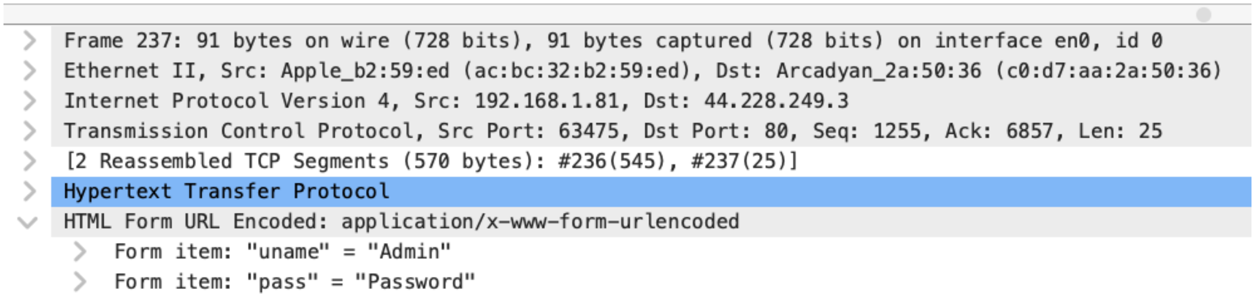
Dear IT Manager,

I have completed the test that you requested on verifying the information within the HTTP traffic. To complete this task, I used Wireshark to capture packets while I accessed a sample website through an HTTP connection and then the same website with an HTTPS connection. I accessed http://testphp.vulnweb.com/login.php and used some example login credentials of Username: Admin and Password: Password. Below, you will find an image from my corresponding packet capture showing my login details in Plain text.



```
>  Frame 237: 91 bytes on wire (728 bits), 91 bytes captured (728 bits) on interface en0, id 0
>  Ethernet II, Src: Apple_b2:59:ed (ac:bc:32:b2:59:ed), Dst: Arcadyan_2a:50:36 (c0:d7:aa:2a:50:36)
>  Internet Protocol Version 4, Src: 192.168.1.81, Dst: 44.228.249.3
>  Transmission Control Protocol, Src Port: 63475, Dst Port: 80, Seq: 1255, Ack: 6857, Len: 25
>  [2 Reassembled TCP Segments (570 bytes): #236(545), #237(25)]
>  Hypertext Transfer Protocol
v  HTML Form URL Encoded: application/x-www-form-urlencoded
     >  Form item: "uname" = "Admin"
     >  Form item: "pass" = "Password"
```

This is quite concerning as it shows just how unsecure an HTTP connection really is. If I had been accessing one of my private accounts with verified credentials, any individual could potentially capture the packets from my computer and access my login details. When accessing the same webpage through an HTTPS connection at https://testphp.vulnweb.com/login.php, the details of my login were hidden from the Wireshark packet. It is clear that we should ensure that all of the secure traffic on our company's network should be configured through the HTTPS port.

Sincerely,
Robert Ajegbo, Security Analyst.