NeverLAN CTF

Pcap : Unsecured Login 2

Value : 75 pts

Difficulty : Easy

Description : Your flag will be in the normal flag{flagGoesHere} syntax.

Attachment : We caught someone logging into their website, but they didn't check their links when submitting data!

Mysite2.pcap

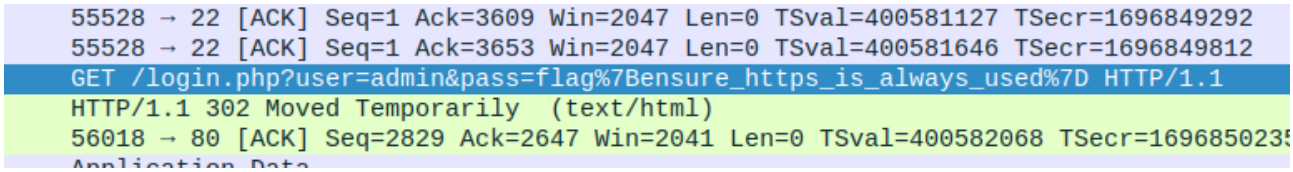
Solution :

A pcap file is given. This file can be opened with Wireshark.
We can still see a user accessing a website. This time, all HTTP requests are redirected to HTTPS.

```
GET /login.php HTTP/1.1
Host: 192.168.23.46
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:72.0)
Gecko/20100101 Firefox/72.0
Accept: text/html,application/xhtml+xml,application/
xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Cookie: PHPSESSID=g9it34ivklcg3kvfo3vo54bvkv
Upgrade-Insecure-Requests: 1

HTTP/1.1 302 Moved Temporarily
Server: nginx/1.14.2
Date: Fri, 24 Jan 2020 19:01:12 GMT
Content-Type: text/html
Content-Length: 161
Connection: keep-alive
Location: https://192.168.23.46/login.php
```

But later in the file, we can see that the user is sending login requests in HTTP first, before being redirected to HTTPS. The first request does not contain the flag. But there is an other which contains the flag instead of the admin account.



flag{ensure_https_is_always_used}