Report to IT Manager

Assignment

45m

Status Incomplete

Introduction

Take a look at a possible scenario. You've finished the recap and you have to report the problems of the servers as your manager has now asked. Your manager wants a test that verifies if the information is passing with the HTTP traffic.

For the test, you will use Wireshark to capture the traffic and analyze the information.

After that test, you have to draft an email that you need to send to the the IT manager explaining the pros and cons of using HTTPS and genuine certificates.

In your email, you must explain the step-by-step process after testing.

Instructions

Start by sniffing your network and capture some packets. Since this is a test, you don't need to test on the company's environment. You'll use another resource, an external website, to experiment. You can still use the virtual machines to run Wireshark, but remember, the virtual machine you use to access the website must be on the same network as the connection that you will analyze.

Since the test will experiment access on an external website, you can use Wireshark to view the traffic.

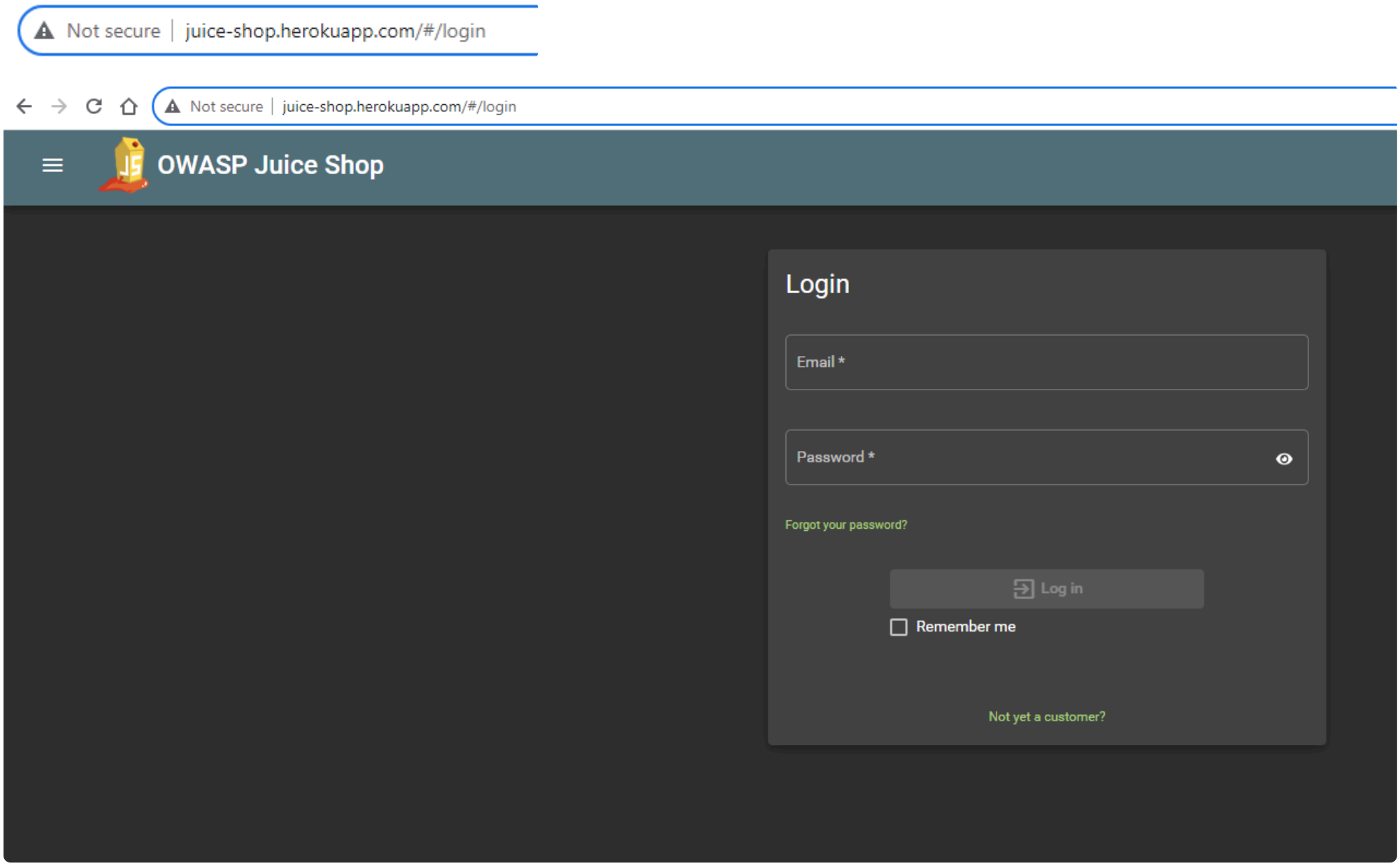
For students using the EVE Environment

You can use Wireshark installed on the Jumphost.

Students using VirtualBox/VMWare

You can use Wireshark installed on either the Linux, Kali, or Windows 11 VM.

To capture the user and password, you can use the website at this link http://juice-shop.herokuapp.com/#/login, and it will open the experimental HTTP webpage as in the image below.



Warning

You can enter any username and password for the login page. The intention of this activity is not to actually login to the website, but to view how network traffic containing user input can look unencrypted.

To experiment with the sniffing, follow the steps below:

1. Start the traffic capture in Wireshark.
2. Access the webpage above and fill out the authentication form with Username and Password and press the Login button.
3. Stop the traffic capture in Wireshark.
4. Filter for the POST using the following filter → http.request.method == “POST” as in the image example below.

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

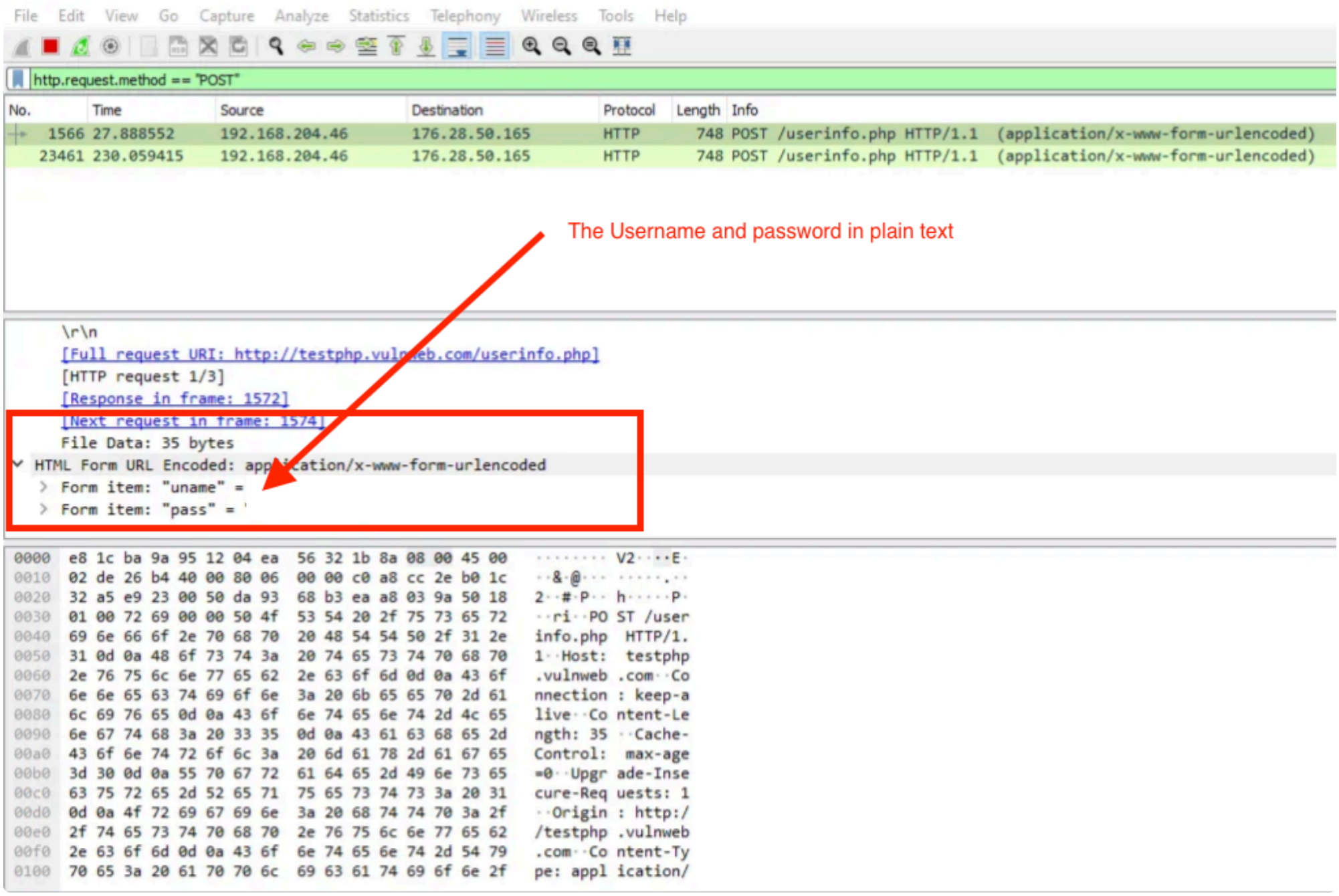
http.request.method == "POST"

No.	Time	Source	Destination	Protocol	Length	Info
1566	27.888552	192.168.204.46	176.28.50.165	HTTP	748	POST /userinfo.php HTTP/1.1 (application/x-www-form-urlencoded)
23461	230.059415	192.168.204.46	176.28.50.165	HTTP	748	POST /userinfo.php HTTP/1.1 (application/x-www-form-urlencoded)

```
> Frame 1566: 748 bytes on wire (5984 bits), 748 bytes captured (5984 bits) on interface \Device\NPF_{AB82FBC5-B2C2-4C79-BCA9-61688E1DB785}, id 0
> Ethernet II, Src: IntelCor_32:1b:8a (04:ea:56:32:1b:8a), Dst: Fortinet_9a:95:12 (e8:1c:ba:9a:95:12)
> Internet Protocol Version 4, Src: 192.168.204.46, Dst: 176.28.50.165
> Transmission Control Protocol, Src Port: 59683, Dst Port: 80, Seq: 1, Ack: 1, Len: 694
> Hypertext Transfer Protocol
> HTML Form URL Encoded: application/x-www-form-urlencoded
```

```
0000  e8 1c ba 9a 95 12 04 ea  56 32 1b 8a 08 00 45 00   ........ V2....E.
0010  02 de 26 b4 40 00 80 06  00 00 c0 a8 cc 2e b0 1c   ..&.@... ........
0020  32 a5 e9 23 00 50 da 93  68 b3 ea a8 03 9a 50 18   2..#.P.. h.....P.
0030  01 00 72 69 00 00 50 4f  53 54 20 2f 75 73 65 72   ..ri..PO ST /user
0040  69 6e 66 6f 2e 70 68 70  20 48 54 54 50 2f 31 2e   info.php  HTTP/1.
0050  31 0d 0a 48 6f 73 74 3a  20 74 65 73 74 70 68 70   1..Host:  testphp
0060  2e 76 75 6c 6e 77 65 62  2e 63 6f 6d 0d 0a 43 6f   .vulnweb .com..Co
0070  6e 6e 65 63 74 69 6f 6e  3a 20 6b 65 65 70 2d 61   nnection : keep-a
0080  6c 69 76 65 0d 0a 43 6f  6e 74 65 6e 74 2d 4c 65   live..Co ntent-Le
0090  6e 67 74 68 3a 20 33 35  0d 0a 43 61 63 68 65 2d   ngth: 35 ..Cache-
00a0  43 6f 6e 74 72 6f 6c 3a  20 6d 61 78 2d 61 67 65   Control:  max-age
00b0  3d 30 0d 0a 55 70 67 72  61 64 65 2d 49 6e 73 65   =0..Upgr ade-Inse
00c0  63 75 72 65 2d 52 65 71  75 65 73 74 73 3a 20 31   cure-Req uests: 1
00d0  0d 0a 4f 72 69 67 69 6e  3a 20 68 74 74 70 3a 2f   ..Origin : http:/
00e0  2f 74 65 73 74 70 68 70  2e 76 75 6c 6e 77 65 62   /testphp .vulnweb
00f0  2e 63 6f 6d 0d 0a 43 6f  6e 74 65 6e 74 2d 54 79   .com..Co ntent-Ty
0100  70 65 3a 20 61 70 70 6c  69 63 61 74 69 6f 6e 2f   pe: appl ication/
```

When you analyze the HTTP, you will find all of the form information, including the username and password you used in the form, as seen in the image below.



Now try the same process with the address: https://juice-shop.herokuapp.com/#/login

Write your Email

Now it's time to analyze. What were you able to see in both protocols?

Report to your manager by email and explain what differences you could find in the experiment with HTTP and HTTPS.

Draft your email on a Google Doc and save it to your PKM.

✓ Mark Completed

Previous
Capture an HTTP and an HTTPS Wireshark PCAP

Next
Hash Functions, Data Integrity and Digital Signatures

How well did this activity help you to understand the content?

Let us know how we're doing

☆ ☆ ☆ ☆ ☆

W07D3

Wed Aug 7

W07D3 Schedule »