The WebOrion Software Solutions

How to prevent your websites from SQL Injection?

www.theweborion.com info@theweborion.in

THE WEBORION SOFTWARE SOLUTION

SQL Injection is a very serious problem that has caused great damage to organizations and websites alike. When you hear in the news about stolen credit cards or password lists, they often happen through SQL injection vulnerabilities. With a simple browser, an attacker can manipulate your site arguments and try to inject his own commands to your SQL database.

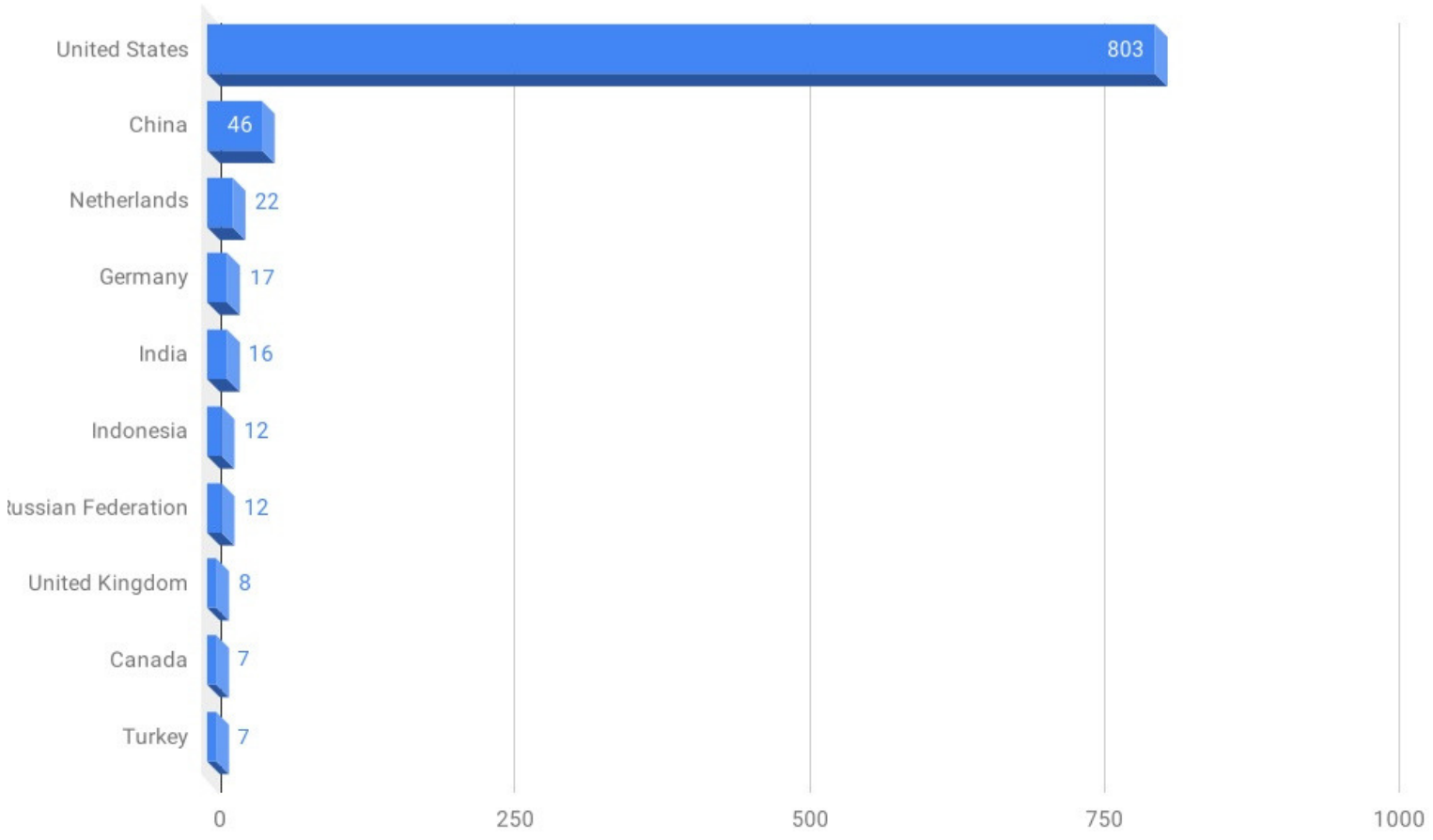
We see more than 50,000 SQL injection attacks per day on Cloud WAF (Website Application Firewall) network.

SQL injection attacks occur when a web application does not validate values received from a web form, cookie, input parameter, etc., before passing them to SQL queries that will be executed on a database server. This will allow an attacker to manipulate the input so that the data is interpreted as code rather than as data.SQL injection attack risk is usually very high and the consequences are severe. A successful attack can bypass authentication and authorization to gain full control of the database, steal sensitive data, change password etc.

TOP 10 countries

SQL Injection attacks in Last 6 Months

The chart below summarise the top 10 attacked countries in six month.



Protecting your websites against SQL Injection

Here is the Some Basic things that you can keep in Mind:

- Encrypt sensitive data.
- Use parameterised queries.
- Use stored procedures.
- Keep all web application software components including libraries, plug-ins, frameworks, web server software, and database server software up to date with the latest security patches available from vendors.
- Do a code review to check for the possibility of second-order attacks.
- Do not use shared database accounts between different web sites or applications.
- Validate user-supplied input for expected data types, including input fields like drop-down menus or radio buttons, not just fields that allow users to type in input.
- always use both side validation client as well as server side .

Protecting your websites against SQL Injection

- always use firewall or proxy and never send direct request to the server.
- configured the “.htacces” file and defined a pattern that only firewall or this types of request will be accepted.
- Configure proper error reporting and handling on the web server and in the code so that database error messages are never sent to the client web browser. Attackers can leverage technical details in verbose error messages to adjust their queries for successful exploitation.

About TheWeborion

- WebOrion™ – Trusted brand since 2012 for Cyber Security
- Our experts convert ideas into reality and add value to our customers by providing quality Cyber Security solutions.
- We thrive in providing security to all types of applications focusing on preventing cyber attacks and data clean-up after cyber incident.

Learn more:

Phone: +1-(202)-765-7053

Email: info@theweborion.com

Website: www.theweborion.com