f1nd_the_d0g's_name

description

> 강아지 이름을 찾아주세요!

문제 풀이

배경

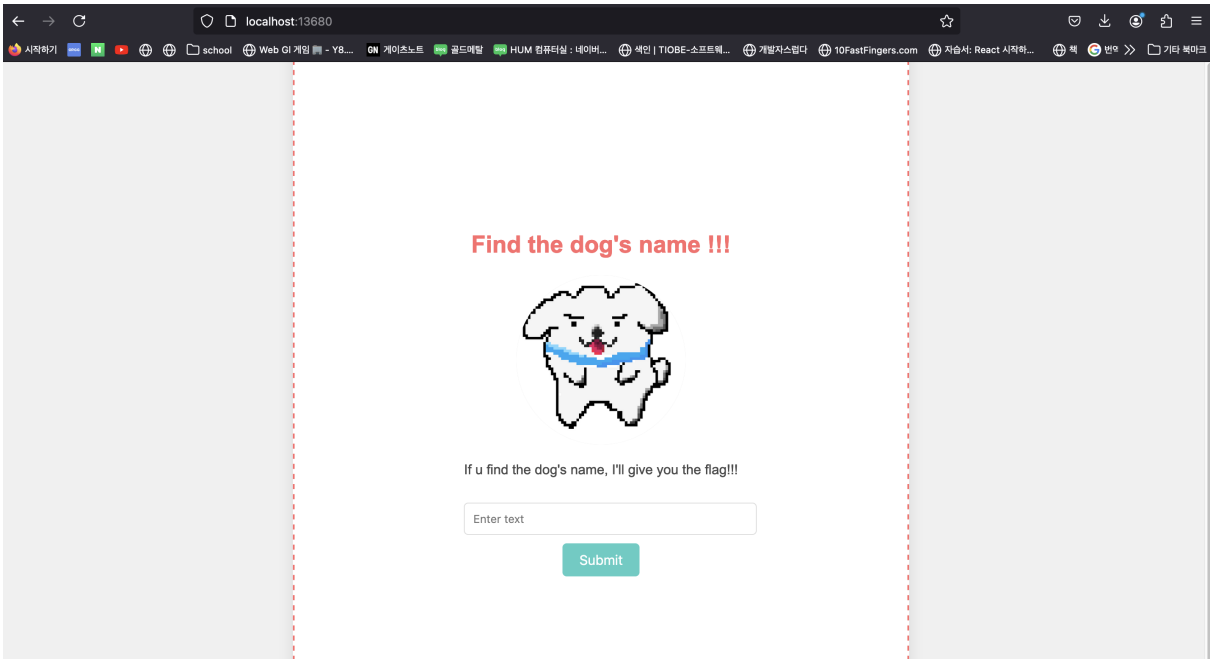
이 `secure-compare`패키지는 안전한 문자열 비교에 사용되는 npm 패키지입니다. 타이밍 공격을 완화하는 방식으로 두 문자열을 비교하도록 설계되었습니다. 이 패키지는 일반적으로 비밀번호 확인과 같이 민감한 데이터의 안전한 비교가 필요한 애플리케이션에서 사용됩니다. 그러나 3.0.1 이전 버전은 `secure-compare`해당 문자열의 실제 내용과 관계없이 패키지가 항상 같은 길이의 두 문자열을 비교할 때 true를 반환할 수 있는 취약성의 영향을 받습니다.

취약점 세부 정보

이 취약점은 `secure-compare`패키지에서 사용된 안전하지 않은 비교 알고리즘에서 발생합니다. 이 알고리즘은 두 문자열의 내용을 제대로 비교하지 못하여 항상 같은 길이의 문자열에 대해 true를 반환하는 상수 시간 비교가 발생합니다. 이는 `secure-compare`안전한 문자열 비교에 의존하는 애플리케이션에서 보안 문제로 이어질 수 있습니다. 공격자는 이 취약점을 악용하여 정확한 문자열 비교에 의존하는 비밀번호 확인 또는 기타 보안 조치를 우회할 수 있습니다.

Insecure Comparison in secure-compare (https://vulert.com/vuln-db/CVE-2015-9238)이다.

"secure-compare": "^3.0.1" 이전 버전에서 `compare('password', password) == true` 를 통해 값을 비교할 경우, 글자 수가 같으면 비교를 우회할 수 있는 취약점이다.




```
if (password == serverPassword) {
            return res.send('Do not hacking!!!!')
        }
        if (secureCompare(serverPassword, password) == true)

        // flag is here!!!!!!
        try {
            const flag = fs.readFileSync('flag.txt', {encodin
            const ip = req.header["x-forwarded-for"] || req.c
            fs.writeFileSync('./server.log', `${ip} | ${passw
            return res.send(`flag is ${flag}`)
        } catch (error) {
            console.log(error)
            return res.send('Internal Server Error')
        }

        } else {
            return res.send('Wrong!')
        }
```

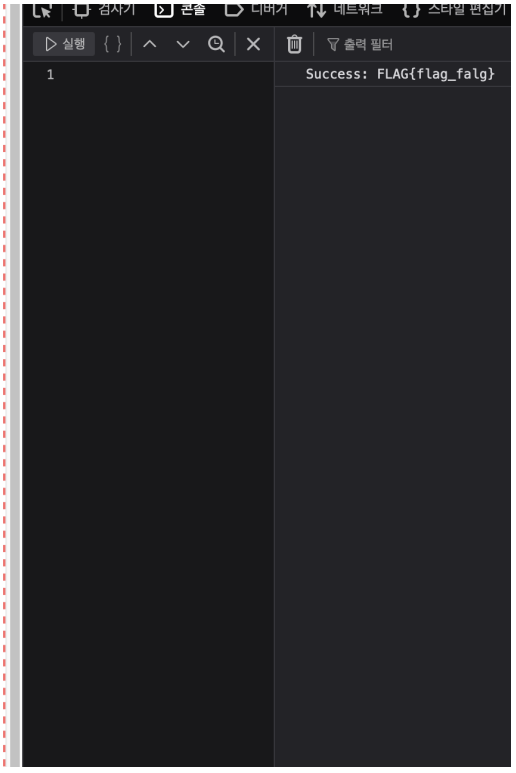
해당 코드를 보면 password 값이 serverPassword로 설정되어 있는 것을 볼 수 있다. 이를 통해 “Enter text”를 입력하는 부분에 해당하는 글자 수만큼 입력해주면 된다.

```
// 서버로 fetch POST 요청 보내기
fetch('/login', {
    method: 'POST',
    headers: {
        'Content-Type': 'application/json',
        'X-Server-Password': 'bb791309f692fea37de49b3f191ddcf55c112472'
    },
```

헤당 값은 response 헤더를 통해 확인 가능하다.

```
if (password == serverPassword) {
            return res.send('Do not hacking!!!!')
```

하지만 해당 값이 그대로 사용하면 'Do not hacking!!!!'라는 문구를 출력한다.



그래서 위의 취약점을 사용해서 해당하는 값만큼의 글자 수를 입력해주면 플래그를 획득할 수 있는 문제이다.

문제 파일

find_the_dogs_name.zip

제공

prov_find_the_dogs_name.zip