IDG Business Network : CFOworld | CIO | CSO | Techworld | ARN

COMPUTERWORLD
THE VOICE OF IT MANAGEMENT

Technology | Reviews | Discussion Forums | Careers | Tools

Scanning tool looks to wipe out vulnerable code

Howard Dahdah (Computerworld) | 14 July, 2005 16:46 | Comments | Like

A new of piece software promises to provide an instant audit of source code, notifying developers of insecure coding practices and vulnerabilities.

CodeScan, developed by CodeScan Labs and released by Security-Assessment.com, analyses source code looking for vulnerabilities such as Cross-site scripting, SQL injection and input filtering.

To process the source files, CodeScan attempts to emulate a Web server by interpreting the source code. The processing starts at the main or global function of the source file, and traces the execution flow into and between functions and other routines. Variable assignments are then tracked, allowing CodeScan to build a picture of what has happened to a variable in its lifetime.

"By tracking the assignment of possible user input, CodeScan can make intelligent decisions about whether the input is used in a dangerous way," said Drazen Drazic, general manager Security-Assessment.com Australia.

He said most of the CodeScan rules are based around the detection of functions that are used with user-supplied input that has not being "filtered or sanitized".

CodeScan traces the possible values of variables as part of its vulnerability detection engine. During the life of a variable, values may be passed through functions that can perform 'filtering' of user-supplied input. CodeScan attempts to rank these functions and gives them a 'filter score'.

According to Drazic, CodeScan comes with information on the most commonly used syntax terms for each language with a predetermined filter score. Filter scores range between 0 and 100.

"Reported results with a low value or a value of zero are more likely to be vulnerable than those results with a higher value. This filtering allows the user to make a good judgement about whether a reported vulnerability could

RELATED WHITEPAPERS

- Legacy Tools: Not Built for Today's Helpdesk
- Pulling the Plug on Legacy Log Management
- The legal risks of uncontrolled web use and email content
- IDC white paper: "Quantifying the business value of VMware View"

COMMUNITY COMMENTS

- "Labor left Loons!" on **Report bombs Aussie broadband**
- "Hell, if it ever went through, it would be a neat and ..." on **AFACT v iiNet: Second chance termination strains resources**
- "Lets say an ISP terminates an account for breach of copyright. What ..." on **AFACT v iiNet: Second chance termination strains resources**

be exploited by a malicious user, and is used to reduce the number of false positives reported," he said.

The current version is for ASP with PHP to follow. Drazic said Java and .Net versions were also in development.

Security-Assessment.com, the sister company of CodeScan Labs, is the distributor and also the reseller of CodeScan in Australia. Drazic said it is currently looking at developing a reseller channel and is in discussions with a few organizations.

Licences are subscription-based and priced on the number of seats. There is also a package for consultants.

"Great logical summary Trevor. Yes, current Libs policy just bad. If they ..." on **Why not do the NBN better, cheaper, faster?**

"RS you ruined my Nemisis thing, I had that one lined up. ..." on **Report bombs Aussie broadband**

Bookmark this page

Share this article

Got more on this story? Email Computerworld

Follow Computerworld on twitter

Comments

Post new comment

NAME

EMAIL ADDRESS

The content of this field is kept private and will not be shown publicly.

COMMENT

Users posting comments agree to the Computerworld comments policy.

Post Preview

Login or register to link comments to your user profile, or you may also post a comment without being logged in.