**Arbitrary code execution vulnerability exists in ESPCMS management system**

**Vulnerability description:**

The vulnerability modifies the content of the homepage template file in the background, and after modification, a PHP suffix file with the same content will be generated. When the frontend accesses the homepage file, local code execution will be triggered.

**Supplier:** https://www.ecisp.cn/

**Vulnerability file:**

espcms\espcms\_public\espcms\_templates\ESPCMS\_Templates.php

**Code Analysis:**

The code execution function eval is called in line 165. The content obtained by the $out variable is the content of the template file. The $fetch\_filename parameter in line 84 is actually the address of the template file. In line 90, it is simply obtained with the file\_get\_contents() function. The contents of the template file are then assigned to $out.

espcms\espcms\_public\espcms\_templates\ESPCMS\_Templates.php  




This function is a function to modify the content of the template file. There are user-controllable input parameters in line 174, and the content is written to the template file in line 211.

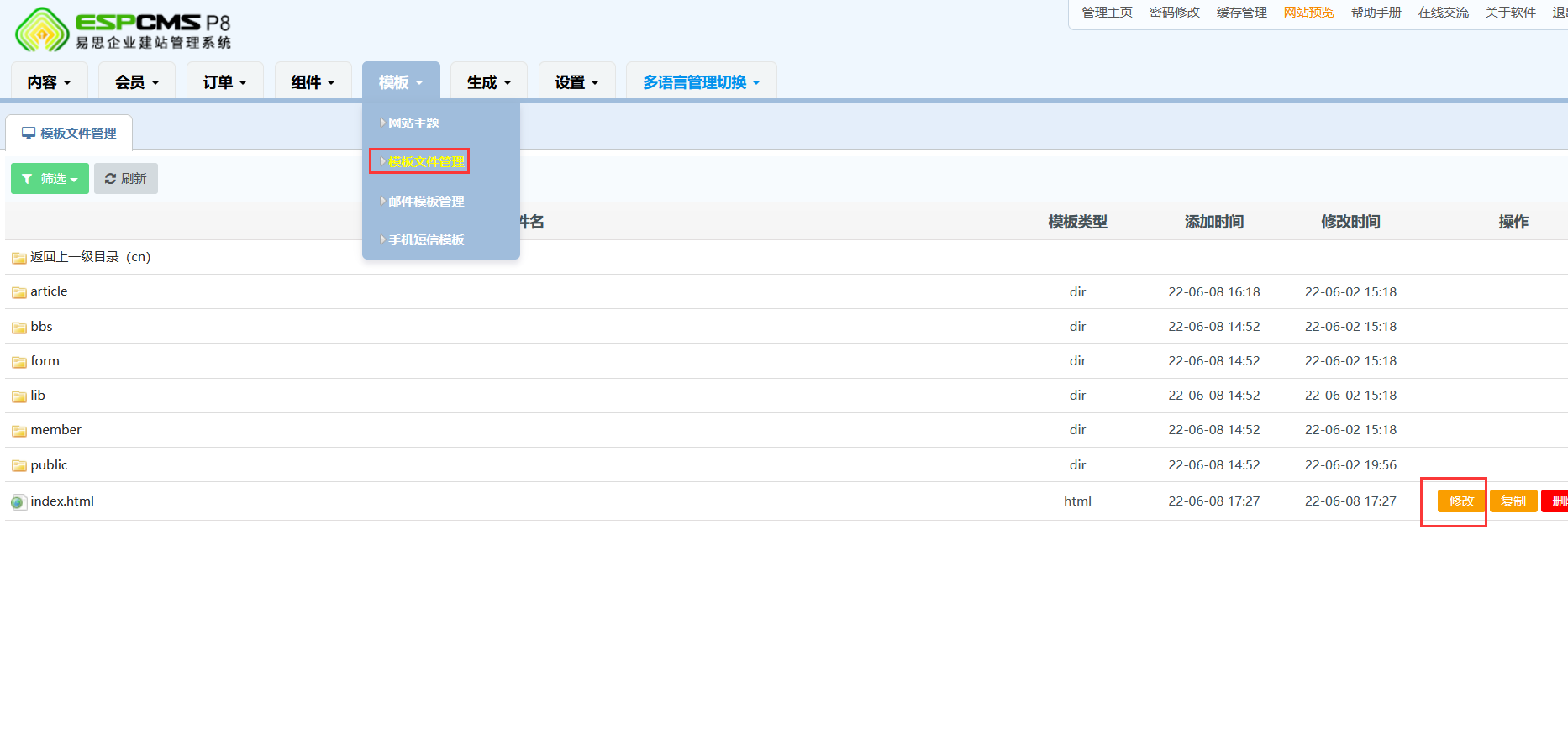
espcms\espcms\_admin\control\TemplateFile.php

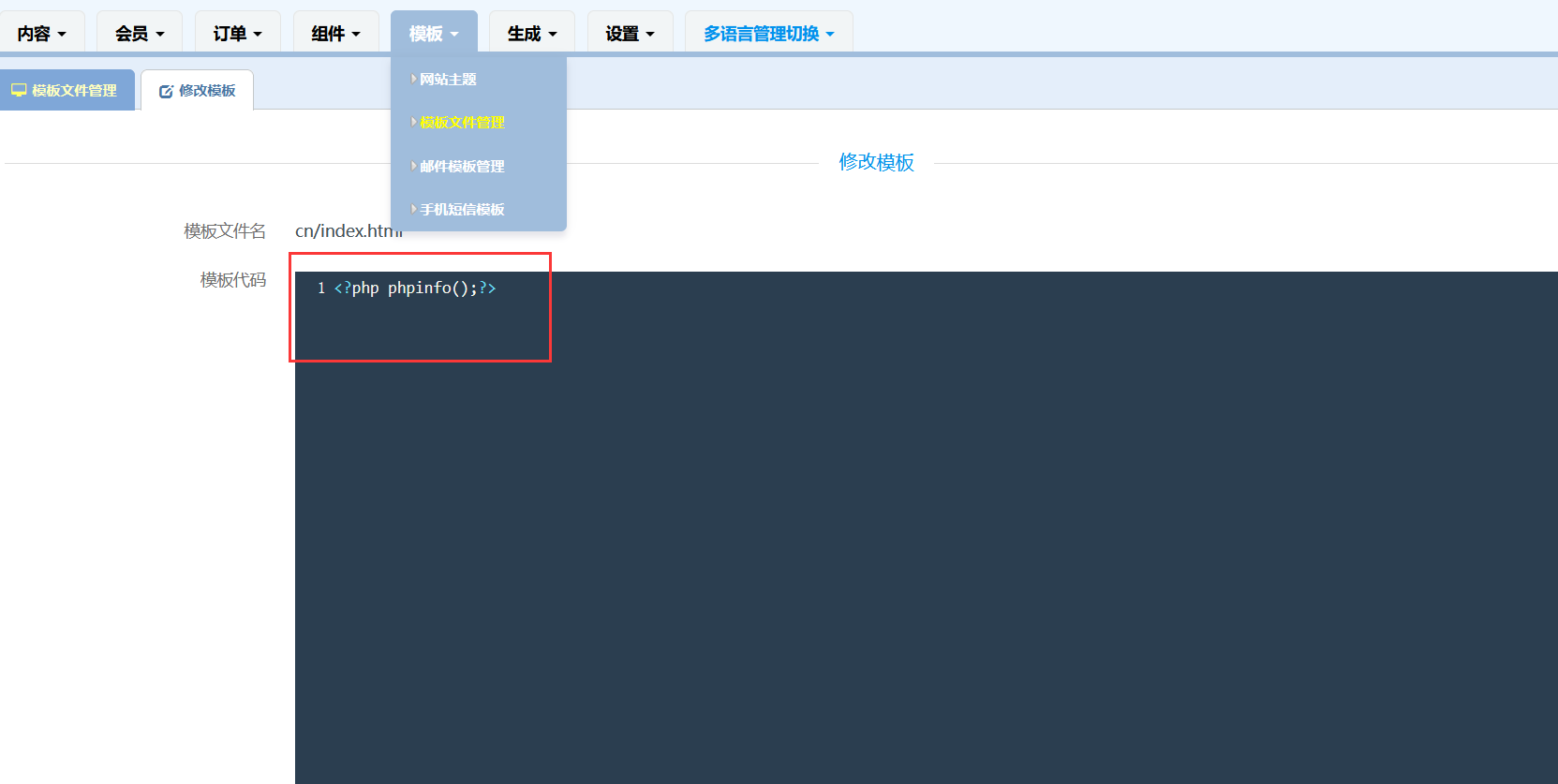




**Steps to reproduce:**

1. Log in to the background management page as an administrator

2. Click Template Management -> Modify and change the content to <?php phpinfo();?>



3. After the modification is successful, save it, and access the home page to cause the code to execute.