TAG WEB

João Pinheiro Leite Pinto

1. HTTP é um protocolo conforme a sigla (hiper text tranfer protocol), é um protocolo de transferência de hipertextos, sendo o mais comumente utilizado na rede mundial de computadores. Esse protocolo atua na quinta camada do modelo OSI. Ele funciona seguindo o paradigma requisição e resposta, no qual o requisitante estabelece uma conexão com o receptor e lhe envia uma requisição que contém a URI, a vesão do protocolo e uma mensagem padrão chamada MIME que possui os modificadores de requisição e informações sobre o cliente. Então o servidor responde com uma linha de status que contem a versão do protocolo, um código que confirma se a operação foi bem sucedida ou se ocorreu um erro além de informações sobre o servidor.

2. Responsecode é um conjunto de respostas enumeradas que informam como foi o requisitado de uma requisição. Os responsecodes 200s podem ser usados por um atacante que busca URIs protegidos por autotização.

3. O header é um pedaço de uma requisiçao HTTP que permite ao cliente ou ao servidor passar informações adicionais. Um uso inseguro desses headers é não informar o navegador que a conexão deve ser feita por meio do protocolo HTTPS.

4. Os métodos de requisição HTTP indicam que ação deve ser realizada para um determinado recurso. Ambos os métodos GET e POST servem para fazer a passagem de dados, a diferença é que o GET passa eles pelo URL por tanto é menos seguro, enquanto o post passa eles pelo corpo da requisição HTTP.

5. O cache é uma cópia de determinado recurso que um servidor web armazena para que quando um cliente faz uma requisição ele apenas envie oque está armazenado reduzindo o tempo de latência.

6. O cookie são dados gerados por um site que o usuário está navegando que ficam salvos no navegador, para “personalizar o site” e reduzir os carregamentos. O principal ataque relacionado a eles é o cookie poisoning. Nele o atacante faz uso de cookies para se passar por um cliente de um determinado site.

7. OWASP é uma organização sem fins lucrativos voltada para a segurança das aplicações web. Seu projeto mais conhecido é o OWASP TOP TEN uma lista dos 10 maiores riscos de segurança da internet, um documento de advertência.

8.

9. Command injection é um ataque que tem como objetivo rodar um comando no sistema operacional do host.