TAG Web Hacking

Nome: Thalles Nonato

- questões de poc estarão em pastas diferentes

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

R: O protocolo HTTP, abreviação de Hyper Text Transfer Protocol é um protocolo de comunicação, que atua na camada de aplicação (segundo o modelo OSI) que determina e define os padrões e regras de trocas de informações entre servidores que abrigam sites e computadores. O protocolo http funciona da seguinte forma, ele segue o modelo de request e response, ou seja, pedido e resposta. Basicamente o usuário clica em um link do browser, o navegador, por sua vez, formata a solicitação e faz o envio ao servidor e o servidor encontra a pagína solicitada. Depois disso, o servidor formata a resposta e envia ao browser, por fim, o browser resgata o HTML e compila em formato visual para o usuário.

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

R: O Response Code é uma resposta que o HTTP retorna após uma requisição. Um dos Responses Codes mais conhecidos é o “203 Non-Authoritative Information”, ela indica que a requisição foi realizada com sucesso porém o conteúdo foi modificado por um proxy da resposta com status 200(OK) do servidor de origem. Um dos programas mais conhecidos que se podem fazer com o Response Code são os leitores de QR Code (Quick Response Code), que são códigos de barra que podem ser facilmente escaneados usando a maioria dos telefones celulares equipados com câmera.

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

R: Os códigos de status HTTP são entregues ao seu navegador no header HTTP. Ele tem a parte de requisição que é feita pelo user-agent ao host e tem a parte da resposta que é a mensagem retornada referente a requisição com um

código de status. Os Headers são divididos em 3 grupos: o header geral, de requisição e entidade. O Header é o local para se passar informações adicionais sobre a requisição e o servidor pode responder de modo diferente dependendo dos campos e valores contidos nele. Um uso inseguro de algum desse cabeçalhos é a ausência do Header “X-Content-Type-Options", isso porque alguns navegadores tentam deduzir o tipo dos dados retornados pelo servidor para tratá-los de forma específica. Isso pode resultar na interpretação incorreta dos dados e favorecer ataques de Cross-Site Scripting (XSS).

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: Os métodos indicam para o servidor qual ação que o usuário deseja realizar. Quando realizamos uma requisição obrigatoriamente precisamos de um método. O método POST é usado quando o usuário deseja enviar dados para processamento ao servidor, como os dados de um formulário, por exemplo. O método GET é usado quando o cliente deseja obter recursos do servidor. O método POST é considerado mais seguro por passar dados invisíveis ao usuário.

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

R: Cache pode ser entendido como uma área de armazenamento onde dados ou processos usados frequentemente são armazenados para um acesso futuro mais rápido, economizando tempo e uso desnecessário do hardware. Entre os principais cache headers temos o cache-control .

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

R: Cookies são arquivos em textos armazenados pelo navegador do lado cliente, que guarda uma série de informações sobre o visitante e a sua navegação pelas páginas de um site, ou domínio, ele só armazena o que o usuário disponibilizou durante a navegação de um site. Os principais ataques são o CSFR e os Sesssion Hijacking , também conhecido como sequestro de cookie.

7) O que é OWASP-Top-Ten?

R: O Top 10 da OWASP é um documento de conscientização padrão para desenvolvedores e segurança de aplicativos da web. Representa um amplo consenso sobre os riscos de segurança mais críticos para aplicativos da Web.

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

R: O ataque de Recon é um tipo de coleta de informações no sistema de rede e serviços de maneira negativa / roubo. Um conjunto de processos e técnicas (Footprinting, Scanning , etc) usados para descobrir e coletar secretamente informações sobre um sistema de destino, muito utilizado em pentests. Sua importância se dá pelo fato de podermos achar as vulnerabilidades e erros de segurança mais facilmente fazendo a coleta dessas informações.

9) Command Injection (SO-Injection)

a) O que é Command Injection?

R: Command Injection é um ataque no qual o objetivo é a execução de comandos arbitrários no sistema operacional host por meio de um aplicativo vulnerável. Os ataques de injeção de comando são possíveis quando um aplicativo passa dados inseguros fornecidos pelo usuário (formulários, cookies, cabeçalhos HTTP etc.

b) Mostre um exemplo de Command Injection (PoC da exploração)

10) SQL INJECTION

a) O que é SQL injection?

R: SQL Injection é uma técnica de ataque baseada na manipulação do código SQL, que é a linguagem utilizada para troca de informações entre aplicativos e bancos de dados relacionais.

b) O que é Union Based Attack?

R: O Union Based Attack é uma técnica de injeção de SQL em banda que utiliza o operador UNION SQL para combinar os resultados de duas ou mais instruções SELECT em um único resultado, que é retornado como parte da resposta HTTP.

c) O que é Blind-SQL-I?

R: Blind-SQL-I é um tipo de ataque SQL injection que faz perguntas verdadeiras ou falsas ao banco de dados e determina a resposta com base na resposta dos aplicativos.

d)Mostre um exemplo de um Blind SQL-Injection (PoC da exploração).

11)) XSS

a) O que é XSS?

R: Os ataques XSS (Cross-Site Scripting) são um tipo de injeção, na qual scripts maliciosos são injetados em sites benignos e confiáveis. Os ataques XSS ocorrem quando um invasor usa um aplicativo da Web para enviar código malicioso, geralmente na forma de um script do lado do navegador, para um usuário final diferente.

b) Quais são os tipos de XSS? Explique-os.

R: XSS Reflected, Stored e DOM.

XSS Reflected: O XSS refletido ocorre quando um invasor injeta código executável do navegador em uma única resposta HTTP. O ataque injetado não é armazenado no próprio aplicativo.

XSS Stored: Um ataque de XSS Stored é quando a carga útil do ataque é armazenada em algum lugar e recuperada conforme os usuários visualizam os dados de destino. Enquanto um banco de dados é esperado, outros mecanismos de armazenamento persistentes podem incluir caches e logs que também armazenam informações por longos períodos.

XSS DOM: XSS baseado em DOM significa simplesmente uma vulnerabilidade de script entre sites que aparece no DOM (Document Object Model) em vez de parte do HTML. Nos ataques reflexivos e armazenados de script entre sites, é possível ver a carga útil da vulnerabilidade na página de resposta, mas nos

scripts entre sites baseados em DOM, o código-fonte HTML e a resposta do ataque serão exatamente iguais, ou seja, a carga útil não pode ser encontrada em a resposta. Isso só pode ser observado em tempo de execução ou investigando o DOM da página.

c) Mostre um exemplo de um XSS Stored (PoC da exploração).

d)Mostre um exemplo de um DOM-XSS (PoC da exploração).

12)

a) O que é LFI?

R: LFI é o processo de inclusão de arquivos, que já estão presentes localmente no servidor em questão, através da exploração de processos de inclusão vulneráveis, implementados na aplicação web.

b) O que é RFI?

R: RFI é um método que permite que um invasor empregue um script para incluir um arquivo hospedado remotamente no servidor da web

c) O que é Path Traversal?

R: É um ataque utilizado por atacantes para obter acesso não autorizado a arquivos e diretórios, e através da sua exploração é possível comprometer completamente o servidor onde a aplicação se encontrar.O Path Traversal é o resultado da falta ou insuficiência de validações de entrada de usuários na aplicação (direto pelo browser).

d)Como aliar Path Traversal e LFI

R: O invasor pode obter o conteúdo de um arquivo que contém uma lista de usuários no servidor. E com isso, o invasor pode aproveitar a vulnerabilidade do Path Traversal para acessar arquivos de log.

e) Mostre um exemplo de LFI utilizando a contaminação de LOGS (PoC da exploração)

13) CSRF e SSRF

a) O que e CSRF?

R: CSRF é um tipo de ataque que ocorre quando um site, email, blog, mensagem instantânea ou programa mal-intencionado faz com que o navegador da web do usuário execute uma ação indesejada em um site confiável quando o usuário é autenticado.

b) Mostre um exemplo de CSRF (PoC da exploração)

c) O que e SSRF?

R: No SSRF, o invasor pode abusar da funcionalidade no servidor para ler ou atualizar recursos internos. O invasor pode fornecer ou modificar um URL para o qual o código em execução no servidor lerá ou enviará dados e, selecionando cuidadosamente os URLs, o invasor poderá ler a configuração do servidor.

d)Mostre um exemplo de SSRF (PoC da exploração)

e) Como evitar ataques de CSRF?

R: Uma das defesas mais famosas do CSRF é fazer o uso de Anti-CSRF Tokens em requisições de maior relevância.