



Pangolin

Amazing SQL Injection world

 White Paper

Pangolin

Amazing SQL Injection world

How dangerous SQL Injection is?

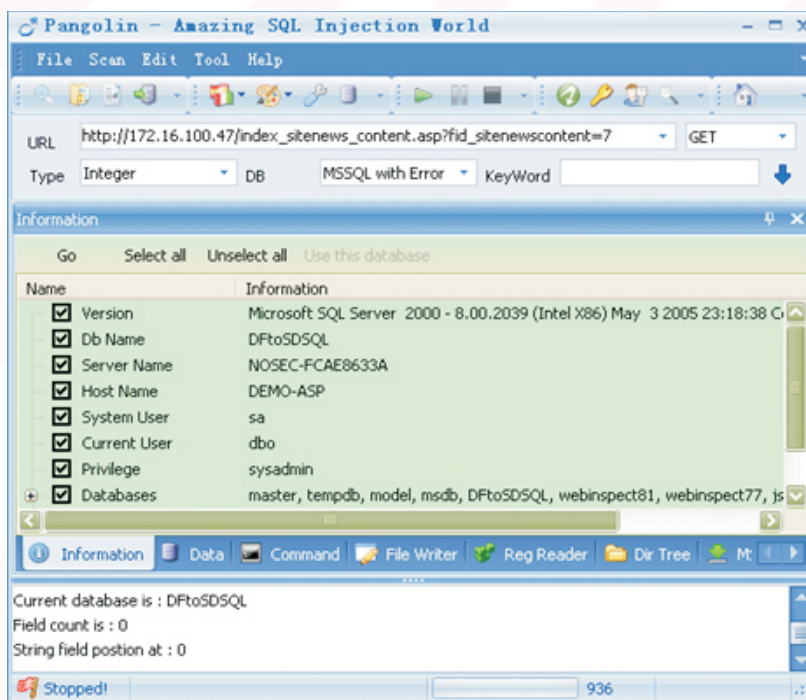
[Injection](#) was listed in OWASP top 10 Web Application Security Risks for 2008, 2009 and 2010. Injection flaws, particularly SQL injection, are common in web applications. Injection occurs when user-supplied data is sent to an interpreter as part of a command or query. The attacker's hostile data tricks the interpreter into executing unintended commands or changing data.

The OWASP Top 10 Web Application Security Risks for 2010 are:

- A1: Injection
- A2: Cross-Site Scripting (XSS)
- A3: Broken Authentication and Session Management
- A4: Insecure Direct Object References
- A5: Cross-Site Request Forgery (CSRF)
- A6: Security Misconfiguration
- A7: Insecure Cryptographic Storage
- A8: Failure to Restrict URL Access
- A9: Insufficient Transport Layer Protection
- A10: Unvalidated Redirects and Forwards

What Pangolin can do?

Pangolin is an automatic SQL injection penetration testing (Pen-testing) tool for Website manager or IT Security analyst. Its goal is to detect and take advantage of SQL injection vulnerabilities on web applications. Once it detects one or more SQL injections on the target host, the user can choose among a variety of options to perform an extensive back-end database management system fingerprint, retrieve DBMS session user and database, enumerate users, password hashes, privileges, databases, dump entire or users specific DBMS tables/columns, run his own SQL statement, read specific files on the file system and more.



↑ Pangolin pull database info through vulnerability if SQL injection was exist.

Pangolin is recommended by many web security experts all over the world

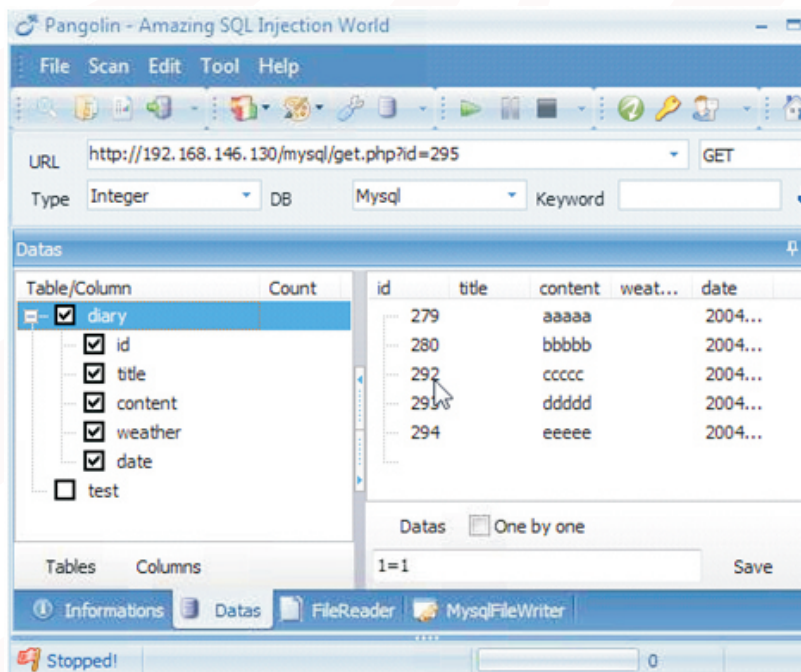
Pangolin is a professional SQL Injection test tools widely used by Cyber Security Experts. Pangolin also listed here:

- OWASP
- Red Database Security
- HACKTIMES
- SECURITY DATABASE
- DARKNET
- TECHIMO
- WAKOOPA
- PENTESTIT

Protects your financial and intellectual property

Once your website been tested by Pangolin. Website administrator will know what should do to protect databases from SQL injection attacks.

It proactively prevents the theft from happening and continuously protects the valuable assets stored in your databases.



↑ Pangolin pull data through vulnerability if SQL injection was exist.

Test many types of databases

Your web applications using Access,DB2,Informix,Microsoft SQL Server 2000,Microsoft SQL Server 2005,Microsoft SQL Server 2008,MySQL,Oracle,PostgreSQL,Sqlite3,Sybase? Pangolin supports all of them.

Protects your reputation

Hackers can gain access to your web server and database console through vulnerability if SQL injection was exist. Once in control, they can use your servers to do whatever they want – such as sending spam and/or attacking other destinations from your servers. If this happens and you end up on a blacklist as a result of this illegal activity, you may find that your legitimate incoming and outgoing traffic is rejected. You'll lose sales, valuable channels of communication with your customers, and end up involved in lengthy, frustrating negotiations to get off the blacklists. Pangolin can tell you all SQL inject possibility.

About NOSEC

NOSEC, Web Application Security Expert, provides products and service to over 100 organizations. Protect Web Application from malware; prevent the loss of confidential information. JSky delivers best-in-class security solutions that allow organizations to work in new, more efficient and innovative ways and that keep employees productive anytime, anywhere.

NOSEC has its roots in Web Application and continues to develop its core strength in discovering and classifying content across all its product offerings. NOSEC helps organizations secure essential information by providing service and products for internal and external Web Application even in the Web 2.0 world.

NOSEC keeps maximize business opportunities while minimizing the unintended consequences of connectedness.



Copyright © 2009 NOSEC Technologies Co., Ltd

All Rights Reserved

NOSEC, the NOSEC logo, JSky, iiScan are trademarks of NOSEC Technologies Co., Ltd in China, other countries or both. Other company, product and service names may be trademarks or service marks of others.

Disclaimer: The customer is responsible for ensuring compliance with legal requirements. It is the customer's sole responsibility to obtain advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulatory requirements that may affect the customer's business and any actions the reader may have to take to comply with such laws. NOSEC does not provide legal advice or represent or warrant that its services or products will ensure that the customer is in compliance with any law or regulation.