

## NAME OF AFFECTED PRODUCT(S)

Online Class and Exam Scheduling System

## VERSION(S)

V1.0

## submitter

lvzhouhang

## Vulnerable File

/pages/profile.php

## Software Link

<https://download.code-projects.org/details/93487762-3e23-48ab-a56f-af5e61441ee1>

## Vulnerability Type

Cross Site Scripting

in /pages/profile.php member\_first and member\_last Parameters have Cross Site Scripting(XSS)

```
</section>
<?php
    $id=$_SESSION['id'];
    $query=mysqli_query($con, query: "select * from member where member_id='$id'" or die(mysqli_error());
    $row=mysqli_fetch_array($query);
?>
```

```
<label>Full Name</label>
<input-group col-md-12">
    <input type="text" class="form-control pull-right" value="<?php echo $row['member_first']. " ".$row['member_last'];?>" name="name" placeholder="Full Name" />
</input-group -->
```

A malicious attacker can use this vulnerability to obtain administrator login credentials or phishing websites

## POC

<http://127.0.0.1/scheduling/pages/profile.php>

scheduling

表

- > cys
- > dept
- > designation
- > exam\_sched
- > member
- > program
- > rank
- > room
- > salut
- > schedule
- > settings
- > signatories
- > subject
- > sy
- > time
- > user

视图

member_id	member_last	member_first	member_rank	memt
# int(11)	varchar(30)	varchar(30)	varchar(50)	Var
27	:rt(1)</script><<"	Admin	Assistant Professor I	Mrs
177	Rizal	Jose	Assistant Professor I	Dr

men

类型  
varchar(30)

不是 null  
是

默认值  
--

注释  
--

/scheduling/pages/profile.php

Hack The Box TryHackMe 嘘，这东西咋

127.0.0.1 显示

1

确定