

easy-login

- 문제 이름: easy-login
- 카테고리: Web
- 난이도: Easy

웹 브라우저로 접속하면 간단한 로그인 폼이 있는 페이지가 나타납니다.
로그인 우회를 통해 플래그를 획득하면 됩니다.

문제 풀이

문제의 핵심은 아래 코드에 있습니다.

```
eval(f"{user} == {pw}")
```

`eval()`은 문자열로 전달된 값을 파이썬 코드로 실행하는 함수로 사용자 입력을 검증하지 않고 `eval()`에 전달할 경우 임의의 코드 실행이 가능해진다는 점을 이용하였습니다.

`id`에 1, `pw`에 1을 입력하면 실제 실행되는 코드는 아래와 같습니다.

```
eval("1 == 1")
```

`1 == 1`은 파이썬에서 정수 비교이며 결과는 항상 `True`가 되기 때문에 `result` 값이 `True`가 되어 `flag`가 출력됩니다.

문자열을 사용한다면 따옴표를 붙인 `'admin'`으로 써야 합니다. 그 이유는 `admin`, `admin`을 입력하게 되면 `eval("admin == admin")`으로 실행되게 되는데 여기서 `admin`은 문자열로 인식되지 않고 정의되지 않은 변수로 인식되기 때문에 `Name error`가

발생합니다. 그리하여 `try except`에 걸려 `Login failed`가 출력됩니다.

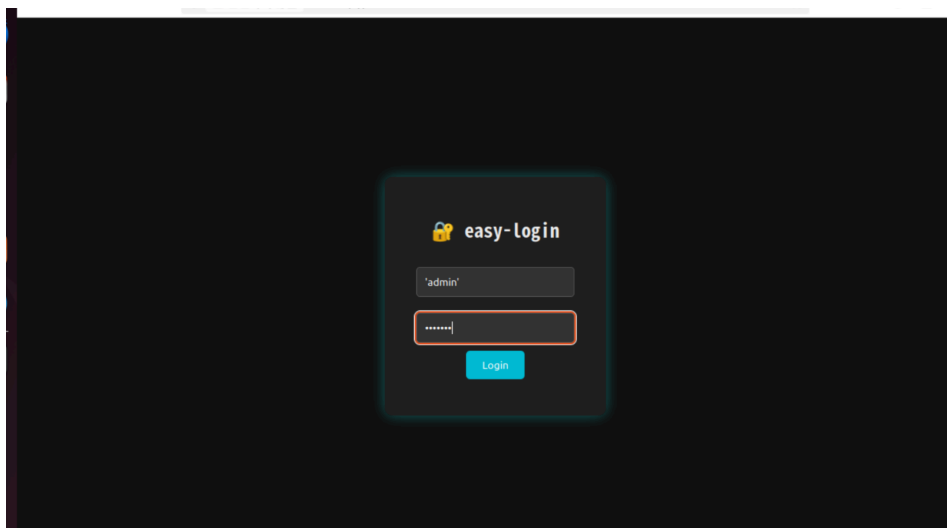
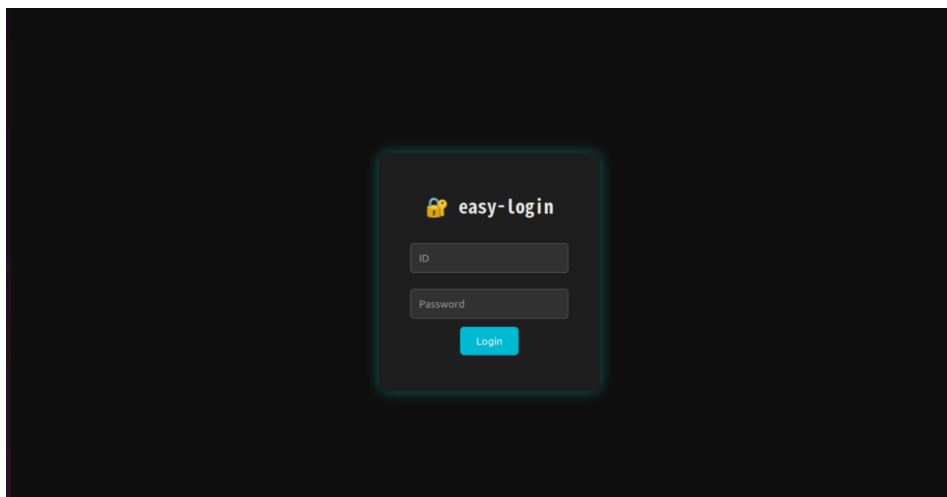
결론


`1, 1`은 문자열 따옴표가 필요 없는 정수 리터럴이기 때문에 정상적으로 비교가 가능해 `True`를 반환합니다.

문자열을 사용하려면 반드시 작은 따옴표나 큰 따옴표로 감싸야 합니다.

ID: `'admin'` PW: `'admin'`

실행화면



← → ↻  안전하지 않음 http://172.17.0.2:8080/login ☆

FLAG: XKSW(welcome)

@Xpert