**Name -** James Braznell

**Student Number -** 1007022

**Award -** MSC Computer Science

**Project Title -**

SQL Injection: - The popular methods, solutions and is it still an issue

**Aim -**

To create a report on SQL Injection database intrusion techniques and its current state as a security threat to be considered

**Objectives -**

* Perform extensive re research into SQL Injection
* Build databases, develop related applications and test numerous database management systems against SQL Injection attack
* Create a report on findings based on research and practical tests

**Deliverable -**

After performing extensive research into SQLIAs and the solutions to that threat there will be several tests on whether SQLIA is still an issue. This will involve the development of test applications that perform specific jobs possibly using several different programming languages such as PHP, Java, HTML, etc in order to test their resilience against this threat and they will be connected to several databases using different Database Management systems(DBMS) such as Oracle, MySQL, Microsoft SQL Server etc with a substantial amount of test data to test their built in methods for dealing with various SQLIA methods and then move on to testing with the addition of third party tools for SQLIA defence that were found based on the research performed beforehand. With the information gained from this artefact there will be a report produced on the research and the findings combined in order to provide an answer on whether SQL Injection is still an issue.

**Research question(s) -**

What are the popular SQL Injection database intrusion methods and has the computing industry made the practice ineffectual?

**Background –**In recent years information security has become more and more of a popular topic of research due to the growing nature of the internet as more and more individuals gain access to it and as such the number of cyber-attacks on businesses and the confidential customer data that they hold has increased as a result. Therefore there has been a fair amount of research into stopping these attacks specifically at the front end of applications that businesses are using to interact with customers however this does leave the back end of the application vulnerable if attackers are able to reach it which is a part of much of the current research in information security, how to deal with the application vulnerabilities that attackers are taking advantage of. One of the bigger vulnerabilities is SQL injection attack (SQLIA) which is a technique where the attacker attempts to alter a SQL query by injecting SQL code into front end applications for example with an empty text box that allows the malicious individual access to the database in order to retrieve sensitive information, alter the database or even wipe the database entirely.

SQLIAs come in several different forms, one of which centres around the SQL command UNION that combines queries, if used for malicious purposes this command will alter the original intended query by merging it with a query devised by the hacker to gain access to more of the database, steal data or damage the database if the correct data types for the columns involved are selected. Another type of SQLIA attempts to bypass any efforts by developers to stop SQLIAs within their code or with third party tools, this is done by altering the malicious query to instead use alternate encoding such as hexadecimal or Unicode which is not a part of developers considerations when it comes to securing their application and database allowing the attacker to perform malicious acts. Another type of SQLIA takes advantage of any leftover sets of SQL commands packaged together as a procedure that came with the particular database management system (DBMS) that a developer may have chosen to support their application, the attacker will attach their malicious SQL statement to a procedure so that when run their statement will allow them to perform malicious acts, a SQLIA similar to this is where the attacker attaches their malicious SQL statement to another non malicious SQL statement by adding a semicolon at the end so that it ends it, this will cause the first statement to be run but also allow the attackers malicious statement to be run. Another SQLIA is where the attacker does not get any prompt from the application that their efforts are being successful in the form of error messages, the attacker instead injects SQL statements that are correct or incorrect and the application will determine this and based on the answer the attacker will learn more about the databases stored data than was intended. Another SQLIA makes use of time centric operators such as BENCHMARK() in the malicious SQL statement as if this is set to repeat a high enough number of times and returns correctly the statement will run and hamper server performance severely as the malicious statement is being run. Another SQLIA makes use of malicious SQL statements that are made purposefully incorrect by the attacker which when injected and run will cause error messages to appear allowing the attacker to learn the structure of the applications database as well as individual records. Another SQLIA makes use of SQL statements that are purposefully set up to be considered correct by the application they are injected into allowing the attacker access to more of the database than they should leading to stolen data and damages.

Based on the research performed on this topic several solutions have been devised to help secure applications against this kind of attack, there are tools that will scan an application in its entirety to look for known vulnerabilities in the code and will depending on the tool, make the user aware of the issue, provide assistance in rectifying the problem code or change the code in question to no longer be vulnerable to SQL injection attack on an automatic basis, while this is very useful for securing applications against known threats it is however ineffective against new SQLIAs that it does not have a solution for making it not very adaptable in the long term.

Another solution for dealing with the threat of SQLIAs is SQLIA detection tools; this is where the tool will run in the background of the normal application runtime and based on the tools method will scrutinize the SQL code that is passed from the front end application to the back end database against known SQLIAs and will block any deemed to be a threat automatically, the tools available do this in various ways and some are even quite adaptable in that they will attempt learn the traits of SQLIAs and be able to block new SQLIAs based on this, however due to the fact that the tools will run in the background of normal operations depending on the tool it may cause a noticeable slowdown in performance.

Another solution for securing against SQLIAs would be to introduce a third party encryption tool that will take the records in the database and encrypt them in such a way so that even if a SQLIA is successful the attacker will only receive data that is essentially useless to them without the password to decrypt them an effective method that has seen much use as a part of standard DBMSs to deal with other types of database threats such as malicious employees for example. Depending on the tool they can offer added benefits such as being easier to implement as well as fine tuning the encryption to what is required whether it be a high level of encryption for added security or light encryption for security with less of a performance cost added to it, as well as other added benefits that such tools bring with them, however depending on the amount of encryption and how widespread its use on the database there will be a performance cost as well as the time needed to decrypt the data whenever it is needed.

Based on this it is clear to see that much has been said and done about the issue of SQLIA, including research on the various methods attackers use to gain access to what should be secure data as well as the solutions that have been devised in an attempt to secure against this and ultimately end the threat that it poses, however despite this there is no all inclusive method for dealing with SQLIA as well as the disadvantages some of the current methods have when implemented. Therefore this paper will look further at the current SQLIA methods in use by attackers, the solutions for dealing with them and from this test against several DBMSs whether SQLIA is still an issue.

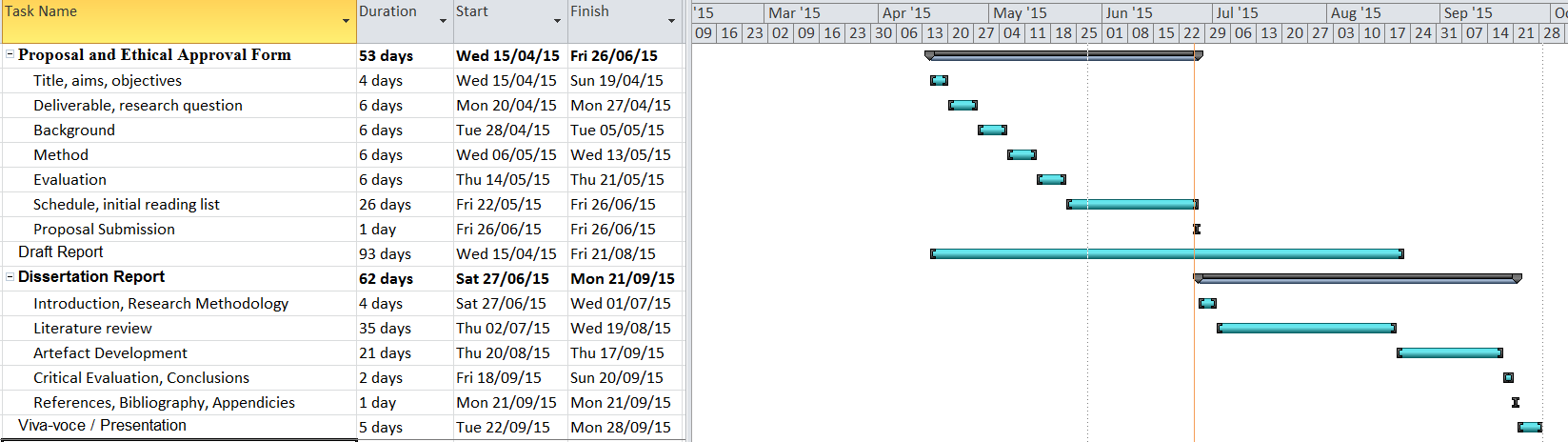
**Method -**

The research method this paper will employ is quantitative as the research performed will be of a secondary basis, copious amounts of journal articles, thesis's, books, conference papers etc from the current research by other researchers will be collected and analysed in order to understand the scope of the issue and be able to see where the research has yet to go or take what has been done further. Research priority will be on case studies where SQLIA occurred in industry, defences were actively used, as well as statistical data on SQLIAs in order to see how much of an issue and how widespread throughout the IT industry it was, where it is now. Statistical data on the various SQLIA methods would be beneficial so as to see which would be best to test against in the artefact as well as the solutions for dealing with them to see which are the most popular for this issue so they can also be used in the artefact and in order to help answer the research question.

The specific research methodology to be used will be the waterfall method, this will involve an analysis of exactly what is required to develop the artefact as well as answering the research question, next a design will be planned out for the proposed artefact which will take advantage of what was learned in the analysis stage, from this the artefact will be developed according to the design and then tested as shown in the deliverable, this will be analysed in order to formulate the answer to the research question.

**Evaluation -**

This paper has looked at various SQLIA methods in use by attackers as well as the solutions for dealing with them and the advantages and disadvantages that come with them, however compared to the amount of research that has been performed in this area it is apparent that this is not a comprehensive introduction to the topic by any means, therefore if there was time this could be improved to find and document even more SQLIA methods and solutions as well as providing examples of statistical data on their use for and against the issue at hand, also including examples of these in use with specific case studies and from this be able to make a more well informed analysis of both sides of SQLIA.

**Provisional schedule -**

**Initial reading list -**

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>

ALLEN, J 2014, 'It's Two A.M.: Do You Know Where Your Data Is and Who Can Access It?', American Journal Of Family Law, 28, 1, pp. 20-24, Academic Search Complete, EBSCOhost, viewed 10 May 2015. Available at:

<http://web.b.ebscohost.com/ehost/detail/detail?sid=352ca9a7-c9ce-4492-b269-d3c382864f4f%40sessionmgr113&vid=2&hid=124&bdata=JnNpdGU9ZWhvc3QtbGl2ZQ%3d%3d#db=a9h&AN=94589596>

Popa, R, Redfield, C, Zeldovich, N, & Balakrishnan, H 2012, 'CryptDB: Processing Queries on an Encrypted Database', Communications Of The ACM, 55, 9, pp. 103-111, Academic Search Complete, EBSCOhost, viewed 11 May 2015. Available at:

<http://web.b.ebscohost.com/ehost/detail/detail?sid=1d1000ae-c4a7-4284-9cfd-34e41ec6b65c%40sessionmgr111&vid=0&hid=124&bdata=JnNpdGU9ZWhvc3QtbGl2ZQ%3d%3d#db=a9h&AN=79648445>

de Morais, W, Lundström, J, & Wickström, N 2014, 'Active In-Database Processing to Support Ambient Assisted Living Systems', Sensors (14248220), 14, 8, pp. 14765-14785, Academic Search Complete, EBSCOhost, viewed 12 May 2015. Available at:

<http://web.b.ebscohost.com/ehost/detail/detail?sid=ecab6623-2d08-49b9-9155-ce5c4126a523%40sessionmgr198&vid=0&hid=124&bdata=JnNpdGU9ZWhvc3QtbGl2ZQ%3d%3d#db=a9h&AN=97665156>

Cho, Y, & Pan, J 2015, 'Design and Implementation of Website Information Disclosure Assessment System', Plos ONE, 10, 3, pp. 1-29, Academic Search Complete, EBSCOhost, viewed 13 May 2015. Available at:

<http://web.b.ebscohost.com/ehost/detail/detail?sid=43b56978-87a6-46e8-a556-e9892551ccbd%40sessionmgr115&vid=0&hid=124&bdata=JnNpdGU9ZWhvc3QtbGl2ZQ%3d%3d#db=a9h&AN=101838118>

Yaseen, Q, & Panda, B 2012, 'Insider threat mitigation: preventing unauthorized knowledge acquisition', International Journal Of Information Security, 11, 4, pp. 269-280, Academic Search Complete, EBSCOhost, viewed 14 May 2015. Available at:

<http://web.b.ebscohost.com/ehost/detail/detail?sid=f9b1c3b2-1f6a-42be-91f4-fb4740d469c4%40sessionmgr115&vid=0&hid=124&bdata=JnNpdGU9ZWhvc3QtbGl2ZQ%3d%3d#db=a9h&AN=77959064>

Chakraborty, A, Majumdar, A, & Sural, S 2010, 'A column dependency-based approach for static and dynamic recovery of databases from malicious transactions', International Journal Of Information Security, 9, 1, pp. 51-67, Academic Search Complete, EBSCOhost, viewed 15 May 2015. Available at:

<http://web.b.ebscohost.com/ehost/detail/detail?sid=fee2b5f0-3760-4f84-bdce-a844c2c97265%40sessionmgr114&vid=0&hid=124&bdata=JnNpdGU9ZWhvc3QtbGl2ZQ%3d%3d#db=a9h&AN=47728631>

Yu, H, Lai, H, Chen, K, Chou, H, Wu, J, Dorjgochoo, S, Mendjargal, A, Altangerel, E, Tien, Y, Hsueh, C, & Lai, F 2013, 'A sharable cloud-based pancreaticoduodenectomy collaborative database for physicians: Emphasis on security and clinical rule supporting', Computer Methods & Programs In Biomedicine, 111, 2, pp. 488-497, Academic Search Complete, EBSCOhost, viewed 16 May 2015. Available at:

<http://web.b.ebscohost.com/ehost/detail/detail?sid=d12e5a0a-0328-4fb4-87a5-6fb4c96f6448%40sessionmgr112&vid=0&hid=124&bdata=JnNpdGU9ZWhvc3QtbGl2ZQ%3d%3d#db=a9h&AN=89136411>

HWEEHWA, P, & XUHUA, D 2014, 'Privacy-Preserving Ad-Hoc Equi-Join on Outsourced Data', ACM Transactions On Database Systems, 39, 3, pp. 23-23:40, Academic Search Complete, EBSCOhost, viewed 17 May 2015. Available at:

<http://web.b.ebscohost.com/ehost/detail/detail?sid=c6fe2ef4-fd11-4840-ab08-a83ea08e79a6%40sessionmgr111&vid=0&hid=124&bdata=JnNpdGU9ZWhvc3QtbGl2ZQ%3d%3d#db=a9h&AN=98910097>

Wei, D, Murugesan, S, Kuo, S, Naik, K, & Krizanc, D 2013, 'Enhancing Data Integrity and Privacy in the Cloud: An Agenda', Computer, 46, 11, pp. 87-90, Academic Search Complete, EBSCOhost, viewed 18 May 2015. Available at:

<http://web.b.ebscohost.com/ehost/detail/detail?sid=45b2a410-a7d1-4465-affb-0899b04e9f84%40sessionmgr111&vid=0&hid=124&bdata=JnNpdGU9ZWhvc3QtbGl2ZQ%3d%3d#db=a9h&AN=92663519>

Boicea, A, Ghita, V, Radulescu, F, & Sarbu, A 2010, 'ENCRYPTION STRATEGIES IN DATABASES', Annals Of DAAAM & Proceedings, pp. 165-166, Academic Search Complete, EBSCOhost, viewed 19 May 2015. Available at:

<http://web.b.ebscohost.com/ehost/detail/detail?sid=1c50ad14-dfa2-4a35-ac90-2165e1abfc4c%40sessionmgr110&vid=0&hid=124&bdata=JnNpdGU9ZWhvc3QtbGl2ZQ%3d%3d#db=a9h&AN=55674541>

NAGY, N, & AKL, S 2010, 'A QUANTUM CRYPTOGRAPHIC SOLUTION TO THE PROBLEM OF ACCESS CONTROL IN A HIERARCHY', Parallel Processing Letters, 20, 3, pp. 251-261, Academic Search Complete, EBSCOhost, viewed 20 May 2015. Available at:

<http://web.b.ebscohost.com/ehost/detail/detail?sid=1f5543fe-6571-4d34-9e08-208750e7b82b%40sessionmgr115&vid=0&hid=124&bdata=JnNpdGU9ZWhvc3QtbGl2ZQ%3d%3d#db=a9h&AN=53843832>

Suciu, D 2012, 'SQL on an Encrypted Database', Communications Of The ACM, 55, 9, p. 102, Academic Search Complete, EBSCOhost, viewed 21 May 2015. Available at:

<http://web.b.ebscohost.com/ehost/detail/detail?sid=2c0daa8e-1793-4ff9-88f0-5856905aa3fc%40sessionmgr111&vid=2&hid=124&bdata=JnNpdGU9ZWhvc3QtbGl2ZQ%3d%3d#db=a9h&AN=79648438>

Roy, S, Singh, A, Sairam, A 2011, ‘Detecting and Defeating SQL Injection Attacks’, International Journal of Information and Electronics Engineering, 1, 1, pp.38-46, Viewed 15 June 2015. Available at:

<http://www.ijiee.org/papers/6-E080.pdf>

Kerner, SM 2013, 'DB Networks Looks to Detect SQL Injection With New Appliance', *Eweek*, p. 1, Academic Search Complete, EBSCO*host*, viewed 24 June 2015. Available at:

<http://web.b.ebscohost.com/ehost/detail/detail?vid=3&sid=9916cce8-fb31-4ff2-94df-2d60ca2f897d%40sessionmgr114&hid=123&bdata=JnNpdGU9ZWhvc3QtbGl2ZQ%3d%3d#db=a9h&AN=91701564>

Kindy, D, Pathan, A 2013, ‘A Detailed Survey on various aspects of SQL Injection in Web Applications: Vulnerabilities, Innovative Attacks and Remedies’, International Journal of Communication Networks and Information Security (IJCNIS), 5, 2, pp.80-92, Viewed 24 June 2015. Available at:

<http://www.ijcnis.org/index.php/ijcnis/article/view/364/115>

Salama, S, Marie, M, El-Fangary, L, Helmy, Y 2012, ‘Web Anomaly Misuse Intrusion Detection Framework for SQL Injection Detection’, International Journal of Advanced Computer Science and Applications(IJACSA), 3, 3, pp.133-157, Viewed 24 June 2015. Available at:

<http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.259.4544&rep=rep1&type=pdf#page=133>

Štampar, M 2013, ‘Data Retrieval over DNS in SQL Injection Attacks’, arXiv13033047, pp.1-7, Viewed 24 June 2015. Available at:

<http://arxiv.org/ftp/arxiv/papers/1303/1303.3047.pdf>

Asha, N, Kumar, M, Vaidhyanathan, G 2012, ‘Preventing SQL Injection Attacks’, International Journal of Computer Applications, 52,13, pp.28-32, Viewed 24 June 2015. Available at:

<http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.258.8182&rep=rep1&type=pdf>

Dogbe, E, Millham, R, Singh, P 2013, ‘A combined approach to prevent SQL Injection Attacks’, Science and Information Conference 2013 October 7-9 London UK, pp.406-410, Viewed 24 June 2015. Available at:

<http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6661770>

Patel, N, Mohammed, F, Soni, S 2011, ‘SQL Injection Attacks: Techniques and Protection Mechanisms.’, International journal on computer science and engineering, 3, 27, pp.199-203, Viewed 24 June 2015. Available at:

<http://www.enggjournals.com/ijcse/doc/IJCSE11-03-01-139.pdf>

Tajpour, A, Ibrahim, S, Sharifi, M 2012, ‘Web Application Security by SQL Injection Detection Tools’, International journal of computer science issues, 9, 2, pp.332-339, Viewed 24 June 2015. Available at:

< http://www.ijcsi.org/papers/IJCSI-9-2-3-332-339.pdf>

Ahmad, K, Shekhar, J, Yadav, K 2011, 'Coalesce Techniques to Secure Web Applications and Databases against SQL Injection Attacks', Electronic Journal of Computer Science & Information Technology, 3, 1, pp.26-30, Viewed 24 June 2015. Available at:

<http://ejcsit.uniten.edu.my/index.php/ejcsit/article/view/14/23>

Jang, Y, Choi J 2014, 'Detecting SQL injection attacks using query result size', Computers & Security (2014), 44, pp.104-118, Viewed 24 June 2015. Available at:

<http://ac.els-cdn.com/S0167404814000595/1-s2.0-S0167404814000595-main.pdf?\_tid=a63e4910-1b5b-11e5-9d41-00000aacb361&acdnat=1435251795\_b38933d613ea110bcdc5f7c3070129ee>

Shar, L, Tan, H 2013, 'Predicting SQL injection and cross site scripting vulnerabilities through mining input sanitization patterns', Information and Software Technology (2013), 55, 10, pp.1767-1780, Viewed 24 June 2015. Available at:

<http://ac.els-cdn.com.ezproxy.wlv.ac.uk/S0950584913000852/1-s2.0-S0950584913000852-main.pdf?\_tid=7fd998a0-1b5c-11e5-a50c-00000aab0f02&acdnat=1435252160\_88dad02114910435c3a5b8d682d01316>

Lei, L, Jing, X, Minglei, L, Jufeng, Y 2013, 'A Dynamic SQL Injection Vulnerability Test Case Generation Model Based on the Multiple Phases Detection Approach', 2013 IEEE 37th Annual Computer Software and Applications Conference (2013), pp.256-261, Viewed 24 June 2015. Available at:

<http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6649829>

Noiumkar, P 2012, ' The SQL Injection Attacking Prevention Applying the Design Techniques of IPTABLES', Journal of Convergence Information Technology (2012), 7, 22, pp.66-75, Viewed 24 June 2015. Available at:

<http://www.globalcis.org/jcit/ppl/JCIT2130PPL.pdf>

Abawajy, J 2013, ' SQLIA detection and prevention approach for RFID systems', Journal of Systems and Software (2013), 86, 3, pp.751-758, Viewed 24 June 2015. Available at:

<http://ac.els-cdn.com/S0164121212003159/1-s2.0-S0164121212003159-main.pdf?\_tid=71891994-1b5f-11e5-a1e8-00000aacb362&acdnat=1435253424\_e943fd8ce08f8aa32e017139e486b240>

Johari, R, Sharma, P 2012, 'A survey on web application vulnerabilities (SQLIA, XSS) exploitation and security engine for SQL injection', Proceedings - International Conference on Communication Systems and Network Technologies, CSNT 2012 (2012), pp.452-458, Viewed 24 June 2015. Available at:

<http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6200667>

Alserhani, F, Akhlaq, M, Awan, I, Cullen, A 2011, 'Event-based alert correlation system to detect SQLI activities', Proceedings - International Conference on Advanced Information Networking and Applications, AINA (2011), pp.175-182, Viewed 24 June 2015. Available at:

<http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5763386>

Mittal, P, Jena, S 2013, 'A fast and secure way to prevent SQL injection attacks', 2013 IEEE Conference on Information and Communication Technologies, ICT 2013 (2013), pp.730-734, Viewed 24 June 2015. Available at:

<http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6558190>

Prabakar M, KarthiKeyan, M, Marimuthu, K 2013, 'An efficient technique for preventing SQL injection attack using pattern matching algorithm', 2013 IEEE International Conference ON Emerging Trends in Computing, Communication and Nanotechnology (ICECCN) (2013), pp.503-506, Viewed 24 June 2015. Available at:

<http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6528551>

Avireddy, S, Perumal, V, Zowraj, N, Kannan, R, Thinakaran, P, Ganapthi, S, Gunasekaran, J, Prabhu, S 2012, 'Random4: An application specific randomized encryption algorithm to prevent SQL injection', Proc. of the 11th IEEE Int. Conference on Trust, Security and Privacy in Computing and Communications, TrustCom-2012 - 11th IEEE Int. Conference on Ubiquitous Computing and Communications, IUCC-2012 (2012), pp.1327-1333, Viewed 24 June 2015. Available at:

<http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6296134>

**Hardware/software needed -**

Modern PC, Oracle and MySQL DBMS

**Supervisor (if known) -**

Jun Li

**UNIVERSITY OF WOLVERHAMPTON**

**SCHOOL OF TECHNOLOGY**

**ETHICAL CONSIDERATION FOR STUDENTS STUDYING TAUGHT PROGRAMMES**

|  |  |  |  |
| --- | --- | --- | --- |
| **Section 1: Your details** | | | |
| **First Name & Surname:** | James Braznell | **Student No:** | 1007022 |
| **Course:** | Computer Science | | |
| **Project Title** | SQL Injection: - The popular methods, solutions and is it still an issue | | |
| **Supervisor:** | Jun Li | | |

|  |  |
| --- | --- |
| **Section 2: Your Project Topic** | |
| **2.1** What problem is this project addressing? (100 words or less) | The issue of SQL Injection attacks, whether it is still an issue, the popular methods, solutions and how it can be dealt with better. |
| **2.2** Will information or artefact resulting from your project be available externally to the University? | Yes/**No**? |
| **2.2.1**  **If you answered ‘yes’ to 2.2,**  Will any such information place anyone at risk or possibly result in any action that might be detrimental to their wellbeing? (See guidelines) | Yes/No? |
| **2.2.2**  In what format will the information or artefact be made available? | In a word document submitted on WOLF |

|  |  |
| --- | --- |
| **Section 3: Method of Data Collection** | |
| **Please attach samples with this form if you intend to do interviews, surveys, or questionnaires.** | |
| **3.1** Does any part of your proposed project involve human participants?  If No go to Section 4. | Yes/**No**? |
| **3.1.1**  **If you answered ‘yes’ to 3.1,**  Is the sole involvement of human participants in order to provide opinions to support the specification or testing of an artefact to be produced as an outcome of the project? | Yes/No? |
| **3.1.2**  **If you answered ‘yes’ to 3.1.1,**  Does this artefact/information have any characteristics which might be detrimental to the wellbeing of any human participants in your project? If so, explain. | Yes/No? |
| **3.2**  **If you answered ‘yes’ to 3.1,**  Are there other ways you might meet your project aims without involving human participants? If not, why?  If yes discuss with your Supervisor how you will achieve this and go to section 4. |  |
| **3.2.1**  How will you select your participants? |  |
| **3.2.2**  How many participants will you contact? |  |
| **3.2.3**  How will you approach potential participants? E.g. email, letter, face to face? |  |
| **3.2.4**  Are your participants adults? (over 18 and competent to give consent) If no, answer 3.2.5 | Yes/No? |
| **3.2.5**  Are your participants children or adults over 18 and not competent to give consent? If yes, why is it necessary to involve these participants? (See guidelines)  Explain how you will ensure parental/guardian consent. |  |
| **3.2.6**  Are you offering any incentives to any of your participants, financial or otherwise? (See guidelines) | Yes/No? |
| **3.2.7**  How much time do you estimate will be needed from any participants? (See guidelines) |  |
| **3.2.8**  Please list the method of data collection and analysis intended to be used |  |
| **3.2.9**  Will all of the data collected contribute towards your results? |  |

|  |  |
| --- | --- |
| **Section 4: Confidentiality and data handling** | |
| **Please read methods of ensuring confidentiality in the guidelines.** | |
| **4.1** Will you ensure the anonymity of data collected from/and about participants? | **Yes**/No |
| **4.2** Will you store/protect data collected from individuals e.g. password protected files? | **Yes**/No |
| **4.3** Once your project is complete and information is no longer needed, will you destroy your data? | **Yes**/No |
| **4.4** Will anyone else have access to the data collected? | Yes/**No** |
| **If so,**  (i) please name the individuals and/or groups that will have access;  (ii) why is access being given to those listed in (i)? |  |

|  |  |
| --- | --- |
| **Section 5: Working with other parties and companies** | |
| **5.1** Will you be using data on subjects held by another party or organisation? | Yes/**No** |
| **If Yes,**  (i) Please give details.  (ii) How will you gain access to this information? |  |
| **5.2** Do you require written permission from a company, organisation or location, e.g. an employer or local authority? | Yes/**No** |
| **If Yes,**  (i) Please complete an [external agreement form](file://C:\Documents%20and%20Settings\in5541\Local%20Settings\Temporary%20Internet%20Files\in7475\Local%20Settings\Documents%20and%20Settings\in7475\Local%20Settings\Documents%20and%20Settings\in5505\Local%20Settings\Temporary%20Internet%20Files\Content.Outlook\0JYTHJ5A\External%20Computing%20Project%20Agreement%20Form.doc) and include this with your submission. |  |
| **NB: If working with another organisation or company please familiarise yourself with their Health & Safety procedures.** | |

**Things you must be aware of:**

**Data Protection Act**: <http://www.ico.gov.uk/what_we_cover/data_protection.aspx>

**Freedom of Information Act**: <http://www.opsi.gov.uk/Acts/acts2000/ukpga_20000036_en_1>

[University of Wolverhampton Ethical Approval Procedural Guidelines](http://www.wlv.ac.uk/PDF/aca-pols-ethics-scrutiny.pdf)

**Checklist:**

1. If you are using a questionnaire or interview sheet please include a list of sample questions with your submission.

2. In addition, please include an introductory cover letter stating some information about you, your project proposal and how your data will be used.

3. If you are undertaking a project involving a company or organisation you will need to show that you have approval from that organisation. Please include a completed copy of the [External Agreement Form](file://C:\Documents%20and%20Settings\in5541\Local%20Settings\Temporary%20Internet%20Files\in7475\Local%20Settings\Documents%20and%20Settings\in7475\Local%20Settings\Documents%20and%20Settings\in5505\Local%20Settings\Temporary%20Internet%20Files\Content.Outlook\0JYTHJ5A\External%20Computing%20Project%20Agreement%20Form.doc).

|  |  |
| --- | --- |
| **Student’s Declaration**  Sign and date against **one** declaration **only** | |
| **Category 0.** I have answered  ‘No’ to questions **2.2** and **3.1**.  My project involves no human participation except for myself and I agree to ensure that any information or artefact produced will not be available outside the University. | James Braznell  26/06/15 |
| **Category A1.** I have answered (delete one from each block)   |  | | --- | | ‘Yes’ to questions **2.2**, **4.1**, **4.2** and **4.3** and ‘No’ to questions **2.2.1** and **4.4**. | | ‘No’ to question **2.2** |   **and**   |  | | --- | | ‘Yes’ to questions **3.1**, **3.1.1** and **3.2.4** and ‘No’ to question **3.1.2** | | ‘No’ to question **3.1** |   My project involves limited human participation and I agree to ensure that   1. any such participation is not detrimental in any way to the interests of the participants; 2. all information collected as a part of the project will be handled in accordance with the answers that I gave to question **4**; 3. No information or artefacts which may place anyone at risk or be detrimental to their wellbeing will be made available outside the University. |  |
| **Category A2.** I have answered  ‘Yes’ to question **3.1**  **or** I have answered  ‘Yes’ to question **2.2**  and my answers to subsequent questions prevent the project being classified as A1.  My project involves human participation and may present some risk to participants. I have considered alternative means of pursuing the project which do not entail this risk but believe that there is no practicable alternative. I agree to ensure that I take all necessary steps to minimise risks to participants and third parties. I agree not to proceed with any activities involving human participation until I have received approval from the Department Ethics Panel. |  |
| **Category B-E.** My project does not conform to Category 0, A1 or A2. I have considered alternative means of pursuing the project which do not entail risk to human participants but believe that there is no practicable alternative to the proposal made. I agree to ensure that I take all necessary steps to minimise risks to participants. I agree not to proceed with any activities involving human participation until I have received approval from the School or University Ethics Committee, as appropriate. |  |

|  |  |
| --- | --- |
| **Supervisor’s Declaration**  Sign and date against **one** declaration **only** | |
| **Category 0 or A1.** I concur with the classification of this project as **0** or **A1** and authorise continuation of the project. I have forwarded a copy of this form to the Department Ethics Panel for monitoring purposes. |  |
| **Other.** I believe that this project should be classified other than **0** or **A1.** I do **not** authorise continuation of the project until approval has been received from the appropriate Ethics Panel or Committee. I have forwarded a copy of this form to the Department Ethics Panel for consideration. |  |

**FOR SUPERVISOR/PANEL/COMMITTEE USE ONLY:**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **CLASSIFICATION ALLOCATED BY SUPERVISOR** | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| **0, A1** |  | **Supervisor Action:** Authorise and forward to DEP | | | | | | | | | | | | | | | | | | Date | | | |  | | | | |
| **DEP Action:** File for possible monitoring | | | | | | | | | | | | | | | | | | | Date | | | |  | | | | |
|  | | Selected for monitoring | | | |  | (tick) | | | | | | | | | | | | Date | | | |  | | | | |
| Classification agreed? | | | | Yes |  | No |  | | | If ‘No’, give: | | | | | | | | | | | | | | | |
| reason | | | |  | | | | | | | | | | | | | | | | | | | | | |
| action | | | |  | | | | | | | | | | | | | | | | | | | | | |
| **Other** |  | **Supervisor Action:** Refer to DEP for decision | | | | | | | | | | | | | | | | | | Date | | | |  | | | | |
| **CLASSIFICATION ALLOCATED BY DEPARTMENT ETHICS PANEL** | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| **0, A1** | |  | **DEP Action:** Project authorised to continue | | | | | | | | | | | | | | | | | Date | | | |  | | | |
| **A2** | |  | **Considered by DEP below** | | | | | | | | | | | | | | | | | Date | | | |  | | | |
| **2.2** Is any risk associated with access to project acceptable in context? If no, give reasons below: | | | | | | | | | | | | | | | | | Yes | | |  | | | No | |  |
|  | | | | | | | | | | | | | | | | | | | | | | | | | |
| **3.1** Is involvement of human participants justified? If no, give reasons below: | | | | | | | | | | | | | | | | | Yes | | |  | | | No | |  |
|  | | | | | | | | | | | | | | | | | | | | | | | | | |
| **3.3** Is experimental method acceptable with regard to risk and inconvenience to participants? If no, give reasons below: | | | | | | | | | | | | | | | | | Yes | | |  | | | No | |  |
|  | | | | | | | | | | | | | | | | | | | | | | | | | |
| **4** Are arrangements for confidentiality and data protection appropriate? If no, give reasons below | | | | | | | | | | | | | | | | | Yes | | |  | | | No | |  |
|  | | | | | | | | | | | | | | | | | | | | | | | | | |
| **5** Do arrangements for working with external bodies protect interests of participants and the external bodies? If no, give reasons below | | | | | | | | | | | | | | | | | Yes | | |  | | | No | |  |
|  | | | | | | | | | | | | | | | | | | | | | | | | | |
| **DEP Action:** Continuation of project approved: | | | | | | | | Yes | | |  | | No | |  | | Date | | | |  | | | | |
| Conditions: | | | | | | | | | | | | | | | | | | | | | | | | | |
| **Other** | |  | **DEP Action:** Refer to School Ethics Committee | | | | | | | | | | | | | | | | | Date | | | |  | | | |
| **CLASSIFICATION ALLOCATED BY SCHOOL ETHICS COMMITTEE** | | | | | | | | | | | | | | | | | | | | | | | | | |
| **0, A1** | |  | **SEC Action:** Continuation of project approved | | | | | | | | | | | | | | Date | | | |  | | | | |
| **A2, B** | |  | **Considered by SEC below** | | | | | | | | | | | | | | Date | | | |  | | | | |
| **2.2** Is any risk associated with access to project acceptable in context? If no, give reasons below: | | | | | | | | | | | | | | | Yes | | |  | | | | No |  |
|  | | | | | | | | | | | | | | | | | | | | | | | |
| **3.1** Is involvement of human participants justified? If no, give reasons below: | | | | | | | | | | | | | | | Yes | | |  | | | | No |  |
|  | | | | | | | | | | | | | | | | | | | | | | | |
| **3.3** Is experimental method acceptable with regard to risk and inconvenience to participants? If no, give reasons below: | | | | | | | | | | | | | | | Yes | | |  | | | | No |  |
|  | | | | | | | | | | | | | | | | | | | | | | | |
| **4** Are arrangements for confidentiality and data protection appropriate? If no, give reasons below | | | | | | | | | | | | | | | Yes | | |  | | | | No |  |
|  | | | | | | | | | | | | | | | | | | | | | | | |
| **5** Do arrangements for working with external bodies protect interests of participants and the external bodies? If no, give reasons below | | | | | | | | | | | | | | | Yes | | |  | | | | No |  |
|  | | | | | | | | | | | | | | | | | | | | | | | |
| **SEC Action:** Continuation of project approved: | | | | | | | Yes | | |  | | No | |  | | | Date | |  | | | | |
| Conditions: | | | | | | | | | | | | | | | | | | | | | | | |
| **Other** | |  | **SEC Action:** Refer to University Ethics Committee | | | | | | | | | | | | | | | | Date | |  | | | | |

**Guidelines**

**Section 1: Categorisation for ethical approval**

**Category 0:** There are no third parties directly involved in the project and any artefacts produced by the project will not be accessible to a general audience.

**Category A1**

Projects involving human volunteers are involved solely for the purposes of:

- providing data to inform the specification of an artefact

- testing the usability or fitness for purpose of an artefact

where the nature of that artefact or its use will present no risk to the volunteers

and, if any artefact is accessible to a general audience, access to that artefact will present no risk.

**Category A2**

Projects involving human volunteers other than those defined in category A1 but not in activities defined in other categories or if any artefact is accessible to a general audience, access to that artefact may present some risk.

**Category B**

Projects involving human volunteers including potential risk, for instance,

studies using new research methodologies, studies involving certain vulnerable

populations or therapeutic interventions or other significant risk to anyone involved in

the research (but not including trials of artefacts intended for therapeutic purposes).

**Category C**

Research being conducted by staff or postgraduate research students involving

Patients, clients staff, records etc. within the sphere of the NHS, Social Services, etc (but not including clinical trials of medicinal or related products).

**Category D**

Research being conducted by undergraduate or taught postgraduate students involving

Patients, clients staff, records etc. within the sphere of the NHS, Social Services, etc (but not including clinical trials of medicinal or related products).

**Category E**

Clinical trials of medicinal or related products involving patients or healthy volunteers as direct users of the product.

**Question 2.2:** You should answer yes if your artefact, product or information might be of direct risk or might lead or encourage people to alter their behaviour in a way which would be detrimental to them. Examples of direct potential risk might be a machine that could injure someone if it malfunctioned or a web resource which contained information which if it was misused would lead to risk (for instance, children’s identities or addresses). Examples of artefacts which might encourage detrimental behaviour could be a web resource offering alternatives to expert (such as GP or lawyer) advice or products which purport to have a therapeutic effect.

**Question 3.2.5:** As a general principle, all participants should be informed of their role in the experiment and freely consent (in writing) to it, which implies competence to give consent. Very occasionally it may be necessary to undertake an experiment without consent, or with participants who are not competent but then any decision about the acceptability of the proposal would be taken on the basis of the absolute benefit of the experiment in a wider context, and it would have to be established that there was no alternative.

**Question 3.2.6:** With regard to freedom of consent, it likely that this principle would be breached of the participants were subject to some kind of inducement or coercion, however minor. For instance, it is likely that participants who were under the management of the person undertaking the experiment would be considered to be under a degree of coercion.

**Question 3.2.7:** It may be considered that expecting a participant to spend undue time or effort participating in an experiment would be detrimental to the interests of that person, particularly where the results of the work offered no clear benefits. It may be appropriate to compensate participants for their time, but it is not acceptable to offer inducements to participate.

**Section 4 Anonymity:**

It is to be expected that due care and attention be paid to protecting information about individuals. Depending on the nature of the experiment, the following may be considered.

* Type 1: Complete anonymity of participants (i.e., You will not meet, or know the identity of participants, as they are part of a random sample and are required to return responses with no form of personal identification)?
* Type 2: Anonymised samples or data (i.e., an irreversible process whereby identifiers are removed from data and replaced by a code, with no record retained of how the code relates to the identifiers. It is then impossible to identify the individual to whom the sample of information relates)?
* Type 3: De-identified samples or data (i.e., a *reversible* process whereby identifiers are replaced by a code, to which you retain the key, in a secure location)?
* Type 4: Subjects being referred to by pseudonym in any publication arising from the project?
* Type 5: Any other method of protecting the privacy of participants? (eg. use of direct quotes with specific, written permission only; use of real name with specific, written permission only)