New issue

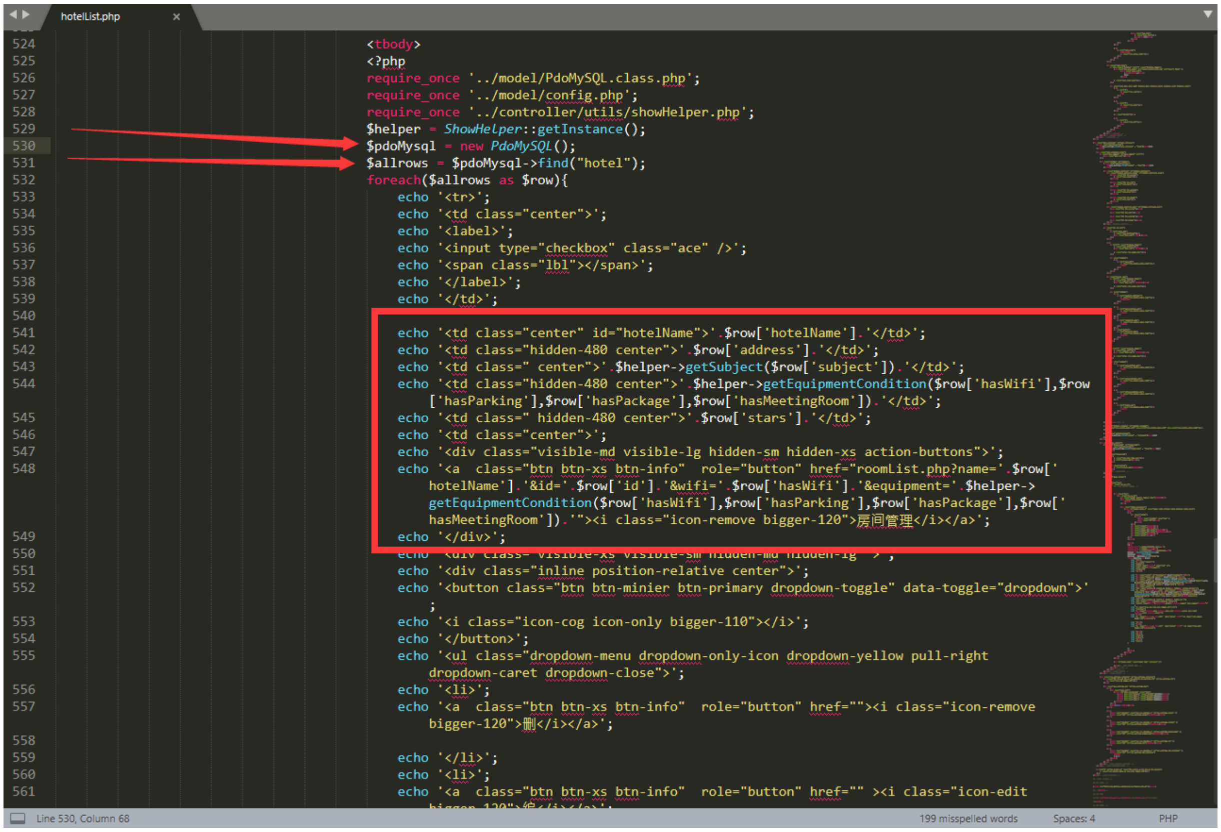
Jump to bottom

XSS Vulnerability in /view/hotelList.php #3

Open Anion3r opened this issue on Jan 23, 2019 · 0 comments

Anion3r commented on Jan 23, 2019

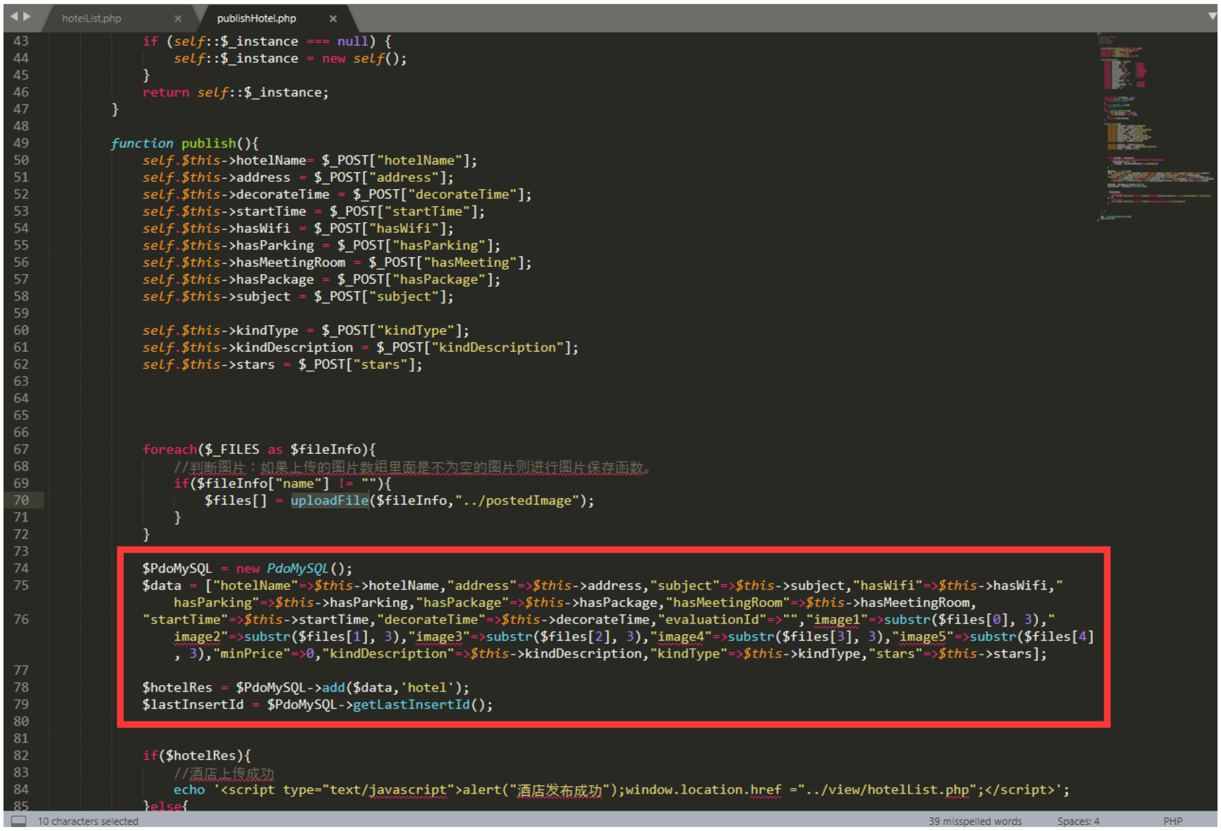
In /view/hotelList.php



```
                <tbody>
                <?php
                require_once '../model/PdoMySQL.class.php';
                require_once '../model/config.php';
                require_once '../controller/utils/showHelper.php';
                $helper = ShowHelper::getInstance();
                $pdoMysql = new PdoMySQL();
                $allrows = $pdoMysql->find("hotel");
                foreach($allrows as $row){
                    echo '<tr>';
                    echo '<td class="center">';
                    echo '<label>';
                    echo '<input type="checkbox" class="ace" />';
                    echo '<span class="lbl"></span>';
                    echo '</label>';
                    echo '</td>';

                    echo '<td class="center" id="hotelName">'.$row['hotelName'].'</td>';
                    echo '<td class="hidden-480 center">'.$row['address'].'</td>';
                    echo '<td class=" center">'.$helper->getSubject($row['subject']).'</td>';
                    echo '<td class="hidden-480 center">'.$helper->getEquipmentCondition($row['hasWifi'],$row
                        ['hasParking'],$row['hasPackage'],$row['hasMeetingRoom']).'</td>';
                    echo '<td class=" hidden-480 center">'.$row['stars'].'</td>';
                    echo '<td class="center">';
                    echo '<div class="visible-md visible-lg hidden-sm hidden-xs action-buttons">';
                    echo '<a  class="btn btn-xs btn-info"  role="button" href="roomList.php?name='.$row['
                        hotelName'].'&id='.$row['id'].'&wifi='.$row['hasWifi'].'&equipment='.$helper->
                        getEquipmentCondition($row['hasWifi'],$row['hasParking'],$row['hasPackage'],$row['
                        hasMeetingRoom']).'"><i class="icon-remove bigger-120">房间管理</i></a>';
                    echo '</div>';
                    echo '<div class="visible-xs visible-sm hidden-md hidden-lg">';
                    echo '<div class="inline position-relative center">';
                    echo '<button class="btn btn-minier btn-primary dropdown-toggle" data-toggle="dropdown">'
                        ;
                    echo '<i class="icon-cog icon-only bigger-110"></i>';
                    echo '</button>';
                    echo '<ul class="dropdown-menu dropdown-only-icon dropdown-yellow pull-right
                        dropdown-caret dropdown-close">';
                    echo '<li>';
                    echo '<a  class="btn btn-xs btn-info"  role="button" href=""><i class="icon-remove
                        bigger-120">删</i></a>';

                    echo '</li>';
                    echo '<li>';
                    echo '<a  class="btn btn-xs btn-info"  role="button" href="" ><i class="icon-edit
                        bigger-120">编</i></a>';
```

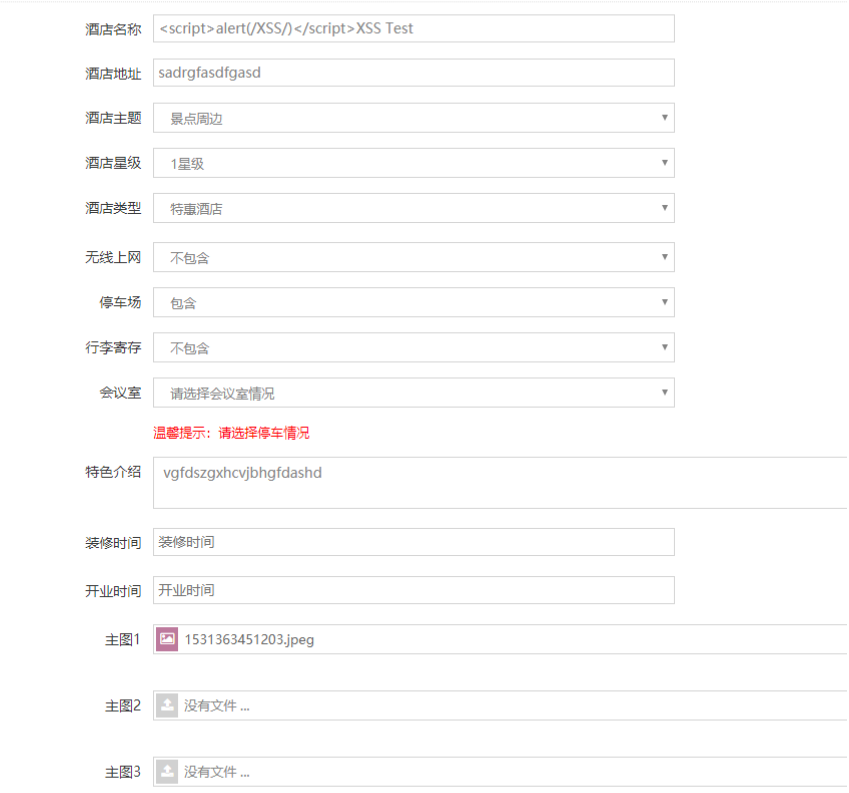
As you see, there are not any filtration in all 'echo's.

Also in /controller/publishHotel.php , these are inserted into database without filtration

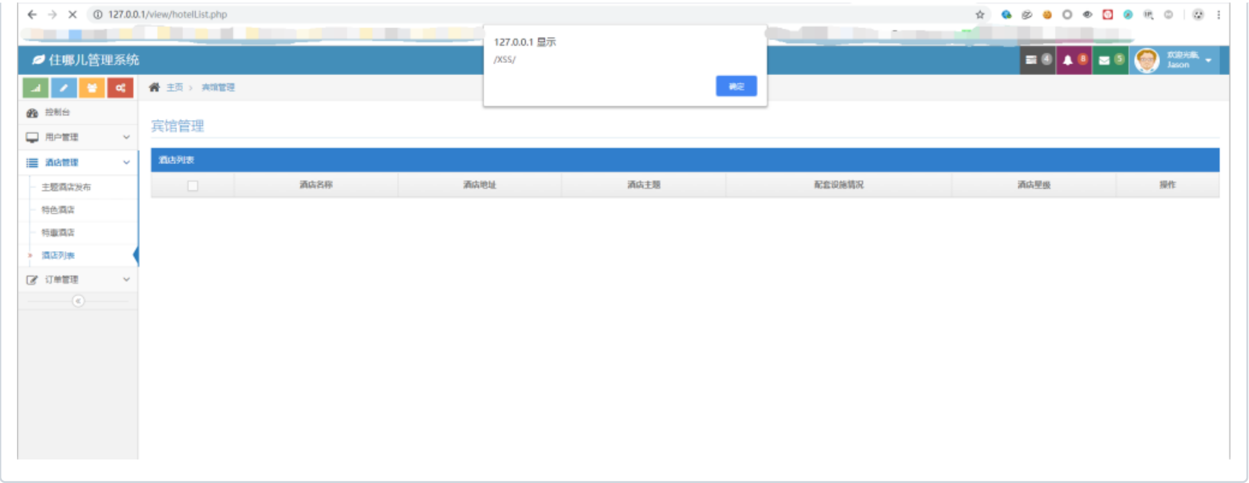


```php
        if (self::$_instance === null) {
            self::$_instance = new self();
        }
        return self::$_instance;
    }

    function publish(){
        self.$this->hotelName= $_POST["hotelName"];
        self.$this->address = $_POST["address"];
        self.$this->decorateTime = $_POST["decorateTime"];
        self.$this->startTime = $_POST["startTime"];
        self.$this->hasWifi = $_POST["hasWifi"];
        self.$this->hasParking = $_POST["hasParking"];
        self.$this->hasMeetingRoom = $_POST["hasMeeting"];
        self.$this->hasPackage = $_POST["hasPackage"];
        self.$this->subject = $_POST["subject"];

        self.$this->kindType = $_POST["kindType"];
        self.$this->kindDescription = $_POST["kindDescription"];
        self.$this->stars = $_POST["stars"];




        foreach($_FILES as $fileInfo){
            //判断图片：如果上传的图片数组里面是不为空的图片则进行图片保存函数。
            if($fileInfo["name"] != ""){
                $files[] = uploadFile($fileInfo,"../postedImage");
            }
        }

        $PdoMySQL = new PdoMySQL();
        $data = ["hotelName"=>$this->hotelName,"address"=>$this->address,"subject"=>$this->subject,"hasWifi"=>$this->hasWifi,"
            hasParking"=>$this->hasParking,"hasPackage"=>$this->hasPackage,"hasMeetingRoom"=>$this->hasMeetingRoom,
        "startTime"=>$this->startTime,"decorateTime"=>$this->decorateTime,"evaluationId"=>"","image1"=>substr($files[0], 3),"
            image2"=>substr($files[1], 3),"image3"=>substr($files[2], 3),"image4"=>substr($files[3], 3),"image5"=>substr($files[4]
            , 3),"minPrice"=>0,"kindDescription"=>$this->kindDescription,"kindType"=>$this->kindType,"stars"=>$this->stars];

        $hotelRes = $PdoMySQL->add($data,'hotel');
        $lastInsertId = $PdoMySQL->getLastInsertId();


        if($hotelRes){
            //酒店上传成功
            echo '<script type="text/javascript">alert("酒店发布成功");window.location.href ="../view/hotelList.php";</script>';
        }else{
```

After all, we can enjoy XSS



酒店名称	<script>alert(/XSS/)</script>XSS Test
酒店地址	sadrgfasdfgasd
酒店主题	景点周边
酒店星级	1星级
酒店类型	特重酒店
无线上网	不包含
停车场	包含
行李寄存	不包含
会议室	请选择会议室情况
	温馨提示：请选择停车情况
特色介绍	vgfdszgxhcvjbhgfdashd
装修时间	装修时间
开业时间	开业时间
主图1	1531363451203.jpeg
主图2	没有文件 ...
主图3	没有文件 ...



127.0.0.1 显示

/XSS/

确定

宾馆管理

酒店列表

□	酒店名称	酒店地址	酒店主题	配套设施情况	酒店星级	操作

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant