

[Full-Disclosure] paFileDB 3.x SQL Injection Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2003-03/0216.html>

From: flur (flur@flurnet.org)

Date: 03/24/03

To: full-disclosure@lists.netsys.com
From: flur <flur@flurnet.org>
Date: Mon, 24 Mar 2003 10:57:56 -0500

Flurnet Security

paFileDB by todd@phparena.net
PHP Arena <http://www.phparena.net>

Tested on:

- paFileDB 3.0 Final
- paFileDB 3.0 Beta 3.1
- paFileDB 3.1 Final

Explanation:

paFileDB is a file management script that supports user file rating. It uses an SQL database backend. Multiple vulnerabilities exist due to the lack of checked input variables. The following exploits exist:

- Modified 'id' tag allows users to submit unlimited ratings.
- Hand-edited 'rating' tag allows users to submit ratings above 10 or below 0.
- Both tags do not check for escape characters and will allow SQL injection.

Proof-Of-Concept Exploits:

[http://target/pafiledb/pafiledb.php?action=rate&id=1\[RANDOM\]&rate=dorate&rating=10](http://target/pafiledb/pafiledb.php?action=rate&id=1[RANDOM]&rate=dorate&rating=10)

Replace [RANDOM] with a random short string and the script will not stop you from voting as many times as you like.

<http://target/pafiledb/pafiledb.php?action=rate&id=1&rate=dorate&rating=1000>

Submit file rating of 1000 out of 10. Drive rate up. Conversely, -1000 would have the opposite effect driving the rating down.

<http://target/pafiledb/pafiledb.php?action=rate&id=1&rate=dorate&rating=`>
<http://target/pafiledb/pafiledb.php?action=rate&id=`&rate=dorate&rating=10>
SQL Injection vulnerability (exploit code not included)

Full-Disclosure: [Full-Disclosure] paFileDB 3.x SQL Injection Vulnerability

Script authors have been notified.

~FluRDoInG flur@flurnet.org

<http://www.flurnet.org>

KEY ID 0x8C2C37C4 (pgp.mit.edu) RSA-CAST 2048/2048

1876 B762 F909 91EB 0C02 C06B 83FF E6C5 8C2C 37C4

Full-Disclosure – We believe in it.

Charter: <http://lists.netsys.com/full-disclosure-charter.html>