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.

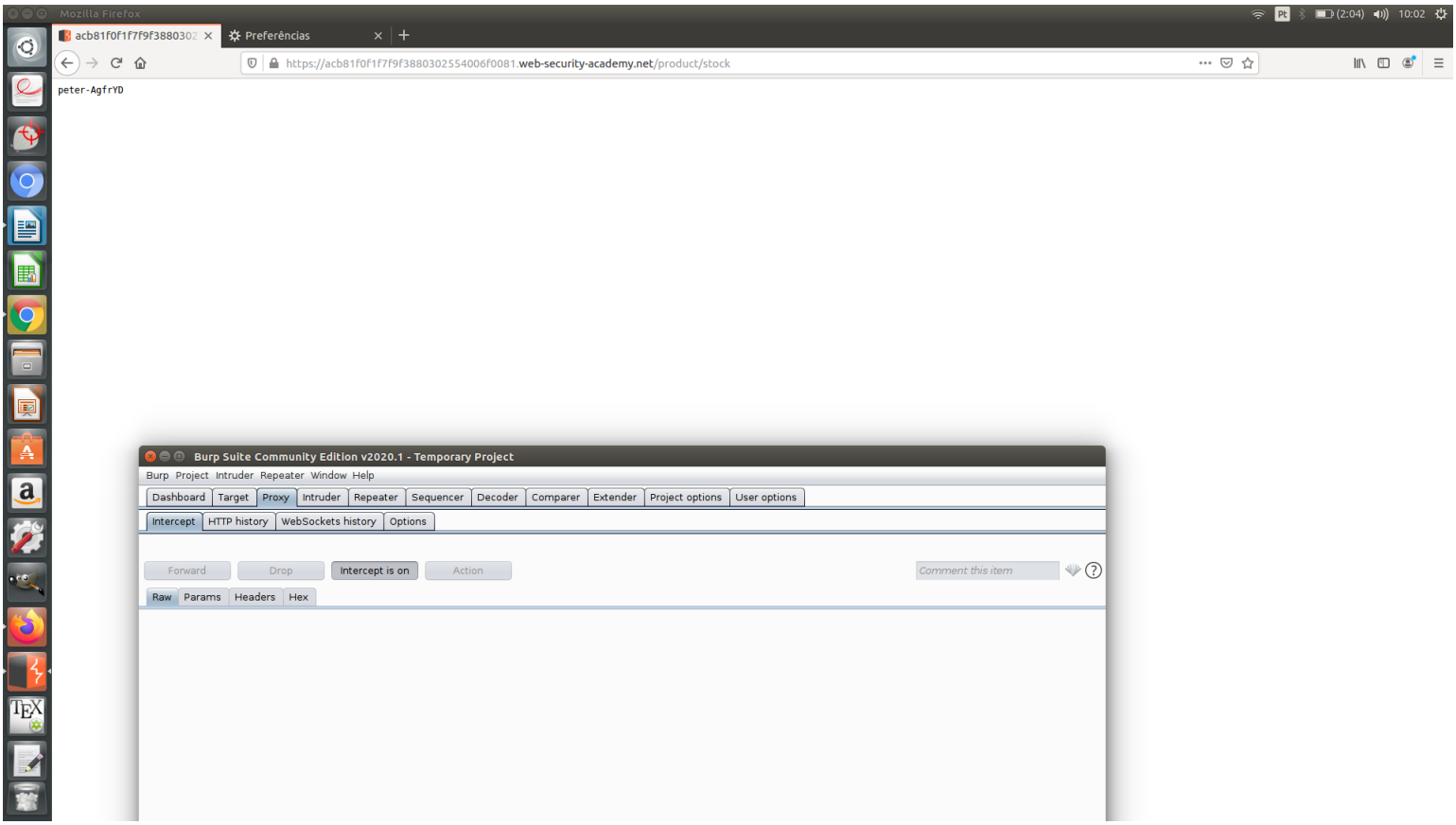
6. O cookie são dados gerados por um site que o usuário está navegando que ficam salvos no navegador, para “personalizar o site” e reduzir os carregamentos. O principal ataque relacionado a eles é o cookie poisoning. Nele o atacante faz uso de cookies para se passar por um cliente de um determinado site.

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. Recon é o processo de reconhecimento de um determinado. Ela é muito comum em bug bountys e é importante pois com ela é possível obter a informação de onde estão as possível falhas no código que está sendo analisado.

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

b) Nesse exercício do site PostWigger eu interceptei uma requisição feita para o site de uma loja e inseri nela um comando whoami para saber qual era o usuário que estava acessando esse site.



10. a) Sql injsction é um tipo de ataque que consiste em injetar um código que afete o banco de dados de um servidor, ele é muito comum em aplicações web.

b) Union based attack é um tipo de sql injection que faz uso da palavra-chave union para poder acessar mais de uma tabela com apenas um comando.

c) Blind sql injection é como um sql-i normal mas com a diferença de que nele o banco de dados não retorna os dados para a pagina web então o atacante tem que obtê-lo a partir de perguntas de verdadeiro ou falso.

11. a) XSS ou cross site scripting é um ataque no qual o atacante faz uso de um site que um usuário confia para rodar softwares maliciosos no computador dele, normalmente em seu navegador.

b) Existem 3 tipos de XSS: o XSS armazenado também denominado persistent ou tipo 1 que ocorre quando um site armazena informações do usuário que ele pega desse site sem muitas

medidas de segurança, oque facilita o trabalho do atacante; o XSS refletido também chamado de non-persistent ou tipo 2 ocorre quando o input fornecido pelo usuário é retornado de forma imadiata, normalmente em mensagens de erro, e nelas vem o código malicioso; por ultimo o XSS DOM-based ou tipo 0 que se diferencia pois nele todos os dados maliciosos nunca saem do navegador.

12. a) LFI é um ataque no qual o atacante inclui arquivos maliciosos que são locais a um servidor neste.

b) RFI é semelhante ao LFI só que neles os arquivos são remotos, vem de fora do servidor atacado.

c) Path traversal é um ataque que visa acessar arquivos que estão fora da raiz do servidor web, ter acesso ao sistema de arquivos do computador que hospeda o servidor.

d) É possível utilizar o path traversal para ter acesso a arquivos que estão fora do servidor e depois inserir um desses arquivos no servidor fazendo assim um LFI.

13. a) CSRF é um ataque que explora a confiança que um site tem nos navegadores de seus usuários, nele os usuários transmitem comendos não autorizados para o servidor.

b)

c) SSRF é uma vulnerabilidade de aplicações web que permite que quem as esteja explorando faça qualquer tipo de requisição http para o servidor, e em casos extremos faça a execução arbitrária de comando.

d)

e) Para que ataques CSRF sejam evitados pode-se fazer uso de tokens que verifiquem se quem está fazendo requisições ao servidor é de fato um usuário autenticado.