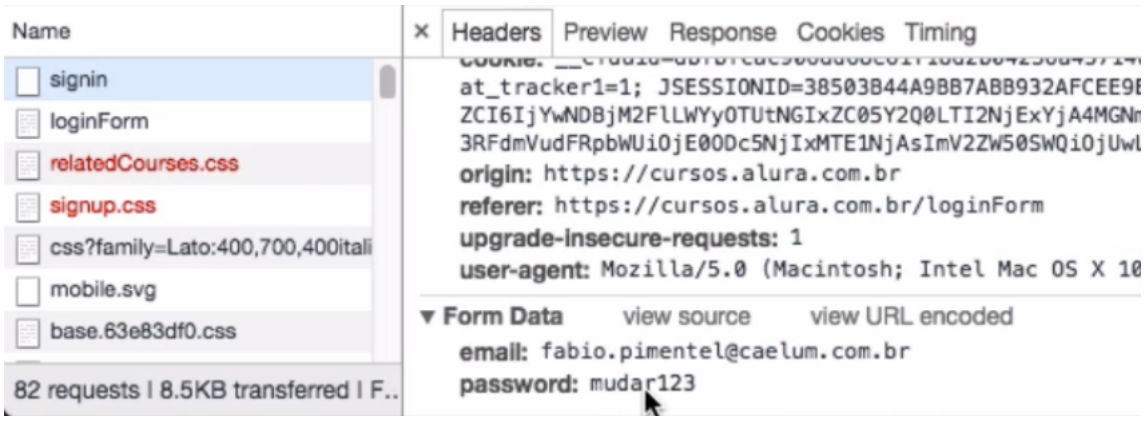
01

HTTPS - A versão segura do HTTP

Transcrição

Sabendo que o HTTP é o protocolo que define as regras de comunicação na web, precisamos observar algumas coisas. Quando usamos o HTTP, todos os dados enviados entre cliente e servidor são *transmitidos em texto puro*, inclusive dados sensíveis, como login e senha!

Quando acessamos a Alura por exemplo, precisamos fornecer informações de autenticação, essas informações são nosso email e senha, que são enviadas e validadas pela plataforma para que assim consigamos assistir as aulas. Estas informações são enviadas em texto limpo e é possível visualizá-las pelas ferramentas do desenvolvedor do navegador. A aba *network* nos possibilita isso.



Mas por que é importante sabermos isso? Quando o navegador pede informações da Alura, nessa comunicação há vários intermediários. Por exemplo, usando uma conexão Wi-Fi, os dados do navegador passam primeiro para o roteador Wi-Fi, e do roteador passam para o modem do provedor, do modem para algum servidor do provedor de internet, como Oi ou NET.

É muito provável que existam outros servidores intermediários no provedor antes que os dados realmente cheguem no servidor da Alura. Com a resposta é a mesma coisa, ela volta passando por esses servidores no meio antes de chegar até nosso navegador. O problema é, quando usamos HTTP, qualquer servidor no meio pode espionar os dados enviados, algo totalmente inseguro! Imagine se essas informações fossem relativas a contas bancárias. Não seria nada seguro!

Para estes outros cenários, existe o HTTP**S**, que basicamente é o HTTP comum, porém com uma camada adicional de segurança/criptografia que antes era SSL, mas posteriormente passou a ser também TLS. É muito comum que estas duas siglas sejam encontradas juntas como SSL/TLS por se tratarem da mesma questão de segurança. Sendo assim, temos dois termos:

1. HTTP: HyperText Transfer Protocol
2. SSL/TLS: Secure Sockets Layer / Transport Layer Security