https://dreamhack.io/wargame/challenges/268/

Reflected-XSS를 이용하여 문제를 푸는 형식

Vuln(xss) page 메뉴를 탐색했을 때 XSS-1과 다르게 스크립트 구문이 실행이 안된다.

스크린샷, 텍스트, 소프트웨어, 멀티미디어 소프트웨어이(가) 표시된 사진

자동 생성된 설명

Memo 메뉴를 들어갔을 때, 아래와 같이 memo라는 문구가 삽입이 된다.

스크린샷, 텍스트, 라인, 화이트이(가) 표시된 사진

자동 생성된 설명

코드를 분석해보면

텍스트, 스크린샷, 폰트, 소프트웨어이(가) 표시된 사진

자동 생성된 설명

Flag 부분을 탐색했을 때

텍스트, 스크린샷, 폰트이(가) 표시된 사진

자동 생성된 설명

아래와 같이 로컬호스트에서 vuln로 라우팅한 후 파라미터값을 실행하는걸 알 수 있다.

다만 무언가에 의해서 <script>~</script>실행은 막히는 것 같으니 스크립트를 우회해야 한다.

텍스트, 스크린샷, 폰트, 화이트이(가) 표시된 사진

자동 생성된 설명

<img src="test" onerror="location.href='/memo?memo='+document.cookie">

위의 명령어는 사이트를 memo로 리다이렉션 한 후 쿠키(=flag)에 있는 값을 메모에 삽입하는내용

텍스트, 라인, 폰트, 스크린샷이(가) 표시된 사진

자동 생성된 설명