DEMO VÍ DỤ VỀ:

LỖI BẢO MẬT THAM CHIẾU THIẾU AN TOÀN

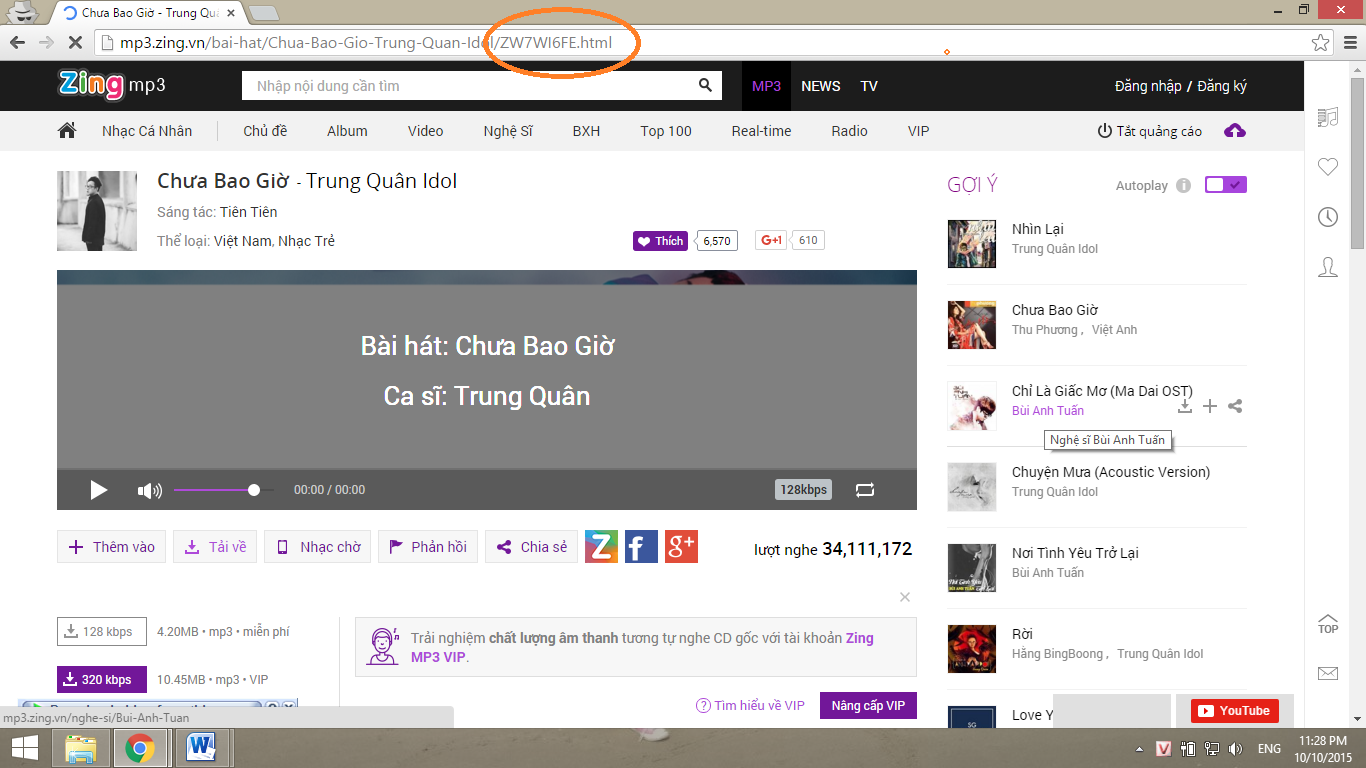
Trương Văn Trang

1. Đặt vấn đề

Lỗi này xuất phát từ việc các trang web thường sử dụng từ khóa của chính dữ liệu trong bảng csdl để tạo ra các link truy cập tới nó. Chúng ta thông qua việc nghiên cứu các đường link hay sự tương tác của các loại quyền người dùng với đối tượng đó ,vì trang web nếu không kiểm soát quyền để truy cập đối tượng thì chúng ta sẽ khai thác nó .

1. Demo việc download nhạc chất lượng cao trên trang web mp3.zing.vn mà không cần tài khoản VIP

Bước 1:   
Khi mở một bài hát ví dụ:



Các bạn sẽ thấy về một mã số (trong ô tròn tô màu)

Tham khảo thêm nhiều bài hát khác tương tự,ta thấy mỗi bài hát đều có một mã khác nhau như thế =>

Có thể mã bài hát này sẽ chính là mã của nó trong cơ sỡ dữ liệu.

Bước 2:

Tham khảo thêm về việc tài khoản VIP của người khác down nhạc thì có link download nhạc :

[*http://mp3.zing.vn/download/vip/song/****mã\_bài\_hát***](http://mp3.zing.vn/download/vip/song/mã_bài_hát)

còn tài khoản thường thì link là :

[*http://mp3.zing.vn/download/song/****mã\_bài\_hát***](http://mp3.zing.vn/download/song/mã_bài_hát)

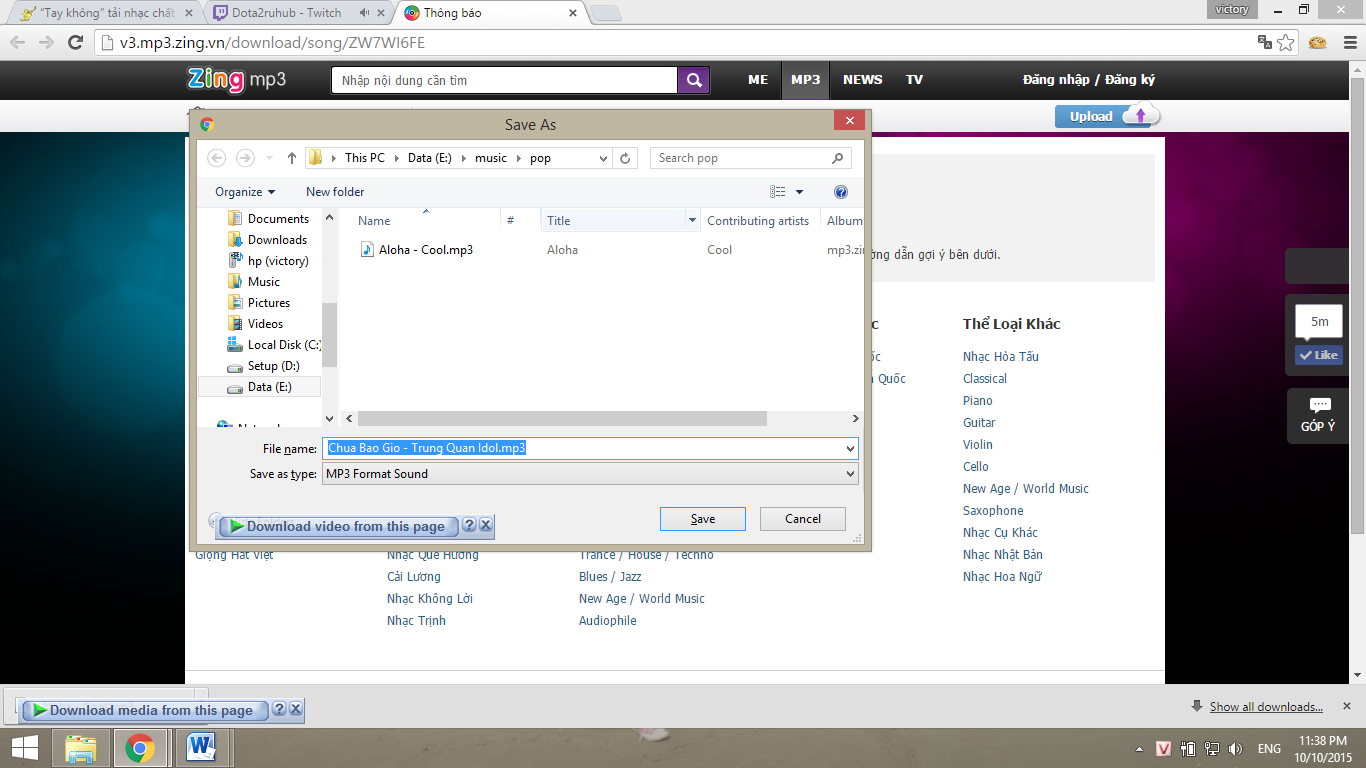
Vậy nên ta có thể thử việc dùng đường link thứ 1 với mã tên bài hát bình thường mà bước 1 ta đã lấy được:

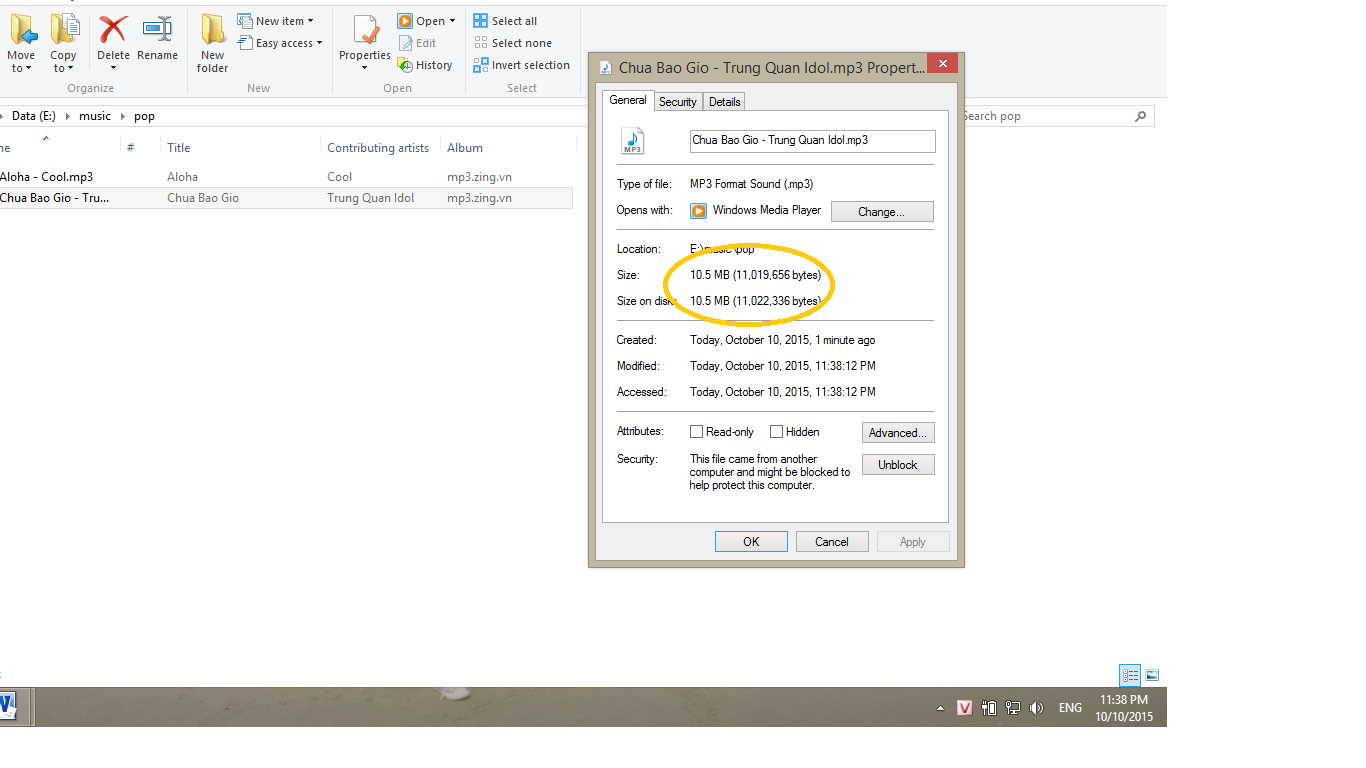
Ví dụ :

[*http://v3.mp3.zing.vn/download/song/ZW7WI6FE*](http://v3.mp3.zing.vn/download/song/ZW7WI6FE)

Và kết quả là ta tới được trang download bài hát chất lượng cao mà không cần tài khoản VIP ( dữ liệu đã được đụng tới mà không cần thông qua việc kiểm soát quyền truy cập gì)

Kết quả:





Ta thấy chất lượng bài hát là ở 320 kbps ( chất lượng cao chỉ có tài khoản vip mới tải về được )