Lista de exercícios – 1

**Disciplina**: Segurança de aplicações web.

**Professor**: Henrique Arcoverde.

**Aluno:** Marcelino Soares.

1. – Escreva um parágrafo descrevendo com suas palavras o que é segurança e como ela se aplica no contexto de aplicações web.

R: Segurança tem como meta garantir que o funcionamento da aplicação esteja exatamente como especificado. Verifica também se o software se comporta adequadamente mediante as mais diversas tentativas ilegais de acesso, visando diminuir e prever possíveis vulnerabilidades.

1. – Escolha, cite e explique 3 princípios básicos de segurança vistos em sala de aula.

R: Minimize a superfície de ataques - Diminuir ponto de vulnerabilidade do sistema.

Habilite as opções segurança por padrão - Sempre habilitar o modo de segurança do sistema.

Negue por padrão - Negar todas as permissão de usuário por padrão no sistema.

1. – Descreva, da forma mais detalhada que conseguir, o que acontece do momento em que um usuário acessa uma URL no browser até a página ser exibida.

R: O browser formata a solicitação e faz o envio ao servidor, que encontra a página solicitada, o servidor formata a resposta e envia para o browser, que resgata o HTML e compila no formato visual para o usuário.

1. – Explique qual o papel de um servidor web.

R: Responsável por atender a todas as requisições HTTP feitas para um endereço via browser na internet.

1. – Cite 3 exemplos de linguagens/tecnologias de programação geralmente utilizadas para o desenvolvimento de aplicações web.

R: java,php e ruby.

1. – Verdadeiro ou falso? O código PHP de uma aplicação web é executado pelo navegador do usuário após o recebimento de uma resposta HTTP. Justifique sua resposta.

R: Falso. É executado pelo lado do servidor web.

1. – Verdadeiro ou falso? O código HTML/JavaScript é tipicamente executado pelo navegador do usuário após o recebimento de uma resposta HTTP. Justifique sua resposta.

R: Verdadeiro. É executado da parte do cliente.

1. – Qual o protocolo da camada de aplicação utilizado por aplicações web?

R: HTTP.

9 – Qual a porta padrão utilizada por servidores web?

R: 443.

1. – Escreva como seria a requisição (request) HTTP gerada por um navegador no momento em que o usuário digita a seguinte URL no navegador: [http://ararwweeaas.com/ssa.sd?p1=rreeww.](http://ararwweeaas.com/ssa.sd?p1=rreeww)

R: GET /ssa.sd?p1=rreeww HTTP/1.1

Host: ararwweeaas.com

1. – Escreva como seria uma possível resposta (response) HTTP relativa a requisição escrita na questão 10.

R: HTTP/1.1 403 Forbidden

Date: Wed, 29 Oct 2020 07:28:00 GMT

1. – Cite e explique 2 métodos (verbos) HTTP.

R: GET, Solicita a representação de um recurso específico. Requisições utilizando o método GET devem retornar apenas dados.

HEAD, Solicita uma resposta de forma idêntica ao método GET, porém sem conter o corpo da resposta.

1. – Explique a diferença entre as famílias de código HTTP 2xx e 3xx.

R: 2xx é codigos de sucesso e 3xx é redirecionamento.

1. – Explique o que significa o problema da falta de estado do protocolo HTTP. Exemplos são bem-vindos.

R: É um protocolo de comunicação que considera cada requisição como uma transação independente que não está relacionada a qualquer requisição anterior, de forma que a comunicação consista de pares de requisição e resposta independentes. Exemplos HTTP ou um servidor FTP.

1. – Qual o mecanismo tipicamente utilizado para resolver o problema da falta de estado no protocolo HTTP?

R: Cookie.

1. – Dentro do contexto de aplicações web, o que significa “sequestro de sessão”?

R: acesso indevido ao cookie de outro usuário na aplicação web.

1. – Para que serve a flag secure e o atributo HttpOnly?

R: A flag secure indica ao navegador que um cookie marcado como Secure deve ser enviado exclusivamente através de um canal de comunicação criptografado (HTTPS).

HttpOnly garante que os cookies não serão acessíveis através de mecanismos client-side como JavaScript, Flash, Applet, etc.

1. – Qual a diferença entre os protocolos HTTP e HTTPS.

R: HTTP é um código responsável por fazer a comunicação entre os dados de uma página na internet e o computador ou dispositivo que está fazendo o acesso.

HTTPS é o protocolo apresenta uma camada SSL. Trata-se de um adicional que possibilita que os dados sejam transmitidos de forma criptografada.

1. – Instale, configure e utilize o Burp Suite (<https://portswigger.net/burp/communitydownload>). Envie screenshots para ilustrar o fato.
2. – Capture uma requisição HTTP utilizando o Burp Suite e altere sua resposta de modo a incluir um HTML/JavaScript de sua autoria.
3. – Para que serve um CAPTCHA?

R: Para diferenciar humano de máquina, prevenindo ataques por meio de spam e descriptografia de senhas.

1. – Explique de maneira dissertativa qual o problema do session fixation.

R: Consiste na não renovação do cookie de sessão após a autenticação. No mo momento que uma página é acessada e efetua a transição da navegação para autenticação em web commerces, por exemplo.

1. – Uma aplicação que viabiliza a distinção entre usuários cadastrados e não cadastrados está suscetível a que tipo de vulnerabilidade?

R: session fixation.