Lab - Network security

Capturing sensitive information

In our first assignment, we'll try to extract sensitive information from captured Internet traffic. We'll use Wireshark to see if we can "listen in" on the information that's submitted in an online form. Do the following:

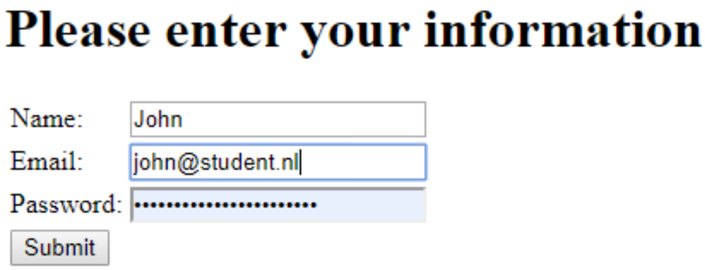
1. Start up your web browser.

2. Start up the Wireshark packet sniffer.

3. Begin Wireshark packet capture. For this exercise, we're interested in HTTP traffic. Set your capture or display filter accordingly.

4. Enter the following URL in your browser. Note that this site does not support HTTPS! http://infra.networksinthenews.com/login.html

5. Your browser should show a simple online form:



Please enter your information

Name: John
Email: john@student.nl
Password: ••••••••••••••••••••••

6. Fill in this form with your personal information (it doesn't really matter what information you enter) and press Submit.

7. Stop Wireshark packet capture.

Normally, HTTP pages are requested from the server using an HTTP GET request. In this case, however, your browser used an HTTP POST request to send the data that was entered on the form back to the server.

By looking at the information in the HTTP POST and response messages, answer the following questions.

8. Is the information you submitted contained in the POST request?

Nee, maar wel in de HTML form URL Encoded tab.

9. According to the capture, what was the password used?

Hoi1234

Using HTTPS and certificates

1. Start a new Wireshark capture. (Don't use a filter for this one.)

2. Now, use your browser to visit your favourite HTTPS-protected website (for example: bol.com or another website where you've done shopping) and login, using your own username and password.

3. Search your capture for your username and password. Can they be found within this capture? Hint: from the menu, use edit -> find packet to search for packets. In this case, search for a **string** in the **packet details**.

Ik kan mijn inloggegevens niet vinden in de packets. Het kan zijn dat mijn wireshark anders is dan de versie die gebruikt werd tijdens het maken van deze opdrachten.

4. Now, go back to your browser. While still displaying the HTTPS-protected website you just visited, look at the certificate for this site to answer the following questions. How to do this depends on what browser you're using. Usually, you can click a padlock shaped icon: 🔒

5. Who was the certificate for this site issued to?

R3, www.bol.com

6. What Certificate Authority provided the certificate?

ISRG Root X1

7. When will the certificate expire?

04-06-2035

8. Now, view the certificate details. Can you find the **public key** in the certificate? If so, how long is this key? (how many bits). If not, explain why not.

Erg lang. 4.096 bits

```
512 bytes : AD E8 24 73 F4 14 37 F3 9B 9E 2B 57 28 1C 87 BE DC B7 DF 38 90 8C 6E 3C E6 57 A0 78 F7 75 C2 A2 FE F5 6A
6E F6 00 4F 28 DB DE 68 86 6C 44 93 B6 B1 63 FD 14 12 6B BF 1F D2 EA 31 9B 21 7E D1 33 3C BA 48 F5 DD 79 DF B3 B8
FF 12 F1 21 9A 4B C1 8A 86 71 69 4A 66 66 6C 8F 7E 3C 70 BF AD 29 22 06 F3 E4 C0 E6 80 AE E2 4B 8F B7 99 7E 94 03
9F D3 47 97 7C 99 48 23 53 E8 38 AE 4F 0A 6F 83 2E D1 49 57 8C 80 74 B6 DA 2F D0 38 8D 7B 03 70 21 1B 75 F2 30 3C
FA 8F AE DD DA 63 AB EB 16 4F C2 8E 11 4B 7E CF 0B E8 FF B5 77 2E F4 B2 7B 4A E0 4C 12 25 0C 70 8D 03 29 A0 E1 53
24 EC 13 D9 EE 19 BF 10 B3 4A 8C 3F 89 A3 61 51 DE AC 87 07 94 F4 63 71 EC 2E E2 6F 5B 98 81 E1 89 5C 34 79 6C 76
EF 3B 90 62 79 E6 DB A4 9A 2F 26 C5 D0 10 E1 0E DE D9 10 8E 16 FB B7 F7 A8 F7 C7 E5 02 07 98 8F 36 08 95 E7 E2 37
96 0D 36 75 9E FB 0E 72 B1 1D 9B BC 03 F9 49 05 D8 81 DD 05 B4 2A D6 41 E9 AC 01 76 95 0A 0F D8 DF D5 BD 12 1F 35
2F 28 17 6C D2 98 C1 A8 09 64 77 6E 47 37 BA CE AC 59 5E 68 9D 7F 72 D6 89 C5 06 41 29 3E 59 3E DD 26 F5 24 C9 11
A7 5A A3 4C 40 1F 46 A1 99 B5 A7 3A 51 6E 86 3B 9E 7D 72 A7 12 05 78 59 ED 3E 51 78 15 0B 03 8F 8D D0 2F 05 B2 3E
7B 4A 1C 4B 73 05 12 FC C6 EA E0 50 13 7C 43 93 74 B3 CA 74 E7 8E 1F 01 08 D0 30 D4 5B 71 36 B4 07 BA C1 30 30 5C
48 B7 82 3B 98 A6 7D 60 8A A2 A3 29 82 CC BA BD 83 04 1B A2 83 03 41 A1 D6 05 F1 1B C2 B6 F0 A8 7C 86 3B 46 A8 48
2A 88 DC 76 9A 76 BF 1F 6A A5 3D 19 8F EB 38 F3 64 DE C8 2B 0D 0A 28 FF F7 DB E2 15 42 D4 22 D0 27 5D E1 79 FE 18
E7 70 88 AD 4E E6 D9 8B 3A C6 DD 27 51 6E FF BC 64 F5 33 43 4F
```

9. Can you find the **private key** in the certificate? If so, how long is this key? (how many bits). If not, explain why not.

De private key is niet te vinden in het certificaat. Deze staat niet vermeld.