**[WEB] But nothing happened…**

**Explanation:**

접속자 세션의 랜덤 sessid에 따라 고정되는 고유한 랜덤 잉어킹을 생성한다.

**Solve:**

flag는 2개의 조각FLAG\_A, FLAG\_B으로 나누어져 있다. 둘 다 flask client-side session cookie를 조작해서 찾아내야 한다.

Flask 기본 session은 다음과 같이 구성되어 있다.

* base64 인코딩된 json 데이터
* SECRET\_KEY 기반의 서명

데이터 부분은 디코딩해서 확인할 수 있으며, 만약 SECRET\_KEY를 알고 있으면 임의의 데이터를 포함한 서명된 세션 쿠키를 생성할 수 있다. flask 기본 세션은 서버에 세션정보를 저장하지 않기 때문에 임의로 생성한 세션 쿠키를 구분할 수 없다.

https://book.hacktricks.xyz/network-services-pentesting/pentesting-web/flask

**FLAG\_A**:

만약 새로 생성된 잉어킹의 color가 (255, 215, 0)으로 황금색이면 하드코딩된 FLAG\_A 텍스트가 잉어킹 이미지에 포함된다. 텍스트, 스크린샷, 폰트이(가) 표시된 사진

자동 생성된 설명

다음과 같이 random seed가 될 sessid를 찾아낸다.

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

자동 생성된 설명

이후 flask-unsign으로 세션 쿠키를 생성해 브라우저에 cookie로 저장한다.

텍스트, 스크린샷, 폰트이(가) 표시된 사진

자동 생성된 설명

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

자동 생성된 설명

새로고침하면 sessid에 대한 새로운 잉어킹이 생성되고 flag의 앞부분이 나타난다.

**FLAG\_B**:

FLAG\_B라는 이름의 환경변수에 flag의 나머지 부분이 저장되어 있다.

화면의 `싸우다` 버튼을 누르면 `/splash` 경로로 GET 요청을 날린다. 그러나 아무 일도 일어나지 않는다…

텍스트, 멀티미디어 소프트웨어, 소프트웨어, 폰트이(가) 표시된 사진

자동 생성된 설명

sessions/{sessid}/move.py에서 동적 import한 move.py 에서 함수 splash를 호출한다.

텍스트, 폰트, 스크린샷, 디자인이(가) 표시된 사진

자동 생성된 설명텍스트, 스크린샷, 폰트이(가) 표시된 사진

자동 생성된 설명텍스트, 스크린샷, 폰트이(가) 표시된 사진

자동 생성된 설명

배경 이미지를 업로드하는 기능이 있으므로, 이미지 대신 .py 파일을 업로드해서 호출되도록 할 것이다. 업로드된 파일은sessions/{sessid}/files/ 경로에 저장되며, 호출하는 move.py 파일은 sessions/{sessid}/ 경로에 있다. 저장하는 파일 이름에는 secure\_filename()이 적용되어 LFI가 통하지 않는다.

텍스트, 스크린샷, 폰트이(가) 표시된 사진

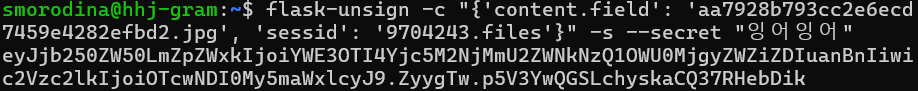
자동 생성된 설명

대신, 우선 sessions/{sessid}/files/ 경로에 move.py 파일을 저장한다.

텍스트, 소프트웨어, 멀티미디어 소프트웨어, 폰트이(가) 표시된 사진

자동 생성된 설명

flask-unsign을 이용해 기존의 sessid를 `{sessid}.files`로 바꾸어 새로 생성한 세션 쿠키를 가지고 `/splash`에 다시 요청을 보낸다.



동적으로 import되는 모듈의 이름이 `sessions.{sessid}.move`이기 때문에 위조된 세션 쿠키의 sessid에 의해 `sessions.{original\_sessid}.files.move`가 되어, 업로드한 move.py의 splash() 함수가 호출된다.

텍스트, 폰트, 스크린샷이(가) 표시된 사진

자동 생성된 설명 텍스트, 스크린샷, 소프트웨어, 멀티미디어 소프트웨어이(가) 표시된 사진

자동 생성된 설명