

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

report sqlinjection vulnerability #951

🔒 Closed pe4ch opened this issue on Feb 23 · 1 comment

Assignees



pe4ch commented on Feb 23

sqlinjection source

falcon-plus/modules/nodata/http/proc_http.go

line 61

```
// config.hostgroup, /group/$grpname
http.HandleFunc("/proc/group/", func(w http.ResponseWriter, r *http.Request) {
    urlParam := r.URL.Path[len("/proc/group/"): ]
    RenderDataJson(w, service.GetHostsFromGroup(urlParam))
})
```

sqlinjection sink http param is "grpName"

falcon-plus/modules/nodata/config/service/host.go

line 24

```
// FIX ME: too many JOIN
```

```
func GetHostsFromGroup(grpName string) map[string]int {
    hosts := make(map[string]int)
```

```
    now := time.Now().Unix()
    q := fmt.Sprintf("SELECT host.id, host.hostname FROM grp_host AS gh "+
        " INNER JOIN host ON host.id=gh.host_id AND (host.maintain_begin > %d OR "+
        host.maintain_end < %d)"+
        " INNER JOIN grp ON grp.id=gh.grp_id AND grp.grp_name='%s'", now, now, grpName) #
    grapName sql injection
```

```
    dbConn, err := GetDbConn("nodata.host")
    if err != nil {
        log.Println("db.get_conn error, host", err)
```

```
}      return hosts
```

```
// provide
```

```
sqlinjection bool True page
```

```
mysql query log
```

```
sqlinjection bool False page
```

```
payload
```

  **laiwei** assigned **710leo** on Feb 28

laiwei commented on Feb 28


Member

@pe4ch 谢谢反馈
assigned to @710leo

  **710leo** mentioned this issue on Mar 6

fix: nodata sql injection #954

 Merged

 **laiwei** closed this as completed on Mar 8

Assignees

 **710leo**

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

3 participants

