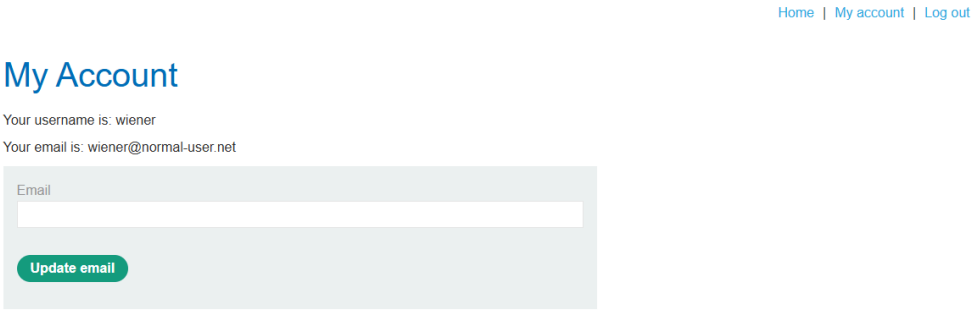
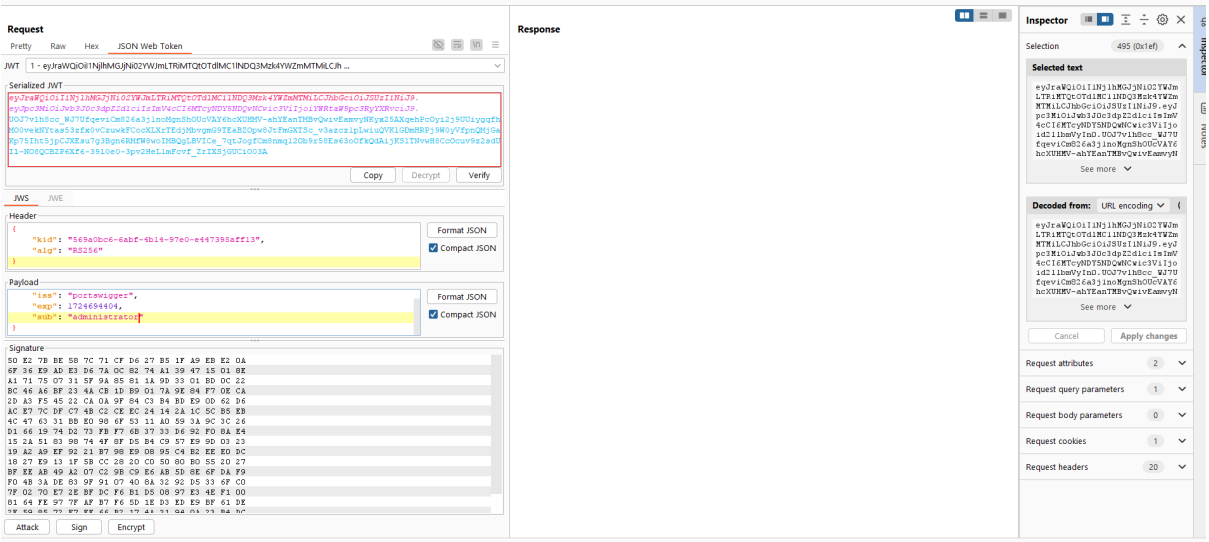
1. **Lab: JWT authentication bypass via unverified signature**

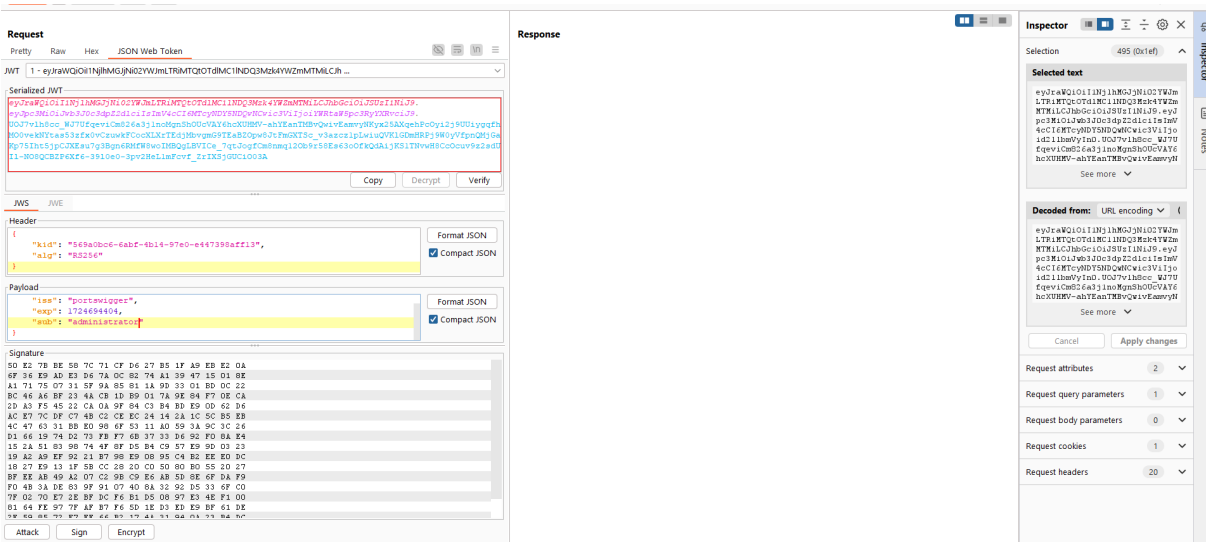
Bước 1: Đăng nhập tài khoản wiener: peter

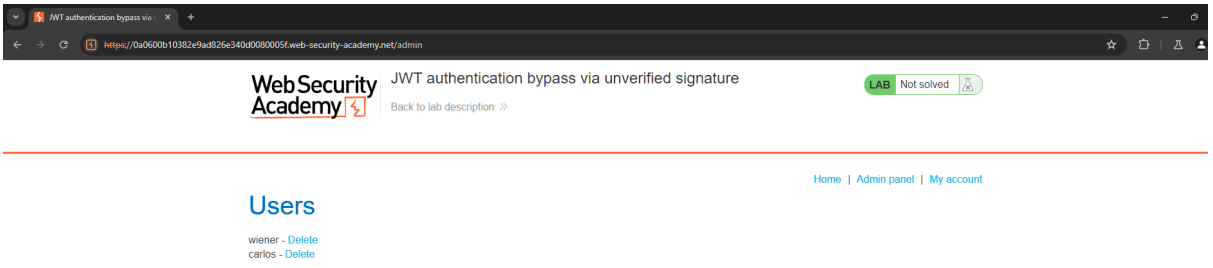


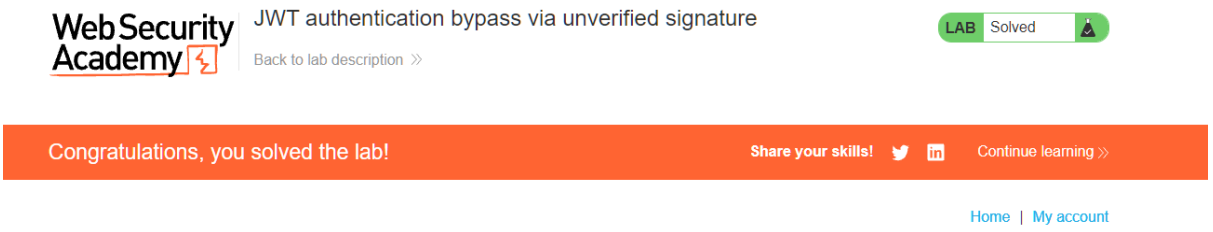
Bước 2: Bắt request đăng nhập, chúng ta thấy rằng ở phần session có lưu trữ một đoạn dữ liệu dài và khi sử dụng extension của burp suite thì nó hiện ra thông tin của người sử dụng



Bước 3: Truy cập vào phần '/admin' của website sau đó thay đổi sub từ wiener sang administrator thì chúng ta đã truy cập vào được tài khoản admin:

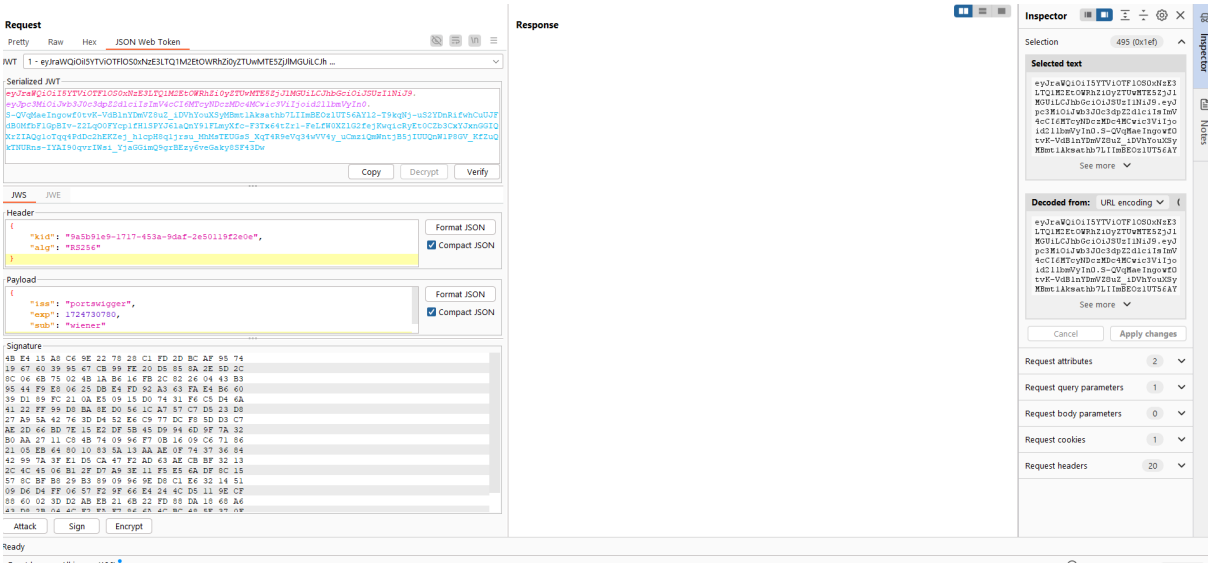




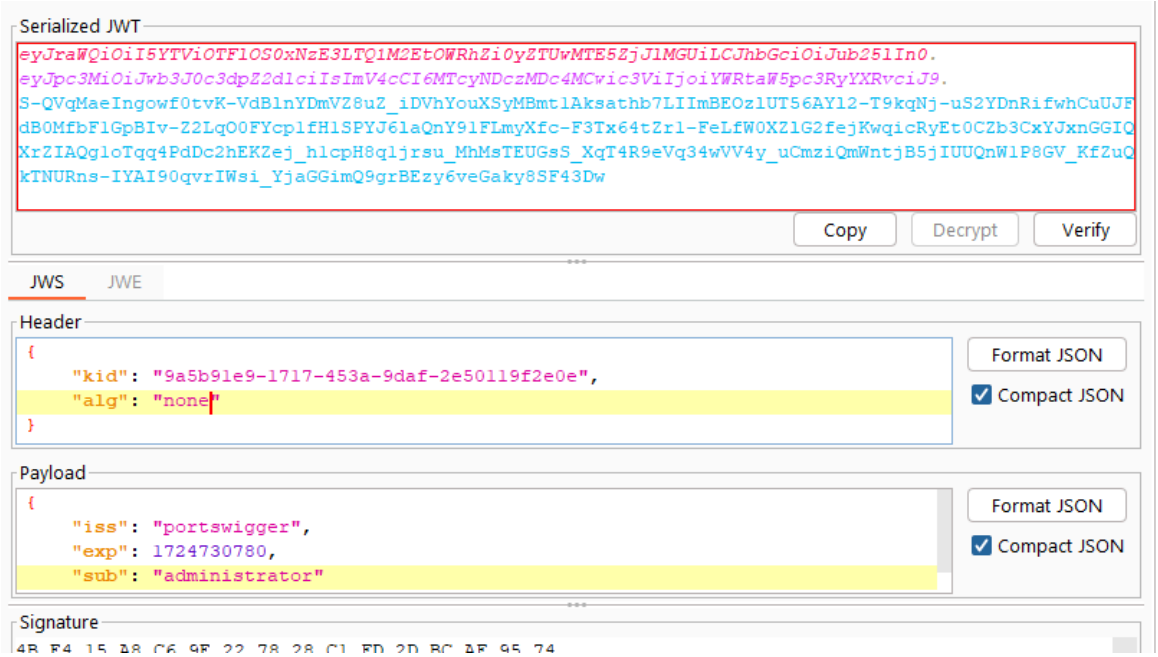


2. Lab: JWT authentication bypass via flawed signature verification

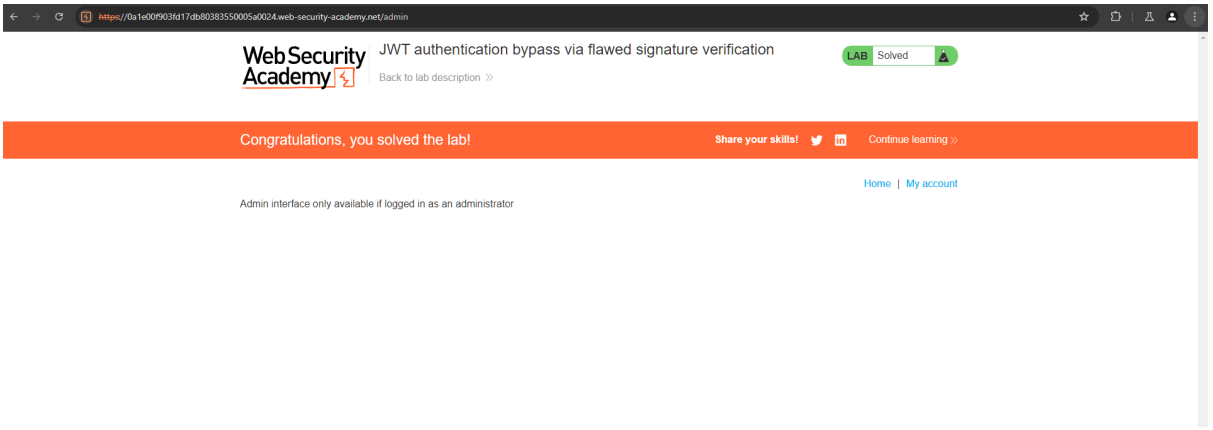
Bước 1: Đăng nhập tài khoản wiener:peter và bắt request:



Bước 2: Thay đổi trường thông tin với sub là ‘administrator’ và alg là ‘none’



Bước 3: Send request, sau đó xóa đoạn chuỗi có màu xanh đi. đổi đường dẫn thành ‘/admin/delete?user=carlos’, thành công xóa được tài khoản carlos:

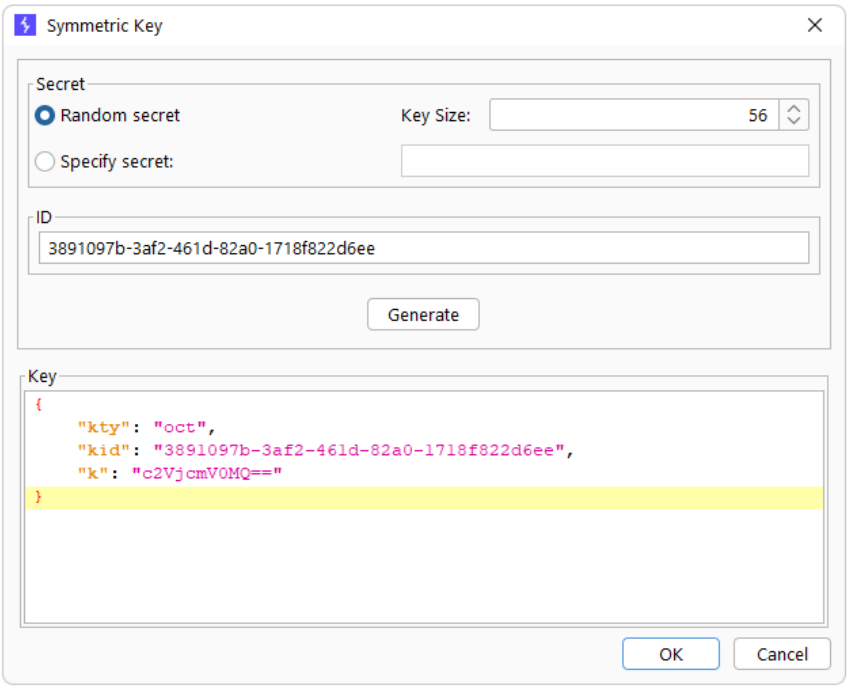


3. **Lab: JWT authentication bypass via weak signing key**

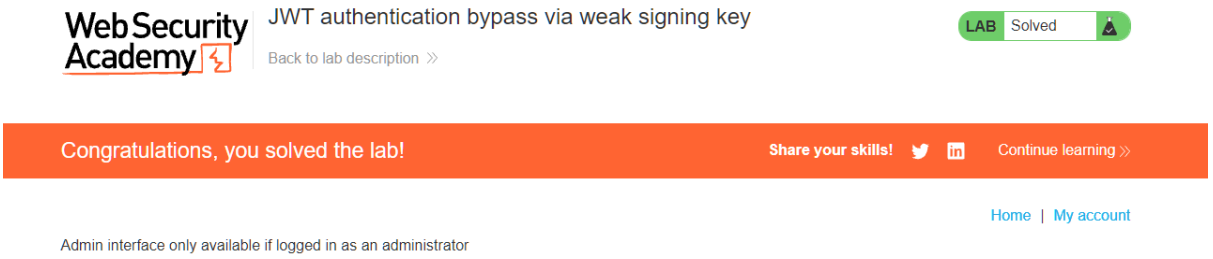
Bước 1: Đăng nhập vào tài khoản wiener:peter, bắt request và copy jwt

Bước 2: Sử dụng hashcat để thực hiện dictionary attack trên jwt này. kết quả thấy được dòng kí tự cuối là ‘secret1’

Encode ‘secret1’ sang base64. Sau đó tạo một Symmetric key từ key đã tìm lúc trước:

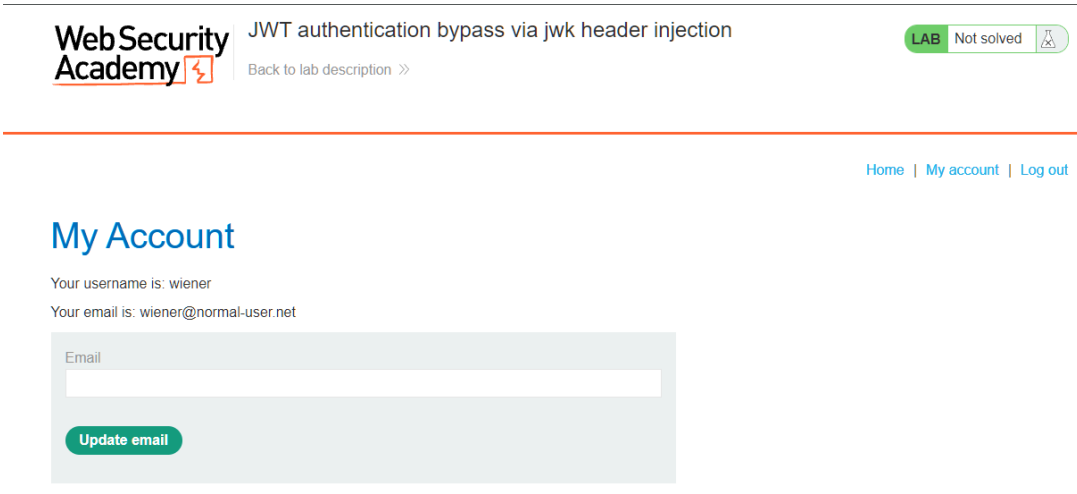


Bước 3: Quay về request lúc nãy, chuyển phần sign thành key đã tạo, chuyển sub thành administrator và chuyển đường dẫn thành /admin/delete?user=carlos, hoàn thành bài lab:

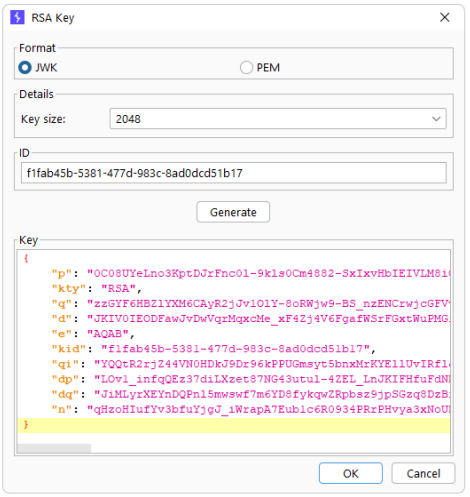


4. Lab: JWT authentication bypass via jwk header injection

Bước 1: Đăng nhập vào tài khoản wiener:peter



Bước 2: Tạo RSA key



Bước 3: Bắt request đăng nhập của user wiener và đưa sang phần repeater, sau đó vào phần JSON web token, nhấn attack và embedd RSA key vừa tạo. Thành công xóa được user carlos:

Web Security Academy | JWT authentication bypass via jwk header injection | LAB Solved

Back to lab description »

Congratulations, you solved the lab! Share your skills! Continue learning »

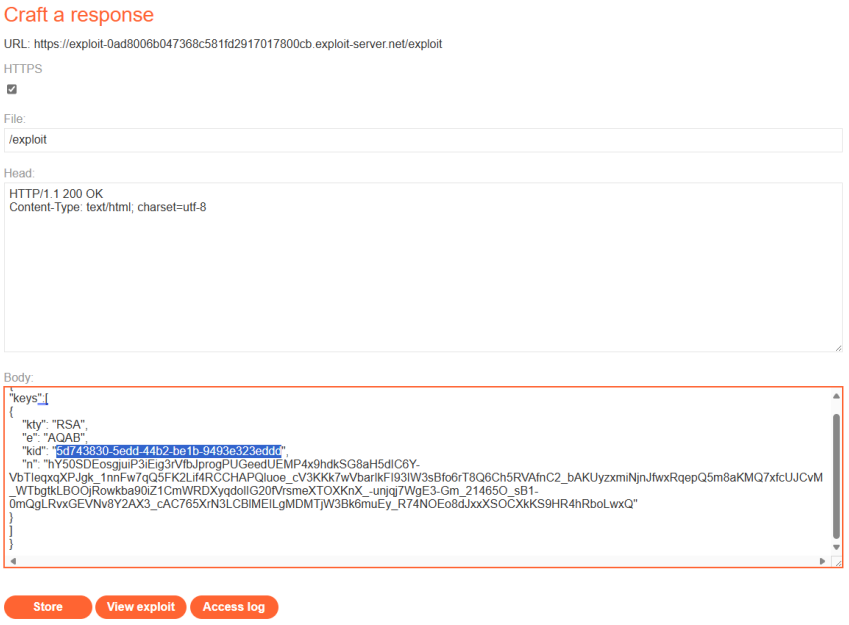
Home | My account

Admin interface only available if logged in as an administrator

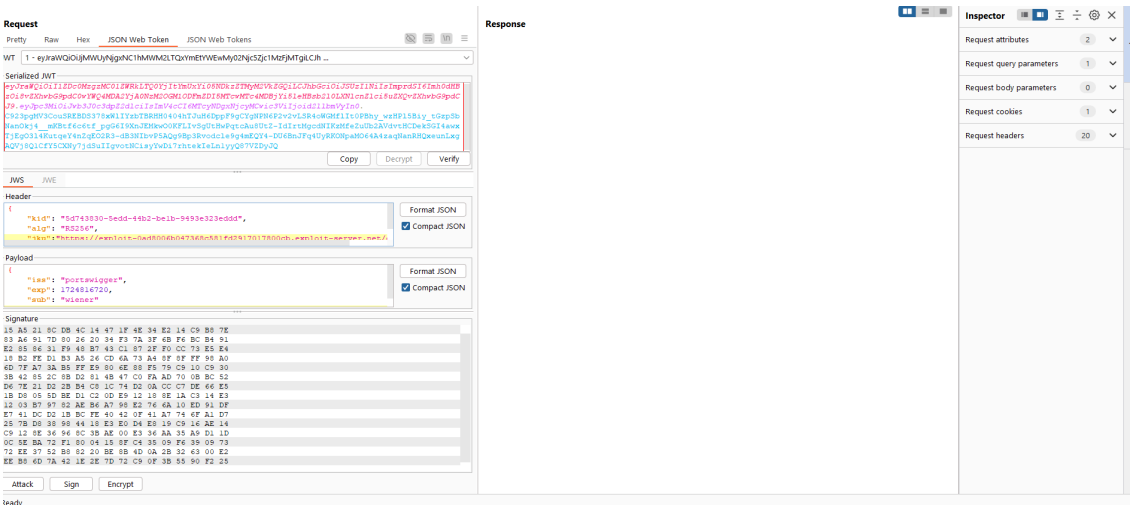
5. Lab: JWT authentication bypass via jku header injection

Bước 1: Đăng nhập vào tài khoản wiener:peter

Bước 2: Tạo RSA key và copy và store trên Exploit server:



Bước 3: Bắt request đăng nhập của user wiener, vào phần JWT Web Token, chỉnh sửa phần kid là giá trị kid của khóa RSA, thêm phần jku là link ở phần Exploit Server, sau đó nhấn Sign và đưa giá trị key đã tạo, sửa đường dẫn thành '/admin/delete?username=carlos':



Web Security Academy

JWT authentication bypass via jku header injection

Back to lab description »

LAB Solved

Congratulations, you solved the lab!

Share your skills!

Continue learning »

Admin interface only available if logged in as an administrator