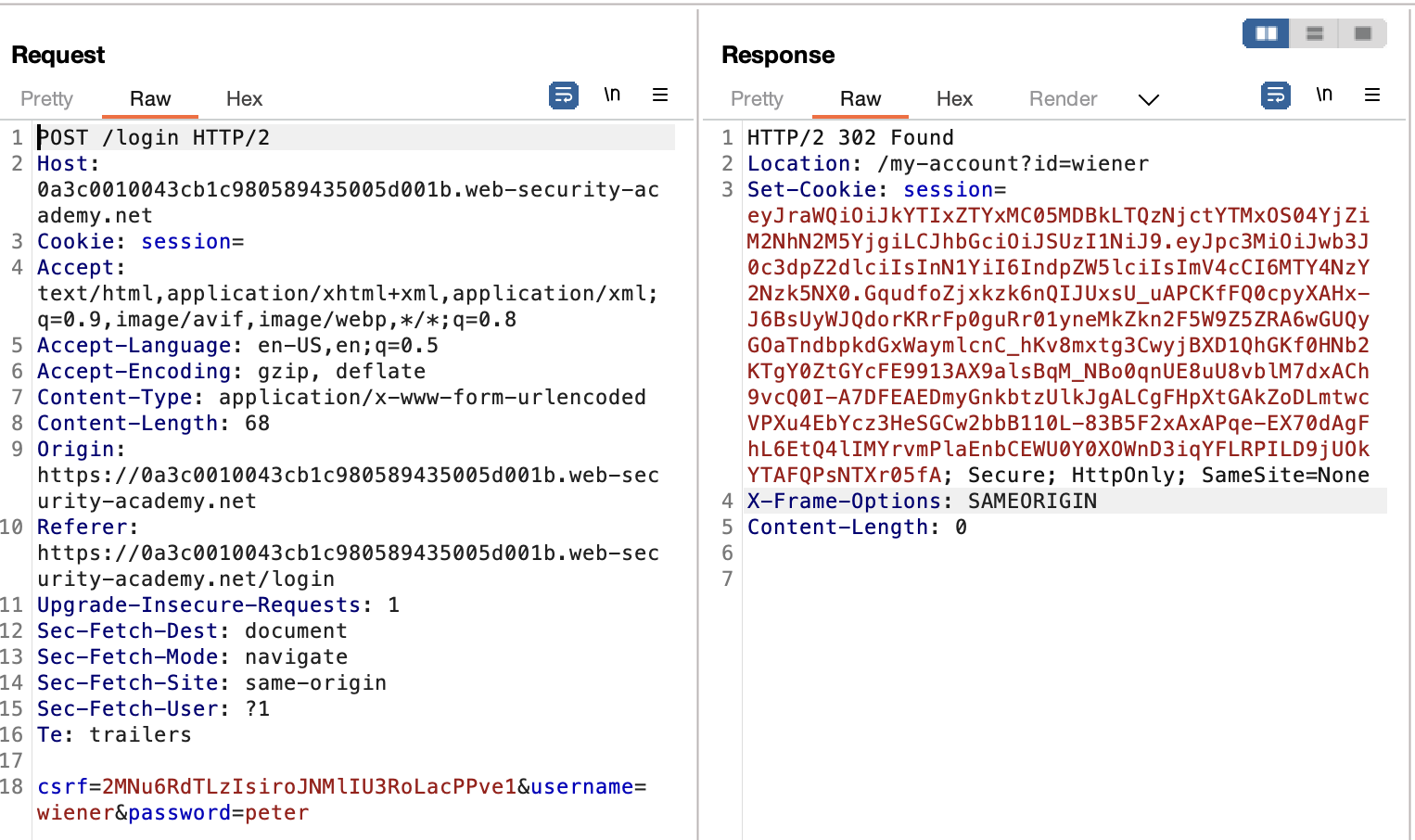
# Bài 1: JWT authentication bypass via unverified signature

Mục tiêu: truy cập trang quản trị admin và xóa người dùng tên carlos

Bài này dùng JWT để xử lí phiên. Do thực thi bị lỗi nên không xác thực bất cứ signature nào nó nhận được.

Đăng nhập vào tài khoản wiener:peter. Máy chủ cấp cho mình 1 session sau:



Vì nó không xác thực signature nên mình có thể lấy signature của wiener để giả là admin.

Vào tab Json Web Token, chỉnh sửa payload thành administrator.

Để xóa carlos mình phải sửa phương thức GET /my-account?id=wiener thành /admin/delete?username=carlos

# Bài 2: JWT authentication bypass via flawed signature verification

Máy chủ bị cấu hình sai nên chấp nhận JWT unsign.Nói cách khác, JWT không cần signature.

* Đăng nhập vào tài khoản wiener:peter
* Sửa url để xóa carlos
* Vào tab Json Web Token, trong header của JWT có tham số alg qui định thuật toán để xác thực bạn đặt là none. Chỉnh sửa payload là admin.
* Chọn Attack-> none signing algorithm

# Bài 3: JWT authentication bypass via weak signing key

Bài này rất hay. Nó dùng 1 secret key yếu để sign và xác thực token.

Tấn công dồn dập để tìm secret key bằng hashcat 🡪 secret1

Biết được secret key và thuật toán bạn có thể tạo signature theo ý muốn

Tạo 1 new symmetric key thay tham số k là secret1 đã được mã hóa base64.

Chỉnh sửa payload theo ý muốn 🡪 chọn sign JWT với key mình đã tạo 🡪 Send

# Bài 4: JWT authentication bypass via jwk header injection

Máy chủ hỗ trợ tham số jwk trong header. Nó thường dùng để nhúng public key để xác thực trong token. Tuy nhiên, máy chủ không thể kiểm tra key đó có đến từ 1 nguồn đáng tin cậy không.

Nguồn không đáng tin cậy ở đây là private key.

Mình sẽ tạo 1 private key là RSA, chỉnh sửa payload.

Chọn Attack 🡪 Embedded JWK (Nó sẽ tự thêm tham số jwk và sign luôn cho mình)

Bạn có thể làm thủ công bằng việc thêm tham số jwk. Tuy nhiên, bạn cũng cần chỉnh sửa tham số kid của JWT để phù hợp với kid của key đã nhúng. Tấn công bằng extension sẽ giúp bạn làm điều này.

# Bài 5: JWT authentication bypass via jku header injection

Máy chủ hỗ trợ tham số jku trong header. Nhưng nó không thể kiểm tra Url đó có thuộc tên miền đáng tin cậy không trước khi tìm key để xác thực token.

Bài này rất dễ, bạn có 1 máy chủ exploit để kiểm soát, tạo 1 file chứa public key.

Chỉnh sửa payload, thêm tham số jku là url đến file đó. Máy chủ sẽ dùng key này để xác thực token.

Chỉnh sửa kid header 🡪 Sign JWT bằng mã RSA.

# Bài 6: JWT authentication bypass via kid header path traversal

Để xác thực signature, máy chủ dùng tham số kid để chọn key tương ứng trong hệ thống tệp.

Bạn trỏ kid đến /dev/null. Vì nó là 1 tệp rỗng, đọc nó sẽ trả về giá trị rỗng. Do đó sign 1 token với chuỗi rỗng sẽ dẫn đến 1 signature hợp lệ.

Tạo 1 symmetric key, thay tham số k là 1 giá trị rỗng đã được mã hóa base64 (AA==)

Chỉnh sửa payload 🡪 sign JWT 🡪 send request