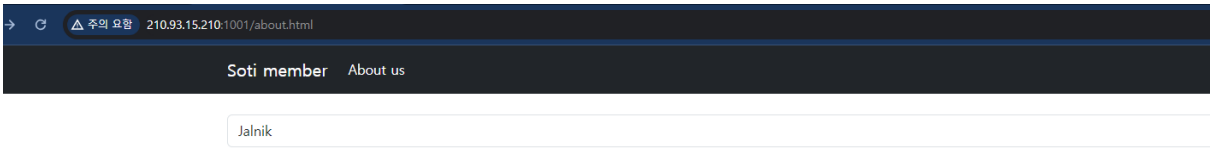
WelcomeToSoti

문제 분류	web
poc 작성자	김재환
문제 개발자	김재환

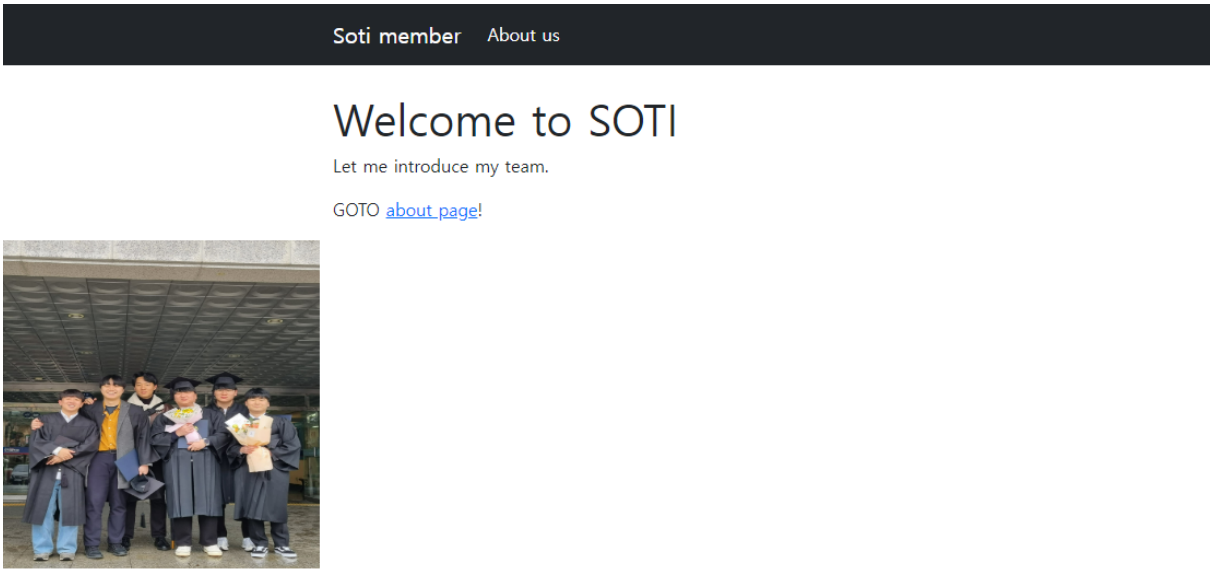
1. 문제

SOTI를 설명하는 사이트입니다.

`/about 경로` 로 이동하면 드롭다운이 표시됩니다.

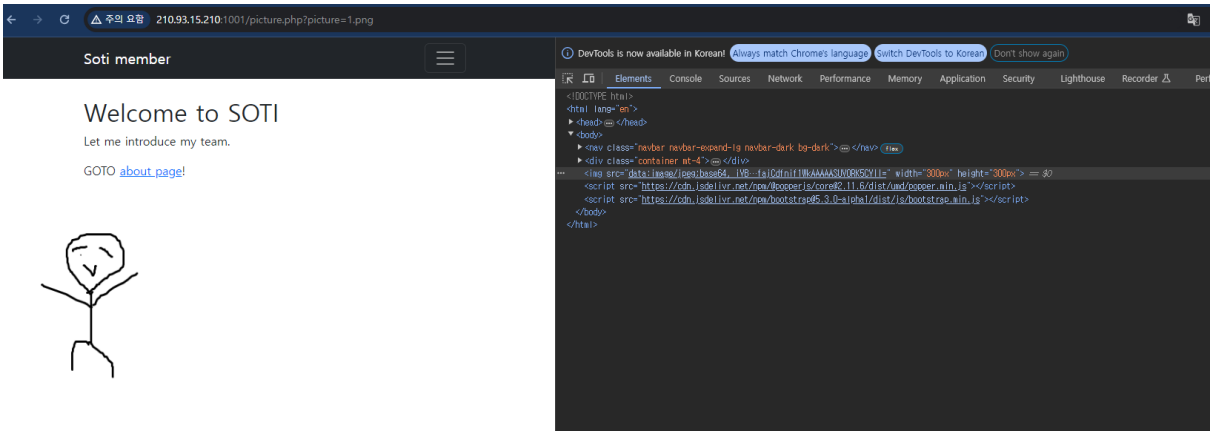


고르는 사진에 따라 사진을 파라미터 형식으로 불러옵니다. 현재는 `2.png` 를 불러왔습니다.



2. 풀이

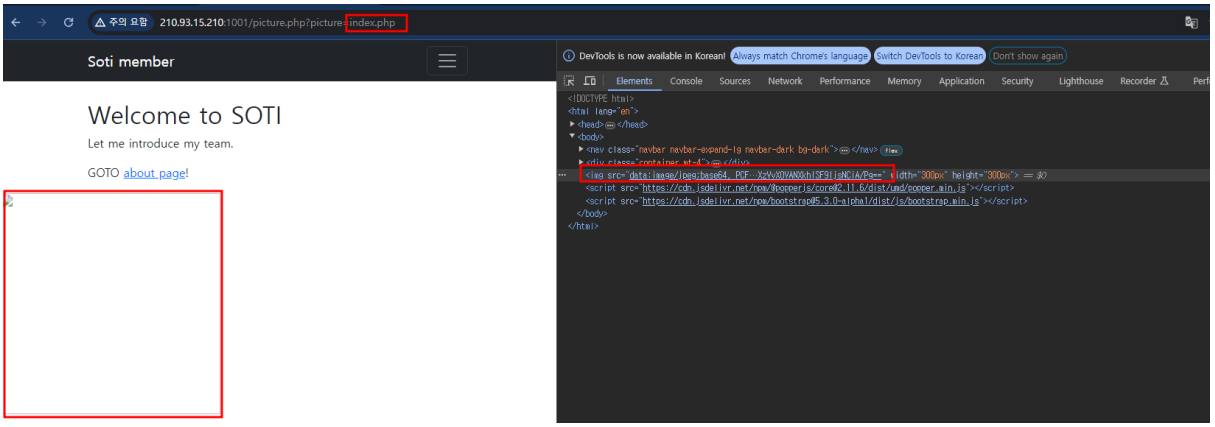
파라미터



- 사진이 렌더링 되는 부분을 자세히 보면, `base64` 데이터 형식으로 가져오는 것을 알 수 있습니다.
- 페이지가 바뀌지도 않고, 파라미터만 변하는데 데이터가 바뀐다는 것은, PHP부분에서 파라미터에 따라 데이터를 읽는다는 것을 알 수 있습니다.

- 데이터를 읽는 함수는 보통 `php스키마` 를 사용할 수 있기 때문에 `LFI` 공격을 시도해 볼 수 있습니다.

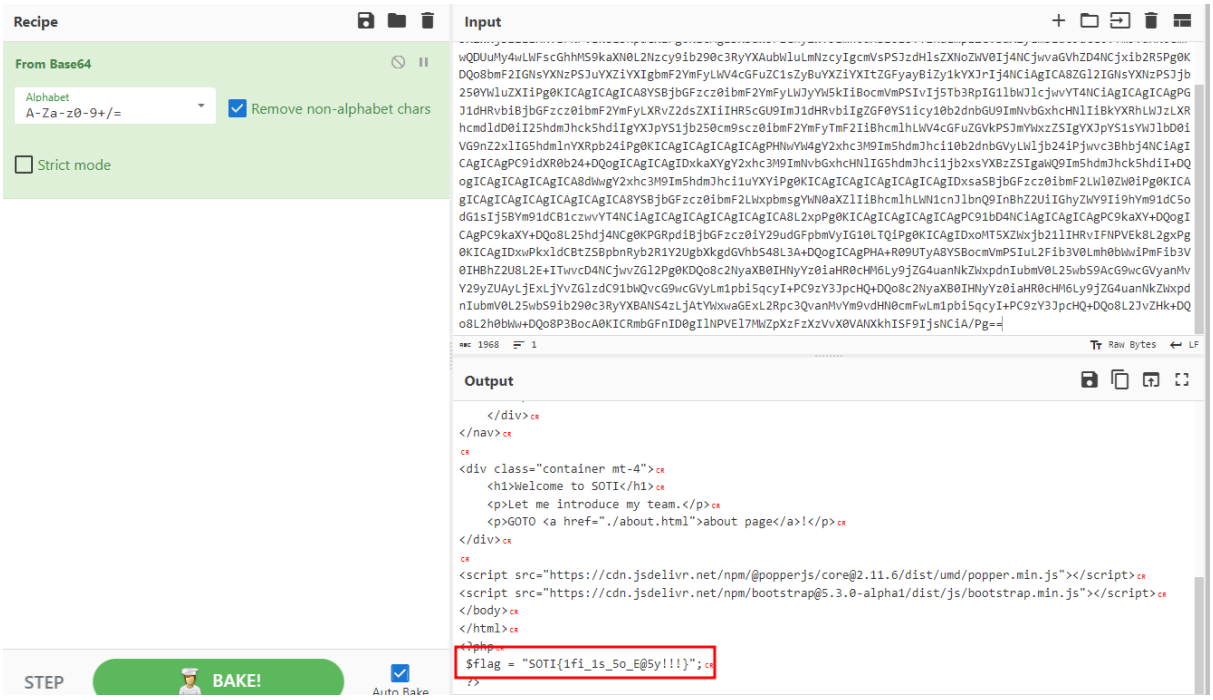
LFI



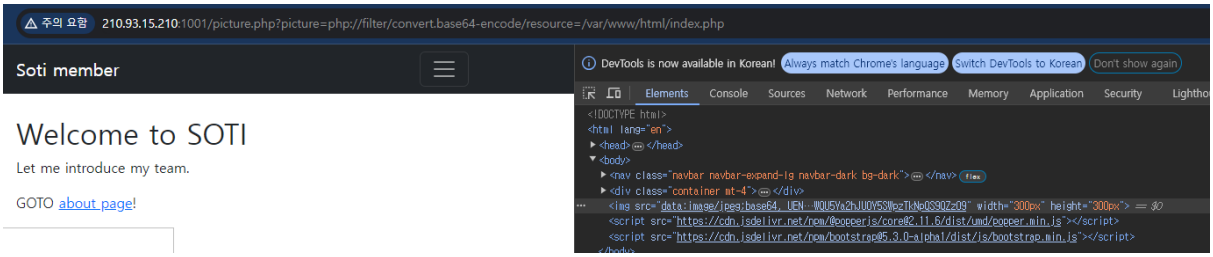
- PHP스키마를 사용하기 전에, 더 간단한 방식으로 접근하기 위해 파라미터에 `index.php` 를 입력합니다.
- img는 깨졌지만, `base64` 인코딩 된 값을 확인할 수 있습니다.

> 💡 LFI?

Local File inclusion으로 말 그대로 `로컬(내부)` 에 있는 파일을 소스코드에 포함시켜 `외부로 노출할 수 있는 취약점을 말합니다.`



- 이를 복호화하면, `index.php`에 박혀있던 flag값을 찾을 수 있습니다.



`php://filter/convert.base64-encode/resource=/var/www/html/index.php` 등 `php wrapper`로 다양한 공격 또한 가능합니다.