# (A2) Broken Authentication

## Authentication Bypasses

### 2. 2FA Password Reset

Modify the parameters `secQuestion0` and `secQuestion1` in the request to `secQuestionA` and `secQuestionB`.

## JWT

### 3. Decoding a JWT token

Use jwt.io to decode the token.

### 5. JWT Signing

Change the user to Jerry and click Reset votes. Then go to the cookie section of the request where you will see an `access\_token`. Modify the JWT accordingly.

A screenshot of a computer program

AI-generated content may be incorrect.

### 8. JWT Cracking

Use John to crack the JWT secret, then use CyberChef to sign it again.

### 10. Refreshing a Token

When loading the lesson, you'll catch a request like this:

POST /WebGoat/JWT/refresh/login HTTP/1.1  
  
...  
  
{"user":"Jerry","password":"bm5nhSkxCXZkKRy4"}

And its response:

{  
 "access\_token" : "...",  
 "refresh\_token" : "etmOBMYjKgqDZHOxCTiC"  
}

Use Jerry's `refresh\_token` to obtain a new token for Tom:

POST /WebGoat/JWT/refresh/newToken HTTP/1.1  
Authorization: Bearer ...  
Content-Type: application/json; charset=UTF-8  
  
...  
  
{  
 "refresh\_token" : "etmOBMYjKgqDZHOxCTiC"  
}

You will receive a new token:

{  
 "access\_token" : "...",  
 "refresh\_token" : "cSxIFRlEhSDkCKXZIBQB"  
}

Insert Tom's new token in the `checkout` request:

POST /WebGoat/JWT/refresh/checkout HTTP/1.1  
Authorization: Bearer ...  
...

### 11. Final Challenge

SQL injection into the `kid` field in the JWT header. The string `bWVv` comes from a UNION SELECT and reveals the key `meo` used to sign the JWT.

A screenshot of a computer

AI-generated content may be incorrect.

## Password Reset

### 4. Security Questions

Use Burp Suite to bruteforce the color table:

username: admin  
color: green

### 5. Creating the Password Reset Link

The email is sent to the `Host` header, so change it to port `9090` (WebWolf’s port) to receive the reset email.

A screenshot of a computer

AI-generated content may be incorrect.

Reset password link received in WebWolf:

A screenshot of a computer program

AI-generated content may be incorrect.

http://127.0.0.1:8080/WebGoat/PasswordReset/reset/reset-password/...