several facets that have been incorporated into its method to dealing with this kind of security threat, the method is tested and the results show it to be an improvement over the current methods in place at the time. The source is similar to the work of Kim, M (2014) as both sources cover the topic of SQL Injection in terms of database security and all that entails for the readers benefit as well as showing solutions to this kind of threat however the first source goes into more detail on all parts of its solution which is important as it gives the reader an insight into the process behind creating such a solution which cannot be said as much for the second source therefore the first source is the better paper.

This source Lee, I (2012) goes over the security threat that is SQL Injection in its various forms with examples and details its own SQL Injection detection method designed to combat this security threat, this is useful as it is another take on the same problem and provides the reader with the results of testing said method against said attacks in order to compare its strengths and weaknesses over its alternatives in order to incorporate what works well and to avoid what does not in order to minimise the risk this security threat poses to the information systems industry. The source is similar to the work of Murray, MC (2010) as both sources discuss the database threat SQL Injection, the first source provides the reader with information on SQL Injection and all that entails but also gives a practical example with its own solution to this problem, the second source while it goes into more details on the different aspects of the problem it does not provide its own solution and therefore the first source is more useful as a learning tool because of this.

The paper by Antunes, N, & Vieira, M (2012) discusses how to implement security as you are building a system as opposed to after it has been created, the types of threats this can help to block, how to test a system for any security loopholes or weaknesses and how to tell if your system is being attacked, this is useful as it provides the reader with a broad understanding of security across the whole system rather than centralised into one area which can give the reader a platform to understand the terminology and be able to delve deeper into information security. The source is similar to the work of Gupta, G (2010) as both sources deal with database security and provide the reader with detailed information on the topic while the first source takes this in a more general sense the second source goes further by discussing this issue on a more specific platform mobile distribute databases instead of databases in a general sense which is very useful as it gives the reader a different viewpoint to consider on the issue therefore the second source does more to improve the industries knowledge of security issues and is the better paper due to this fact.

Murray, MC (2010) talks specifically about security in the database area and discusses exactly what this entails specifically who has access to the database and what they can do, views, how this extends to the front end application, the kinds of database security weaknesses there are for example SQL Injection as well as how to track the actions of those who have access to the database, this is useful because it gives the reader a generalised description of the topics included in this specific security area in order to learn the terms and keywords involved so that further research is an easier prospect thanks to the knowledge gained through this paper. The source is similar to the work of Shar, L (2013) as both sources give a generalised description of database security however the first source takes this further by going into more depth on the topic specifically on the solutions to this issue therefore this can be considered a better paper although the second source is still useful despite this, nonetheless both sources only describe the issue and do not include a practical solution of their own making which degrades their usefulness as academic papers.

Ying-Chiang, C (2015) deals with the fact that more and more services are being pushed to the cloud resulting in an influx of the storage of private data which intern leads to more systems with security weaknesses that can be exploited by malicious individuals using various methods especially SQL Injection, therefore the paper includes a proposed tool to highlight weaknesses in modern websites, the testing was successful in showing how said tool can be used to strengthen information systems. This is useful as not only does the paper provide the reader with information on the affects of cloud computing popularity on information security as well as the methods used by attackers but also shows off its design for a tool to detect security loopholes and includes testing to add to its credibility, the reader therefore gains useful information in this topic which can be used to enhance security on information systems as well as ideas on possible security loophole detection tools. The source is similar to the work of Kundu, A (2010) as both sources deal with the need to improve information security as the internet grows in popularity; however the first source talks about security in a general sense while the second source focuses closer on database security which suits the purposes of this paper better, the first source is still useful as I provides the reader with necessary knowledge to understand the finer details.

Herranz, J (2014) deals with the problem of database security in a specific location in this case hospitals, this is an issue as there is no unified system in place to keep the data stored confidential and secure therefore the paper looks to solve this with its own protocol which it shows to be a more efficient and secure option than its competitors, this is useful as its provides the reader with very specialised information on database security in a particular setting and shows how a problem was ascertained and a solution devised which will help said reader with their overall knowledge of information security and an idea into how they might go through the process of dealing with security issues via this papers example. The source is similar to the work of Ying-Chiang, C (2015) as both sources cover information security in a specific setting as well as their own solutions to the issue however the first source closer relates to database security and is therefore the better source for this paper, the second source is still a useful source of information and helps this paper analyse the topic involved.

Gupta, G (2010) discusses the issue of security in databases other than relational specifically mobile distributed database as mobile computing is becoming more and more popular than in recent years, the paper gives a brief description of the topic areas involved with this particular issue such as database consistency, backing up the database, database security including the threats and the solutions. The paper is useful in helping to give the reader an understanding of database centric issues in a specific field as well as providing information on the topics involved in order to raise awareness of these issues in the information systems industry. The source is similar to the work of Dorai, R (2011) as both sources cover database security and all that topic entails however the second source merely covers the topic as a whole and does not go into more depth such as the first source which hones in on a specific area of database security which makes it the better source of information for this papers analysis, the second source is still useful and as such has been left in to also be a provider of knowledge on the subject.

Kundu, A (2010) describes the use of intrusion detection systems that should be employed due to the rapidly increasing number of security attacks in recent years in order to be able to tell when a system is under attack with the help of a sequence alignment tool. The paper goes over the sub topics within this particular field such as intrusion detection, sequence alignment, how these two are linked and the results of testing this combination. This is useful as it provides the reader with detailed information on a different take on how to secure a system in particular how to see when it is under attack as well as an understanding on the technologies involved so that the reader can then be better suited to creating a secure web application system. The source is similar to the work of Lee, I (2012) as both sources cover database security in particular their own solutions to the threats that databases encounter however the first sources method deals with all types of threats to the database while the second source deals with SQL Injection specifically which as a source of information provides the reader with a higher level of knowledge due to its specific and detailed nature and as such is the better source for this paper, the first source is still useful as any database security solution is a welcome addition to the knowledge base in industry in order to improve information security and in the case of this paper the analysis of this topic.

Therefore based on the literature that has been reviewed there is plenty of academic content on this topic which shows its importance to the industry and it seems there have been leaps and bounds in improvements on database security over the years, however it also appears that more research and development on the threats and solutions to database security is needed in order to improve on the current standards in place due to the industry’s growing popularity leading to increasing numbers of attacks on databases.

In conclusion this paper has covered database security, the various potential attacks that are involved the different methods that may be implemented to keep it secure as well as why it is necessary to do so all of which is reflected in the literature that has been gathered and reviewed.

References:

Shar, L, & Tan, H 2013, 'Defeating SQL Injection', Computer, 46, 3, pp. 69-77, Academic Search Complete, EBSCOhost, viewed 9 May 2015.

Available at: <http://web.b.ebscohost.com/ehost/detail/detail?sid=d15044ea-dcee-4f89-92c5-2b8ba737f5cb%40sessionmgr115&vid=0&hid=124&bdata=JnNpdGU9ZWhvc3QtbGl2ZQ%3d%3d#db=a9h&AN=86642466>

Dorai, R, & Kannan, V 2011, 'SQL Injection-Database Attack Revolution and Prevention', Journal Of International Commercial Law & Technology, 6, 4, pp. 224-231, Academic Search Complete, EBSCOhost, viewed 9 May 2015.

Available at: <http://web.b.ebscohost.com/ehost/detail/detail?sid=efa309f6-4288-4ded-a88b-e67f95acfb88%40sessionmgr111&vid=0&hid=124&bdata=JnNpdGU9ZWhvc3QtbGl2ZQ%3d%3d#db=a9h&AN=67217369>

Kim, M, & Lee, D 2014, 'Data-mining based SQL injection attack detection using internal query trees', Expert Systems With Applications, 41, 11, pp. 5416-5430, Academic Search Complete, EBSCOhost, viewed 9 May 2015.

Available at: <http://web.b.ebscohost.com/ehost/detail/detail?sid=00dc6188-3a98-4251-bcf5-3ef2674d7f68%40sessionmgr198&vid=0&hid=124&bdata=JnNpdGU9ZWhvc3QtbGl2ZQ%3d%3d#db=a9h&AN=95713988>

Pinzón, C, De Paz, J, Herrero, Á, Corchado, E, Bajo, J, & Corchado, J 2013, 'idMAS-SQL: Intrusion Detection Based on MAS to Detect and Block SQL injection through data mining', Information Sciences, 231, pp. 15-31, Academic Search Complete, EBSCOhost, viewed 9 May 2015.

Available at: <http://web.b.ebscohost.com/ehost/detail/detail?sid=e2420720-2d0e-4d8f-a4ca-87267c368cc0%40sessionmgr110&vid=0&hid=124&bdata=JnNpdGU9ZWhvc3QtbGl2ZQ%3d%3d#db=a9h&AN=85615586>

Lee, I, Jeong, S, Yeo, S, & Moon, J 2012, 'A novel method for SQL injection attack detection based on removing SQL query attribute values', Mathematical & Computer Modelling, 55, 1/2, pp. 58-68, Academic Search Complete, EBSCOhost, viewed 9 May 2015.

Available at: <http://web.b.ebscohost.com/ehost/detail/detail?sid=ee7215cf-7be2-4a8d-aae0-90ff03d332c0%40sessionmgr111&vid=0&hid=124&bdata=JnNpdGU9ZWhvc3QtbGl2ZQ%3d%3d#db=a9h&AN=67248440>

Antunes, N, & Vieira, M 2012, 'Defending against Web Application Vulnerabilities', Computer, 45, 2, pp. 66-72, Academic Search Complete, EBSCOhost, viewed 9 May 2015.

Available at: <http://web.b.ebscohost.com/ehost/detail/detail?sid=831dbbd8-2528-44a5-85db-a2962b9c4d1a%40sessionmgr111&vid=0&hid=124&bdata=JnNpdGU9ZWhvc3QtbGl2ZQ%3d%3d#db=a9h&AN=73617939>

Murray, MC 2010, 'Database Security: What Students Need to Know', Journal Of Information Technology Education, 9, pp. IIP61-IIP77, Academic Search Complete, EBSCOhost, viewed 9 May 2015.

Available at: <http://web.b.ebscohost.com/ehost/detail/detail?sid=5d0a5e04-5e4d-49e1-a009-84dd663228b0%40sessionmgr113&vid=0&hid=124&bdata=JnNpdGU9ZWhvc3QtbGl2ZQ%3d%3d#db=a9h&AN=60636410>

Ying-Chiang, C 2015, 'IMPLEMENTATION AND ANALYSIS OF WEBSITE SECURITY MINING SYSTEM, APPLIED TO UNIVERSITIES' ACADEMIC NETWORKS', Tehnicki Vjesnik / Technical Gazette, 22, 2, pp. 279-287, Academic Search Complete, EBSCOhost, viewed 10 May 2015.

Available at: <http://web.b.ebscohost.com/ehost/detail/detail?sid=571a8a6d-e87c-4d39-913d-f9079b3dcc36%40sessionmgr113&vid=0&hid=124&bdata=JnNpdGU9ZWhvc3QtbGl2ZQ%3d%3d#db=a9h&AN=102356271>

Herranz, J, & Nin, J 2014, 'Secure and efficient anonymization of distributed confidential databases', International Journal Of Information Security, 13, 6, pp. 497-512, Academic Search Complete, EBSCOhost, viewed 10 May 2015.

Available at: <http://web.b.ebscohost.com/ehost/detail/detail?sid=6c949ea3-2aee-404c-94ac-c72f0aa4d893%40sessionmgr113&vid=0&hid=124&bdata=JnNpdGU9ZWhvc3QtbGl2ZQ%3d%3d#db=a9h&AN=98899381>

Gupta, G, Sharma, A, & Swaroop, V 2010, 'Consistency and Security in Mobile Real Time Distributed Database (MRTDDB): A Combinational Giant Challenge', AIP Conference Proceedings, 1324, 1, pp. 191-197, Academic Search Complete, EBSCOhost, viewed 10 May 2015.

Available at: <http://web.b.ebscohost.com/ehost/detail/detail?sid=30cd6171-8066-4ad7-b406-31882eefba54%40sessionmgr110&vid=0&hid=124&bdata=JnNpdGU9ZWhvc3QtbGl2ZQ%3d%3d#db=a9h&AN=55595619>

Kundu, A, Sural, S, & Majumdar, A 2010, 'Database intrusion detection using sequence alignment', International Journal Of Information Security, 9, 3, pp. 179-191, Academic Search Complete, EBSCOhost, viewed 10 May 2015.

Available at: <http://web.b.ebscohost.com/ehost/detail/detail?sid=7d86bc60-aa9c-467e-8fa9-040b57ae05b1%40sessionmgr114&vid=0&hid=124&bdata=JnNpdGU9ZWhvc3QtbGl2ZQ%3d%3d#db=a9h&AN=51039820>