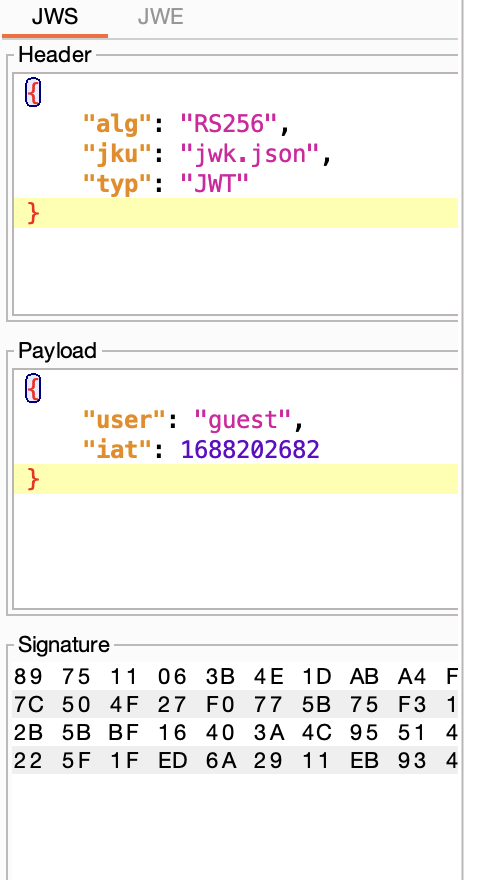
**Bài 1: JWT - Unsecure Key Handling**

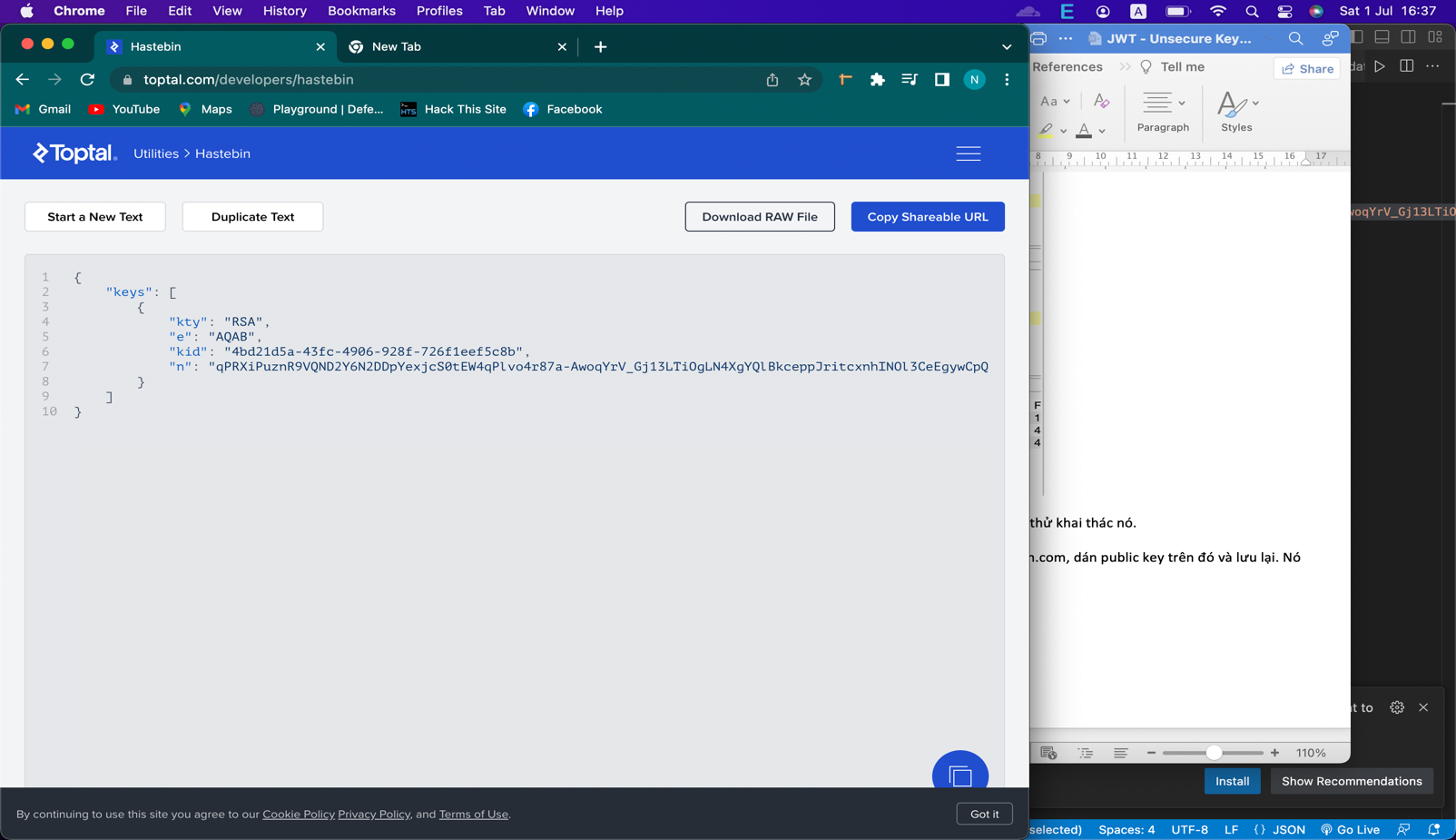
Mục tiêu của bài này là truy cập được trang admin để xem flag.

JWT ban đầu như sau:

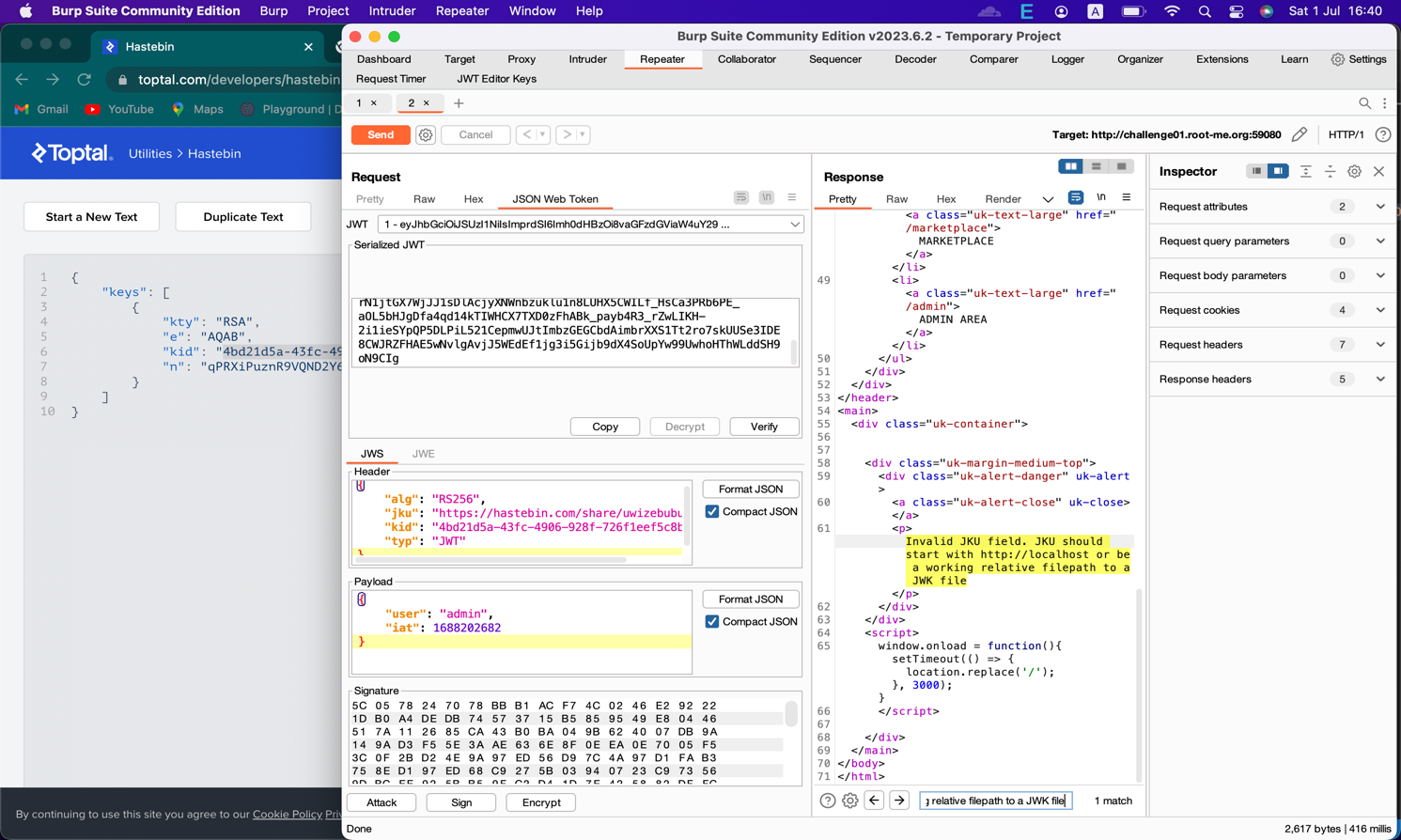


Ứng dụng hỗ trợ tham số jku. Mình sẽ thử khai thác nó.

Mình tạo 1 RSA key. Lên trang Hastebin.com, dán public key trên đó và lưu lại. Nó sẽ cho mình giao diện sau:



Tiếp theo, mình sẽ thay đổi header và payload của JWT như sau:

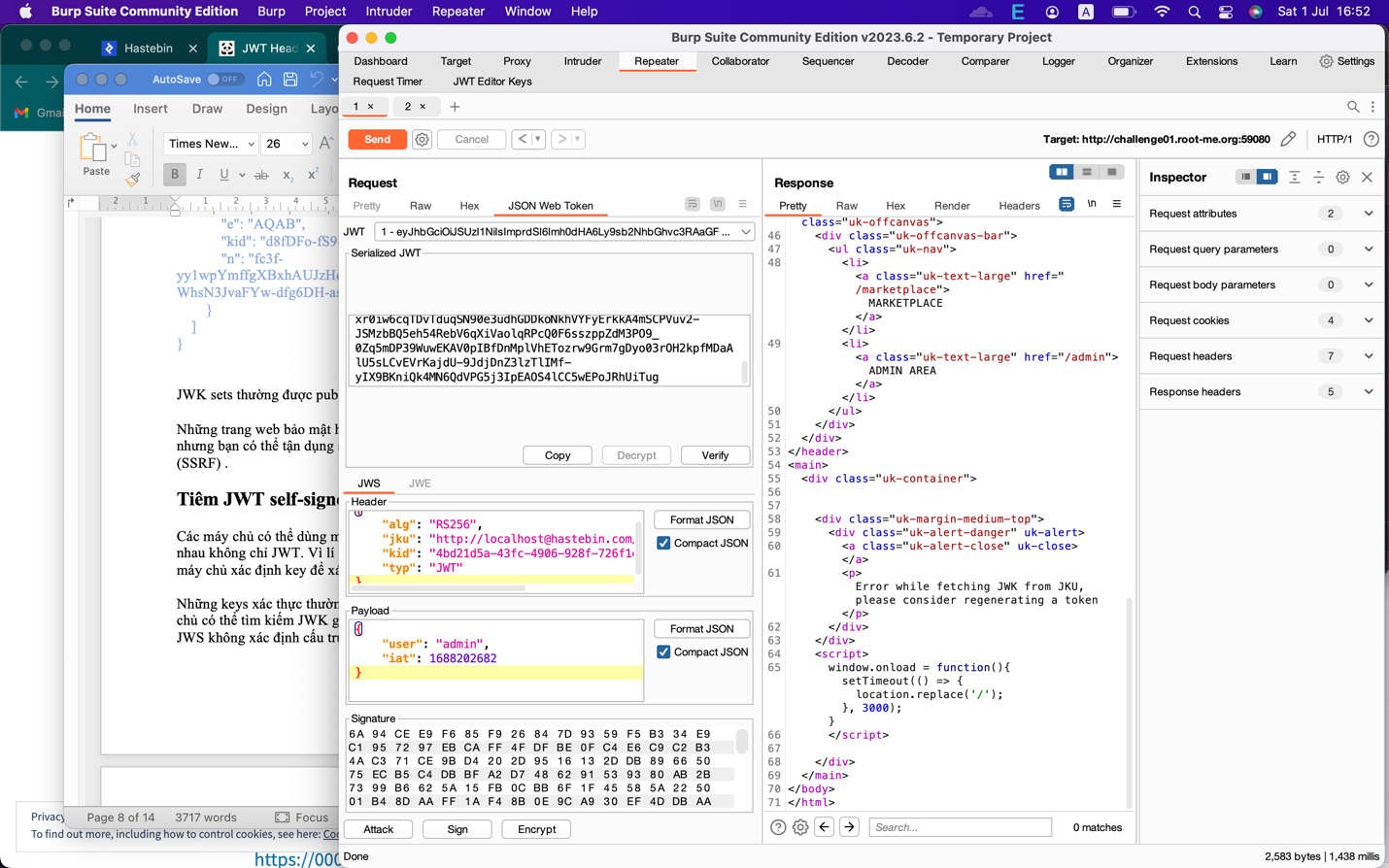


Thông báo lỗi cho thấy url của jku phải bắt đầu từ http://localhost hay 1 tệp jwk.json trong hệ thống.

Như mình đã đề cập, điểm hay của Root me là solution để giải các challenge liên quan đến chủ đề không bao giờ giống hoàn toàn với kĩ thuật khai thác trong các document mà các bạn đọc.

Để bypass filter này:

Cách 1: mình thử tận dụng sự khác biệt trong Url parsing (SSRF):

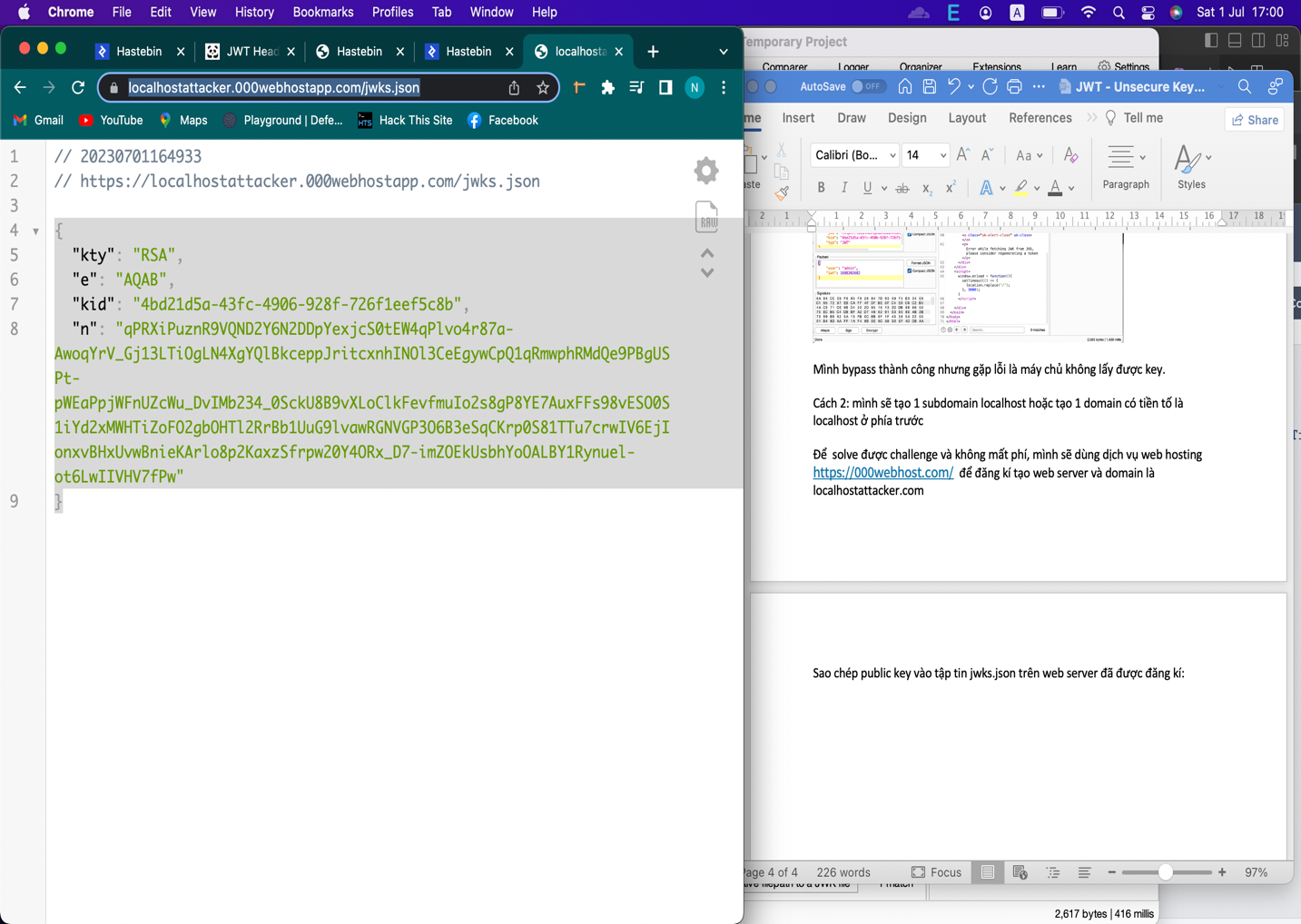
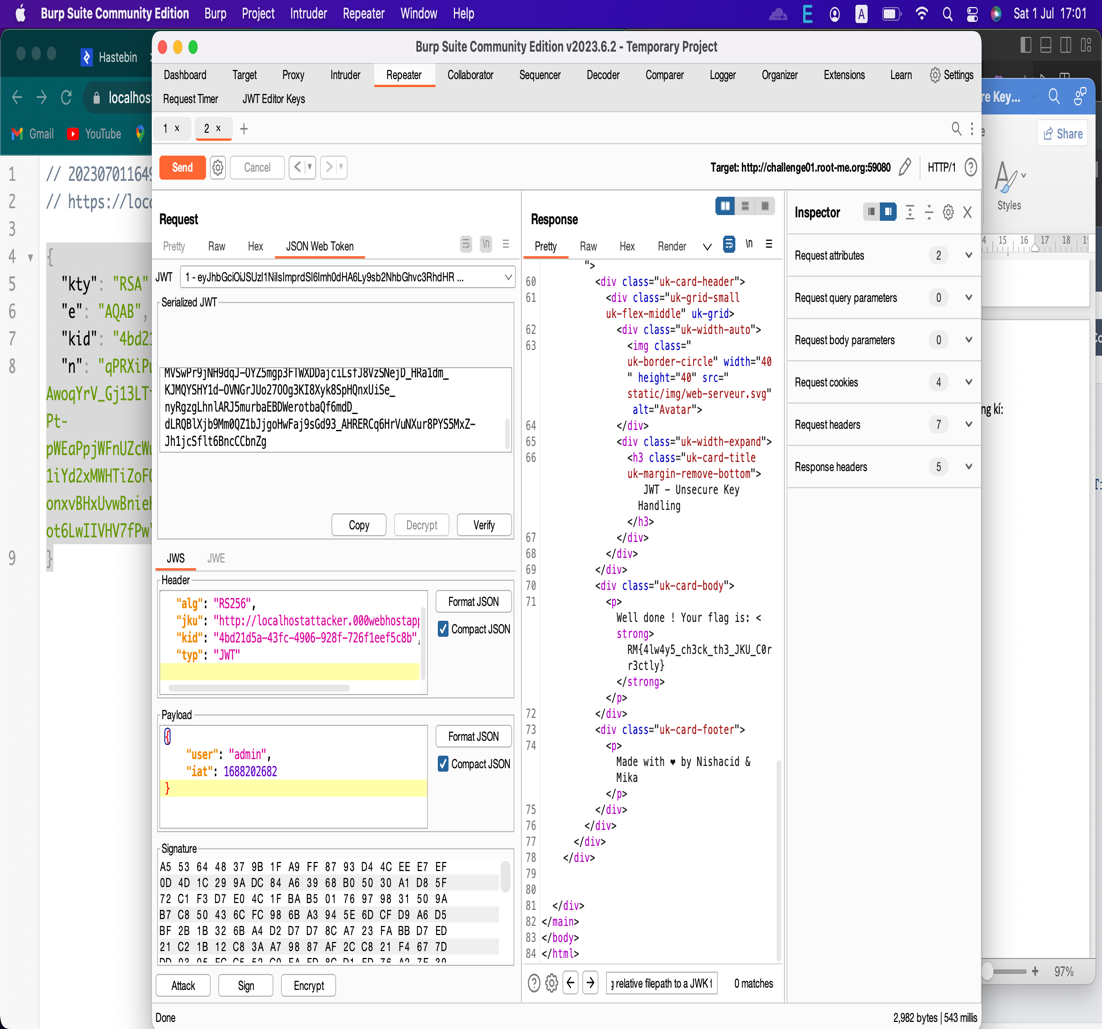


Mình bypass thành công nhưng gặp lỗi là máy chủ không lấy được key.

Cách 2: mình sẽ tạo 1 subdomain localhost hoặc tạo 1 domain có tiền tố là localhost ở phía trước

Để solve được challenge và không mất phí, mình sẽ dùng dịch vụ web hosting <https://000webhost.com/> để đăng kí tạo web server và domain là localhostattacker.com

Sao chép public key vào tập tin jwks.json trên web server đã được đăng kí:

Điều mình không hiểu là tại sao file jwks.json như vậy thì không được:

{

"keys": [

{

"kty": "RSA",

"e": "AQAB",

"kid": "4bd21d5a-43fc-4906-928f-726f1eef5c8b",

"n": "qPRXiPuznR9VQND2Y6N2DDpYexjcS0tEW4qPlvo4r87a-AwoqYrV\_Gj13LTiOgLN4XgYQlBkceppJritcxnhINOl3CeEgywCpQ1qRmwphRMdQe9PBgUSPt-pWEaPpjWFnUZcWu\_DvIMb234\_0SckU8B9vXLoClkFevfmuIo2s8gP8YE7AuxFFs98vESO0S1iYd2xMWHTiZoFO2gbOHTl2RrBb1UuG9lvawRGNVGP3O6B3eSqCKrp0S81TTu7crwIV6EjIonxvBHxUvwBnieKArlo8p2KaxzSfrpw20Y4ORx\_D7-imZOEkUsbhYoOALBY1Rynuel-ot6LwIIVHV7fPw"

}

]

}

Rõ ràng định dạng này mình đã làm trên portswigger.