UFRRJ UNIVERSIDADE FEDERAL RURAL DO RIO DE JANEIRO

Nome:	Claudia Barreto de Oliveira
Matrícula:	20200019331
Turma:	PROVA 1 - WEB 0

1. Sobre HTTP, analise as assertivas e assinale a alternativa que aponta a(s) correta(s). (1 PONTO)

I. O HTTP é um protocolo, do tipo requisição-resposta que mantém estado e roda sobre TCP.
II. O protocolo HTTP especifica quais mensagens (conteúdo) os clientes podem enviar para os servidores e quais respostas recebem de volta.
III. Os cabeçalhos de solicitação e respostas são dados em UTF-8 neste protocolo.
IV. O HTTP é um protocolo da camada de aplicação.

a) Apenas I está certa.
b) Apenas I, II e III estão certas.
c) Apenas II e IV estão certas.
d) Apenas II, III e IV estão certas.
e) Todas as afirmativas estão ccorretas.

RESPOSTA: LETRA **C)** Apenas II e IV estão corretas

2. Considere um cliente HTTP que queira obter um documento Web em um dado URL. Ao acessar o site, ele percebeu que na barra de endereços do navegador, em vez de HTTP está sendo mostrado HTTPs. O navegador informa para ele que o site não é seguro. O que pode ter acontecido para que o navegador mostre essa informação? (1 PONTO)

RESPOSTA: O cliente(HTTP) recebe a resposta pelo navegador de que o site não é seguro pois ele enquanto cliente HTTP não possui o certificado de segurança/ não utiliza o TSL/**SSL** para efetuar a comunicação com a fonte destino que está utilizando pois comunica-se por HTTPs.
O navegador também pode indicar que o site não é seguro em casos em que o certificado está inválido, expirado ou não autenticado por uma entidade raiz.

3. Como funciona o GET condicional? Inclua na sua resposta a indicação da informação presente na resposta HTTP que é utilizada na resposta à requisição GET condicional. (1,5 PONTOS)

RESPOSTA: Na requisição GET condicional , o cabeçalho especifica a data da versão armazenada no pedido HTTP na forma if-modified-since: <date> (a fim de se referir a versão do pedido) para a verificação no lado do servidor se o objeto não foi modificado, ou se foi modificado. Caso o objeto não tenha sido modificado, teremos como resposta

HTTP/1.0 304 Not Modified, se o objeto estiver modificado, o cliente receberá em resposta HTTP/1.0 200 OK e o objeto atualizado.

4. Tomando como base a figura abaixo informe o que acontece se o recurso no path “spot1265/light” não existir? Qual o código da mensagem de resposta nesse caso? (1,5 PONTOS)

RESPOSTA: Se o path do recurso não existir no destino, teremos como resposta o erro 404.Ademais, se fosse o caso de erro na requisição seria Bad Request 400, contemplando assim os principais códigos de mensagem 4XX.

5. O HTTP é stateless (não mantém estado). O que isso significa? No seu entendimento, quais as vantagens de não manter estado? quais as desvantagens? (1,5 PONTOS)

RESPOSTA: O servidor não mantém a informação sobre as requisições passadas dos clientes. Para cada novo recurso requisitado, uma nova requisição é feita, ou seja, temos requisições distintas e independentes. Na requisição não temos nenhuma informação que guarde o estado. No navegador isso funciona de modo que: recebe a resposta do servidor e fecha a conexão TCP.
A vantagem é se um cliente “morre” no meio de uma operação/transação, nenhuma parte do sistema precisa ser responsável pela limpeza do estado atual do servidor.
As desvantagens são o tempo, e a quantidade de requisições a serem recebidas serão maiores (pois será uma conexão a cada objeto), diferentemente do estado “stateful”(se mantém o estado, ou seja, persistente) onde a conexão é estabelecida e todos os objetos são enviados sem mais novas requisições. Ademais, importante acrescentar, observamos o estado stateful principalmente em HTTPs.

6. Considere que um usuário deseja acessar uma página com 3 objetos (3 imagens, por exemplo). Quantos RTTs serão necessários em uma conexão usando o HTTP 1.0. Quantos são necessários usando o HTTP 1.1 com conexão persistente? E, se além do persistente, for usado pipeline no HTTP 1.1. (1,5 PONTOS)

RESPOSTA: Em HTTP 1.0, 2 RTTS são utilizados por objeto. 1 para iniciar a conexão TCP e 6 RTTS (em detrimento dos 3 objetos), totalizando 7 RTTs. Referente ao HTTP 1.1 (persistente), é necessário 1 RTT por objeto, ou seja, 1 para iniciar a conexão TCP e 3 RTTs (novamente, em detrimento dos 3 objetos), totalizando 4 RTTs. Já no caso do pipelining (HTTP 1.1 persistente), será utilizado 1 RTT para conexão TCP e 1 RTT para obter todos os objetos, ou seja, 2 RTTs no total.

7. Observe as afirmações abaixo e marque-as com “V” ou “F” para as verdadeiras e falsas, respectivamente. (1 PONTO)

RESPOSTA:

(**V**) É correto afirmar que o navegador mantém o registro das autoridades certificadoras que ele considera confiáveis.

(**V**) É comum que as configurações sobre proxies não transparentes sejam realizadas no sistema operacional (como Windows e Linux, por exemplo), mas existem navegadores (como o Firefox) que permitem que essas configurações sejam feitas apenas no navegador.

(**F**) Códigos de resposta que iniciadas com 3 (ex: 305) são códigos utilizados para indicar um erro.

(**F**) Os servidores HTTP funcionam ouvindo requisições nas portas padrões 80 e 443.

(**V**) Os servidores HTTP funcionam no navegador, no lado do cliente, para tratar a interação do protocolo HTTP.

8. Dê um exemplo de uso de cache (aponte onde podem ser mantidos os caches). Em seguida, apresente um fator positivo e outro negativo que podem ser obtidos com o uso de cache. (1 PONTO)

RESPOSTA: Um exemplo de uso de web cache, e de onde é mantido são os proxy servers. O acesso a web é feito por meio de um proxy, e o cliente envia as requisições e estas são filtradas pelo proxy. Se o objeto existir em cache, ele retorna o objeto, do contrário, ele solicita o objeto original ao destino(servidor original). Um lado positivo,é a redução de resposta ao cliente, redução de tráfego e de requisições no destino(servidor original), e o lado negativo é referente a limpeza que deve ser feita no cache do proxy, pois o cliente pode receber dados antigos ou desatualizados.

Importante acrescentar, que quanto aos dados caches guardados nos navegadores, um dos lados negativos é que atacantes podem infectar o computador e fazer o sequestro de dados armazenados ou em cache (ou seja, logins, senhas, entre outras informações sensíveis podem ficar vulneráveis).