

18 February 2009

By: Lucian Constantin, Web News Editor

INTERNATIONAL
Herald TribuneThe website of the
International Herald
Tribune affected by
SQL injection
International Herald
Tribune

[International Herald Tribune SQL Injection](#)

Database information and editors' login credentials exposed

The Romanian HackersBlog outfit [disclosed](#) a SQL injection vulnerability in the website of the International Herald Tribune, the international edition of the New York Times. A poorly-sanitized parameter allowed the hackers to obtain access to the database, including the table containing the login credentials of the newspaper's editors.

The International Herald Tribune ([IHT](#)) is a renowned newspaper sold in over 180 countries. It is currently owned by the New York Times Company and shares the vast majority of the editors with the company's flagship publication, the New York Times. In 2008, the websites of the IHT and the New York Times merged.

"I discovered an unsecured parameter which allows access to the data base," the ethical hacker calling himself "unu" announces in a post on the HackersBlog website. Published screenshots reveal that the website is using MySQL 5.0.51a as database engine, with two databases available - "test" and "web," while the username employed to access them is "ASOchs."

"Besides the wealth of information in the database, we also found an interesting table containing login details of 161 affiliates, editors, reporters and other associates of the famed newspaper," the Romanian hacker notes. A screenshot with the login credentials is also provided and includes those of IHT's Director of Digital Operation, Steven Schattenberg, those of IHT's Online Sales Services Manager, Dominique Piteux, or Timothy B. Lee's, policy analyst and IHT contributor.

The HackersBlog has attracted a lot of media attention lately, after it disclosed several SQL injection vulnerabilities on websites belonging to top antivirus vendors such as [Kaspersky](#), [Bitdefender](#) and [F-Secure](#). Bitdefender in particular has been affected twice, [first](#) by a vulnerability found on the website of its partner in Portugal, for which it denied responsibility, and more recently by a lower-risk flaw in the news section of its own site.

It looks like the Romanian crew might be directing its attention away from av vendors for the moment and focuses on popular publications instead. "I will continue with other newspapers soon," "unu" warns. Meanwhile, "2fingers," another admin of the hacking website, [has apologized](#) in a different post for the longer period of time between disclosures. This has been due to their being willing to give webmasters more time to address the problems before releasing info about them to the general public, he explains.