**JWT - Public Key**

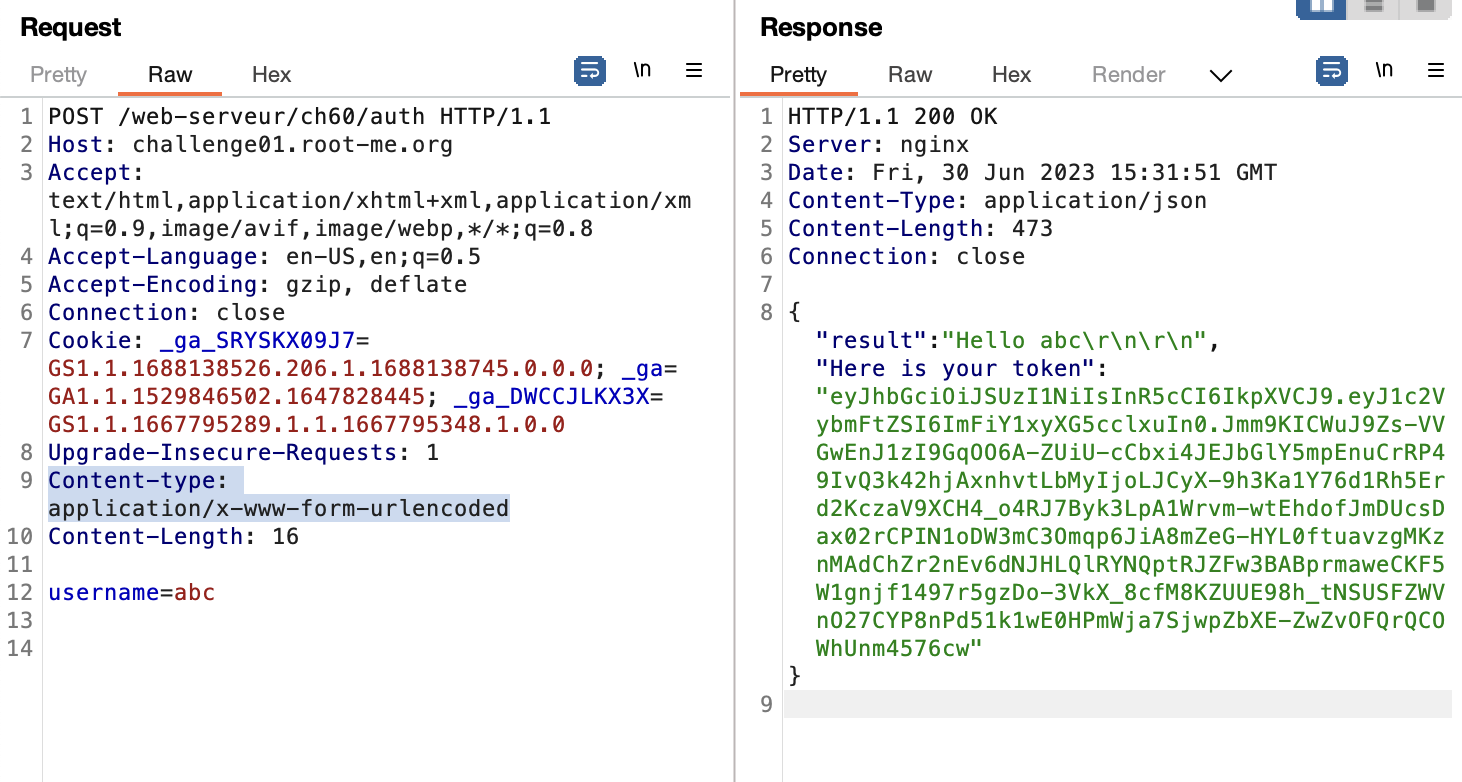
Bài này cho ta 1 giao diện rất đơn giản với 3 endpoints sau:

/key (Get): Bạn sẽ nhận được 1 public key ở định dạng sau:



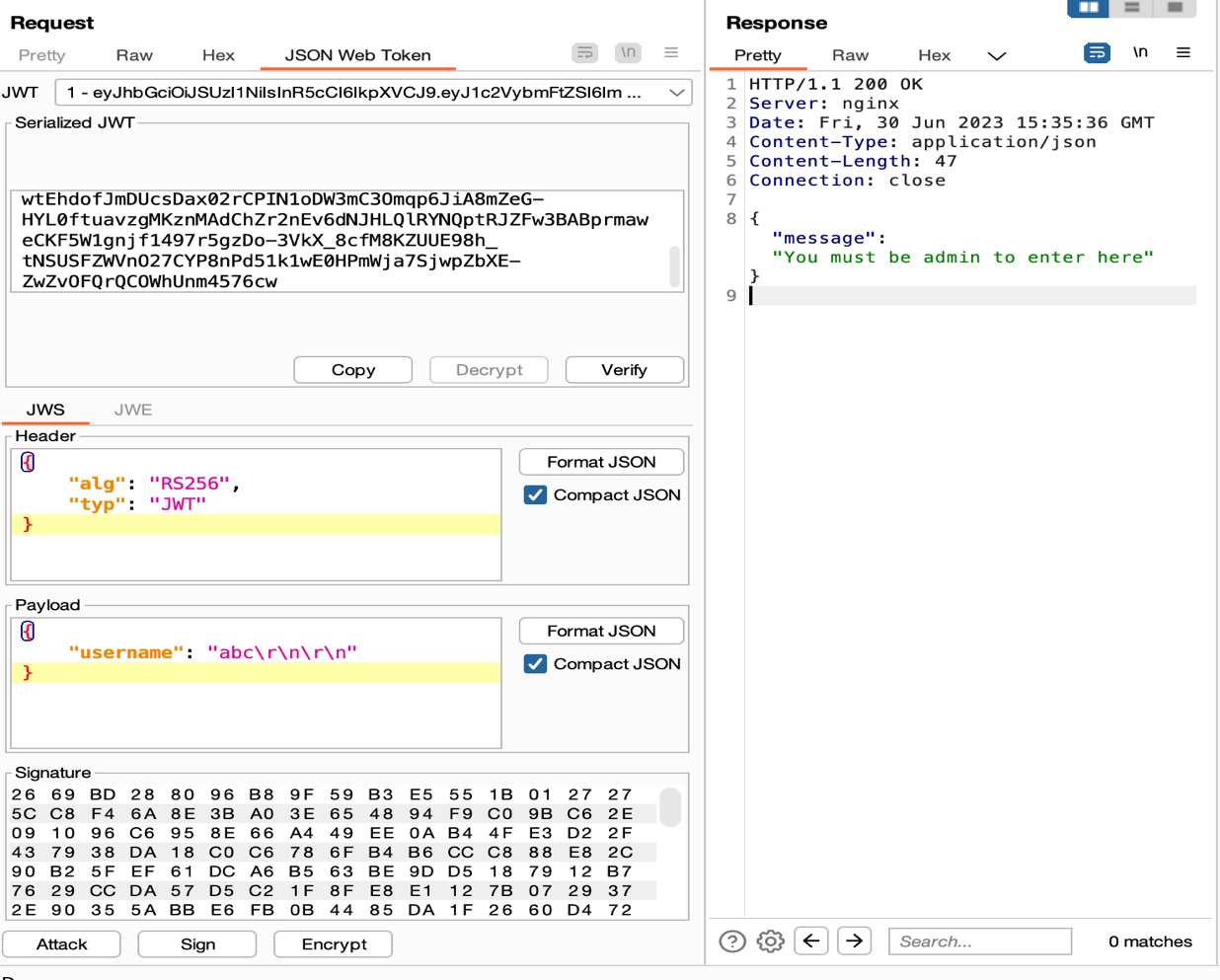
/auth (Post)

Bạn phải thêm trường **Content-type: application/x-www-form-urlencoded**; username=abc thì ứng dụng sẽ cấp cho mày 1 token.



/admin (Post): Bạn sẽ dùng token mới nhận được để vào trang admin. Thêm header **Authorization: Bearer <token>**

Chắc chắn sẽ không truy cập được vì bạn chỉ là abc. Cùng phân tích Json Web Token nào:



Bây giờ mình có public key với thuật toán là RS256 mình chỉ nghĩ đến confusion attack.

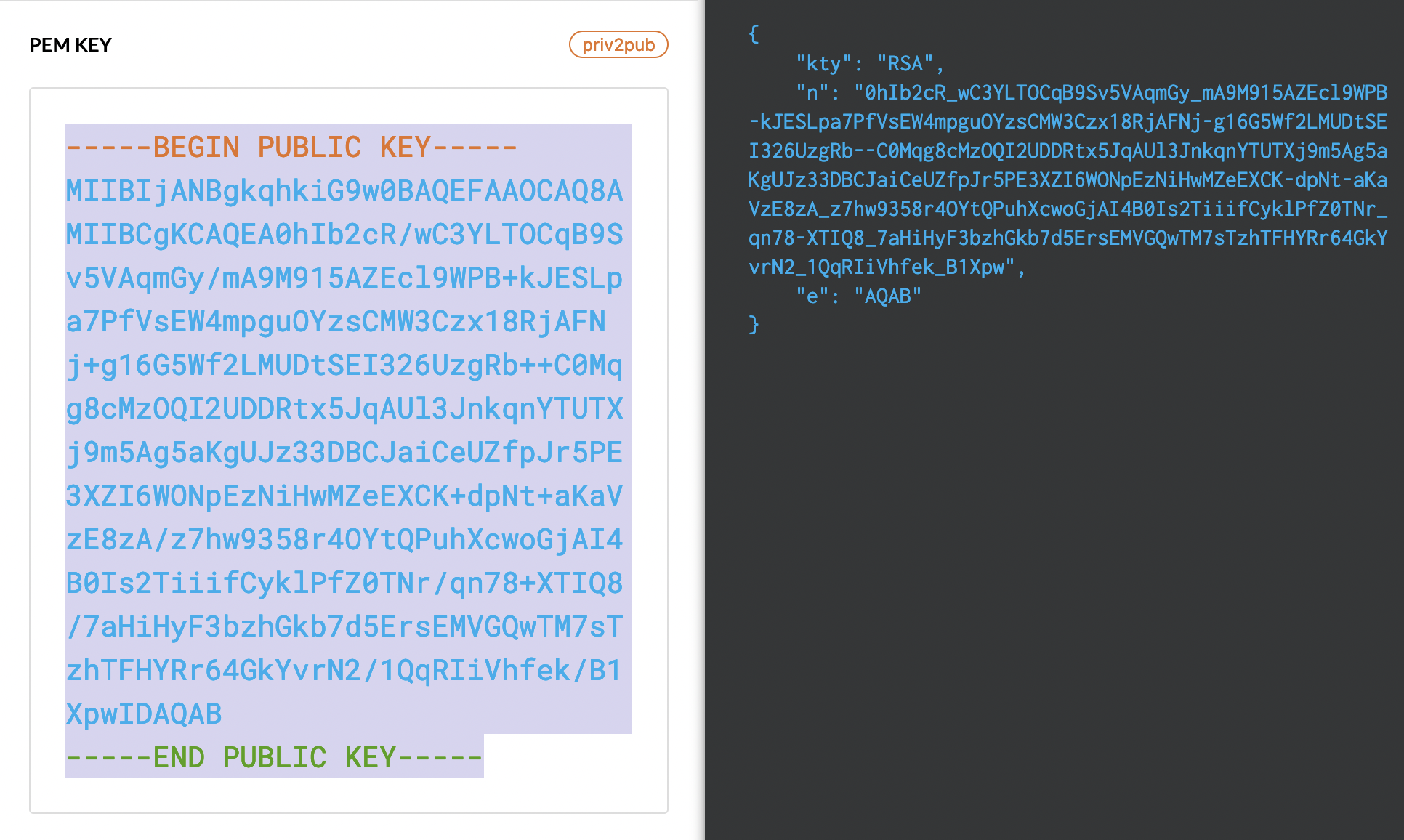
Điều quan trọng là public key phải có định dạng giống với key được lưu trữ trên máy chủ.

Mình thấy key nó đã ở định dạng pem, chỉnh sửa 1 xíu và mã hóa base64 để đặt vào tham số k của 1 symmetric key. Sửa tham số alg là HS256 và payload là admin thì nó báo lỗi.

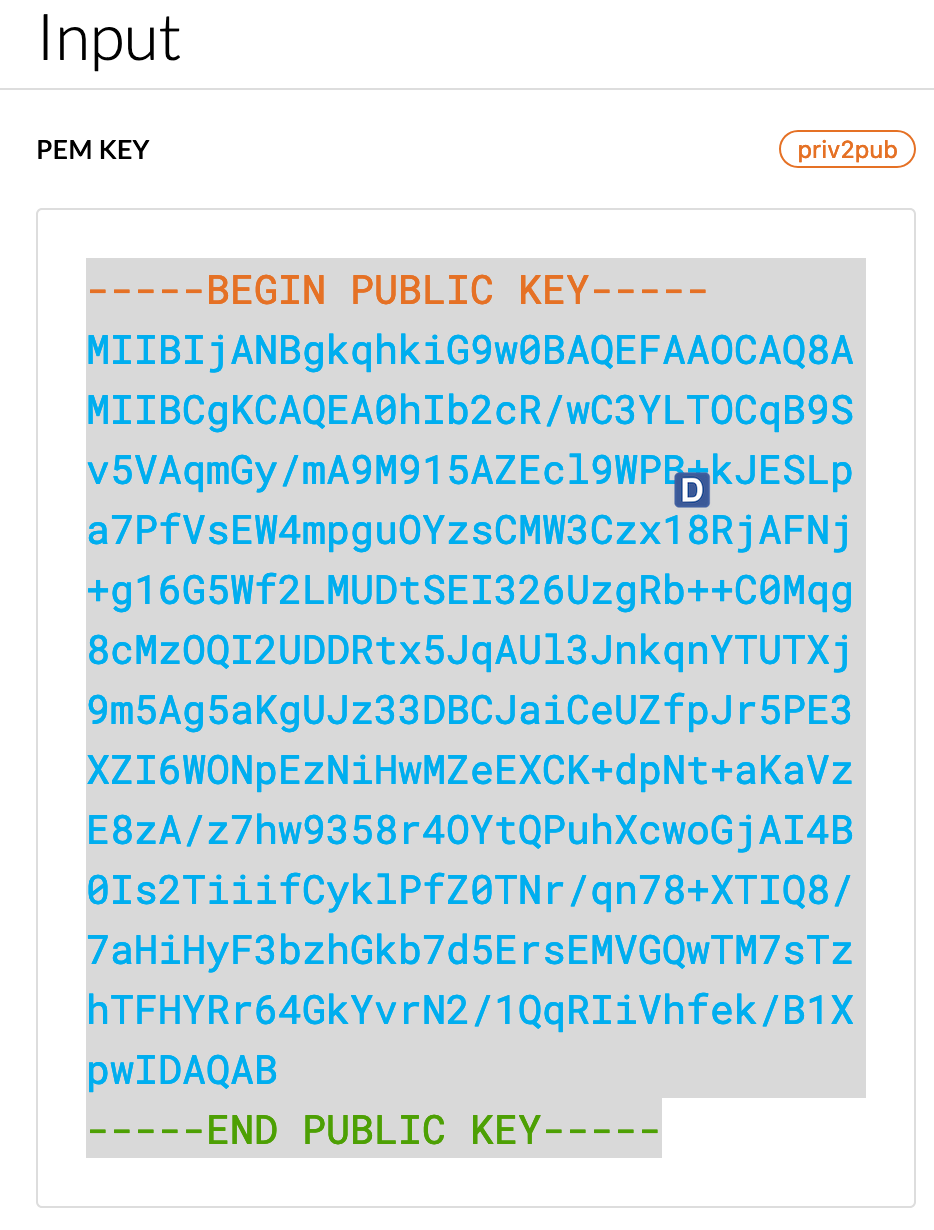
Mình nghĩ vấn đề nằm ở public key. Mình thử nhiều định dạng khác nhau nhưng cũng không được. Bài lab này chỉ có thể giải theo confusion attack nhưng mình đã thật sự hết ý tưởng. JWT khá mơ hồ.

Sau một hồi cố gắng suy nghĩ, mình mới biết định dạng của public key sai.

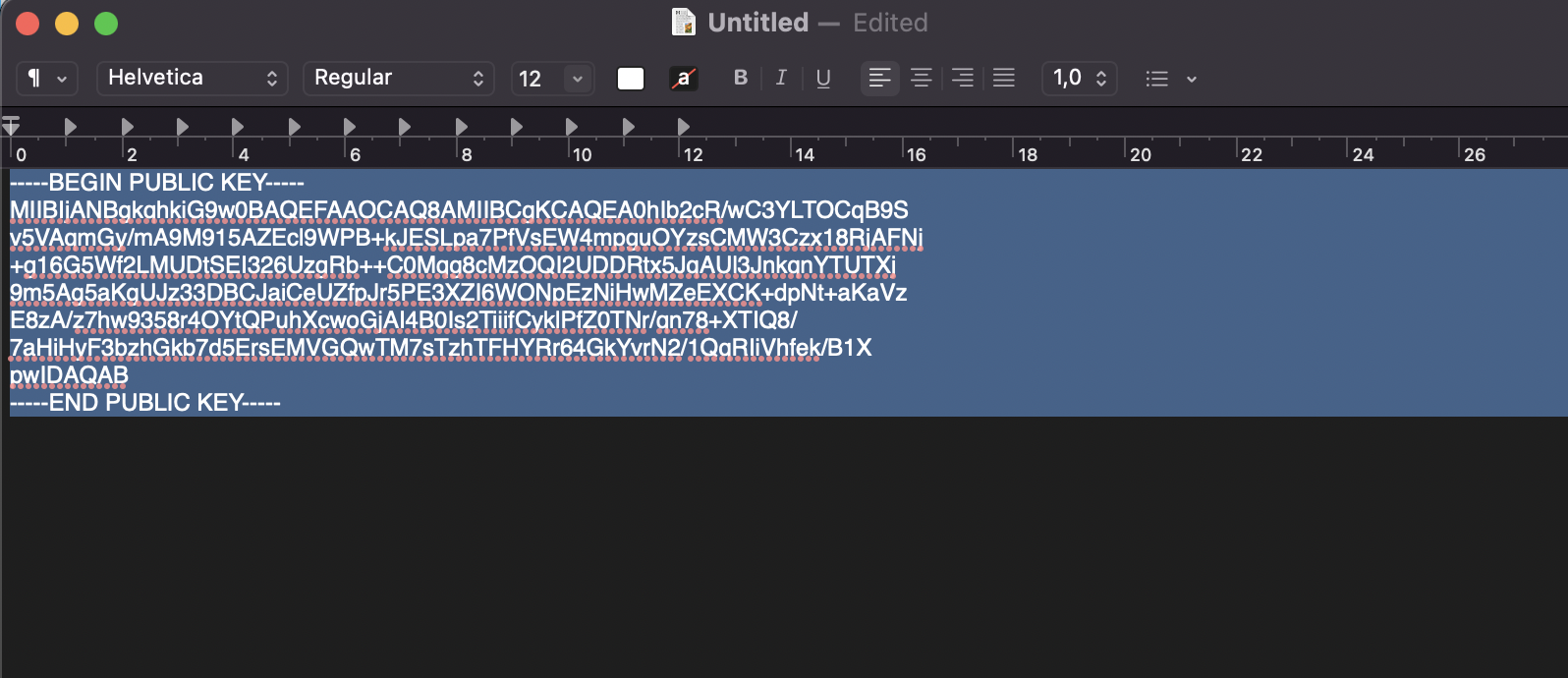
Ban đầu mình xóa dấu ngoặc kép, dấu phẩy và viết liền như sau:



Cách làm đúng là sau dấu phẩy bạn phải xuống dòng:



Khi sao chép ở text edit, bạn phải bôi đen hết dòng chữ như sau:



Mình đã có được đúng định dạng Pem, thực hiện confusion attack như bình thường và nhận flag:

**Flag: HardcodeYourAlgoBro**