New issue

Jump to bottom

Function leafInfo.match() use path.join() to deal with `wildcardValues`, which may lead to cross directory risk. #4961

Closed runner361 opened this issue on May 23 · 4 comments · Fixed by #5025

Assignees

Labels activity/CCFOS activity/weopen-star

runner361 commented on May 23 • edited Contributor

Function leafInfo.match() use path.join() to deal with `wildcardValues`, which may lead to cross directory risk.

- **poc1: route end with `*.*` can use `../` to cross directory and set evil value for `:path` .**

beego/server/web/tree.go
Line 414 in 64cf44d

```
414     ctx.Input.SetParam(":path", path.Join(path.Join(wildcardValues[:len(wildcardValues)-1].
```

beego/server/web/tree.go
Line 431 in 64cf44d

```
431     ctx.Input.SetParam(":path", path.Join(path.Join(wildcardValues[index:len(wildcardValues
```

For route `/book1/:name/fixPath1/*.*` , urls below can match, and set `:path=evil`

`/book1/name1/fixPath1/mybook/../evil.txt => :name=name1`

`/book1/name1/fixPath1/mybook/../../../evil.txt => :name=name1`

`/book1/name1/fixPath1/mybook/../.././///evil.txt => :name=name1`

`/book1/../fixPath1/mybook/../.././///evil.txt => :name=..`

`/book1/./fixPath1/mybook/../.././///evil.txt => :name=.`


```
//Test code as below:
web.Router("/book1/:name/fixPath1/*.*", &controllers.BookController{}, "get:SearchByName")
func (b BookController) SearchByName() {
        fmt.Println(":path=" + b.Ctx.Input.Param(":path"))
        fmt.Println(":name=" + b.Ctx.Input.Param(":name"))
        b.Data["json"] = "OK"
        b.ServeJSON()
}
```

- **poc2: regex route can use `../` to cross directory and replace wildcard with evil value**

  beego/server/web/tree.go
  Line 445 in `64cf44d`

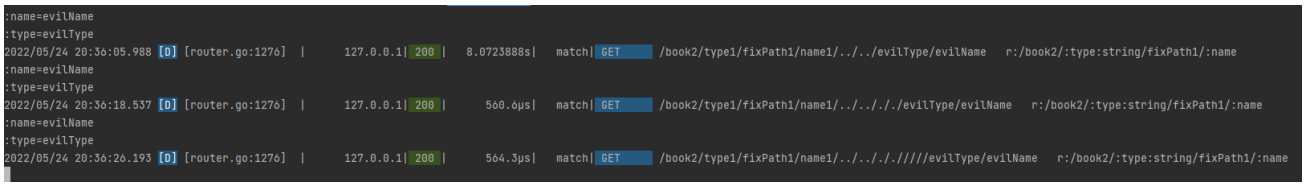
  ```
  445      if !leaf.regexps.MatchString(path.Join(wildcardValues...)) {
  ```

  For regex route `/book2/:type:string/fixPath1/:name` ,urls below can match and value of `:type` `:name` can be replaced with evil value.

  `/book2/type1/fixPath1/name1/../../evilType/evilName => :type=evilType :name=evilName`

  `/book2/type1/fixPath1/name1/../.././../evilType/evilName => :type=evilType :name=evilName`

  `/book2/type1/fixPath1/name1/../../././///evilType/evilName => :type=evilType :name=evilName`




```
//Test code as below:
web.Router("/book2/:type:string/fixPath1/:name", &controllers.BookController{}, "get:SearchByType")
func (b BookController) SearchByType() {
        fmt.Println(":name=" + b.Ctx.Input.Param(":name"))
        fmt.Println(":type=" + b.Ctx.Input.Param(":type"))
        b.Data["json"] = "OK"
        b.ServeJSON()
}
```

flycash commented on May 23 — Collaborator

yes, can you help to fix it?

flycash added the activity/weopen-star label on May 23

flycash assigned **runner361** on May 23

flycash added the activity/CCFOS label on May 23

runner361 commented on May 24 • edited — Contributor — Author

> yes, can you help to fix it?

Ok, I will try. Url need to be normalized before route, and path.join() should be replaced with strings.join().

flycash commented on May 24 — Collaborator

> yes, can you help to fix it?
>
> Ok, I will try. Url need to be normalized before route, and path.join() should be replaced with strings.join().

But if you use strings.join, you need to handle the case that different platform use different symbol as path separator

runner361 commented on May 24 — Contributor — Author

> But if you use strings.join, you need to handle the case that different platform use different symbol as path separator

Url only use "/" as split char, no need to care about different platform.

runner361 mentioned this issue on May 24

fix issue 4961 Function leafInfo.match() use path.join() to deal with wildcardValues, which may lead to cross directory risk #4964

Merged

runner361 closed this as completed on Jun 1

---

flycash linked a pull request on Jul 30 that will close this issue

Fix issue 4961 #5025 Merged

Assignees

runner361

Labels

activity/CCFOS activity/weopen-star

Projects

None yet

Milestone

No milestone

Development

Successfully merging a pull request may close this issue.

Fix issue 4961
GuoHuiPeng/beego

2 participants