Open Source > Development Lib > Reporting Tool

GVP **anji-plus / AJ-Report**

👁 Watch ▾ 804   ☆ Star 7.5K

</> Code   ▦ Issues 60   ⭙ Pull Requests 2   ....ines   ᐧⱴ Service ▾

Gitee Pages   JavaDoc   sonarqube Quality Analysis

Jenkins for Gitee   Baidu Efficiency Cloud   Tencent CloudBase

Tencent Cloud Serverless   OPENSCA 悬镜安全

Don't show this again

Issues / 详情

Authentication Bypass vulnerability

◉ Backlog   #I5VVZ0   ⚇ JOHNSON   Opened this issue 2022-10-15

这是英文的漏洞报告，中文的在(This is the English report, the Chin...

Description

The program uses a fixed JWT key, and the stored Redis key uses usernam...
in within an hour. JWT Token can be forged with his username to bypass ...

Login API

com.anjiplus.template.gaea.business.modules.accessuser.controller.AccessUserController#login

Make redis key of format username, Although uuid is used, uuid is not involved in authentication.

com.anjiplus.template.gaea.business.modules.accessuser.service.impl.AccessUserServiceImpl#login

com.anjiplus.template.gaea.business.constant.BusinessConstant#GAEA_SECURITY_LOGIN_TOKEN

Uses a fixed JWT secret key

spring-boot-gaea-2.0.5.RELEASE.jar!com.anji.plus.gaea.utils.JwtBean#createToken

Status

◎ Backlog

Assignees

Not set

Labels

Not set

Milestones

No related milestones

Pull Requests

None yet

Successfully merging a pull reque...
issue.

Branches

No related branch

Planed to start - Planed t
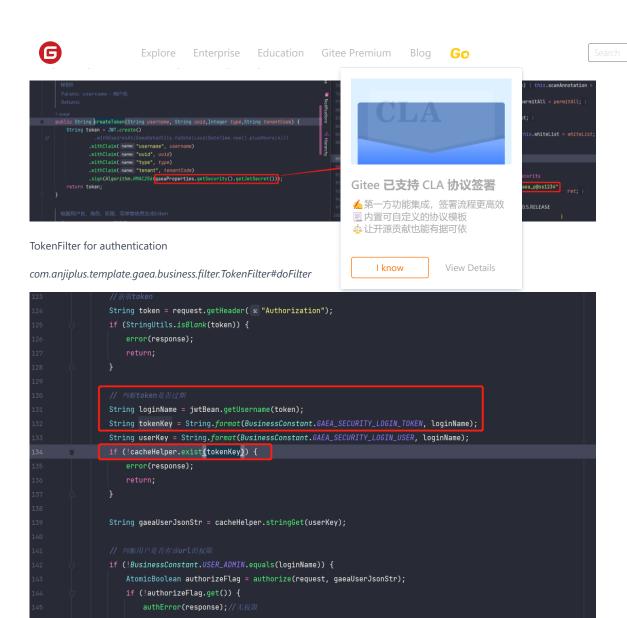
Unscheduled ⁻ Unschedule

Top level

Not Top

Priority

Not specified

参与者（1）

TokenFilter for authentication

com.anjiplus.template.gaea.business.filter.TokenFilter#doFilter
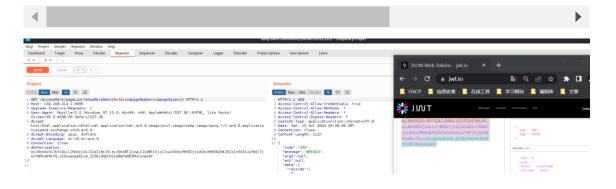

Forge different users' Tokens by modifying the username field

```
{
    "type": 0,
    "uuid": "",
    "tenant": "tenantCode",
    "username": "admin"
}
```

eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ0eXBlIjowLCJ1dWlkIjoiIiwidGVuYW50IjoidGVuYW50Q29kZSIsInVzZXJuYW1lIjo

"version":1.
"roleCode":"root"
"roleName":"超级管理
"deleteFlag":0.
"enableFlag":1.
"authorityList":nu
"accessKey":"89175

"id":2.
"createdBy":"root"
"createdView":"nul
"createTime":"2019
"updateBy":"root".
"updateByView":"nu
"updateTime":"2019
"version":1.

baseAddr2Dtorder(payload).
url_plus_gano_a6ts72]

⊞ 🧑 JOHNSON created **任务**   a month ago

Sign in to comm...

Ⓖ gitee

Git Resources	Gitee Reward	OpenAPI	About Us	📞 777320883
Learning Git	Gitee Stars	Help Center	Join us	✉ git@oschina.cn
CopyCat	Featured Projects	Self-services	Terms of use	知 Gitee
Downloads	Blog	Updates	Feedback	📞 +86 400-606-0201
	Nonprofit		Partners	
	Gitee Go			

Mini Program

OpenAtom Foundation Cooperative code hosting platform   🔷 违法和不良信息举报中心   粤ICP备12009483号   🌐 简体