**Mô tả:**

Tôi đã quên cookies có thể được điều chỉnh bên phía máy khách vì vậy bây h tôi quyết định encrypt nó.

Nhìn vào trang web, nó nói chào mừng đến trang tìm kiếm nhưng chức năng tìm kiếm chỉ cho admin.

Cookie như sau:

auth\_name=d0JsYmw3MVczNGRVQlFGQ1FRdFdzbytWR0RHQTFOVk9lMEE0VzN4YTg0Q1c1MWFoQm5WMU01ZHZJbmFYWExSZkVaV2xGZlhoVGN0SEE4MTVlaWNoV211bU9Cc09FbElvOEI0NitZVi9hdFgwZmFMb0d1UTRLUDhvb3YvaVZodGc=

Nó là base64 nhưng khi giải mã thì vẫn lộn xộn. Vậy nên nó bị encrypted. Cùng xem hướng dẫn

Hint 1: https://en.wikipedia.org/wiki/Homomorphic\_encryption

Cookie đã được mã hóa Homomorphic, không thể truy ngược.

Mình thử thay cookie=admin thì máy chủ không thể giải mã cookie.

Bài này không mong có thể decrypt được nhưng các chữ cái CBC được viết hoa trong phần mô tả. Vì vậy nó là cuộc tấn công bit-flip. Điều đó có nghĩa là văn bản đã bị encrypt chứa 1 bit xác định xem nó là admin hay là không, ví dụ admin=0 nhưng ta không biết nó ở vị trí nào vì vậy phải tấn công dồn dập.