

1Panel-dev / MaxKB Public

<> Code Issues 68 Pull requests 6 Actions Security and quality 19

Commit 026a2d6

shaohuzhang1 authored 3 weeks ago · ✓ 1/1 · Verified

fix: Inject application name through XSS (#4919)

v2 (#4919) · v2.8.0

1 parent 378cbf5 commit 026a2d6

1 file changed +3 -2 lines changed

↑ Top ⚙️

Filter files...

apps/common/middleware

chat_headers_middleware.py

1 file changed +3 -2 lines changed

Search within code ⚙️

...ommon/middleware/chat_headers_middleware.py

@@ -10,6 +10,7 @@

10 10

11 11 from common.cache_data.application_access_token_cache import
get_application_access_token

12 12 from maxkb.const import CONFIG

13 + from html import escape

13 14

14 15

15 16 class ChatHeadersMiddleware(MiddlewareMixin):

@@ -24,8 +25,8 @@ def process_response(self, request, response):

24 25 if application_access_token is not None:

25 26 white_active = application_access_token.get('white_active',
False)

26 27 white_list = application_access_token.get('white_list', [])

```
27 -         application_icon =
        application_access_token.get('application_icon')
28 -         application_name =
        application_access_token.get('application_name')
28 +         application_icon =
        escape(application_access_token.get('application_icon') or '')
29 +         application_name =
        escape(application_access_token.get('application_name') or '')
29 30         if white_active:
30 31             # 添加自定义的响应头
31 32             response[

```

Comments 0



Please [sign in](#) to comment.