Audience

This paper has been written for senior management and the tactical security professional. An elementary understanding of information security is assumed.

Background and Introduction

The software bug has existed since the first electromechanical tabulating computers engaged their relay contacts in the late 19th Century. The exploitation of the more modern bug in software has become an unfortunate yet common place security threat in today's information systems.

The seminal Phrack article "NT Web Technology Vulnerabilities" authored by the esteemed hacker Rain Forrest Puppy in 1998, broke the ice on the weaknesses of database security. This paper released new knowledge and methods for attacking a database behind a security infrastructure on the Internet. Be it ethical or not, a new era of database attacks were born.

Firewalls and other intrusion prevention mechanisms allow users and attackers alike to browse an e-commerce website through the hypertext transfer protocol (HTTP). Through this opening and with the knowledge of how to query a database, it now became possible for customers and unethical hackers to reach out and touch the back end of e-commerce infrastructures, to browse and touch the core of a business. In 1998, the crest[12] of the Internet dot com boom wave had begun – see figure 1, as it opened doors for new and old businesses the wave also brought along with it the oldest ill gains of society – crime – see figure 2.

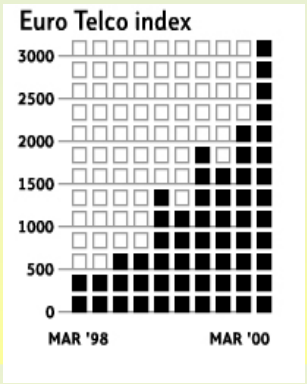

Figure 1 - The dot-com boom (Taken from BTPLC)

Figure 2 – Internet crime (Taken from the Home Office)

The Department for Trade and Industry has been producing statistical reports based on information security attacks on UK businesses for the past 15 years. These reports have observed and reported trends on the effects of security vulnerabilities and the success of mitigation on business – from a business perspective. For the past 5 years the SANS institute has been producing a top 20 of the most common security vulnerabilities for a technical-hands-on audience. This top 20 list has provided a water mark by which to lower the Internet security threats to online businesses.

As a result of these publications, businesses should now be more aware than ever of the security problems that SQL injection can bring. The fledgling white-hat community of security experts in 1998 has arguably increased and improved over the eight years since the dot-com boom. However, businesses are ***still*** threatened or suffering from security risks and attacks caused by old problems such as SQL injection attacks.

SQL injection – is this a business or technical problem?

Ordinary common sense dictates that a business exists because of the revenue it generates from its customers. Technology provides a means to an end. To clarify the problems of SQL injection we first need to distil a business into simple terms. A business is made up of two camps:

- Strategic planners, the long term thinkers – C level officers, directors and managers who drive the business direction.
- Tactical implementers, short term thinkers – IT designers, implementers, support staff drawing on the strategic direction to produce products for the business and provide a support framework around it.

Based on this hypothesis and simplification of the structure of a business, it is arguable that SQL injection is a problem for both camps. The problems and solutions that have and are being tried and tested will now be discussed further.

[1] Top 10 dot-com flops, CNET , http://www.cnet.com/4520-11136_1-6278387-1.html [Online] (Accessed 27th May 2006)
[2] The boom and the crash, http://www.btplc.com/thegroup/Networkstory/HTML/slide.aspx_slide=97.html [Online] (Accessed 27th May 2006)

Since the turn of the 21st century, information security due diligence in business has evolved in leaps and bounds from a business policy and technical viewpoint. The understanding of the return on investment on technical mitigation has improved, along with an understanding that security is not just a product, but rather a chain of best practice processes.

CERTS spanning across public and private sector entities have evolved and integrated into the security research community. Frameworks such as BS7799 (now ISO 27001) and OCTAVE have become internationally accepted standards, leading the way on corporate security policy. The Common Criteria has evolved from the US Orange Book standards as a watermark for secure software and development. Businesses are now able to quantify and qualify risks mitigation to the business and the technical functions. The business leadership are increasingly able to understand each others problems. Yet, the problem of SQL injection still exists. Open source or closed source, Oracle or MySQL, databases are still being attacked through SQL problems. The economics of information with the likes of phishing and pharming motivate crime and increase the black market value of corporate information; keeping SQL injection exploitation alive.

Professor Ross Anderson in a paper based on the economics of information security - Why Information Security is Hard – states that for all the investment in technology and processes to improve information security, it costs more to defend a computer system than it does to attack it. The paper goes on to argue that the attacker requires little investment other than time in comparison to the resources a government or company invest in defence.

Reflecting on this information it can be viewed that information security alone is not a panacea to halting all risks to the business (think internal as well as external threats). Investment in education and staff training is also critical along with the technical solutions. Oracle, Microsoft, MySQL and other software vendors have, working with the security community evolved their patching routines and business relationships improving security along the way.

In spite of all of this mitigation, problems of SQL injection are still occurring, even in new technologies such as RFID. Some answers may rest in software engineering and academic training; however, a great number of SQL web developers are not computer science graduates. So why maintain the use of SQL? The answer is that SQL is easy to understand, easy to use, as well as to develop and solve data based business problems. With this ease of use and comprehension comes flexibility. Flexibility provides a path of least resistance for a business to develop an application to interface with a database. This has resulted in products that customers can evolve and develop to their own needs. Economics and market demand is the leader, the path of least resistance, not security.

Is there a solution?

Bruce Schneier stated in his book Secrets and Lies, “Security is a process, not a product” and he goes on to describe how information security will struggle to gain power to influence at board level, when it doesn’t drastically effect the “bottom-line”. Legislation helps to bind corporations into protecting personal data such as the Data Protection Act 1998 (especially principle seven – security).The Computer Misuse Act 1990 has been arguably effective in deterring and punishing criminals, but legislation is a very slow means of enforcing change.

Industry regulation such as BASIL II is a means of enforcing IT security change for the financial services. However, there are few regulations for other markets. There is a third means of influence; ironically, information security mitigation is sometimes viewed as being like insurance. If insurance companies were to demand (for lower premiums) that software is certified to a certain level, then these costs would come to the attention of the board or senior civil servants in government. This is likely if it is not already to be the next turning point for information security and the mitigation of security threats such as SQL injection.

There is of course more than one perspective and solution to the problem. Database vendors continue to improve patching methodologies and the security of their code and appear to be helping to solve their side of the problem (not every security researcher agrees). However, SQL injection is mostly a problem from and for the consumer. As stated previously, SQL provides the database consumer with flexibility to manipulate data as they wish (i.e. SQL though PHP, Java and PL/SQL). This is something that would be difficult to change, especially as it is a good idea! For that reason, until database consumers are encouraged to mitigate the security threats of SQL injection, the problem will persist. This is why the educational relationships between the vendor, customer and security community are more important than ever in solving the short term as well as the long term problems of SQL injection.

Notes

Wikipedia - Caution should be observed on the content of definitions and descriptions, as moderation is evolving and improving all the time. As such references and validation checks should always be carried out against academic and commercial binding or persuasive authority.

Author: Stuart Thomas