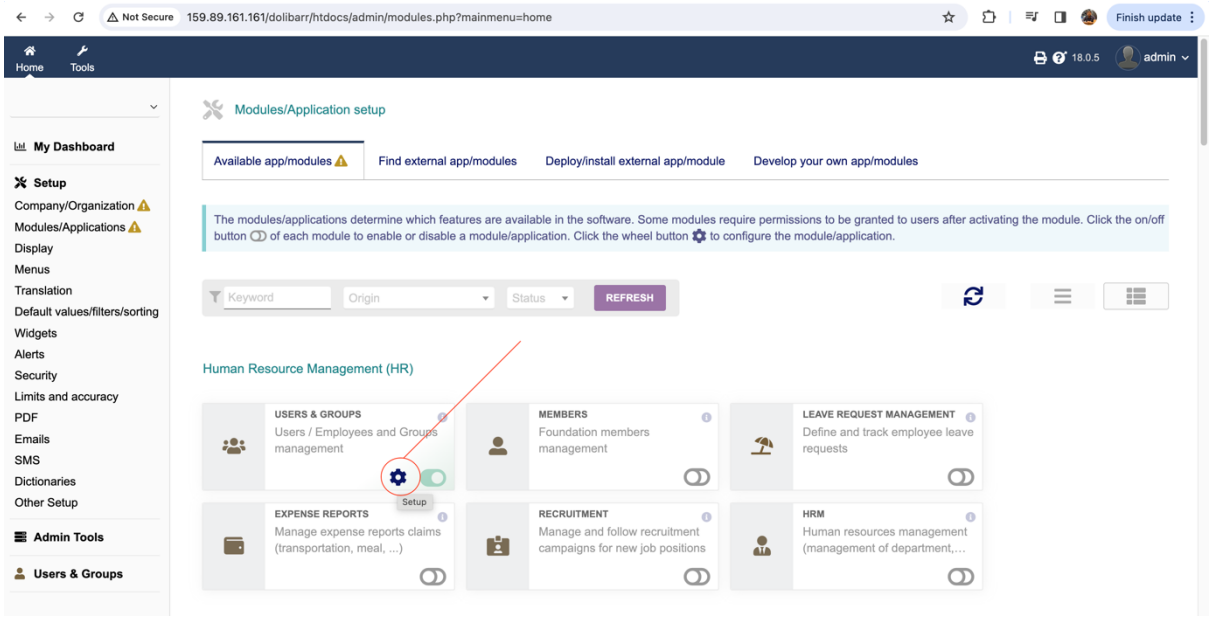
Dolibarr ERP/CRM – Improper Input Sanitization leads to Remote Code Execution on version 18.0.5

Description:

An admin can perform an arbitrary command execution on the Dolibarr 18.0.5 application

Steps to Reproduce:

1. Login as admin
2. Navigate to Setup --> Modules/Application
3. Click on the setup icon on Users& Groups, and you will navigate to the 'Users module setup' page

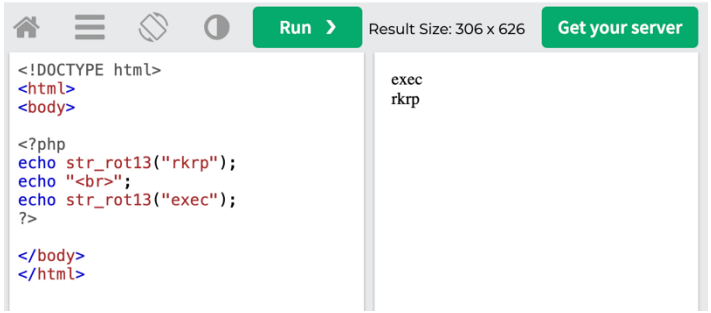


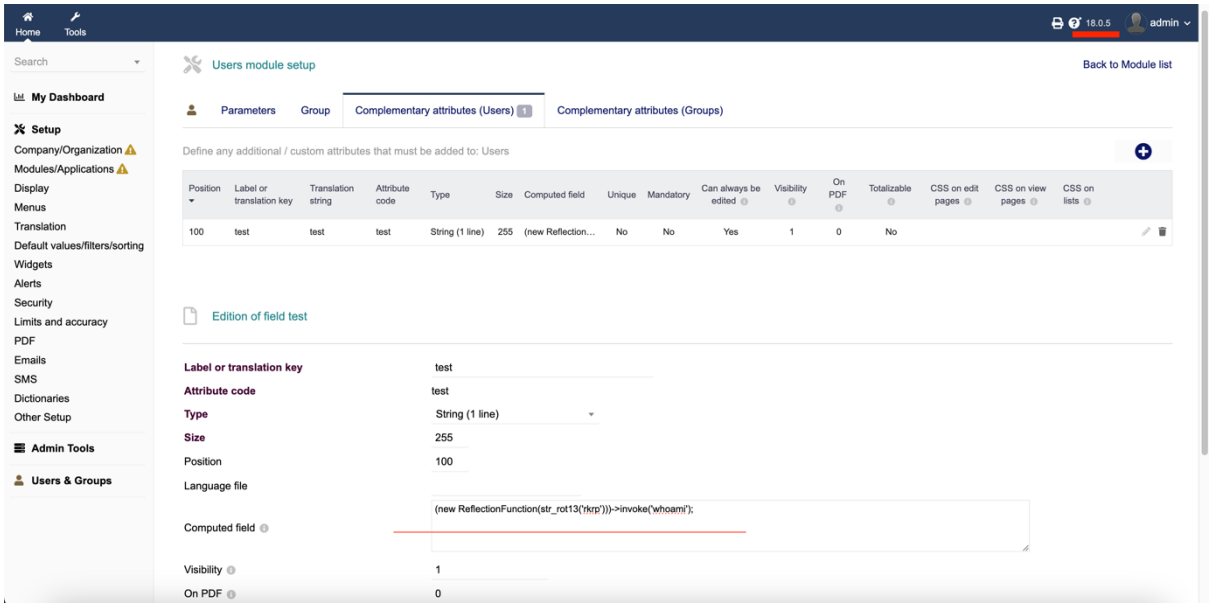
4. Click on the Complementary attributes(Users) tab
5. Create an attribute by clicking the plus(+) icon, named as 'test'
6. Add this payload for the "Computed field" and Save the form

```
(new ReflectionFunction(str_rot13('rkrp')))->invoke('whoami');
```

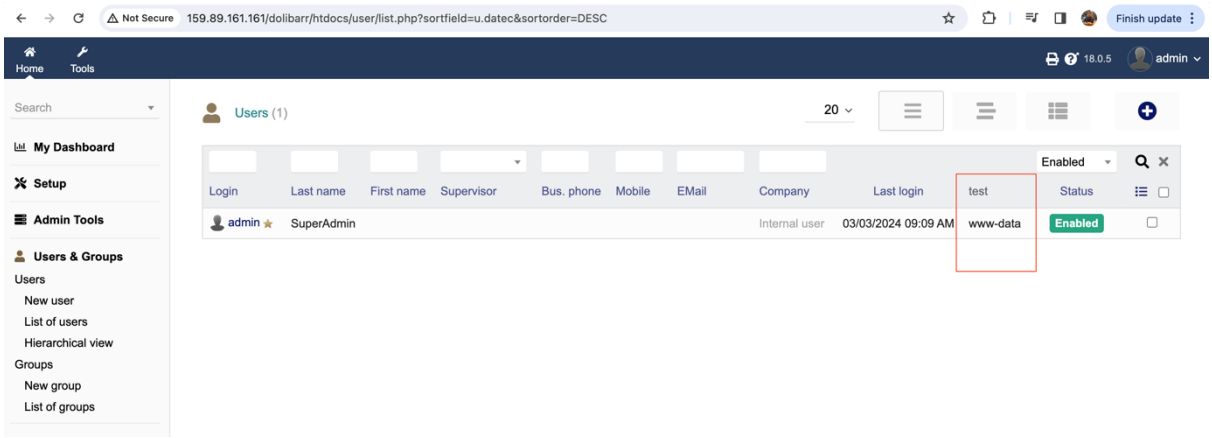
The above payload is a bypass for the existing protection filter

About str_rot13 function: The ROT13 encoding shifts every letter 13 places in the alphabet





7. Now, navigate to "Users& Groups"
8. Click on Full list users
9. Observe the test field value with computed value (www-data)



10. This confirms the arbitrary command execution
11. Please find the video POC here

https://vimeo.com/918820618?share=copy

password: @123