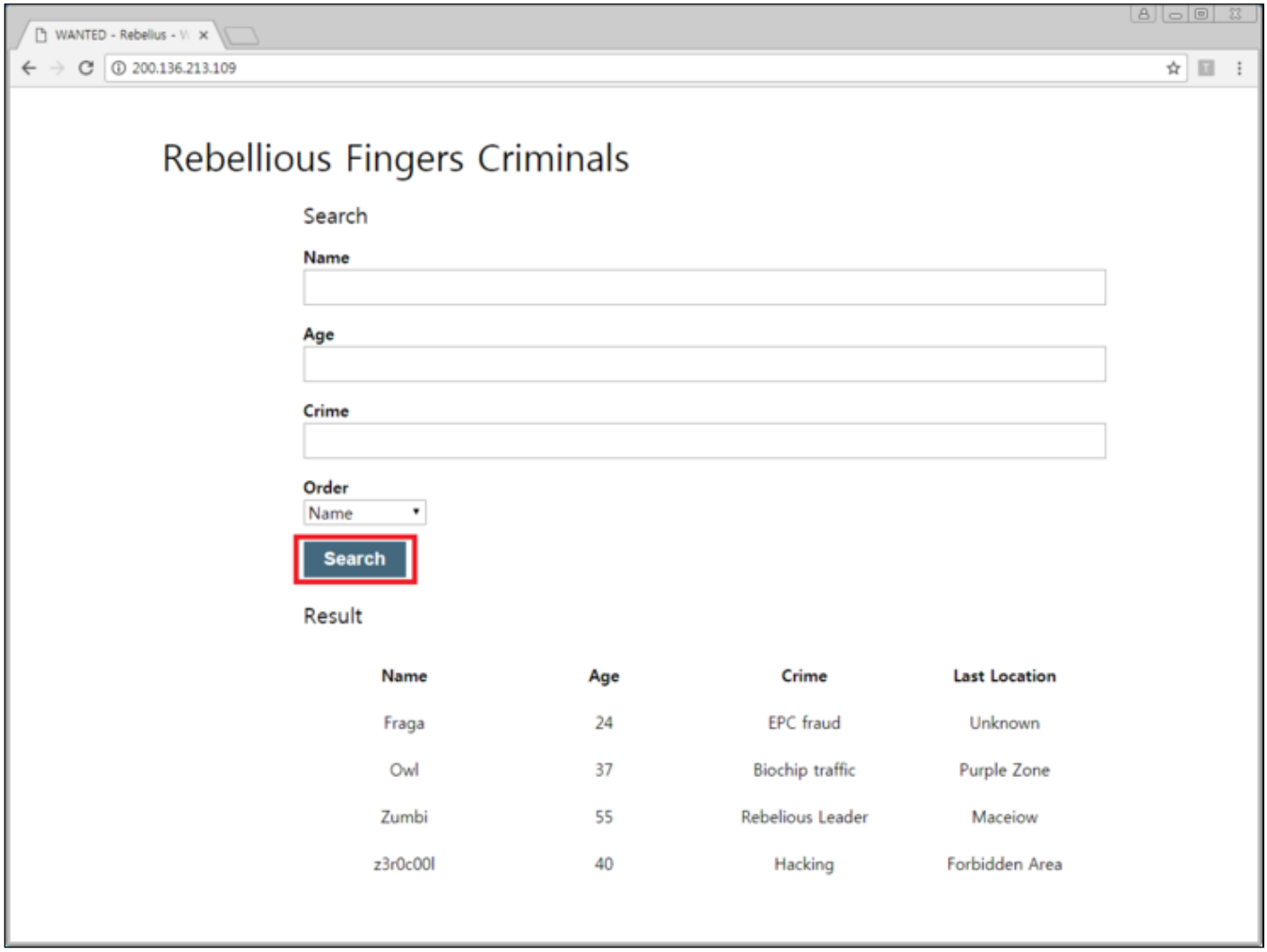
[Pwn2win_CTF_2017] WEB - Criminals

문제 풀이

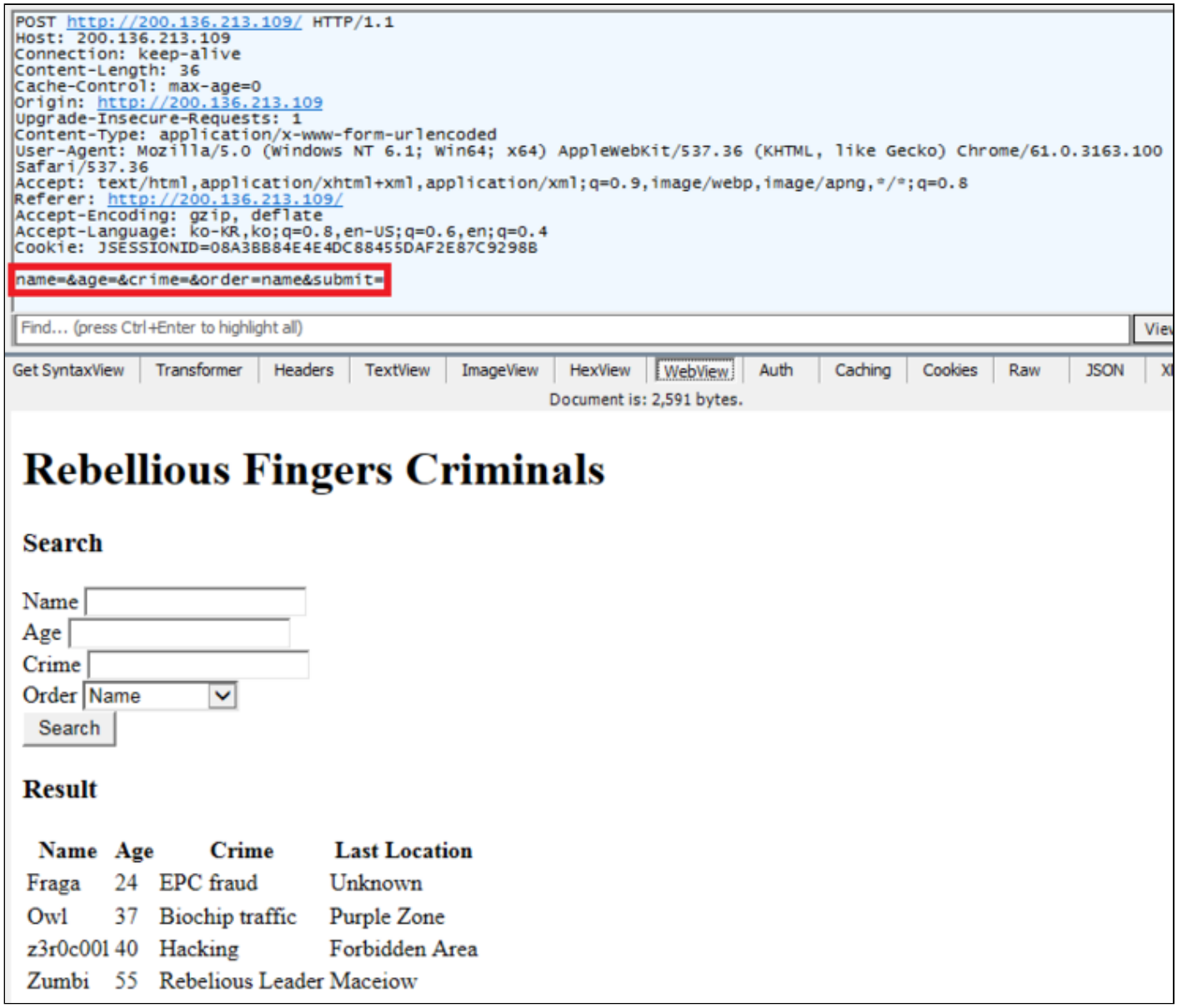
2017/10/25 21:44 http://blog.naver.com/kby88power/221125280421

문제는 다음과 같다.



단순한 웹 사이트다. Search 기능 하나만 존재한다.

Search 버튼을 눌러본다.



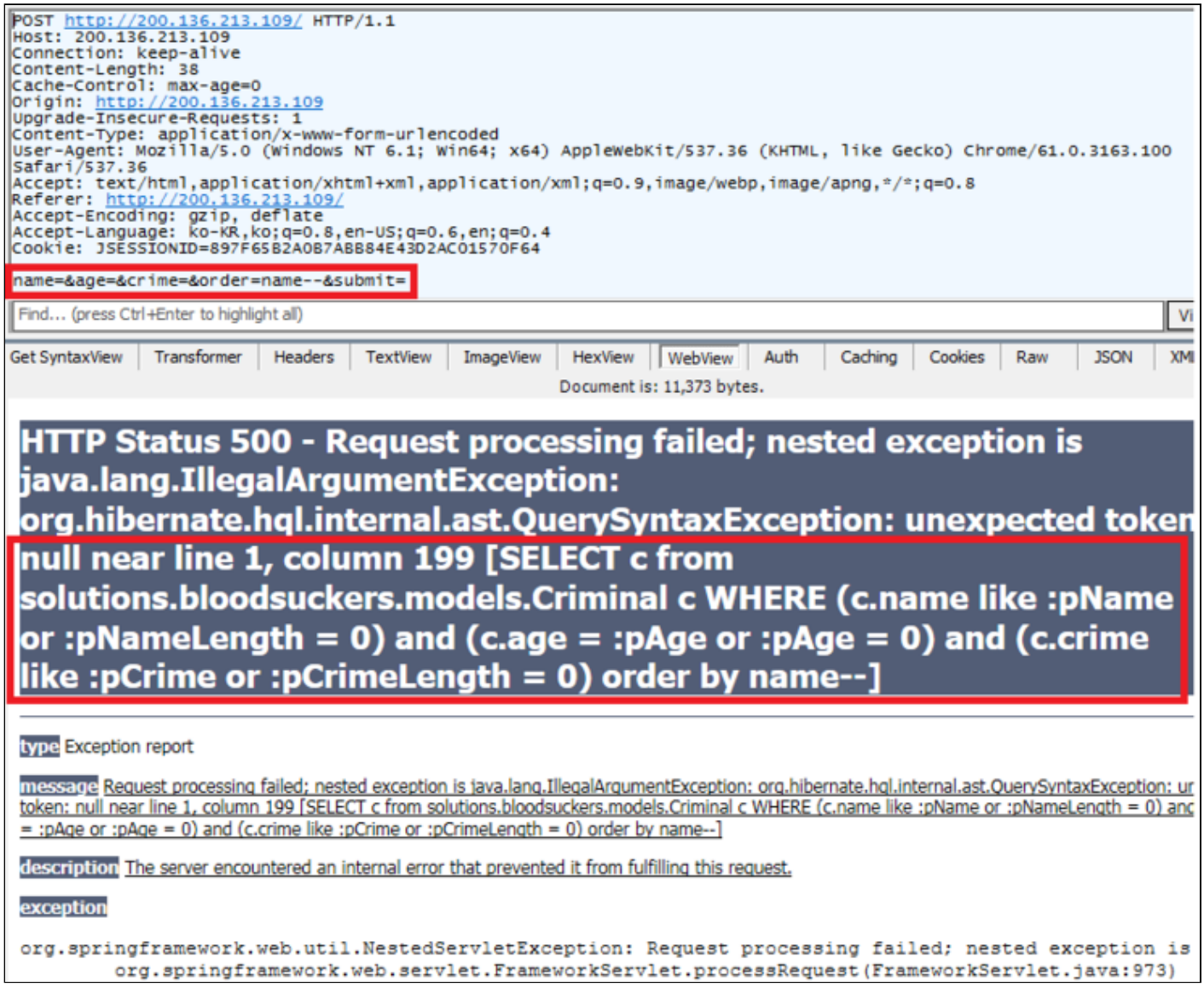
파라미터 중에 order 파라미터 값만 존재한다. 값은 name이다.

눈치 빠른 사람은 바로 알 것이다. order by절이다.

name 컬럼명으로 검색 결과를 정렬하는 것으로 보인다.

SQL Injection이 들어가는 파라미터 값을 찾아야 하겠다.

가장 먼저, 수상한 order 파라미터 값을 확인해보았다.

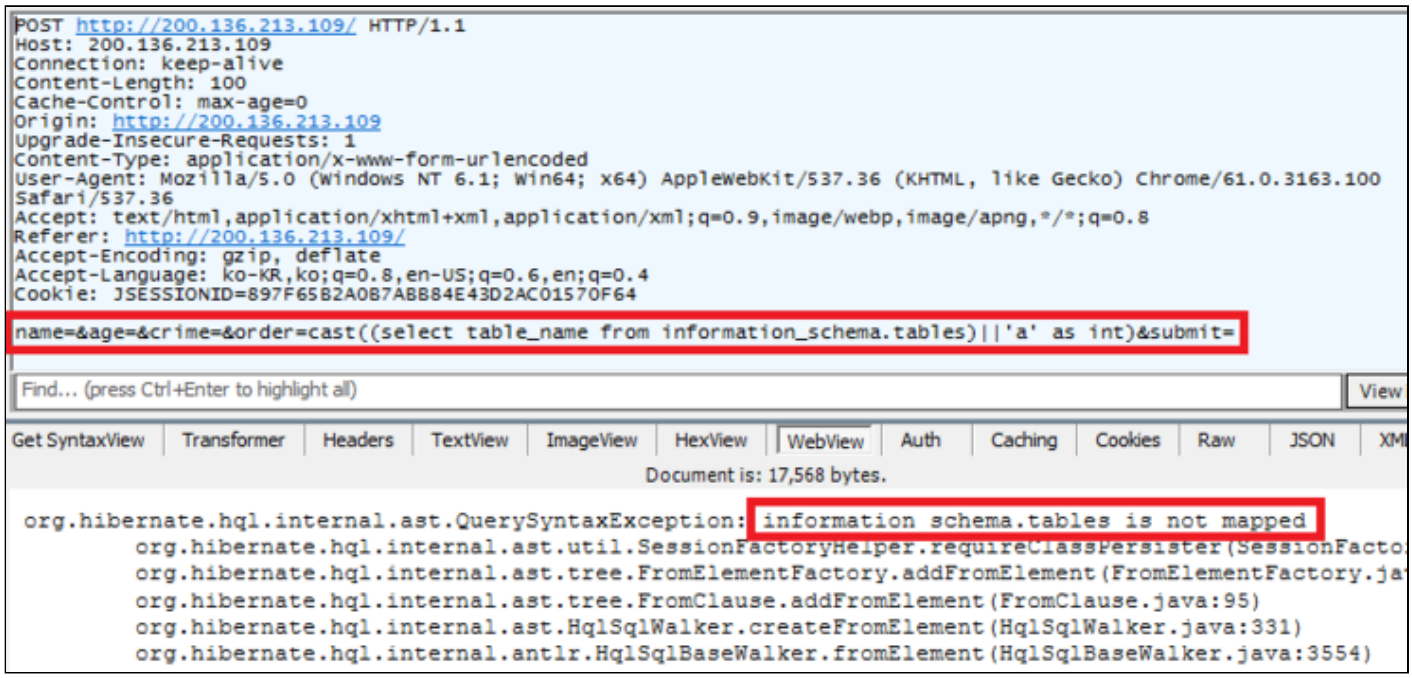


주석을 추가하면 에러가 발생하는데, 에러 메시지에 쿼리가 노출되고 있다. 전형적인 Error Based SQL Injection 문제이다.

SELECT c from solutions.bloodsuckers.models.Criminal c WHERE (c.name like :pName or :pNameLength = 0) and (c.age = :pAge or :pAge = 0) and (c.crime like :pCrime or :pCrimeLength = 0) order by **name--**

:pName 과 같은 표현은 Hibernate SQL (HQL) 에서 사용하는 표현으로, 변수값을 받아 동적으로 쿼리를 생성하기 위한 안전한(Secure Coding) 표현 방법이다. 쿼리에 변수를 '+' 문자열로 합쳐 주는 방식은 취약하며, order 파라미터 값이 이러한 취약한 방식으로 확인된다.

SQL Injection 공격을 시도해본다.



information_schema.tables is not mapped 에러메시지가 출력된다.

Hibername SQL (HQL) 에서는 일반적으로 소스코드에 정의해놓은 테이블에만 접근이 가능하므로, 정의되지 않은 테이블에 접근 시 에러가 발생한다.

일반적이지 않은 방법을 사용해야한다.

여기서 Postgresql 데이터베이스의 매직 함수 하나를 소개한다.

> query_to_xml(query text, nulls boolean, tableforest boolean, targetns text)

query_to_xml executes the query whose text is passed as parameter *query* and maps the result set.

query_to_xml을 사용하면 소스코드에 정의하지 않은 테이블에 접근이 가능하다. 이 함수의 결과는 xml 형태로 출력되는데, xml 을 처리해주는 함수를 하나 더 소개한다.

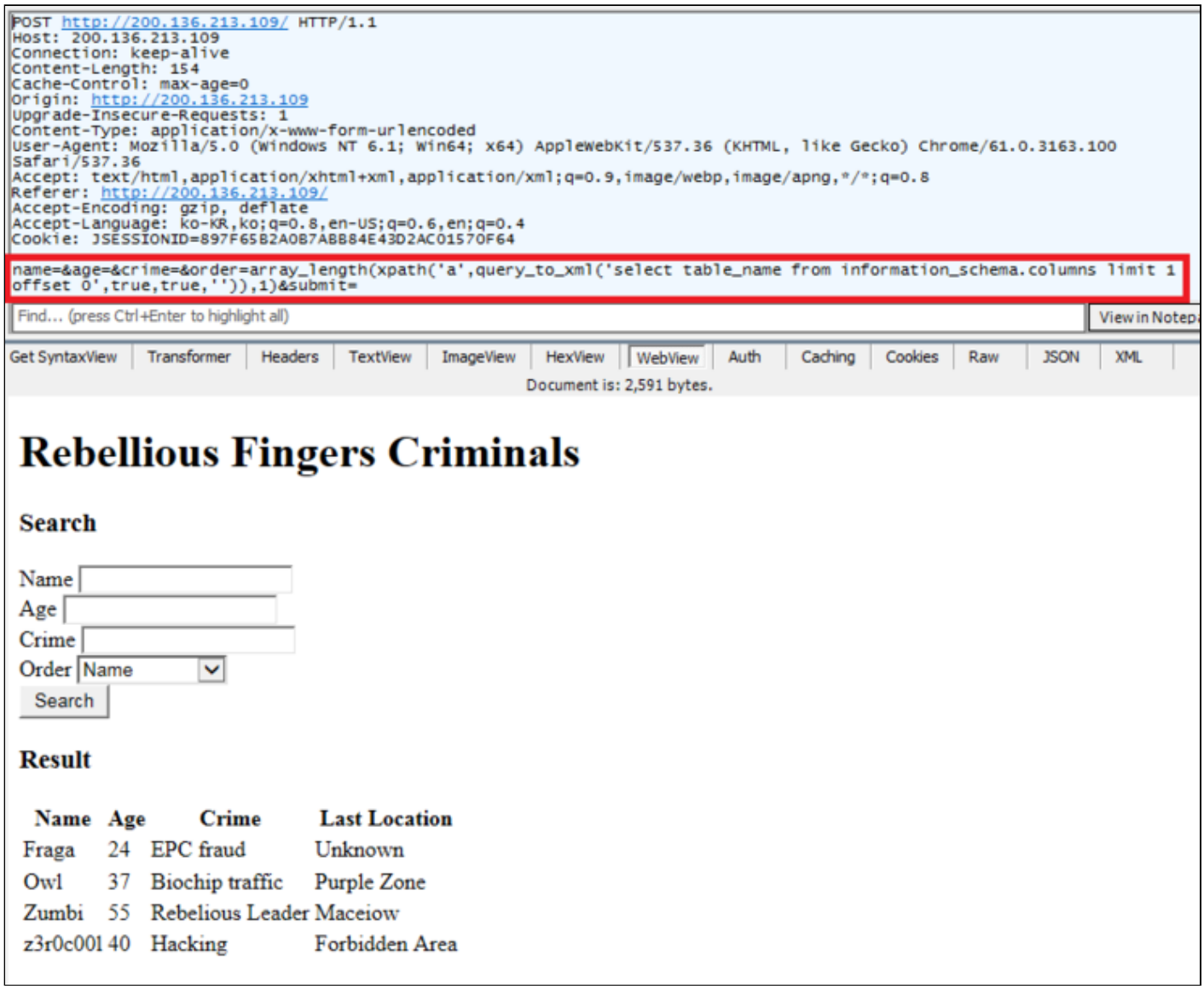
> xpath(*xpath*, *xml* [, *nsarray*])

The function xpath evaluates the XPath expression *xpath* (a text value) against the XML value *xml*. It returns an array of XML values corresponding to the node set produced by the XPath expression. If the XPath expression returns a scalar value rather than a node set, a single-element array is returned.

xpath는 xml 값을 xpath 배열로 출력해주는 함수다.

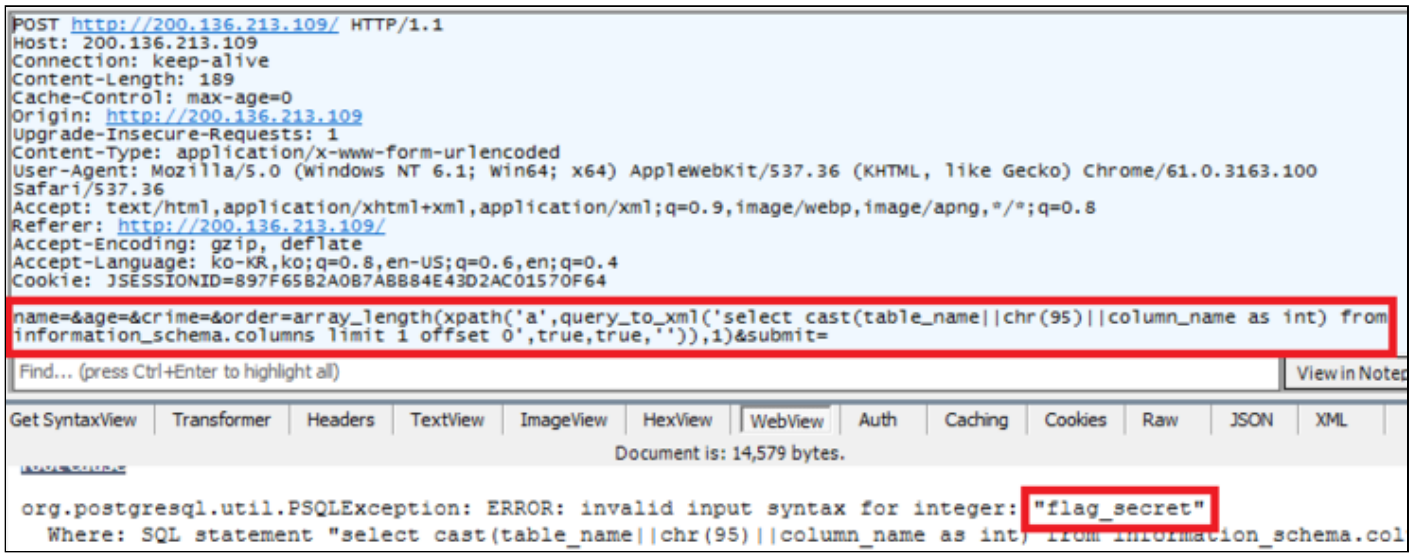
배열 형태를 order by 절에 오게끔 하려면 컬럼명, 혹은 숫자(인덱스)로 출력해주어야 한다. 당연하지만 숫자가 간단하다.

배열(Array) 함수중 결과 값이 숫자인 함수를 이용하여 공격 쿼리를 완성해보자.



에러없이 잘 실행된다!

cast 함수를 이용하여 강제로 에러를 내본다.



테이블명과 컬럼명이 출력된다. 이제 원하는 값을 뽑아내면 되겠다!

- Reference -

https://www.postgresql.org/docs/10/static/functions-xml.html

https://www.postgresql.org/docs/10/static/functions-array.html