TAG WEB 1

Nome: Thomaz Veloso Rebelo da Silva
Data: 16/02/2020

TODOS OS PRINTS ESTÃO EM OUTRO DOCUMENTO

Perguntas:

1-

O HTTP(HiperText Transfer Protoco) e um protocolo para transferência de arquivos, principalmente entre servidor e client,frequentemente usado na internet. Após ser aberta uma comunicação com o servidor, o client faz uma requisição de um arquivo, o servidor, caso encontre, manda o arquivo junto com um Response Code e acaba com a conexão,se isso nao acontecer ele envia um erro (outro Response Code). Então, o navegador procura por possíveis outros arquivos que são requisitos, e repete o processo para os arquivos requisitos (fazendo uma recursão) até receber o Response Code para encerrar a sessão.

2-

É o código de Status da Requisição, se deu certo, ocorreu algum erro, entre outros. Pode-se criar um programa que avalia o Código de Resposta e reporta se deu certo ou não, e a partir disso pode ser feito um Crawler(rastreador de redes).

3-

Header(cabeçalho), onde ficam informações adicionais sobre a requisição/respost que pode ser ou não necessárias para a comunicação. O header pode ter informações sobre o servidor.

4-

São duas formas de enviar comandos ou informações para algum servidor o GET envia formulários e informações pela url e o POST faz a mesma coisa mas pela requisição.O POST além de ser mais seguro pois como e por requisição não existe url para ficar salva e também se pode enviar mais dados com ele

5-

O Cache é um armazenamento que guarda sites recentemente visitados. Quando o servidor retorna um arquivo, geralmente ele manda a data de expiração do último assim evitando transferência de dados que não existem necessidades de serem feitos. Cache-control, Pragma, Expires, Validators.

6-

Cookie é um registro de sessão, serve para o servidor lembrar dos acessos recentes. Cookie Stealing.

7-

O OWASP-Top-Ten é um documento que fala sobre os maiores riscos de segurança para aplicações web.

8-

Recon (reconhecimento, em inglês) refere-se a prática de prática de fazer o reconhecimento do Sistema a ser atacado, seja quais softwares estão sendo usados, suas versões, outros diretórios e arquivos, entre outros.

9-

a) Quando por meio de manipulação de entrada um comando é injetado (rm -fr/).

b) Foi feito em servidor privado dentro do LEP1 Imagens: "ssrf cmd injection.png" e "ssrf cmd injection2.png" String usada no campo: "; curl 127.0.0.1:8081/secret.txt" (o 13 foi feito junto olhe nos prints)

10-

a)Quando por meio de manipulação de entrada um comando de SQL é injetado (Login: '; /* Passowrd: */ OR 1 = 1 --)

b)São ataques a sistemas SQL baseados no comando UNION, e com certa facilidade consegue extrair informações sobre o banco de dados.

c)São ataques onde não se vê o resultado da Query SQL.

11-

a)Cross-Site Scripting, quando coloca um código e o client roda esse código.

b)Não persistente: Mais comum, é um script que roda apenas uma vez, ou quando o script é injetado, seja numa barra de busca, ou outra coisa.Persistente: Ocorre quando é o script injetado vira algo permanente no site, como uma resposta em um forúm ou descrição num site de bate papo.

c/d) Para ambos foram usados o site: http://xss-game.appspot.com XSS Stored está exemplificado na imagem: "xss injection stored" feito apartir do lvl 2.XSS DOM-XSS está exemplificado na imagem: "xss injection dom" feito apartir do lvl 1.

12-

a)Local File Inclusion: processo onde inclui-se arquivos já existentes no servidor, geralmente acontece com servidores PHP.

b)Remote File Inclusion: processo onde inclui-se arquivos que não existiam no servidor.

c)Usar '../' para acessar pastas anteriores.

d)Pode-se usar o '../' para que seja incluido o arquivo 'etc/passwd' no sistema.

e)

13-

a)Cross-Site Request Forgery: o atacante se aproveita da confiança do servidor para enviar ou realizar algo malicioso.

b)

c)Server-Site Request Forgery: o atacante faz o servidor abrir uma conexão para outro endereço, muitas vezes ganhando acesso privilegiado.

d)Foi feito em servidor privado dentro do LEP1 Imagens: "cmd_injection" e "
" String usada no campo: "; curl 127.0.0.1:8081/secret.txt"

e)Para clientes:

- Realizar logout
- Evitar "Lembre-se de mim"

Para servidor:

- Reduzir a vida útil dos Cookies