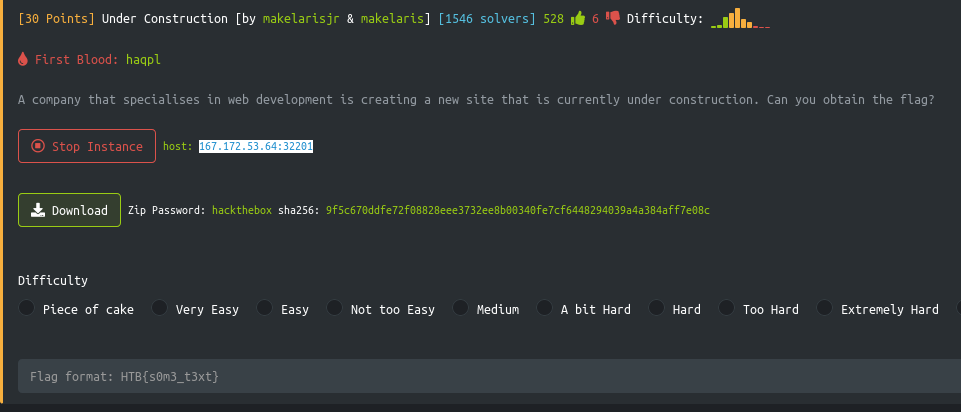
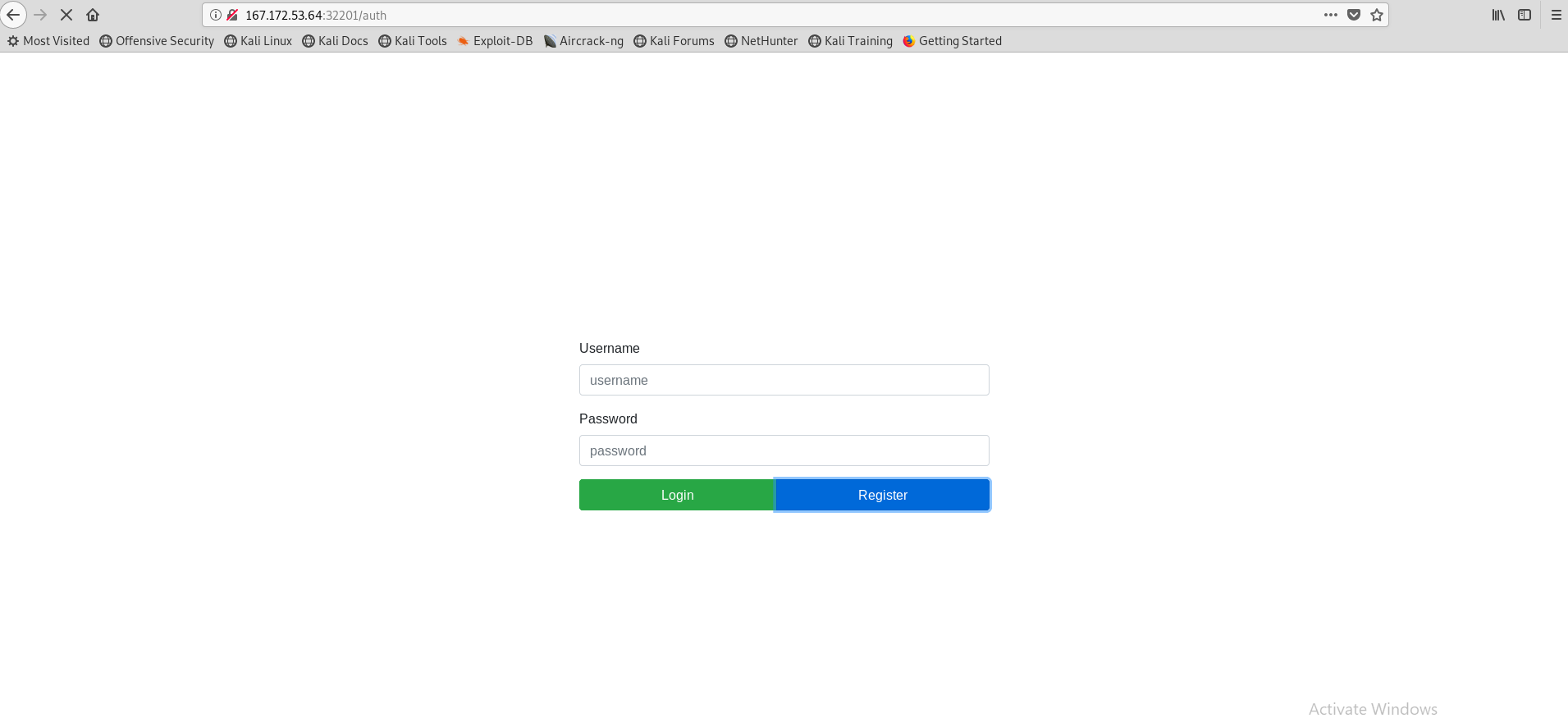
**Under Construction**



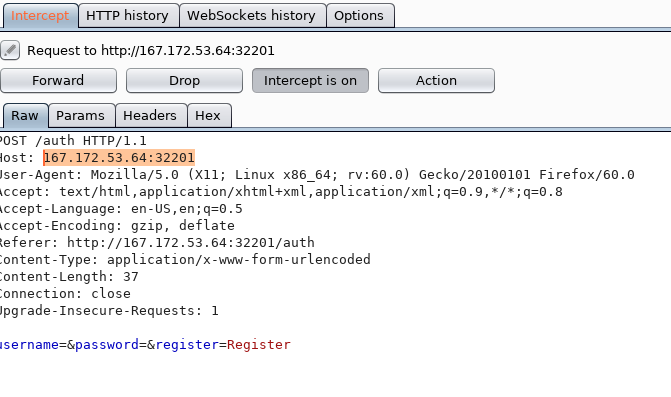
I entered URL in firefox: 167.172.53.64:32201



I tried clicking register and nothing happened. Looked like it was loading but never did

That is when I realized the game is called “Under Construction”. Maybe the exploit is in the register button since it is “Being worked on”

I opened Burp Suite and ran the URL the proxy and got this:



I then entered in the username “Kyle” and the password “Test”

I then clicked register and then Forward on Burp suite and saw that the registration said Successful

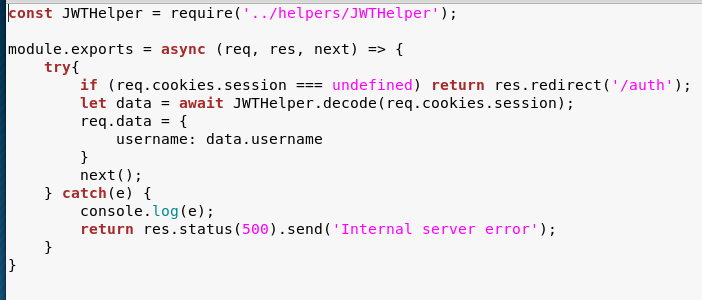
I then logged into the website with the credentials above

I looked at burp suite and found a cookie session with a long hash



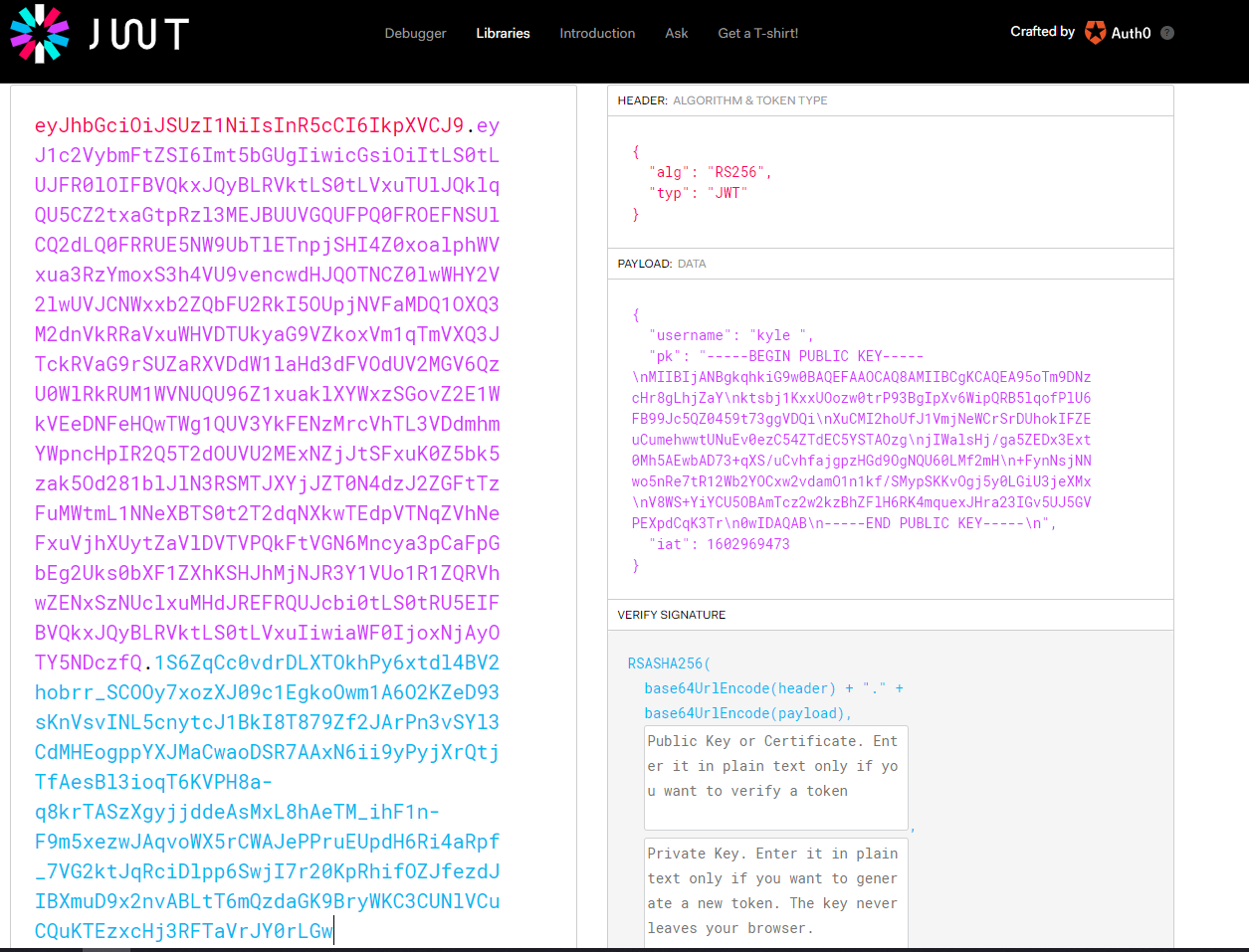
I copied the hash and saved it in leaf pad for now

The CTF came with a download called middleware.js



The file above is called JWTHelper, assuming now the website using a JSON Web Token

<https://jwt.io/> this website can reveal what is inside that long cookie session ID

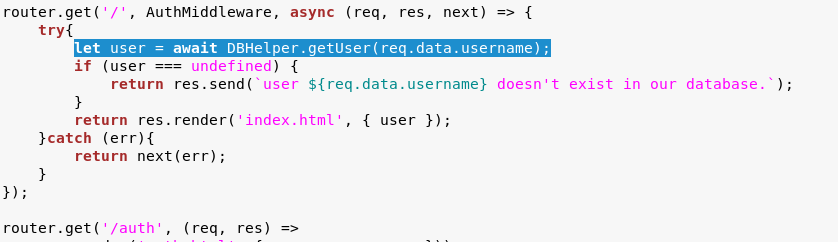


It shows my username and along with a public key

Storing public key for now

Going back to the file I downloaded at the start there is a folder /route/index.js

I found a line in the code called: let user = await DBHelper.getUser(req.data.username);



This function above basically means a login attempt was successful

Going back to file I downloaded at the beginning, there is a program in /helper/DBHelper.js

I ran DBHelper.js and saw a line in the code for the username:



The username runs through a SELECT query (Possible SQL injection can be made)

Now with that I can do ‘kyle’ or 1=1-- - and should return the log in as success

BUT – the private key must equal the value of the sign in which is mentioned in the JWTHelper.js

After being stuck on this for a while, someone in Hackthebox forum gave a hint to look for vulnerabilities in the JW tool – someone from the forum found a ticarpi (jwt\_tool) for me to use. I opened my terminal and installed it

git clone <https://github.com/ticarpi/jwt_tool>

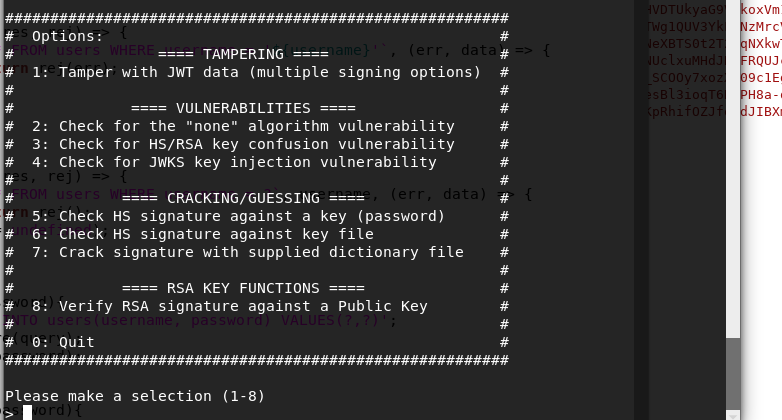
then I went to cd jwt\_tool/ and tried to run it and got it denied



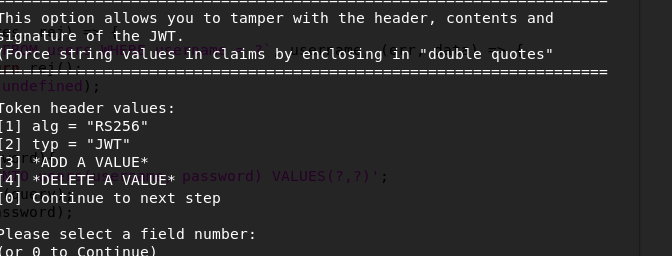
I then had to make it executable chmod +x jwt\_tool.py

Now I run it again

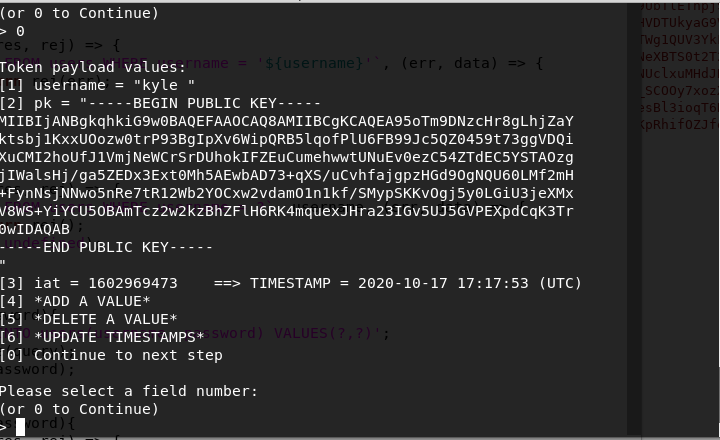




Selected 1 and hit enter



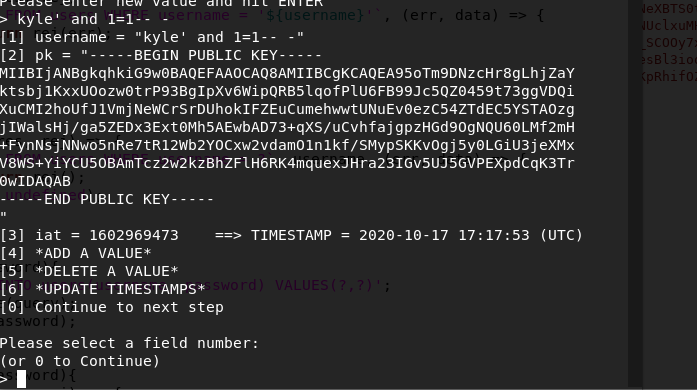
Selected 0 and continued



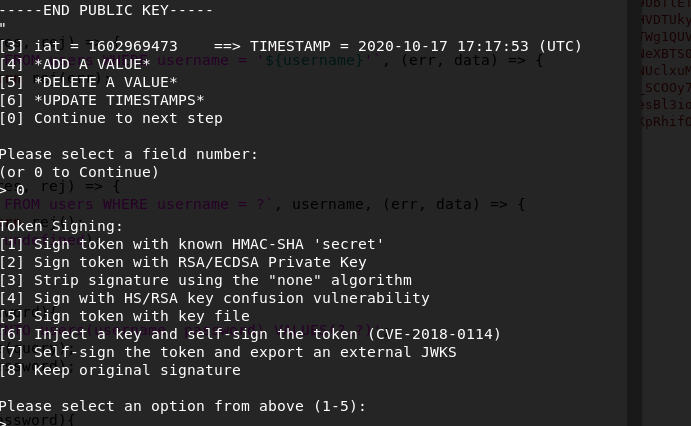
Now I can see my username with the public key

Now I can enter my SQl injection into this field

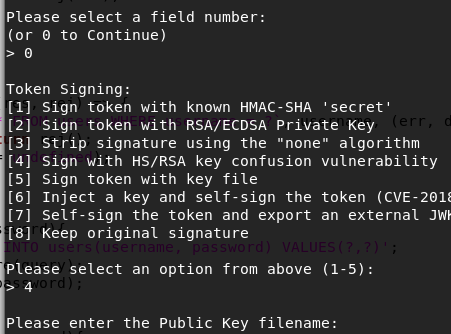
kyle’ and 1=1-- -



None of those options seemed good. So, I clicked 0 and continued



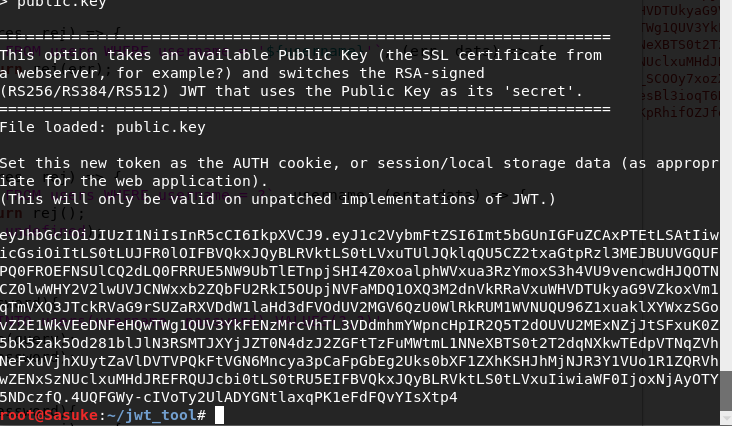
Option 4 seemed promising



It is asking for a public key

From the website that gave me the public key, I saved a public.key file in the same directory as jwt\_tool

And ran it



Now I must send this value through burp suite