Tag: Web-Hacking

Nome: Gabriel Silva Pereira

Data: 20/02/2020

1) O que é o protocolo HTTP e Como ele funciona?

É um protocolo que permeia a camada de aplicação do modelo OSI. É o protocolo de transferência de hypertexto. Utilizado para padronizar a disponibilização de páginas marcadas e montadas atráves da linguagem de marcação de hypertexto a partir de requisições feitas por programas que são chamados de navegadores de rede.

Foi criada na mesma época do HTML para servir de arcabouço padronizador do do WWW, a World Wide Web, por diversos pesquisadores e o famoso Tim Berners-Lee.

De maneira resumida, funciona com uma requisição de uma página a partir de um cliente, na forma de um agente de usuário, e a resposta da página a partir de um servidor, na forma de um local na rede. Ou seja, parte da premissa que precisa de uma máquina que hospede uma aplicação/programa que serve as máquinas clientes que fazem as requisições.

2) O que é um Response Code? Cite um exemplo de um programa que você pode fazer com ele?

Response Status Code é qual o estado, ou identificação, da resposta enviada pelo servidor. É dividido em 5 categorias. Possui 3 digitos decimais. As categorias são associadas ao primeiro dígito de 1 a 5. Enumerando-as : Informacional, Sucesso, Redirecionamento, Erro do Cliente, Erro do Servidor.

É possível utilizar o que deve ser interpretado dos códigos de respostas oficiais, ou os não oficiais, e até mesmo utilizar um número que não é indexado para ser interpretado pelo script do lado do cliente (Javascript) para redirecionar para uma ação específica.

3) O que é um HEADER? Cite um uso INSEGURO desse cabeçalho.

É o cabeçalho pelo qual pode ser passado parâmetros de operação e informações adicionais de uma comunicação em HTTP. Tal cabeçalho pode estar presente tanto na requisição quanto na resposta.

Passar informações de maneira errada ou desnecessária. Do ponto de vista do cliente, informações sensíveis do usuário de maneira não encriptada. Do ponto de vista do servidor, informações que super identificam a maquina servidora e acaba deixando uma digital.

4) O que é um Método HTTP? Explique ofuncionamento do método POST, o funcionamento do método GET. Explique qual é considerado mais seguro e por que.

É o tipo da requisição a ser passada para o servidor.

5) O que é Cache e como ele funciona? Cite os principais HEADERS de Request e Response responsáveis pelo controle de Cache.

6) O que é Cookie? Qual é o principal ataque relacionado a ele?

Nasceu no manual da função fseek da biblioteca padrão do C em 1979, como Magic Cookie. Se refere a um punhado de informação que não tem significado para o programa que

recebe, mas tem significado para o programa que enviou. Dessa forma é utilizado como identificador.

Já um Web cookie serve para o servidor saber o estado e/ou informações adicionais sobre o usuário. Permite manter o usuário logado, manter informações sobre a atividade na página, e etc.

Um ataque com cookie seria utilizando man-in-the-middle para capturar o cookie de um usuário válido para se passar por ele e fazer atividades como se fosse ele sem que se saiba a senha ou algo do gênero.

7) O que é OWASP-Top-Ten?

Primeiro, OWASP é um projeto de deixar as aplicações web mais seguras através de produção de conteúdo voltado para orientar a mitigação de incidentes de segurança.

OWASP-Top-Ten é um dos subprojetos dessa comunidade, mantendo atualizado, sobre os 10 riscos mais comuns e mais críticos existentes em aplicações web espalhadas pelo mundo. Enumerando essa lista atualmente : Injection, Broken Auth, Sensitive Data Exposure, XXE, Broken Access Control, Misconfiguration, XSS, Insecure Deserialization, Packages with CVE, Lack of Logging and Monitoring.

8) O que é Recon e Por que ela é importante?

Recon é um jargão militar para a palavra reconhecimento. No contexto da segurança da informação significa extrair informações de um sistema que podem servir como vulnerabilidades.

É importante pois é necessário “reconhecer” a posição do alvo para poder “atirar” nele.

9) Command Injection (SO-Injection)

a) O que é Command Injection?
b) Mostre um exemplo de Command Injection(PoC da exploração)

10) SQL INJECTION
a) O que é SQL injection?
b) O que é Union Based Attack?
c) O que é Blind-SQL-I?
d) Mostre um exemplo de um Blind SQL-Injection (PoC da exploração).

11) XSS
a) O que é XSS?
b) Quais são os tipos de XSS? Explique-os.
c) Mostre um exemplo de um XSS Stored(PoC da exploração).
d) Mostre um exemplo de um DOM-XSS (PoC da exploração).

12) LFI , RFI e Path Traversal
a) O que é LFI?
b) O que é RFI?
c) O que é Path Traversal?
d) Como aliar Path Traversal e LFI
e) Mostre um exemplo de LFI utilizando acontaminação de LOGS (PoC da exploração).

13) CSRF e SSRF
a) O que e CSRF?
b) Mostre um exemplo de CSRF(PoC da exploração)
c) O que e SSRF?
d) Mostre um exemplo de SSRF(PoC da exploração)e)Como evitar ataques de CSRF?