New issue

Jump to bottom

There is a directory traversal vulnerability in mindoc #788

Closed **binganao** opened this issue on Apr 24 · 0 comments

binganao commented on Apr 24

请按照一下格式提交issue，谢谢！

1. 你当前使用的是哪个版本的 MinDoc(`godoc_linux_amd64 version`)?
   v2.1-beta.5

2. 你当前使用的是什么操作系统?
   Centos

3. 你是如何操作的?
   进入后台，我的项目，导入项目，导入恶意zip文件

4. 你期望得到什么结果?
   在根目录生成RCE!.txt

5. 当前遇到的是什么结果?
   生成了该文件，没有对zip文件进行过滤，导致可以任意上传文件，如果上传恶意文件到计划任务，则可以导致任意命令执行

[Suggested description]

There is an arbitrary file upload vulnerability in mindoc. Hackers can construct malicious zip files containing "../" to upload files to any directory. If you upload it to the scheduled task folder of Linux, you can execute any command

[Vulnerability Type]

Directory Traversal

[Vendor of Product]

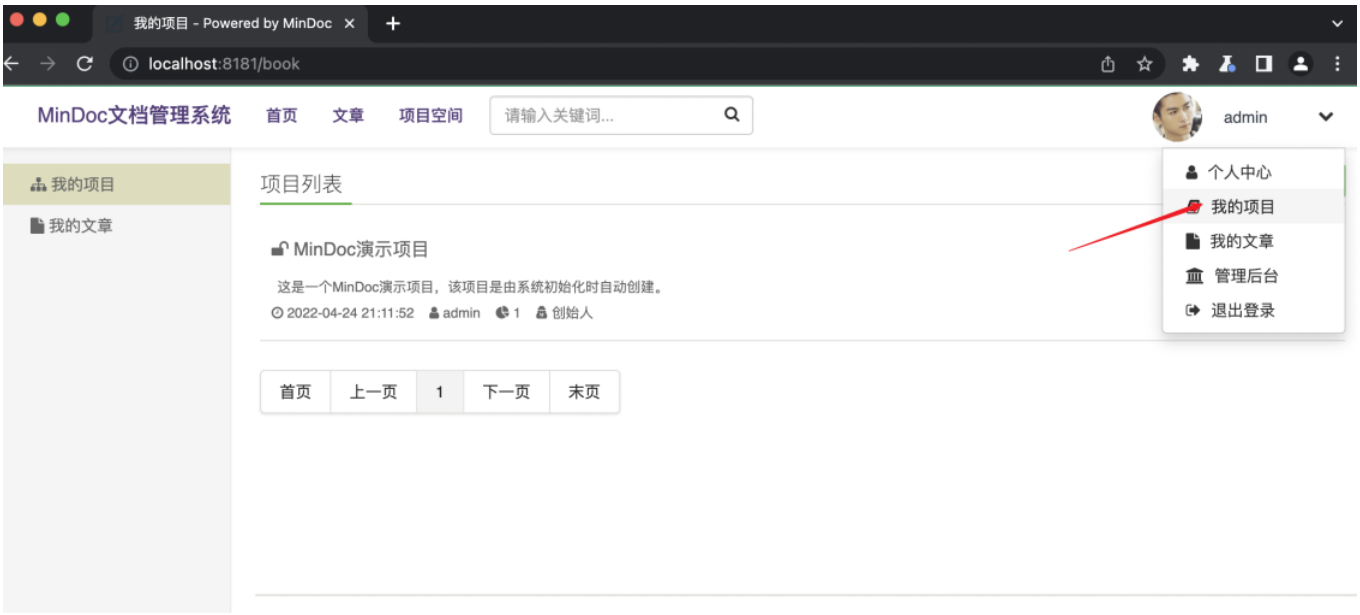
https://github.com/mindoc-org/mindoc

[Affected Product Code Base]

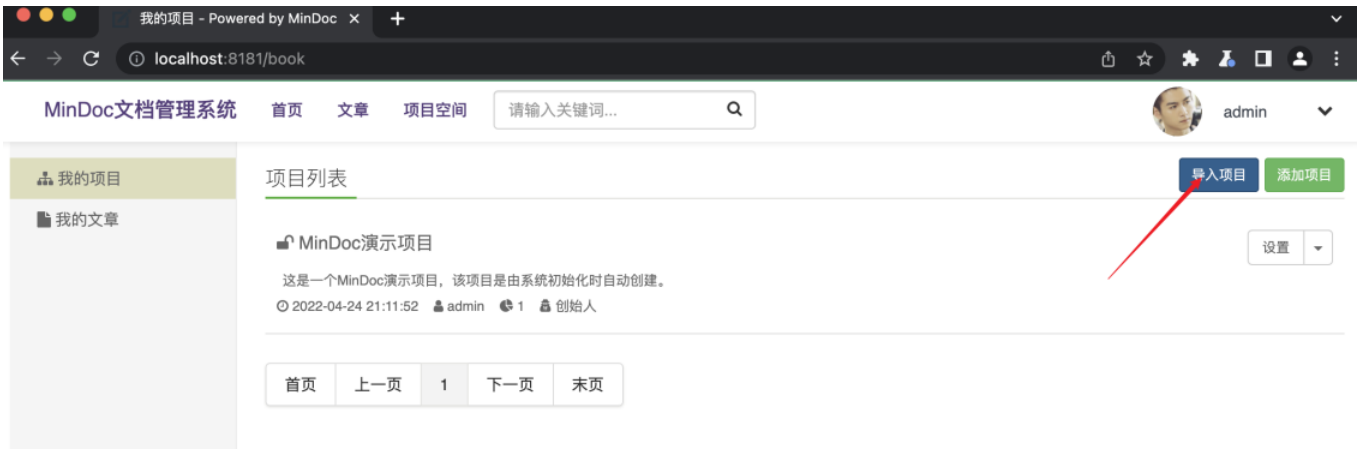
v2.1-beta.5

[Affected Component]

First, you need to log in to the background and enter "我的项目"

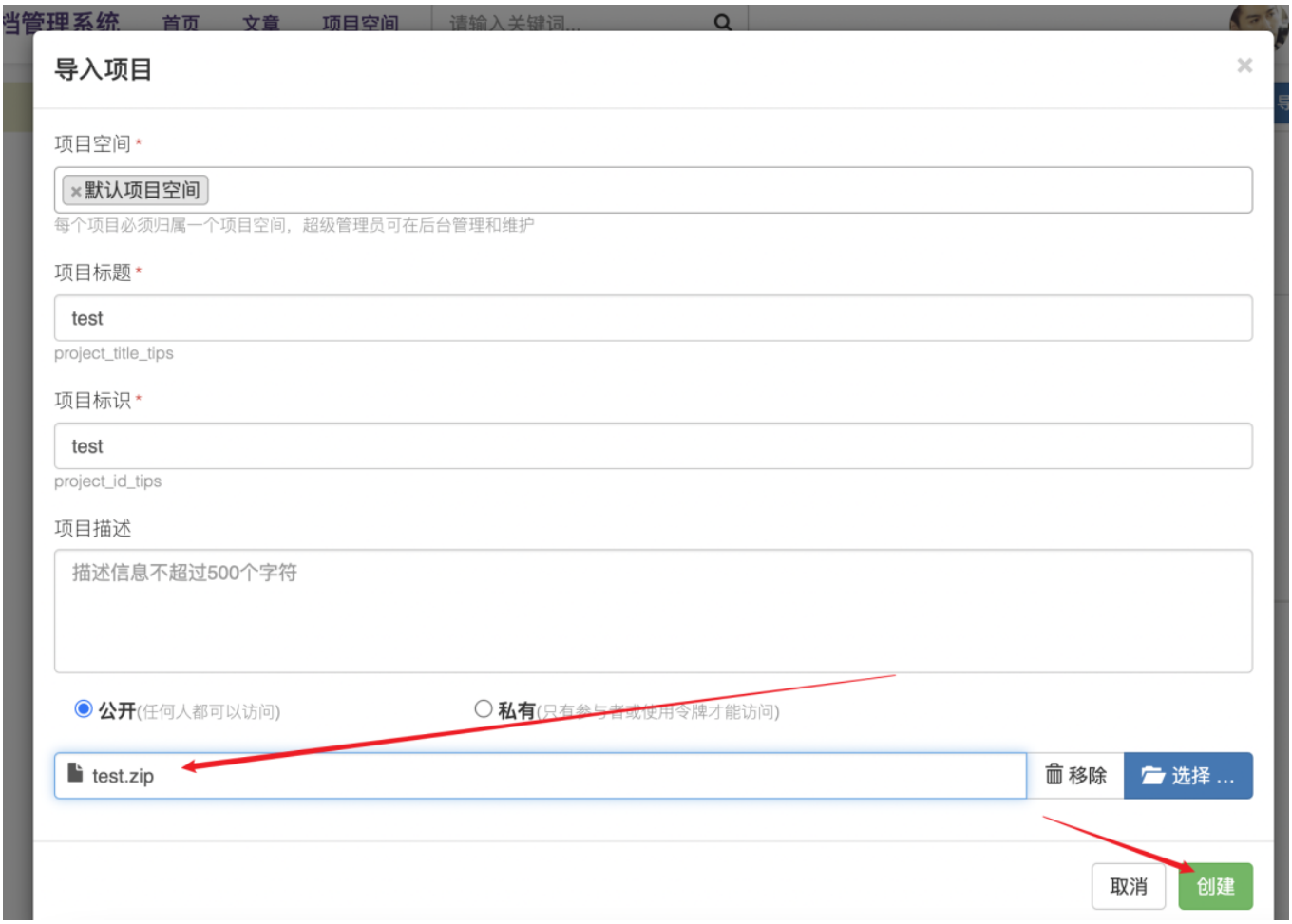


Then use the "导入项目" function



"项目标题" and "项目标识" can be filled in arbitrarily, as long as it meets its basic requirements. Then upload the constructed zip file. What I constructed here is "../../../../../../../../RCE!.txt"

test.zip



After clicking upload, he will create a new "RCE!.txt" in the root directory of the server

[Defective code]

```
/utils/ziptil/ziptil.go
```

```go
func Unzip(zipFile, dest string) (err error) {
    dest = strings.TrimSuffix(dest, "/") + "/"
    // 打开一个zip格式文件
    r, err := zip.OpenReader(zipFile)
    if err != nil {
        return err
    }
    defer r.Close()
    // 迭代压缩文件中的文件，打印出文件中的内容
    for _, f := range r.File {
        if !f.FileInfo().IsDir() { //非目录，且不包含__MACOSX
            if folder := dest + filepath.Dir(f.Name); !strings.Contains(folder, "__MACOSX") {
                os.MkdirAll(folder, 0777)
                if fcreate, err := os.Create(dest + strings.TrimPrefix(f.Name, "./")); err == nil {
                    if rc, err := f.Open(); err == nil {
                        io.Copy(fcreate, rc)
                        rc.Close() //不要用defer来关闭，如果文件太多的话，会报too many open files 的错误
                        fcreate.Close()
                    } else {
                        fcreate.Close()
                        return err
                    }
                } else {
                    return err
                }
            }
        }
    }
    return nil
}
```

[Discoverer]

Bingan

Go-Go-Farther mentioned this issue on Jun 20

bugfix: 修复zip的slip问题，防止上传恶意zip，增强服务器安全性。Fixes mindoc-org/mindoc#788 #798

Merged

gsw945 closed this as completed in `c15da23` on Jun 27

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

---

1 participant