NeverLAN CTF

## Pcap : Unsecured Login

Value : 50 pts

Difficulty : Easy

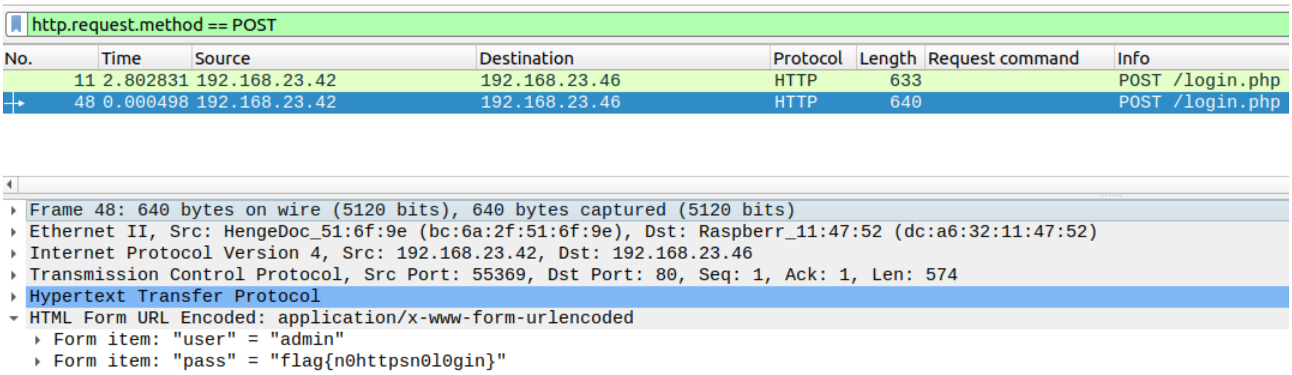
Description : Your flag will be in the normal flag{flagGoesHere} syntax.

Attachment : We caught someone logging into their website, but they didn't use https!

Mysite.pcap

## Solution :

A pcap file is given. This file can be opened with Wireshark.
In this file, we can see that a user accessed a website without using HTTPS.
We might want to find the credentials of the user, if he tried to connect to his account.
There is a high probability that the password is sent to the server in a post request.
We can apply a filter in Wireshark for post requests (http.request.method == POST).
There are two results. The first is a simple password for a generic user. The other one is a connection to the admin account. The flag is in the password field.



http.request.method == POST

| No. | Time | Source | Destination | Protocol | Length | Request command | Info |
|---|---|---|---|---|---|---|---|
| 11 | 2.802831 | 192.168.23.42 | 192.168.23.46 | HTTP | 633 | | POST /login.php |
| 48 | 0.000498 | 192.168.23.42 | 192.168.23.46 | HTTP | 640 | | POST /login.php |

```
▸ Frame 48: 640 bytes on wire (5120 bits), 640 bytes captured (5120 bits)
▸ Ethernet II, Src: HengeDoc_51:6f:9e (bc:6a:2f:51:6f:9e), Dst: Raspberr_11:47:52 (dc:a6:32:11:47:52)
▸ Internet Protocol Version 4, Src: 192.168.23.42, Dst: 192.168.23.46
▸ Transmission Control Protocol, Src Port: 55369, Dst Port: 80, Seq: 1, Ack: 1, Len: 574
▸ Hypertext Transfer Protocol
▾ HTML Form URL Encoded: application/x-www-form-urlencoded
  ▸ Form item: "user" = "admin"
  ▸ Form item: "pass" = "flag{n0httpsn0l0gin}"
```

**flag{n0httpsn0l0gin}**