New issue

Jump to bottom

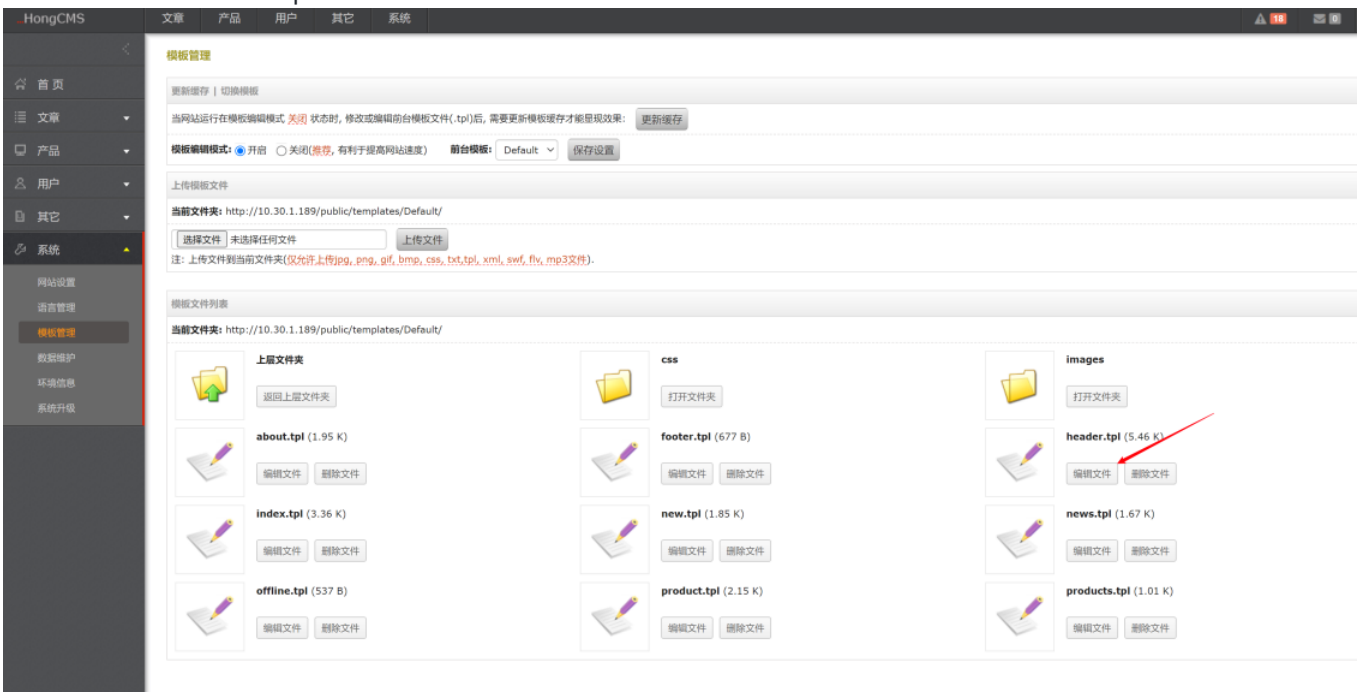
HongCMS 3.0 - Getshell by template/edit (Administrator Privilege) #19

Open **Rixo1043** opened this issue on Jun 1 · 0 comments

Rixo1043 commented on Jun 1 • edited

1.Login to the backstage as the administrator.

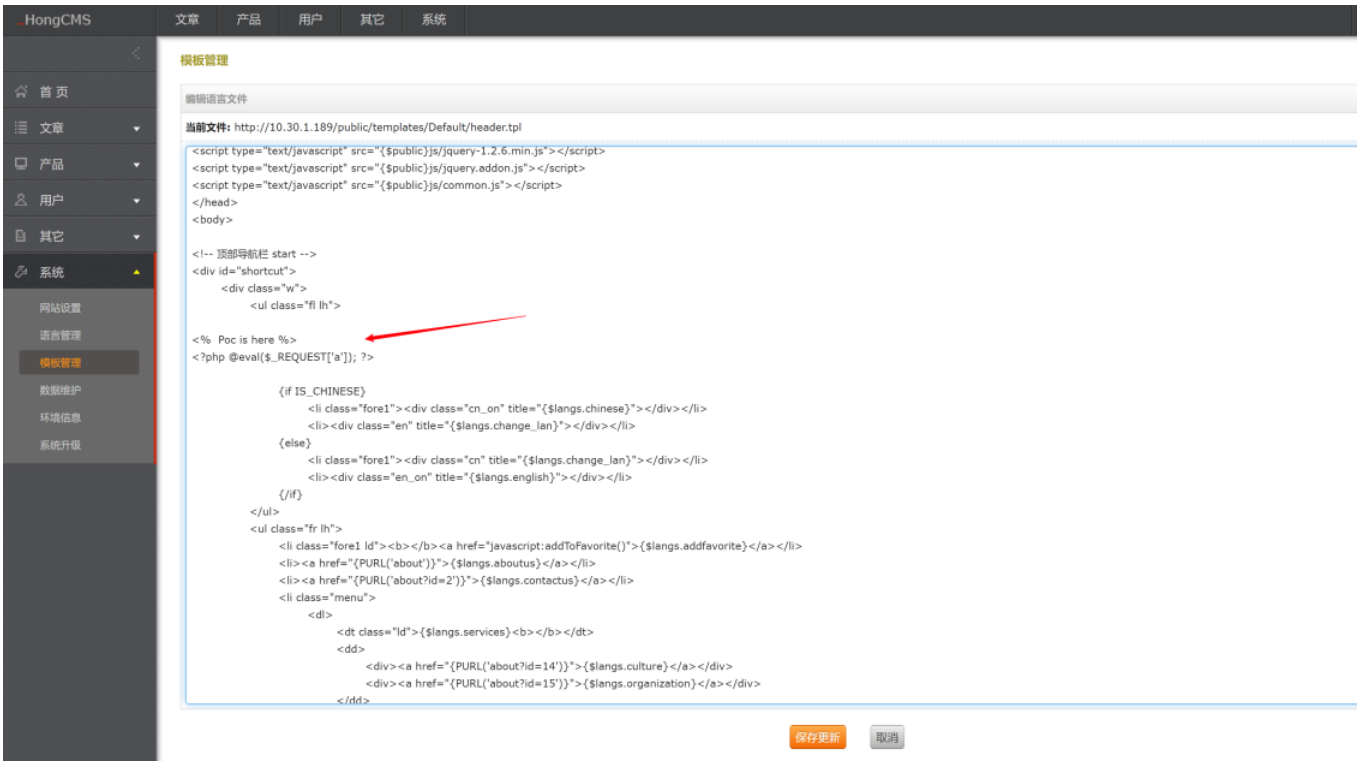
2.You need to edit the tpl file



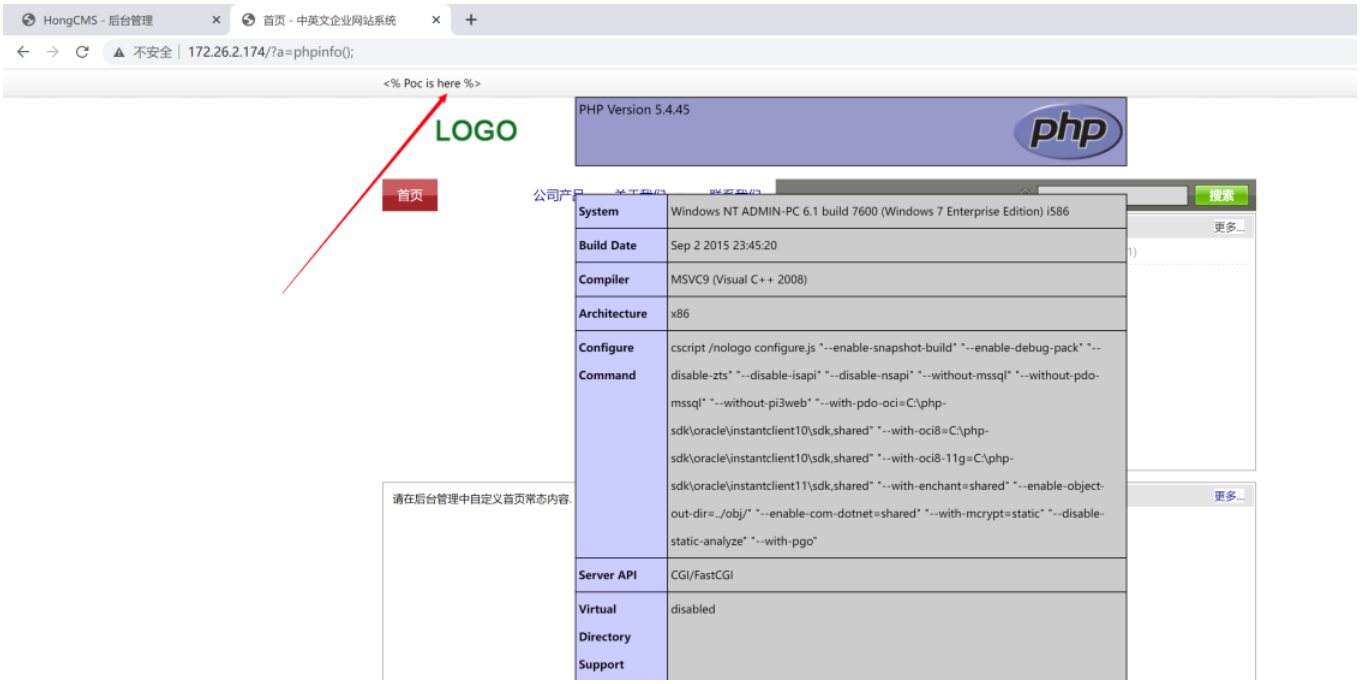
3. Because the default safe mode configuration is off， so you can edit tpl file to getshell。
The vulnerability code is as follows:

```
3  //STpl模板类
4  class STpl{
5          var $_tpl_vars             = array();
6          var $tpl_left_delimiter  =  '{';
7          var $tpl_right_delimiter =  '}';
8          var $tpl_template_dir    =  'templates/';
9          var $tpl_compile_dir     =  'cache/';
0          var $tpl_safe_mode = false;
1          var $tpl_check = true;
2
        //编译
        private function _compile($content){
                $left_delimiter_quote = preg_quote($this->tpl_left_delimiter);
                $right_delimiter_quota= preg_quote($this->tpl_right_delimiter);

                //安全模式，替换php可执行代码
                if($this->tpl_safe_mode){
                        $pattern="/\\<\\?.*\\?>/msUi";
                        $content = preg_replace($pattern, '<!-- PHP CODE REPLACED ON SAFE MODE -->', $content);
                }

                //替换注释：{*xxx*}
                $pattern="/{$left_delimiter_quote}\*(.*)\*{$right_delimiter_quota}/msU";
                $content = preg_replace($pattern, "<?php /*\\1*/?>", $content);

                //调用_match函数编译
                $pattern="/{$left_delimiter_quote}([\S].*){$right_delimiter_quota}/msU";
                return preg_replace_callback($pattern, array(&$this, '_match'), $content);
        }

        //清空当前模板缓存
        public function clear_compiled_tpl(){
                tpl_remove_cache($this->tpl_compile_dir);
        }
}
```

5. Add you webshell code in tpl file.



6. Then you can getshell in index file.



Repair suggestion:

1、Set safe mode true by default.

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant