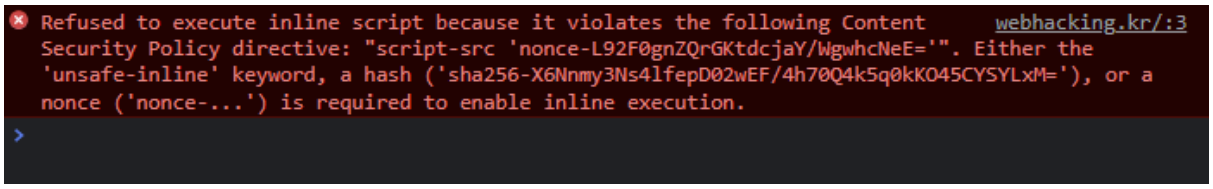
BABY 문제 write-up

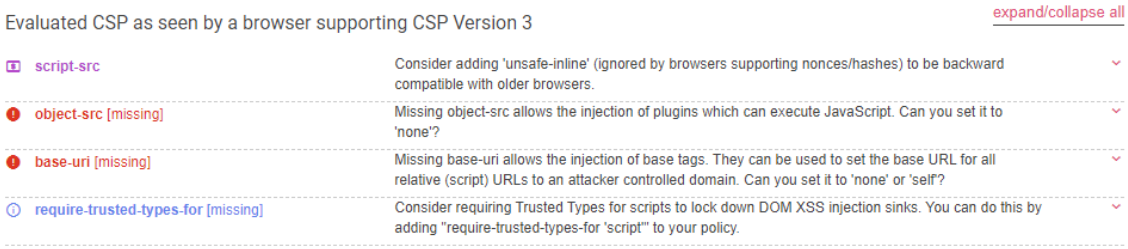
강승민

문제를 보면 inject라는 파라미터를 받아서 출력해준다. 이를 보고 XSS가 가능할 것 같아서 시도해보았더니

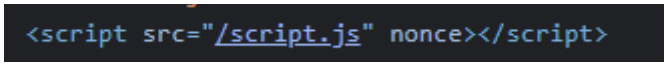
이와 같이 동작하지 않는 모습을 볼 수 있었다. 무엇이 문제인지 파악하다 개발자도구의 콘솔을 보았더니



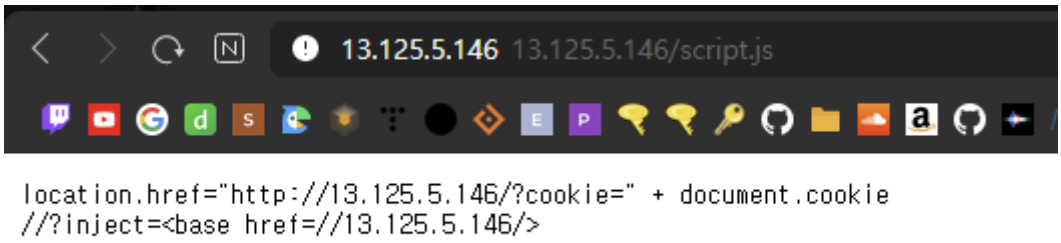
이와 같은 에러가 보였는데 CSP가 동작하여 스크립트 동작을 차단했다는 에러 문구 였다.



에러문구에서 보았듯이 CSP가 적용되어 있어서 이를 더 자세히 알기 위해 적용중인 CSP를 알려주는 사이트에 검색해보았더니 에러문구에서 보였던 script-src만 적용된 것을 볼 수 있다.

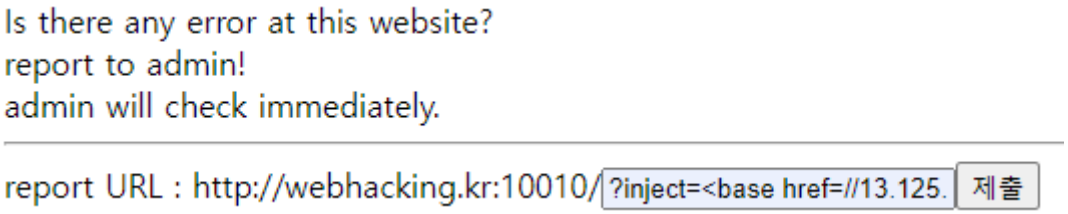


script-src는 위 사진과 같이 /script.js 파일의 스크립트만 동작 시키겠다는 것인데 여기서 생기는 문제가 웹사이트 주소를 제외하고 적혀 있기 때문에 html의 <base hre=//>태그를 이용하여 바꿔주면 XSS가 가능할 것 같다.

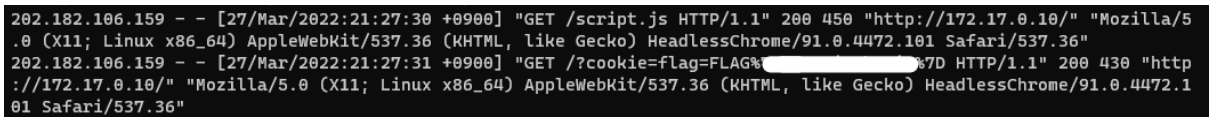


그래서 개인서버에서 /script.js 경로로 파일을 만들고 쿠키를 가져올 자바스크립트 코드를 작성했다.

이후 이렇게 접속하니 XSS가 가능했고



Flag를 쿠키에 가진 봇이 XSS에 당하게 만들기 위해 error report를 해주면



이와 같이 개인서버의 로그에 쿠키 값으로 Flag를 얻을 수 있다.