Jump to bottom

Bypass password access to encrypted articles #135



New issue

⊙ Closed 3 4 of 6 tasks kingz40o opened this issue on Apr 4, 2019 · 3 comments

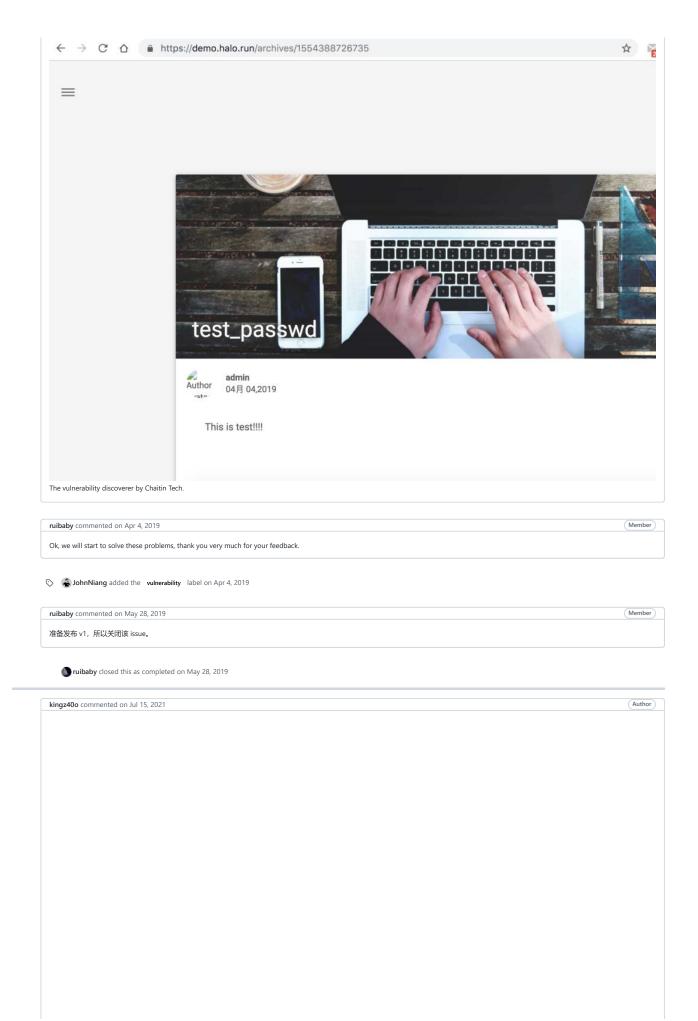
Labels

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.getPostId() in the cookie, but it does not verify that the password is correct.
   //判断文章是否有加密
            if (Strutt1.isNotEmpty(post.getPostPassword())) {
   Cookie cookie = ServletUtil.getCookie(request, "halo-post-password-" + post.getPostId());
                  if (null == cookie) {
  If (noil == cookle) {
    post.setPostSummary("该文章为加密文章");
    post.setPostContent("そorm id="postPostswordForm\" method=\"post\" action=\"/archives/verifyPostPassword\">该文章为加密文章、输入正确的密码即可访问。input
type=\"hidden\" id=\"postId\" name=\"postPassword\" value=\"" + post.getPostId() + "\"> <input type=\"password\" id=\"postPassword\" name=\"postPassword\"> <input type=\"submit\"
id=\"passwordSubmit\" value=\"#述次"></form>");
              model.addAttribute("post", post);
             return this.render("post");
Send the postld 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
```







2021年7月13日 上午12:54 (2天前)

cve-request@mitre.org

发送至 我、 cve-request ▼

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

Hash: SHA256

- > [Suggested description]
- > Incorrect Access Control vulnearbility in Halo 0.4.3, which allows a
- > malicious user to bypass encrption to view encrpted articles via

- > [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

