New issue

Stored XSS in MaxKB #24

Open

AnalogyC0de opened last month · edited by AnalogyC0de Edits Owner

Stored XSS in MaxKB

Identification

- **Project:** MaxKB
- **Repository:** https://github.com/1Panel-dev/MaxKB
- **Affected Version/Commit:** <= v2.6.1

CVE Description

A Stored Cross-Site Scripting (XSS) vulnerability exists in MaxKB. Authenticated users can inject malicious JavaScript into the application name or icon fields when creating an application. When a victim visits the public chat interface (`/ui/chat/{access_token}`), the `ChatHeadersMiddleware` retrieves the application data and directly inserts the unescaped application name and icon into the HTML response via string replacement. This allows an attacker to execute arbitrary JavaScript in the victim's browser context.

Affected Component

- **File(s):** `apps/common/middleware/chat_headers_middleware.py` , `apps/application/serializers/application.py`
- **Function / Method:** `ChatHeadersMiddleware.process_response()` , `SimplateRequest.to_application_model()` , `WorkflowRequest.to_application_model()`
- **Entry Point:** `name` and `icon` parameters in POST `/api/application/`

Reproduction Summary

1. An authenticated attacker sends a POST request to `/api/application/` with the application `name` set to a payload like `</title><script>alert('XSS')</script><title>`.
2. A victim visits the chat URL at `/ui/chat/<access_token>`.
3. The server returns an HTML response with the `<title>` tag replaced by the unescaped malicious payload.
4. The victim's browser parses the HTML and executes the embedded JavaScript.

Technical Details

Entry Point Code (`apps/application/serializers/application.py`):

```
@staticmethod
def to_application_model(user_id: str, workspace_id: str, application: Dict):
    return Application(
        id=uuid.uuid7(),
        name=application.get('name'),  # ← NO HTML ESCAPING
        desc=application.get('desc'),
        # ... other fields
    )
```

Sink / Vulnerable Middleware (`apps/common/middleware/chat_headers_middleware.py` lines 33-37):

```
def process_response(self, request, response):

    if request.path.startswith(CONFIG.get_chat_path()) and not request.path.startswith(
            CONFIG.get_chat_path() + '/api'):
        access_token = request.path.replace(CONFIG.get_chat_path() + '/', '')
        if access_token.__contains__('/') or access_token == 'undefined':
            return response
        application_access_token = get_application_access_token(access_token, True)
        if application_access_token is not None:
            white_active = application_access_token.get('white_active', False)
            white_list = application_access_token.get('white_list', [])
            application_icon = application_access_token.get('application_icon')
            application_name = application_access_token.get('application_name')
            if white_active:
                # 添加自定义的响应头
                response[
                    'Content-Security-Policy'] = f'frame-ancestors {" ".join(white_list)}'
            response.content = (response.content.decode('utf-8').replace(
                '<link rel="icon" href="./favicon.ico"/>',
                f'<link rel="icon" href="{application_icon}" />')      # ← UNESCAPED
                .replace('<title>MaxKB</title>', f'<title>{application_name}</title>').encode
                "utf-8"))                                             # ← UNESCAPED
    return response
```

Proof of Concept - Malicious Request:

```
POST /api/application/ HTTP/1.1
Host: maxkb.example.com
Authorization: Bearer <attacker_token>
Content-Type: application/json

{
  "name": "</title><script>alert('XSS')</script><title>",
  "desc": "Malicious application",
  "dialogue_number": 0,
  "type": "SIMPLE",
  "dataset_setting": { ... },
  "model_setting": { ... },
  "problem_optimization": false
}
```

AnalogyC0de changed the title ~~Stored RCE via Function Library Code Execution in Maxkb~~ Stored XSS in MaxKB last month

shaohuzhang1 3 weeks ago

Fixed: 1Panel-dev/MaxKB#4919

Metadata

Assignees

No one assigned

Labels

No labels

Projects

No projects

Milestone

No milestone

Relationships

None yet

Development

Code with agent mode

No branches or pull requests

Participants