Lista de exercícios – 1

**Disciplina**: Segurança de Aplicações web (Testes de Segurança).

**Professor**: Henrique Arcoverde.

**Aluno:** Alan Garcia.

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

R: Promover garantindo que a aplicação esteja em normalidade no seu funcionamento da forma como a mesma fora projetada. Analisando seu comportamento com intuito de prevenir e se possível se antever a ataques, de maneira que possa verificar as possíveis vulnerabilidades para minimizar a superfície de ataque.

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

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

Minimize a Superfície de Ataques – Verificar e diminuir os possíveis pontos de   
 vulnerabilidade do sistema com medidas protetivas para possíveis ataques.

Habilitar Opções de Segurança por Padrão - Sempre habilitar o modo de segurança

padrão do 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: Após a confirmação do site na barra de endereço supondo que não há erro de digitação, a solicitação é enviada ao servidor após ter sido formatada pelo browser, o servidor ao encontrar a página solicitada e após formatá-la, envia a resposta para o navegador (browser), e esse (browser/navegador) por sua vez recebe a resposta do servidor resgatando o HTML que será compilado no formato para visualização do usuário.

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

R: Responder aos requests (requisições) HTTP feitas para um site/endereço da internet via web browser (navegador).

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

R: C# , php , java, ruby, python.

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. O código php que desenvolveu a página da web será executado no 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. Após o envio e o processamento de resgate do código para exibição do HTML, que se dará na 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 é o verbo que passa variáveis por URL, é útil para você compartilhar uma página de produto, fazer paginação, etc. Ou seja, você pode reproduzir uma busca apenas copiando a URL, já que as variáveis estão nela. Podemos dizer ainda que o método GET vai requisitar/pegar os dados que devem ser retornados mediante solicitação.

POST é o verbo que fora projetado para solicitar que o servidor web aceite os dados anexados no corpo da mensagem de requisição para armazenamento. Comummente usado quando se efetua um upload de um arquivo ou envio de formulário completamente preenchido. Podemos dizer ainda que POST vai incluir/criar uma nova informação ou um novo dado.

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

R: 2xx indica que a solicitação foi entendida e recebida e que será processada com sucesso pelo servidor. 3xx indica que haverá redirecionamento, acontece geralmente quando a página fora alterado.

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

R: Ocorre devido a comunicação que considera cada requisição como uma transação independente que não está relacionada a qualquer requisição anterior, ou seja conhecido também por ser stateless (seme estado, estático), 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 em uma aplicação. Geralmente aplicações web, ou que transitam seu funcionamento pela 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 e transitar exclusivamente por meio de comunicação criptografado (HTTPS). O marcador HttpOnly faz com que o conteúdo do cookie não seja disponibilizado para o engine JavaScript, sendo apenas transitado no cabeçalho da requisição HTTP. Prevenindo que os cookies não serão acessíveis por meio de mecanismos client-side (executadas no lado do cliente/navegador), como por exemplo: Flash, JavaScript, etc.

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

R: Hypertext Transfer Protocol Secure, ou seja HTTPS, é uma versão idêntica do protocolo HTTP sobre uma camada SSL. Essa camada adicional permite que os dados sejam transmitidos através de uma conexão criptografada e que se verifique a autenticidade do servidor e do cliente através de certificados digitais.

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: Além de ser também uma medida de segurança conhecido como autenticação por desafio e resposta, a serventia principal da CAPTCHA é diferir entre humanos e máquinas.

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

R: Decorre na não renovação do cookies que acontece na maioria das vezes ao acessar uma aplicação web, por exemplo: transitar entre nevegar para logado. Ou seja, quando se navega e posteriormente se faz login, o cookie pode não ser renovado ficando mais vulnerável ao sequestro de sessão. Então o atacante pode tirar proveito disso fixando a sessão (session fixation).

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

R: Session Fixation.