TAG- Web Hacking
Nome: Mariane Ferreira

1) O que é o protocolo HTTP e Como ele funciona?
R: É um protocolo usado pela World Wide Web e é ele quem define como as páginas vão ser mostradas no navegador e quais decisões ele ou um servidor deve tomar ao receber um comando. O protocolo funciona da seguinte maneira: Você digita uma URL no seu navegador e ele envia um comando HTTP para o servidor mostrar a página que foi solicitada via URL.

2)O que é um Response Code? Cite um exemplo de um programa que você pode fazer com ele?
R: É uma mensagem de resposta que o protocolo HTTP retorna quando é solicitada uma requisição. Por exemplo, se o cliente solicita uma página e o servidor não consegue encontrá-la, o HTTP vai retornar um código de 4xx. Eu posso criar uma aplicação na qual exige-se que o usuário esteja logado para acessar determinada URL, e quem tentar acessar esta URL sem estar logado ou com credenciais inválidas, eu peço para o HTTP retornar um código 401 (Unauthorized).

3)O que é um HEADER? Cite um uso INSEGURO desse cabeçalho.
R: Um Header é onde fica as requisições feitas pelo user-agent ao host e os response code que são retornados após uma requisição. Um uso inseguro pode ser feito usando o Content-Location, que oferece uma localização alternativa aos dados que foram dados, muito utilizada em sites que tem versões com multi idiomas. Eu posso alterar a URL que foi imposta e colocar outra URL, uma de minha preferência.

4)O que é um Método HTTP? Explique o funcionamento do método POST, o funcionamento do método GET. Explique qual é considerado mais seguro e por que.
R: Método HTTP é uma requisição na qual é responsável por apontar qual ação deve ser realizada. O método POST é usado para enviar dados para um servidor, e ele envia através do corpo da requisição. O método GET é similar, porém envia os dados através do cabeçalho da requisição. A diferença é que, como o POST envia os dados pelo corpo da requisição, todos os dados enviados ficam ocultos ao usuário padrão, enquanto o GET, por enviar pelo cabeçalho, acaba por mostrar esses dados na URL, o que torna o POST um método mais seguro.

5)O que é Cache e como ele funciona? Cite os principais HEADERS de Request e Response responsáveis pelo controle de Cache.
R: É o armazenamento temporário de dados de páginas WEB no HD. Os navegadores guardam uma cópia dos arquivos no HD temporariamente, para não ter que carregá-los novamente na próxima vez que a página em questão for acessada novamente. Um dos principais HEADERS de cache é o Cache-Control.

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

R:É uma informação que a aplicação envia ao navegador do usuário. É armazenada localmente pelo navegador para ser enviada nas próximas requisições. Muito usadas em páginas que exigem autenticação, evitando que o usuário tenha que logar toda vez que sair/atualizar a página. Os principais ataques relacionado a Cookies são o CSRF e o Session Hijacking.

7) O que é OWASP-Top-Ten?
R: É uma página WEB que disponibiliza uma lista com os 10 principais riscos críticos existentes em aplicações.

8)O que é Recon e Por que ela é importante?
R: Recon é a abreviação de Reconnaissance, que basicamente faz o reconhecimento de força de uma determinada aplicação, coletando dados sobre a aplicação antes de fazer um pentest. É uma etapa importante, pois pode facilitar a exploração, já que através dela dá para se ter uma noção das brechas de segurança.

9)Command Injection (SO-Injection)
a) O que é Command Injection?
R: É um ataque no qual tem como objetivo executar ações no sistema operacional de um host através de uma brecha de segurança de uma determinada aplicação. Ele usa funções padrões da aplicação, sem necessidade de injetar códigos.
b)Mostre um exemplo de Command Injection (PoC da exploração)
R: Imagens 1 e 2 da pasta "command injection" (softwares utilizados: mutillidae e burp suite)

10) SQL INJECTION
a) O que é SQL injection?
R: É o ataque cujo o atacante consegue rodar códigos de SQL através das entradas de dados de uma aplicação, com o objetivo de roubar dados ou apagá-los
b)O que é Union Based Attack?
R:São comandos de SQL cujo o objetivo é recuperar dados da tabela de banco de dados, estendendo os resultados retornados pela consulta original.
c) O que é Blind-SQL-I?
R:É um ataque na qual o atacante faz perguntas true or false para o banco de dados, e determina a resposta de acordo com a resposta da aplicação
d)Mostre um exemplo de um Blind SQL-Injection (PoC da exploração).
R: Imagens 3 e 4 da pasta blind sql injection

11) XSS
a) O que é XSS?
R: É um ataque que insere códigos de Javascript nas entradas da aplicação e tem como objetivo enganar o usuário com informações falsas, para obter dados. Pode obter dados com formulários falsos ou com redirecionamento para sites maliciosos.
b)Quais são os tipos de XSS? Explique-os.
R: Reflected: O servidor da página WEB retorna o que o usuário digitou, sem filtrá-la. O código malicioso não é armazenado pelo site.

Stored: Semelhante ao Reflected, porém, é armazenado pelo site, para todos os usuários que visitá-lo, clicarem no link malicioso.
DOM: Executa todos os códigos maliciosos no navegador da vítima, sem ter contato com o servidor. Necessita de um componente especial no navegador para funcionar em tempo real.
c) Mostre um exemplo de um XSS Stored (PoC da exploração).
R:Imagens 5, 6 e 7 da pasta xss stored, detalhe para a imagem 7 com o usuário "anonymous", porém, sem nenhum comentário. Os script alert são executados toda vez que o usuário atualiza a página.
d)Mostre um exemplo de um DOM-XSS (PoC da exploração).
R:
https://192.168.1.105/mutillidae/index.php?page=password-generator.php&username=you%22;}catch(e){}var%20login%20=%20prompt%20(%22Digite%20seu%20login%20para%20gerar%20a%20senha%22);%20var%20senha%20=%20%20prompt%20(%22Digite%20sua%20antiga%20senha%20para%20gerar%20a%20nova%22);try{a=%22
O link (que não é acessível) mostra uma página para um gerador de senhas (imagem 8 da pasta dom xss). Ao clicar no link, o usuário é solicitado a colocar o login e a senha antiga para gerar a nova senha. o usuário não consegue entrar no gerador sem colocar os dados solicitados (imagens 9 e 10).

12) LFI , RFI e Path Traversal
a) O que é LFI?
R:É um ataque na qual é possível ter acesso a dados privados e inserir novos arquivos no site, através da própria URL.O arquivo está hospedado localmente pode ter um código malicioso incluído, que será executado assim que estiver no site.
b)O que é RFI?
R: É um ataque semelhante ao LFI, a diferença é que o arquivo pode estar hospedado remotamente e não localmente, para ser incluído no site.
c) O que é Path Traversal?
R:É o envio de arquivos para o site/servidor, com scripts cujo o objetivo é encontrar uma URL na qual será possível fazer a exploração de arquivos do alvo.
d)Como aliar Path Traversal e LFI
R: Pode-se enviar um arquivo localmente (LFI), com scripts que procuram uma URL para fazer a exploração de arquivos em um ataque Path Transversal.

13) CSRF e SSRF
a) O que e CSRF?
R: É falsificar uma requisição de um site,roubando dados da sessão de um usuário legítimo para burlar a autenticação.
b)Mostre um exemplo de CSRF (PoC da exploração)
R: Na imagem 11 (pasta csrf) o usuário loga com seu login e senha, mas a conexão é interceptada pelo burp suite (imagem 12), contendo o login e a senha do usuário. Para logar sem digitar os dados na página, o atacante intercepta o site (imagem 13) , clona a requisição bem sucedida e dá forward com a nova requisição e consegue logar sem digitar os dados (imagem 14).
c) O que e SSRF?

R: É semelhante ao CSRF, só que a falsificação é feita através de um servidor vulnerável.
e)Como evitar ataques de CSRF?
R: Implementando uma verificação por Token, que gera um código aleatório que é solicitado ao realizar o login,como por exemplo, em aplicativos de bancos.

Observações:
*A letra "e" do exercício 12 e a letra "d" do exercício 13 não foram feitos, pois eu não tinha ideia de como fazê-los.
*As respostas estão curtas, pois li uns livros e fiz pesquisas na internet e tentei escrever um resumo do que eu entendi.