




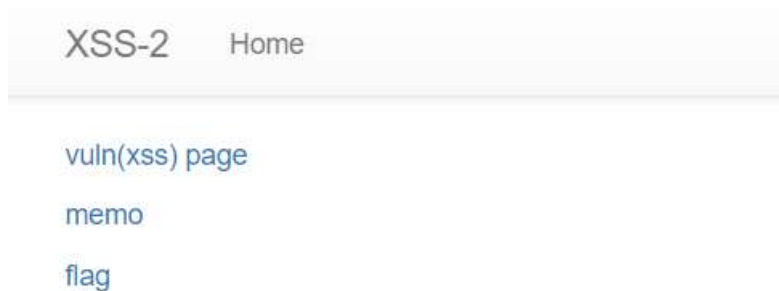


Dreamhack xss-2

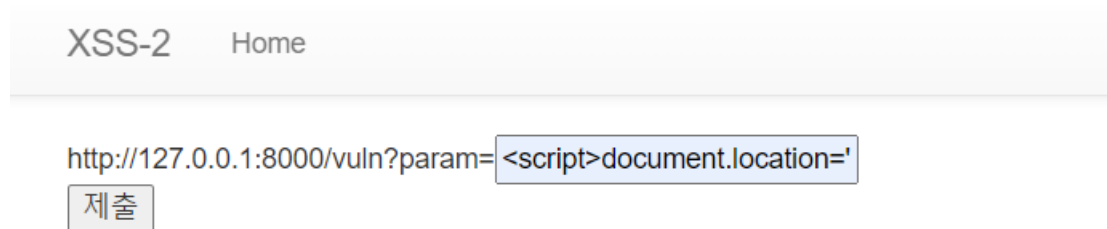
Xss-2 문제는 기본적으로 코드 구성이 xss-1과 유사하다. 그러나 html 파일의 구성에서 차이를 보인다.

 base.html	2024-09-17 오후 7:09	Chrome HTML Do...	2KB
 flag.html	2024-09-17 오후 7:09	Chrome HTML Do...	1KB
 index.html	2024-09-17 오후 7:09	Chrome HTML Do...	1KB
 memo.html	2024-09-17 오후 7:09	Chrome HTML Do...	1KB
 vuln.html	2024-09-17 오후 7:09	Chrome HTML Do...	1KB

Xss-1과 비교하여 보면 vuln.html이 추가된 것을 확인할 수 있다.



서버에 연결해 보면 xss-1과 유사한 웹페이지가 뜬다.



시험삼아 xss-1과 동일한 방법을 사용해 보았으나, flag값을 얻을 수 없었다. 이후 새로 추가된 vuln.html 파일을 확인해 보았다.

```

sers / gram / Downloads / 9d2e6bd5-b795-46d0-8aas-ff191a556568 / deploy / templates / vuln.html
{% extends "base.html" %}
{% block title %}Index{% endblock %}

{% block head %}
    {{ super() }}
    <style type="text/css">
        .important { color: #336699; }
    </style>
{% endblock %}

{% block content %}
    <div id='vuln'></div>
    <script>var x=new URLSearchParams(location.search); document.getElementById('vuln').innerHTML = x.get('para
{% endblock %}

```

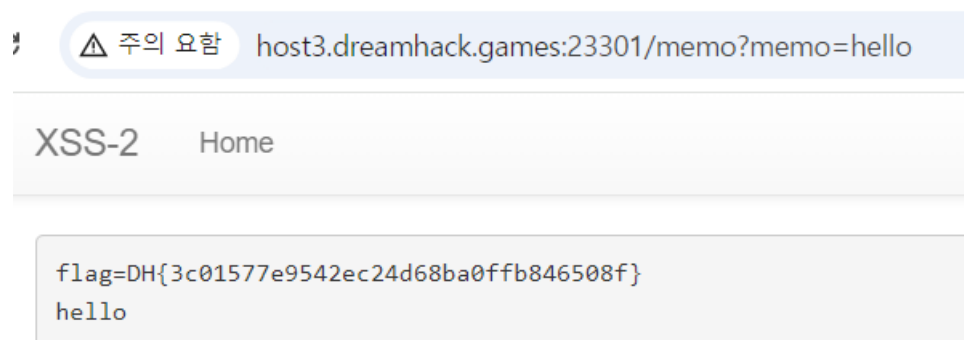
여기서 주목할 것은 innerHTML 속성이다. innerHTML 속성은 선택된 HTML 요소의 내부 내용을 설정하거나 반환하는 데 사용된다.

innerHTML은 HTML을 포함한 모든 문자열을 요소 안에 삽입하기 때문에, 사용자가 자바스크립트 코드를 쿼리 파라미터로 삽입하면 그 스크립트가 실행될 수 있다. 그러나 위에서 확인했던 것처럼 <script>를 이용할 수는 없고 다른 방법을 찾아야 한다.

이 뒤를 잘 모르겠어 xss 우회에 대해 인터넷 서치를 하던 중 다음과 같은 방법을 발견해 사용해 보기로 했다.

<https://noirstar.tistory.com/309>

이 티스토리에서 알아낸 방법과 xss-1에서 사용한 방법을 조합해 보면 flag 페이지에 다음과 같이 입력해야 된다는 것을 알 수 있다: **<svg onload="location.href = '/memo?memo=' + document.cookie">**



Flag페이지에 입력하고 memo페이지를 다시 확인해보니

DH{3c01577e9542ec24d68ba0ffb846508f} 라는 플래그를 확인할 수 있었다.