**JWT - Token bị thu hồi**

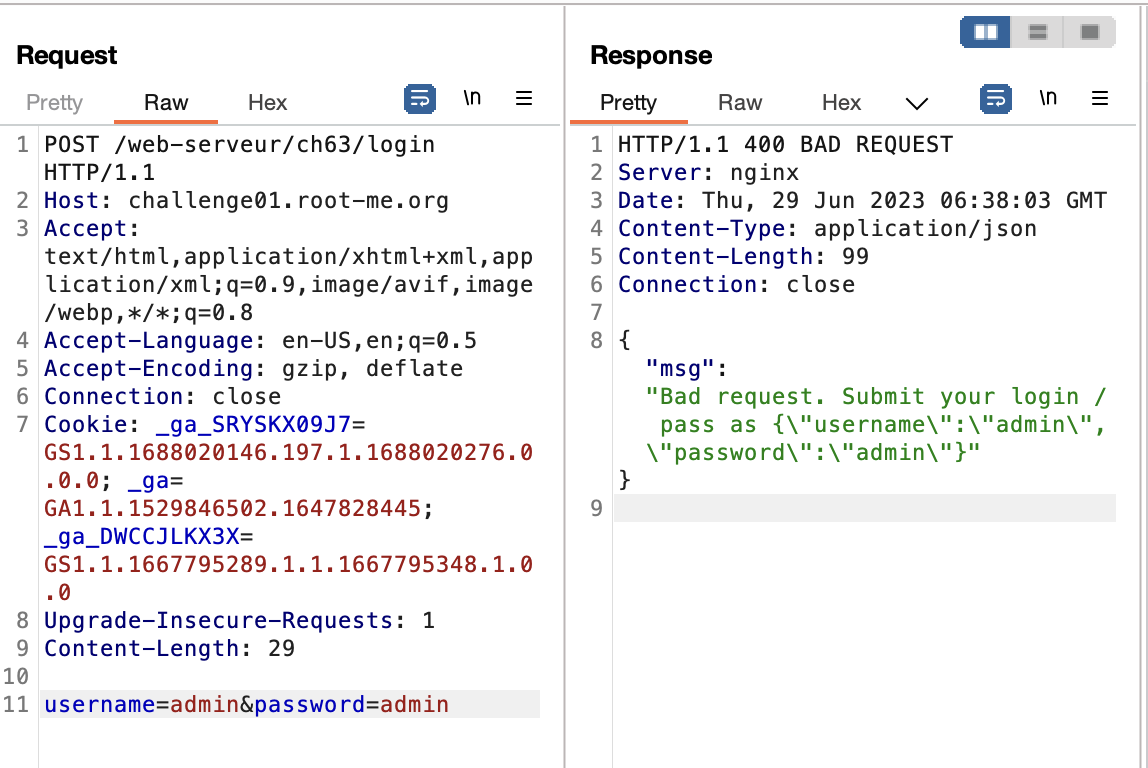
Đây là bài source đầu tiên mà mình làm nên cảm thấy rất khó khăn.



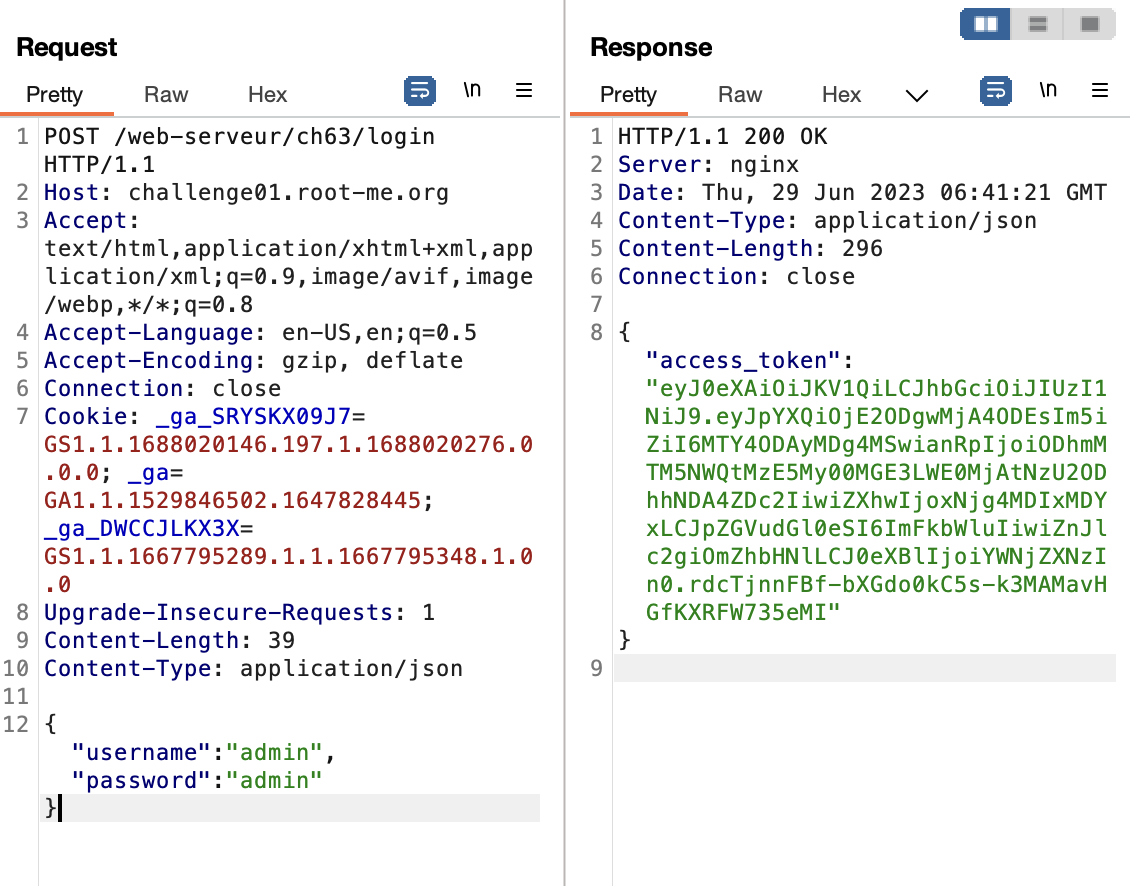
Nó cho ta 2 điểm vào:

* POST : /web-serveur/ch63/login
* GET : /web-serveur/ch63/admin

Mình thử đăng nhập tài khoản admin:



Đọc code, ta thấy nó yêu cầu truyền thông tin đăng nhập bằng json. Mình thêm content-type là application/json. Nó sẽ cấp cho mình một token của admin.



Thay tên người dùng là abc, nó sẽ báo lỗi “Bad username or password”.

Bạn có thể dùng token đó để vào trang /admin bằng cách thêm header Authorization: Bearer <token> nhưng nó sẽ báo “Token is revoked” vì token này ở trong blacklist của ứng dụng.

Giải thích một chút về revoke?

Bản chất của JWT là stateless. Chúng ta không lưu JWT trên máy chủ mà lưu ở trên client, tức là server không biết trạng thái của người dùng nào cả. Khuyết điểm của nó là chúng ta không thể thu hồi access token được.

Ví dụ 1: Ở server, chúng ta muốn chủ động đăng xuất một người dùng thì không được, vì không có cách nào xóa access token ở thiết bị client được.

Ví dụ 2: Client bị hack dẫn đến làm lộ access token, hacker lấy được access token và có thể truy cập vào tài nguyên được bảo vệ. Dù cho server biết điều đấy nhưng không thể từ chối access token bị hack đó được, vì chúng ta chỉ verify access token có đúng hay không chứ không có cơ chế kiểm tra access token có nằm trong danh sách blacklist hay không.

Trong lab này, máy chủ giả sử token của admin bị attacker lấy được nên bị thu hồi.

**Để lấy được flag, phải tạo 1 token không ở trong blacklist.**

Trong hàm main, thực thi hàm delete\_expired\_tokens: duyệt các token trong blacklist, nó sẽ decode bằng secret key và alg là HS256. Trường hợp ngoại lệ là token đã expired, nó sẽ bị xóa khỏi blacklist.

Ban đầu, mình thấy code sau:

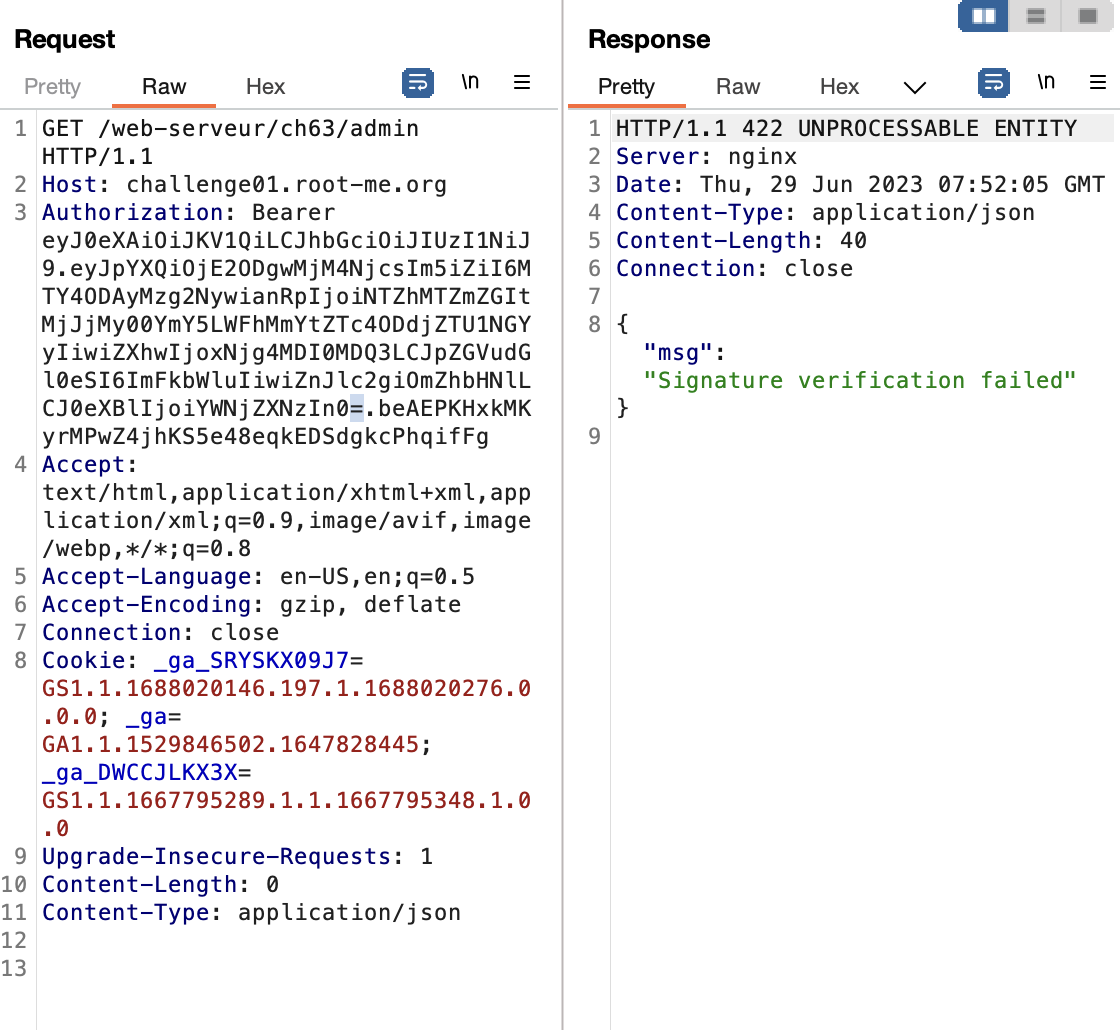
app.config['JWT\_SECRET\_KEY'] = SECRET

Tưởng nó để lộ key nên mình tạo 1 HS256 key, nhúng SECRET đã được mã hóa base64 vào tham số k và sign token mình sẽ có 1 token khác nên không ở trong blacklist. Nhưng kết quả là signature xác thực không thành công.

Tiếp theo mình set tham số alg là none và no signature thì nó báo lỗi là "The specified alg value is not allowed".

Mình thử thêm vào giá trị trong header hoặc payload một giá trị nào đó không ảnh hưởng khi xác thực nhưng tất nhiên khi thêm thành công vì signature sẽ không đúng rồi, đó là nguyên tắc mà… Nhưng …

Tại sao mình lại cố inject vào header của JWT để nó vẫn có nghĩa và không nằm trong blacklist? Mình còn cách khác mà đúng không? mình nghĩ đến việc add kí tự đặc biệt/null byte vào giá trị JWT để khác với JWT đã bị thêm vào blacklist nhưng về nghĩa thì vẫn có thể verification thành công. Và mình nghĩ thực hiện add “=” vào cuối header và payload trong JWT. Vì khi decode base64, kí tự “=” sẽ được bỏ qua và về context trả về sẽ giống nhau. Và mình thử thực hiện với suy nghĩ trên thì không được.



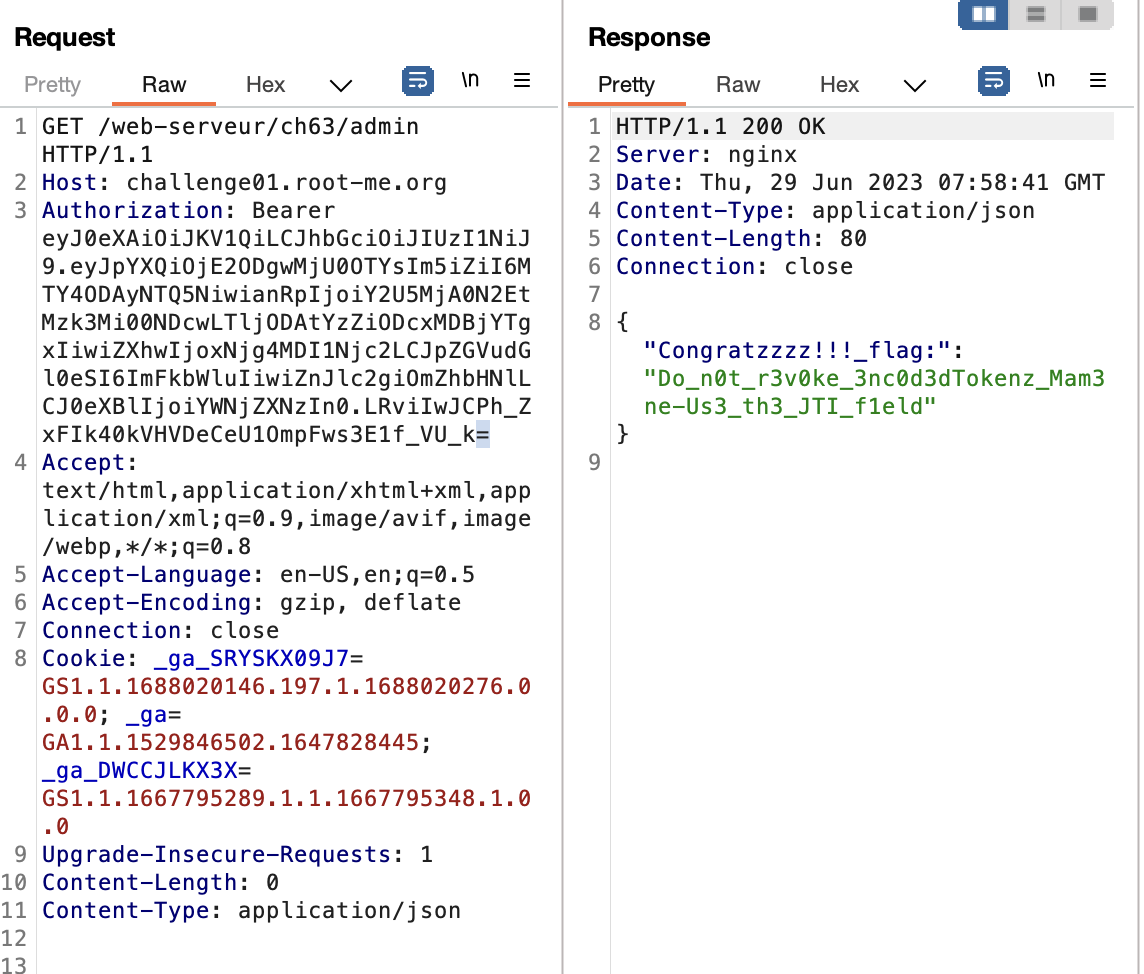
Đơn giản là vì khi thay đổi giá trị trên thì signature có được sẽ không đúng nữa. Remind lại cách JWT được tạo ra:

key= 'secretkey'

unsignedToken=encodeBase64(header) + '.' + encodeBase64(payload)

signature=encodeBase64(HMAC-SHA256(key,unsignedToken)

Và rồi mình thực hiện thay đổi tại giá trị signature với phương pháp đó thì …



Nhìn chung, lỗ hổng này xảy ra khi Developer thay vì thực hiện revoke JTI (JWT id), họ sẽ thực hiện blacklist full JWT hoặc hash của JWT trên. Phương pháp Dev nên triển khai là khi user logout khỏi ứng dụng, ứng dụng nên lưu trữ tham số jti (hoặc trường dữ liệu tương tự trong JWT) vào blacklist, quá trình xác thực gồm hai bước, thực hiện verify JWT đòng thời sau đó kiểm tra tham số jti có nằm trong blacklist hay không. Lợi dụng việc lưu trữ full jwt, như có thể thực hiện ở challenge trên, kẻ xấu có thể add vào một vài kí tự không có ý nghĩa để bypass blacklist đã được thêm vào.

Ở đây, ngoài trừ trường hợp thêm “=” vào cuối signature. Chúng ta cũng có thể sử dụng 2 phương pháp sau:

* Generate JWT cho đến khi giá trị access Token có dấu “\_”, thực hiện thay đổi “\_” thành “/” (khi thực hiện decode base64, hai kí tự này là tương đương nhau)
* Với các kí tự non-alphabet, việc Decode base64 sẽ ignore các kí tự trên. (Phương pháp này từ một tác giả trên Medium)