

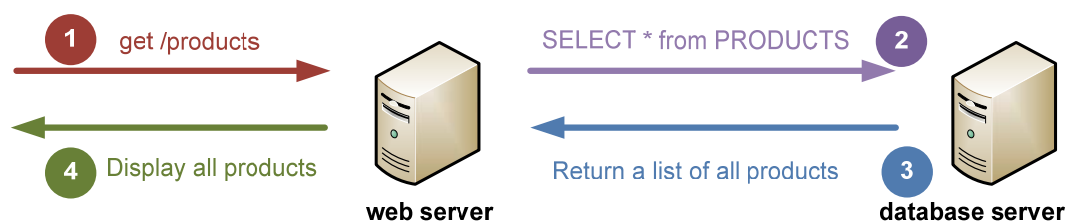
***There was once a time when SQL injection attacks were used to steal information but in recent times we are seeing SQL injection attacks being used to store information. Whilst inserting data into a database doesn't seem to be that threatening, when we consider the possibilities of just what can be inserted and the impact it can have on other users of the database it is a very sinister form of attack. Seccom Global recently analysed a real SQL injection attack that took place and the impact it had.***

A lot of information is stored in databases these days and in many cases we are actually using a database of some form without even knowing it. A huge number of web sites are merely front ends to national or international databases. If you have accessed Facebook, Paypal, SMH, eBay or Amazon then you are using a web driven interface to a SQL database. If you have any sort of e-commerce web site then you need to be conscious of the fact that you need to secure your web server, web applications, database server and databases.

SQL injection attacks are directed at the database and will use any interface available, whether it be a direct connection to the database or via a web based interface (an API) to the database. SQL injection attacks play on the fact that when we design databases and web sites we forget two fundamental best practices:

- checking the length of any data being entered
- checking the format of any data being entered

If we have a database which stores telephone numbers, for example, but we do not specify that a phone number should only contain numbers (0-9) and should not be more than 20 characters in length then we are opening ourselves up to a possible SQL injection attack. A SQL injection attack in very simple terms works by injecting a SQL statement into a data input field. That SQL statement will either obtain data using the SQL SELECT command , modify data using the SQL UPDATE command or add data using the SQL INSERT command.

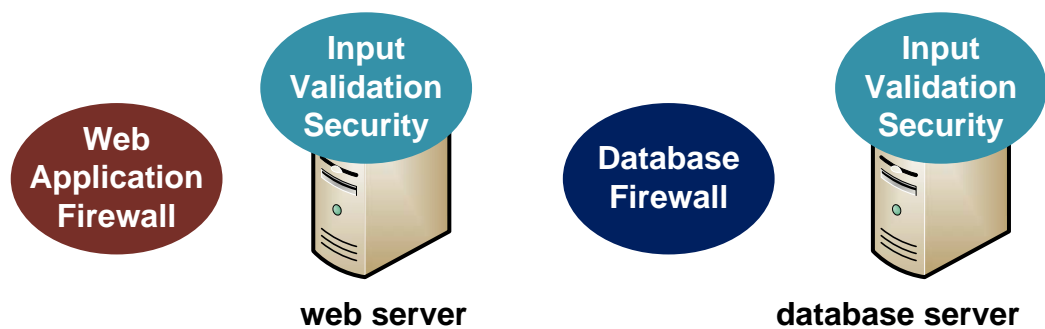


Suppose an online retailer has a database of products that are searchable and browseable from their web site and what was inserted into the products database was some JavaScript that would be selected from the database and executed by a potential customer's browser when he or she attempted to browse the products page. Now, thus far this still does not seem very threatening. On the other hand, if that JavaScript was written to exploit a known browser exploit and download malware or a Trojan from another site without the user's knowledge, and that malware or Trojan also turns the computer into a zombie (or member of a botnet) then this is where the danger lies. Through no fault of the potential customers on a legitimate and seemingly harmless web site simply by trying to locate a product to buy their computer has been compromised.

Can this type of attack be avoided? Absolutely! But it requires due diligence on the part of the web user and, to a greater extent, the web application owner.

Frequently new security issues and bugs are found in web browsers and when the browser vendors create updates and patches these should be applied promptly. This will go a long way to protecting users who browse malicious web sites.

Despite this there are always threats which can not be stopped with patched browsers so it is important that merchants and web application owners also take responsibility for trying to ensure a safe environment. There are a few ways this can be achieved. Ideally a merchant or web application owner would ensure that their web application and database are configured correctly to define the length and format of all contents that can be entered into the database, either directly or via the web site. This technique is known as input validation. Beyond this, where off the shelf products are used we can apply additional layers of security to constantly audit and protect web applications and databases. These types of solutions are referred to as web application and database firewalls.



***To find out how best to eliminate these threats contact Seccom Global on +61 2 96886933 or email us at [info@seccomglobal.com](mailto:info@seccomglobal.com)***