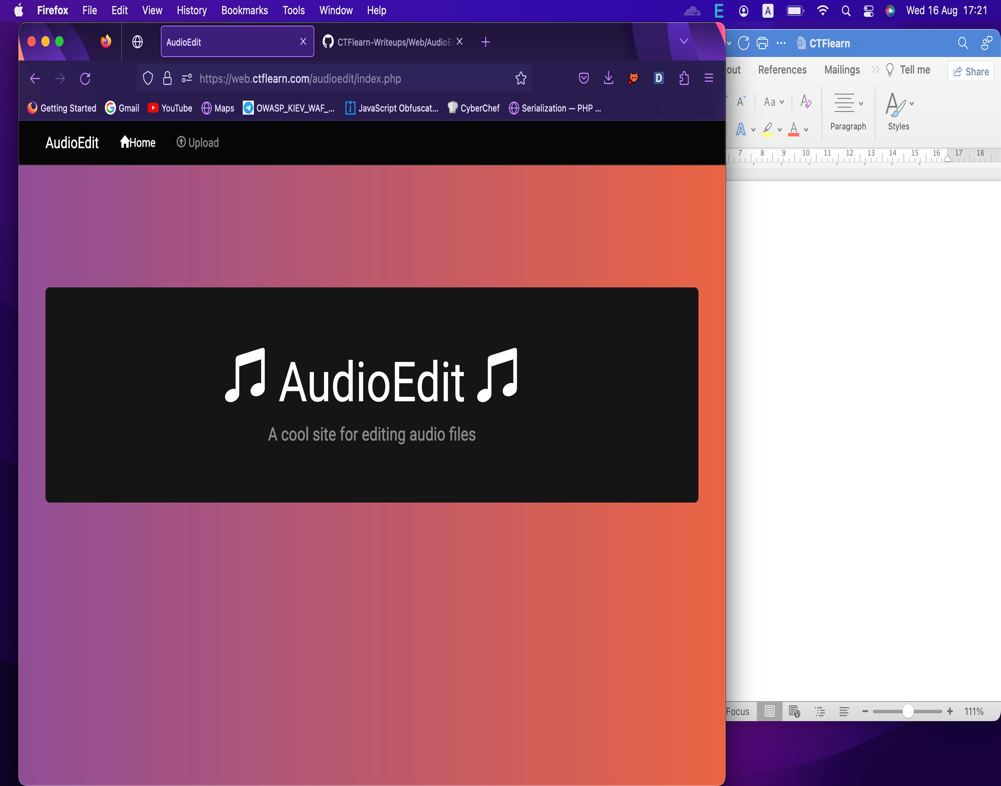
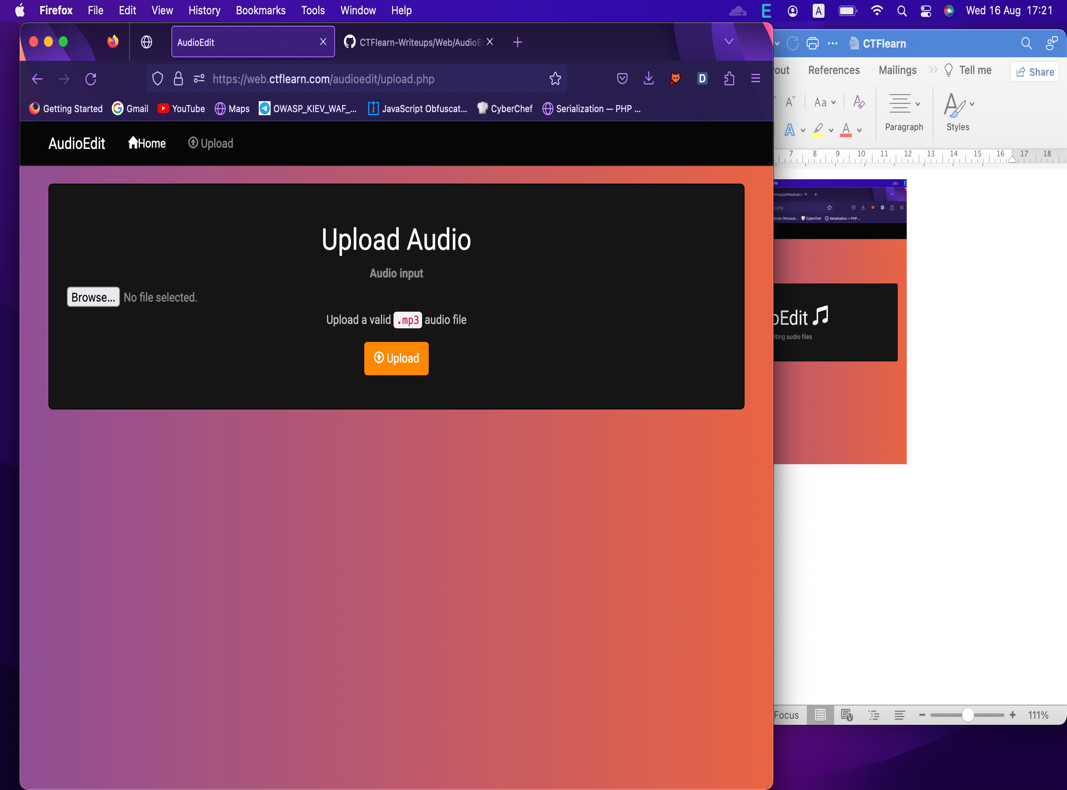
**Bài 1: Audio Edit**

Đây là giao diện của trang web:

Mình thử up file webshell.php nhưng nó báo lỗi : Invalid file format

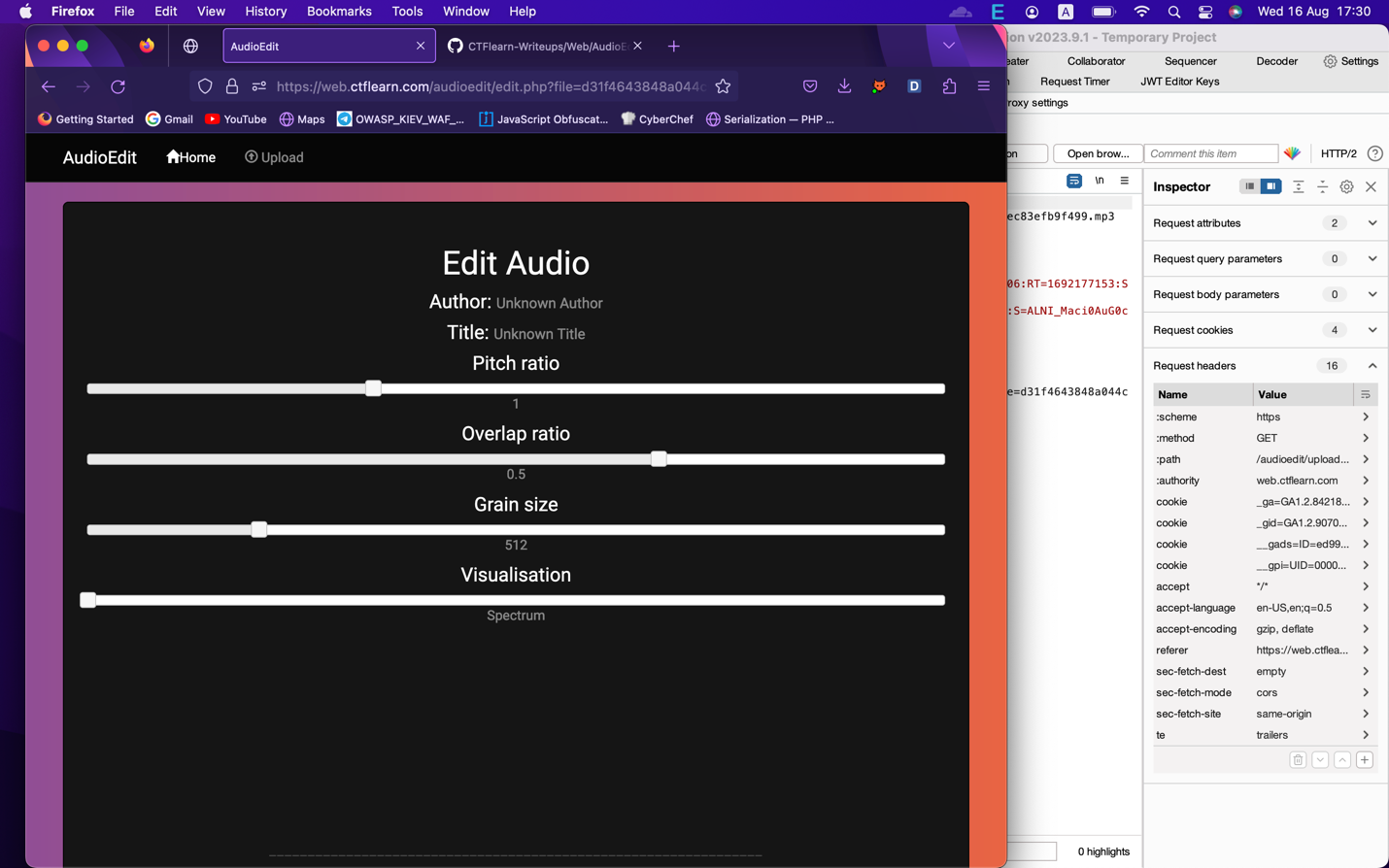
Mình thử điều chỉnh content-type là application/x-httpd-php hay double extension nhưng cũng không được. Nó yêu cầu 1 file .mp3. Nhưng kích thước của file phải nhỏ thôi cỡ 200 mb mới được.

Mình nghĩ đến php polygot file. Phải có 1 file test.mp3 và webshell.php

cat test.mp3 webshell.php> webshell.mp3

Sau đó mình bật intercept lên, phải đổi webshell.mp3 là .php thì mới thực thi code được.

Nhưng quan trọng là ứng dụng không cho mình biết file nằm ở đâu để thực thi. Nó cho chúng ta chỉnh sửa:



Và 1 điều nữa là file\_name bạn đặt là gì đi nữa nó sẽ thay đổi theo mong muốn của ứng dụng.

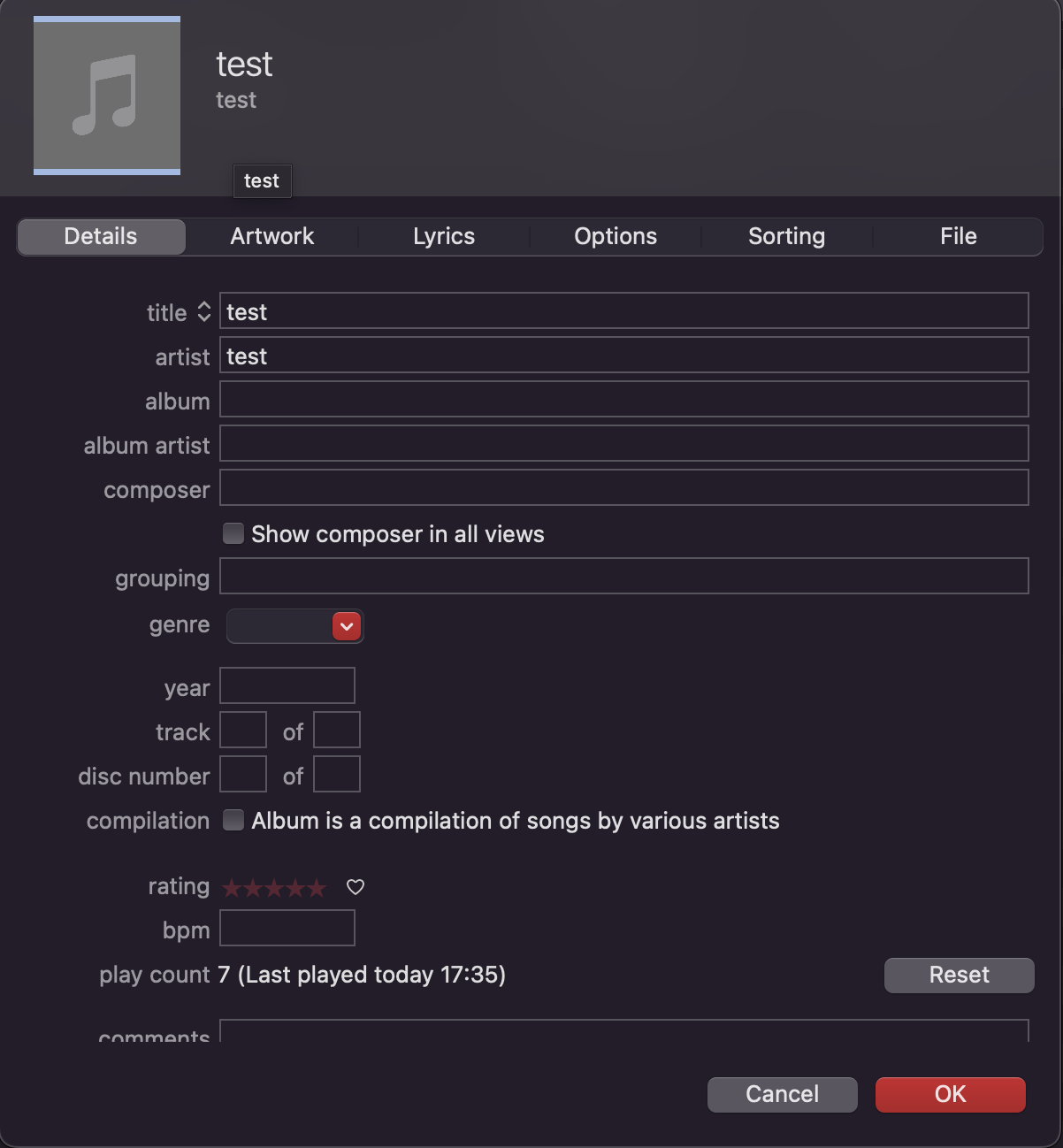
GET /audioedit/edit.php?file=d31f4643848a044c6b27d647fb4fec83efb9f499.mp3

Nên lỗ hổng upload file không thể khai thác được.

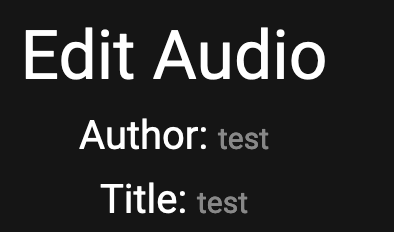
Nhưng bạn thấy Author và Title chứ: Unknown.

Đó là dữ liệu chúng ta có thể kiểm soát được. Làm như thế nào? Mình sẽ chỉnh sửa metadata của 1 file .mp3

Nếu là trên mac, bạn bật ứng dụng music lên, chọn 1 bài hát và get info.



Mình sẽ chỉnh sửa title và artist là test và up lại trên app.



Có vẻ ứng dụng đang dính lỗi sql injection (insert).

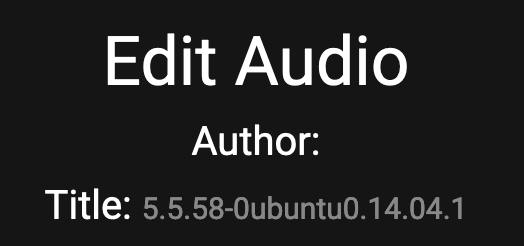
Giả định: insert into table\_name (author,title) values ('test','test')

Mình cho author: ',select@@version)-- ; title: test

🡪 Query: insert … values ('',(select@@version))--', 'test')

Nó báo lỗi : Error inserting into database!

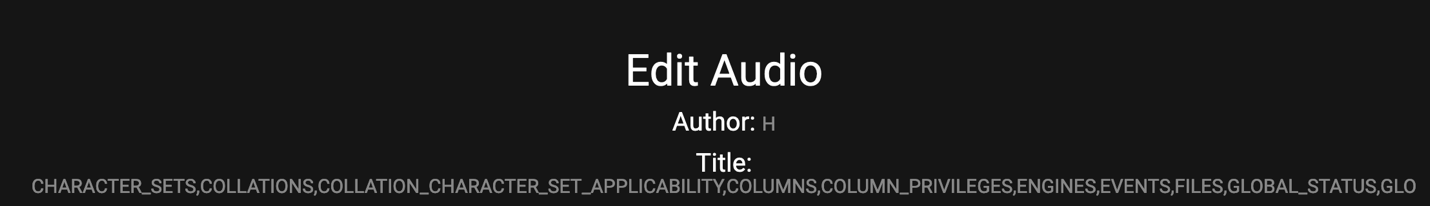
Mình đã sai comment, cơ sở dữ liệu là mysql nên comment là --+ hoặc #.



Vì thủ tục hơi rườm rà nên mình mất rất nhiều thời gian ☹

Mình thử select table\_name from information\_schema.tables nhưng nó báo lỗi câu truy vấn.

Vì author chỉ trả về 1 hàng nên phải group\_concat(table\_name) nhưng dữ liệu trả về cũng không có ích cho việc khai thác.



Mình tìm thử cơ sở dữ liệu:

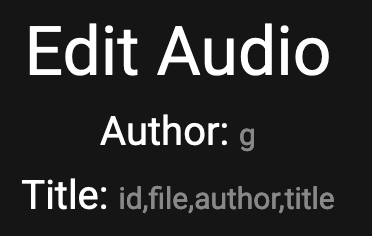
author: ',(select database()))--+ 🡪 audioedit

Tìm bảng trong cơ sở dữ liệu:

author: ',(select table\_name FROM information\_schema.tables WHERE table\_type = 'base table' AND table\_schema='audioedit'))--+ 🡪audioedit

Tìm cột trong bảng audioedit:

author: ',(select group\_concat(column\_name) FROM information\_schema.columns WHERE table\_name='audioedit'))--+



Tìm kiếm cột title:

author: ',(select title FROM audioedit limit 0,1))--+

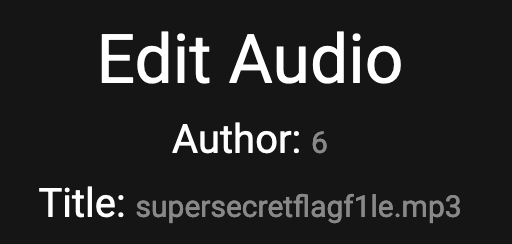
Nhưng thông báo lỗi ☹

Vấn đề ở đây là bạn không thể select từ 1 bảng mà bạn đang insert vào trong bảng đó cùng 1 lúc.

author: ',(select title FROM audioedit as blue limit 0,1))--+ 🡪flag

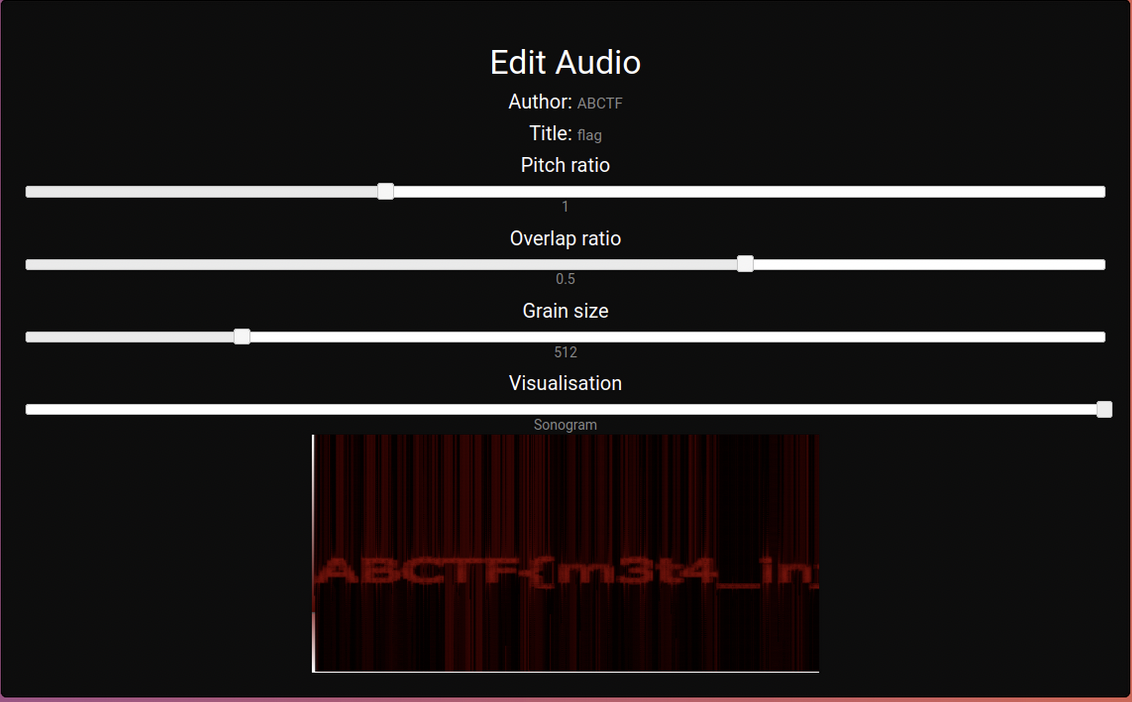
Tìm flag:

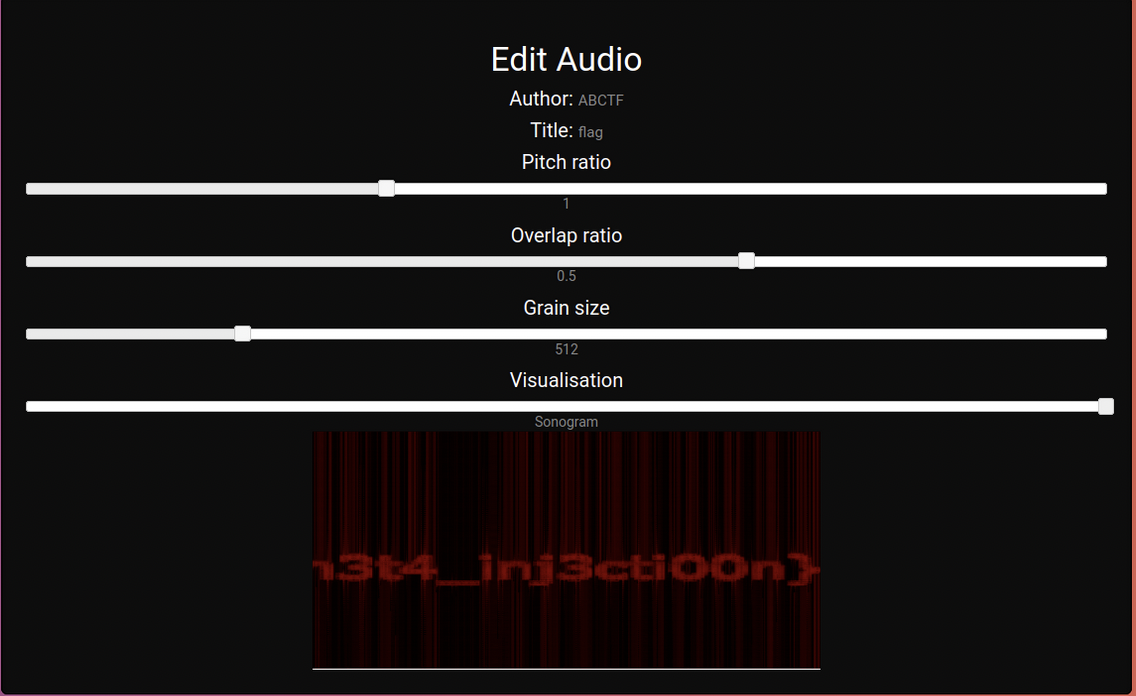
author: ',(select file FROM audioedit as blue limit 0,1))--+



Tiếp theo bạn duyệt đến url đã khai thác:

https://web.ctflearn.com/audioedit/edit.php?file=supersecretflagf1le.mp3





**Flag: CTFlearn{m3t4\_inj3cti00n}**