Controle de Acesso Quebrado

Uma vulnerabilidade de controle de acesso interrompida refere-se a uma falha no design da aplicação da Web em que o acesso não autorizado a um objeto sensível (como um diretório ou registro) é aplicado de forma inadequada ou insuficiente. Por exemplo, pode ser que qualquer usuário anônimo possa exibir determinados arquivos em um site simplesmente sabendo qual URL solicitar; ou a aplicação pode executar uma função que pressupõe que algum nível de autenticação ou autorização tenha ocorrido sem primeiro confirmar que é esse o caso

Verificar as permissões de usuário no nível do objeto de dados

Este mecanismo resolve o problema primário causador da vulnerabilidade: verificação de acesso ausente ou insuficiente. Não se deve confiar somente nas validações do lado do cliente, pois elas podem facilmente ser contornadas.

Ao implementar controles de acesso do lado do servidor, é relativamente óbvio adicionar verificações de autorização no nível de funcionalidade ou de rota. Um problema comum que causa essa vulnerabilidade são verificações de acesso ausentes para proteger contra IDs manipulados em URLs. É necessário aplicar controles de acesso aos dados verificando se o usuário requisitante é proprietário ou tem permissões para acessar os dados solicitados.

A aplicação deve também executar validação sintática para verificar entradas suspeitas – estabelecer critérios para os dados de entrada e rejeitá-los se os critérios não são atendidos. Exemplos: tamanho mínimo ou máximo, intervalo (para valores numéricos), tipos de dados, caracteres aceitáveis, etc. [Oreilly, 2022].

Evite expor referências diretas aos objetos

No lugar de solicitar as referências na URL, use a informação já presente na sessão do usuário do lado do servidor para localizar os recursos a prover. No exemplo do perfil 132355, se os usuários são permitidos a ver apenas os próprios perfis, podemos utilizar o ID de sessão do usuário conectado para o localizar, eliminando assim a necessidade de passar o ID como parâmetro [Oreilly, 2022].

Usar mapeamento de referências indiretas

Se não é possível evitar a exposição das referências na URL, a técnica do mapeamento de referências indiretas é útil. A ideia por trás desse método é substituir a referência direta na URL por um valor aleatório que seja difícil de prever (tal como um GUID) ou específico apenas para o usuário conectado.

O mapeamento de referências indiretas armazena as relações entre a referência interna de um objeto e a referência indireta correspondente que é exibida na URL. Voltando ao exemplo do perfil: ao invés de usar uma referência direta, como example.com/profile.php?id=132355, pode ser usada uma

referência indireta como example.com/p/kjbEEc24jkLUvAKJhv0p. Esse mapeamento deve ser mantido em um local seguro no servidor [Oreilly, 2022].

Protegendo contra travessia de diretório

Para se prevenir contra esse ataque, é necessário tomar providências no nível de configuração do sistema e também no nível de aplicação [Oreilly, 2022]:

- No nível de sistema, configure o diretório raiz e a lista de controle de acesso para confinar o acesso do usuário e restringir acesso a arquivos fora da raiz da página web;
- No código, faça validação de entrada do usuário para prevenir caracteres correspondentes à travessia de diretório.