SUMÁRIO

1. SEGURANÇA PHP: FERRAMENTAS AUXILIARES

Para lidar com as mais variadas demandas de um aplicativo seguro, além de paradigmas, técnicas e metodologias, existem ferramentas automatizadas que abstraem a necessidade de realizar todos os procedimentos manualmente.

Esse documento irá abordar esse tipo de ferramenta, cujo objetivo é exatamente ajudar os desenvolvedores a reduzir as vulnerabilidades do sistema, bem como ofertar formas melhores de realizar alguns procedimentos, como armazenamento de dados sensíveis.

Existem muitas tecnologias disponíveis no mercado para suprir essas demandas. Elas podem ser gratuitas, pagas ou de código aberto. A maioria das ferramentas gratuitas e de código aberto estão disponíveis no GitHub.

2. FERRAMENTAS DE VERIFICAÇÃO DE VULNERABILIDADES

Os scanners de vulnerabilidade têm suas maneiras de fazer trabalhos. São ferramentas que detectam brechas de segurança no escopo do código, do banco de dados, do servidor, sistema operacional, da rede etc.

Para ler mais sobre ferramentas de análise de vulnerabilidades, clique aqui.

2.1.1. PHP MALWARE FINDER (PMF) – ANÁLISE DO CÓDIGO E ARQUIVOS

PHP-malware-finder faz o seu melhor para detectar código ofuscado / duvidoso, bem como arquivos usando funções PHP frequentemente usadas em malwares / webshells.

Clique aqui para acessar a ferramenta no Github.

2.1.2. RIPS – ANÁLISE DO CÓDIGO

O RIPS é um software de análise de código estático para a detecção automatizada de vulnerabilidades de segurança em aplicativos PHP e Java.

Seu desenvolvimento original foi abandonado desde 2013, devido a algumas de suas limitações fundamentais, dando lugar a uma nova versão paga, totalmente reformulada e adaptada para os tempos atuais.

Clique aqui para acessar o site da ferramenta.

2.2. NIKTO2 – ANÁLISE DO SERVIDOR

O Nikto2 é um software de verificação de vulnerabilidades de código aberto que se concentra na segurança de servidores aplicativos da web. Ele pode alertar sobre problemas de configuração do servidor e executar verificações de servidor da Web em um tempo mínimo.

O Nikto2 não oferece nenhuma contramedida para vulnerabilidades encontradas, nem fornece recursos de avaliação de risco.

Clique aqui para acessar o site da ferramenta.

3. FERRAMENTAS PARA ARMAZENAR DADOS SENSÍVEIS

Um aplicativo depende de muitos recursos para funcionar corretamente, como bancos de dados, APIs de terceiros, ferramentas de registro e monitoramento e muito mais.

No estado de execução, ou, no ambiente de produção, esses recursos dependem de dados para funcionar, e que são confidenciais, isto é, que não ser vistos e acessados por qualquer usuário, porque, se assim ocorre, a aplicação pode ser comprometida. Exemplos desse tipo de dados são as senhas dos usuários, chaves criptográficas, Tokens OAuth etc.

Existem muitas maneiras de armazenar essas informações. Normalmente, essas elas são armazenadas em arquivos de configuração do aplicativo. Uma prática já comentada em outros documentos, é a utilização do **arquivo .env** fora da pasta pública, ou com acesso restringido por meio do arquivo .htaccess.

Mas essa abordagem, apesar de não expor os dados no código da aplicação, e não permitir que o arquivo seja acessado pela URL, via HTPP, ainda persiste dados sensíveis no local, isto é, na máquina. Eles podem ser acessados por, por exemplo, usuários do computador, ou até mesmo por atacantes que consigam invadir o seu sistema de arquivos de alguma forma.

Para resolver essa situação, o que muitos fazem é criptografar esses arquivos, o que, de certa forma, é uma solução redundante, porque para acessar o arquivo ainda será necessária uma chave criptográfica que será deverá ser persistida.

3.1.1. VAULT DA HASHICORP

O Vault da Hashicorp é uma **ferramenta projetada para armazenar e acessar os dados confidenciais** do aplicativo com segurança. Isso nos ajuda a construir um serviço centralizado de gerenciamento de segredos. O Vault pode gerar os segredos, criptografar os dados, limitar o acesso aos dados armazenados e pode ajudar na revogação do acesso.

É muito importante para qualquer empresa saber quem está acessando os segredos e torna-se difícil implementar com as abordagens mencionadas acima. O Vault resolve esse problema coletando e publicando registros de auditoria. Os logs de auditoria conter requeste responseobjeto de cada interação com o Vault.

Além disso, o Vault permite reter um número configurável de versões secretas. Isso permite que os dados das versões mais antigas sejam recuperados em caso de exclusão indesejada ou atualizações dos dados. Além disso, suas operações de verificar e definir podem ser usadas para proteger os dados de serem sobrescritos acidentalmente.

Além de conceder acesso a um recurso, também é importante revogar o acesso. O Vault torna isso muito fácil, dando um contrato a alguns tipos secretos. O usuário pode consumir dados pelo período válido ou Time-To-Live (TTL) especificado no lease e, uma vez expirado, o acesso é revogado automaticamente.

Clique aqui para acessar o site oficial da ferramenta. No site existe a documentação completa da ferramenta.

FONTES

https://dicasdeinfra.com.br/17-melhores-ferramentas-de-verificacao-para-avaliacao-de-vulnerabilidades/

https://faun.pub/vault-securely-manage-sensitive-data-3a528e3c18f8