

New issue

Jump to bottom

Bypass password access to encrypted articles #135

Closed

4 of 6 tasks

kingz40o opened this issue on Apr 4, 2019 · 3 comments

Labels

vulnerability

kingz40o commented on Apr 4, 2019 · edited

我确定我已经查看了 (标注 [] 为 [x])

- ☒ Halo 使用文档
- ☒ Github Wiki 常见问题
- ☒ 其他 Issues

我要申请 (标注 [] 为 [x])

- ☒ BUG 反馈
- ☐ 添加新的特性或者功能
- ☐ 请求技术支持

The password accessing the article is flawed. The code only verifies the "halo-post-password-" + post.getId() in the cookie, but it does not verify that the password is correct.

```
//判断文章是否有加密
if (StringUtil.isEmpty(post.getPassword())) {
    Cookie cookie = ServletUtil.getCookie(request, "halo-post-password-" + post.getId());
    if (null == cookie) {
        post.setPostSummary("该文章为加密文章");
        post.setPostContent("<form id='postPasswordForm' method='post' action='/archives/verifyPostPassword'><p>该文章为加密文章，输入正确的密码即可访问。</p><input type='hidden' id='postId' name='postId' value='\" + post.getId() + \"'> <input type='password' id='postPassword' name='postPassword'> <input type='submit' id='passwordSubmit' value='提交'</form>");
    }
    model.addAttribute("post", post);
    return this.render("post");
}
```

Send the postId to the server by entering the wrong password, and then add the cookie "halo-post-password-4027 (current article id) = 96e79218965eb72c92a549dd5a330112 (any md5 encrypted string)" to access the encrypted article content.

```
HTTP/1.1 302 Found
Server: nginx/1.15.8
Date: Thu, 04 Apr 2019 15:02:04 GMT
Content-Length: 0
Connection: close
Location: https://demo.halo.run/archives/1554388726735
Content-Language: zh-CN
Set-Cookie: halo-post-password-4032=96e79218965eb72c92a549dd5a330112
Strict-Transport-Security: max-age=31536000
```



 Author **admin**
04月 04,2019

This is test!!!!

The vulnerability discoverer by Chaitin Tech.

ruibaby commented on Apr 4, 2019

Member

Ok, we will start to solve these problems, thank you very much for your feedback.

🔖  **JohnNiang** added the **vulnerability** label on Apr 4, 2019

ruibaby commented on May 28, 2019

Member

准备发布 v1, 所以关闭该 issue。

 **ruibaby** closed this as completed on May 28, 2019

kingz40o commented on Jul 15, 2021

Author

Re: [scr673014] your CVE ID requests

外部

收件箱 x

cve-request@mitre.org

发送至 我、cve-request ▾

2021年7月13日 上午12:54 (2天前)

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA256

> [Suggested description]

> Incorrect Access Control vulnerability in Halo 0.4.3, which allows a
> malicious user to bypass encryption to view encrypted articles via
> cookies.

>

> -----

>

> [Vulnerability Type]

> Incorrect Access Control

>

> -----

>

> [Vendor of Product]

> <https://github.com/halo-dev/halo/>

>

> -----

>

> [Affected Product Code Base]

> halo - 0.4.3

> [Impact Information Disclosure]

> true

>

> -----

>

>

> [Attack Vectors]

> View identity to view encrypted articles.

> <https://github.com/halo-dev/halo/issues/135>

>

> -----

>

>

> [Reference]

> <https://github.com/halo-dev/halo/issues/135>

>

> -----

>

>

> [Has vendor confirmed or acknowledged the vulnerability?]

> true

>

> -----

>

>

> [Discoverer]

> chaitin.com

Use CVE-2020-19037.

No one assigned

Labels

vulnerability

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

3 participants

