Insper

Tecnologias Hacker

Aula – Web server e Protocolo HTTP

Objetivos da aula

- Conhecer as características do protocolo HTTP;
- Características web server Apache.

O Protocolo HTTP

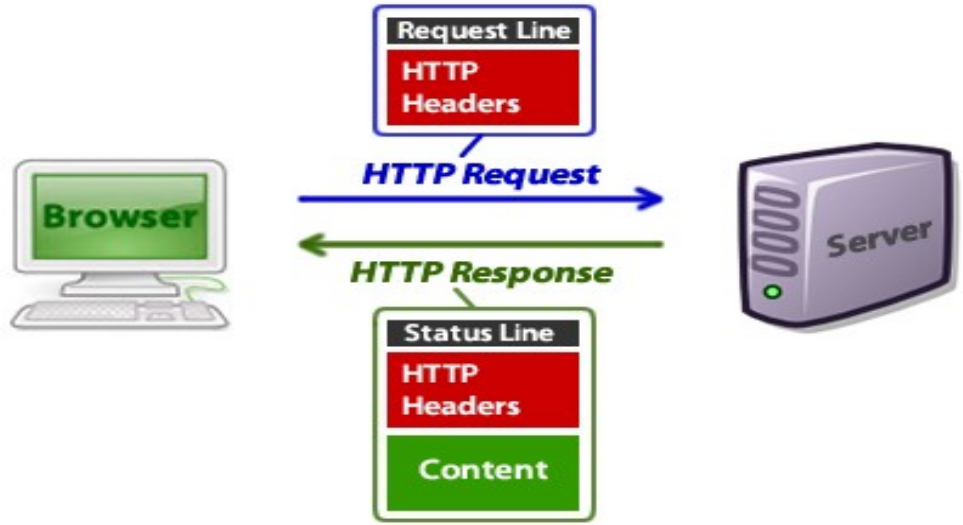

Figura: http://www.devfuria.com.br/php/metodo-http-get-post/

Características

- Funcionamento baseado na troca de requisição e reposta entre um cliente e um servidor;
- Protocolo que funciona na camada de aplicação do modelo de referência OSI e TCP/IP;
- Não guarda o estado entre conexões distintas, ou seja, cada conexão é nova para o servidor. Para contornar esta característica, surgiram os Cookies HTTP, que são pequenos arquivos que são injetados nas máquinas clientes (por meio do navegador do usuário), que permite a preservação e basicamente o estado de uma conexão/sessão.

Características

Não orientado a conexões. Vale reforçar que um protocolo orientado a conexão, tem como principal característica a garantia de entrega de dados entre a origem e o destino de uma comunicação. O protocolo de camada de transporte, TCP, é o protocolo utilizado em uma comunicação HTTP. As características destes passos são muito exploradas em certos tipos de ataque, como por exemplo os ataques de negação de serviço DOS e DDOS (Denial of Service e Distributed DoS) .

Código Status Respostas http

Classe de status 1XX – Informativa

Indica que a solicitação foi recebida e que o servidor está pronto para dar continuidade ao processo.

Os códigos mais comuns dessa classe são: 100 Continuar; 101 Mudando protocolos.

Código Status Respostas http

Classe de status 2XX – Sucesso

Essa classe indica que a solicitação foi recebida, entendida e que será processada com êxito pelo servidor.

Os códigos mais comuns dessa classe são: 200 OK; 201 Criado; 202 Aceito; 203 não-autorizado; 204 Nenhum conteúdo; 205 Reset; 206 Conteúdo parcial.

Código Status Respostas http

Classe de status 3XX – Redirecionamento

Indica que a conexão será redirecionada a outra página. Isso acontece, por exemplo, quando a URL que você pesquisou foi alterada, mas o administrador do site te redireciona para a página atual.

Os códigos mais comuns dessa classe são: 300 Múltipla escolha; 301 Movido Permanentemente; 302 Encontrado; 304 Não modificado; 305 Use Proxy; 307 Redirecionamento temporário.

Código Status Respostas http

Classe de status 4XX – Erro do cliente

Esse status indica que o servidor não conseguiu processar a solicitação porque o cliente a fez de forma errada ou que não dependa dele, como por exemplo uma página excluída.

Os códigos mais comuns dessa classe são: 400 Requisição inválida; 401 Não autorizado; 402 Pagamento necessário; 403 Proibido; 404 Não encontrado; 405 Método não permitido; 407 Autenticação de proxy necessária.

Código Status Respostas http

Classe de status 5XX – Erro do servidor

Esse status indica que, por um erro do servidor, a sua solicitação não pode ser atendida. Na maioria das vezes está relacionada a permissões dos arquivos ou pastas de software.

Os códigos mais comuns dessa classe são: 500 Erro interno do servidor; 502 Bad Gateway; 503 Serviço indisponível; 504 Gateway Time-Out; 505 HTTP Version not supported.

Métodos HTTP

Dois métodos são geralmente utilizados para um pedido e resposta entre um cliente e servidor HTTP, são eles o GET e POST.

GET

é uma operação apenas de leitura (read-only), como por exemplo, um cliente solicita uma página específica de um site.

POST

Uma solicitação POST é usada para enviar dados para o servidor, por exemplo, informações de clientes, upload de arquivos, o envio de dados de um formulário HTML.

Segurança

Do ponto de vista da segurança, é importante olhar para o caminho que a entrada é passada para a aplicação web. Em uma solicitação GET os parâmetros de entrada são incluídos no caminho da solicitação, em um pedido POST eles são incluídos no corpo da solicitação.

Um pouco sobre o Apache

Características

- Arquivo de configuração
  - */etc/apache2/apache2.conf*
- *Arquivos de logs*
  - *var*/log/apache2
- Sites gerenciados (vhost)
  - */etc/apache2/sites-enable*

Formato de log

LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\" %T %v" full

LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\" %P %T" debug

LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\"" combined

LogFormat "%h %l %u %t \"%r\" %>s %b" common

LogFormat "%{Referer}i -> %U" referer

LogFormat "%{User-agent}i" agent

Arquivo conf site

ServerAdmin webmaster@localhost
ServerName www.aula.com.br
DocumentRoot /var/www/html

ErrorLog ${APACHE_LOG_DIR}/error.log
CustomLog ${APACHE_LOG_DIR}/access.log combined

Estrutura de log

198.143.37.153 - - [16/Apr/2018:06:25:22 +0000] "GET /wp-content/uploads/2018/04/banner-site-780x440-1-780x440.png HTTP/1.1" 200 588708 "-" "facebookexternalhit/1.1 (+http://www.facebook.com/externalhit_uatext.php)"

Formato do log

%b - Bytes enviados, excluindo cabeçalhos HTTP.

%h - Máquina cliente.

%l - O nome de login remoto enviado pelo identd (se fornecido).

%P - A identificação do processo filho que serviu a requisição.

%r - A primeira linha da requisição.

%s - Status. Para requisições que foram redirecionadas. internamente. Este é o status de uma requisição *original*. Use %s para a última.

%t - Hora, no formato do arquivo de log (formato inglês padrão).

Formato do log

%T - O tempo necessário para servir a requisição, em segundos.

%u - Usuário remoto (através do auth, pode ser falso se o status de retorno (%s) for 401).

%U - O caminho da URL requisitada.

%v - O nome canônico definido por ServerName que serviu a requisição.

%V - O nome do servidor de acordo com a configuração de UseCanonicalName.