Ciência da Computação / Sistemas de Informação

Estudo e proposta de diretrizes de segurança contra vulnerabilidades relacionadas à verificação de acesso à URLs para sistema para aplicação de avaliações no contexto de ensino de algoritmos.

Jonatha Levi Dos Santos Lustosa - 7° módulo de Engenharia de Controle e Automação, UFLA, iniciação científica voluntária PIVIC/UFLA, bolsista PIBIC/CNPq.

Joaquim Quinteiro Uchôa - Orientador DCC, UFLA. - Orientador(a)

Resumo

O projeto Vesperto, um Ambiente Virtual de Aprendizagem em desenvolvimento, tem como objetivo favorecer um maior aprendizado dos alunos no desenvolvimento de algoritmos. Para garantir uma plataforma mais segura para usuários e para aplicação de atividades avaliativas, é necessário um controle de anexos para o Vesperto. Para agilizar o desenvolvimento, este controle deverá ser baseado em soluções adotadas em outra plataforma que já demonstrado eficácia nessa tarefa. Tendo em vista esta situação, foram traçados alguns métodos para o desenvolvimento do trabalho, inicialmente o levantamento de algumas plataformas e foram selecionadas duas de código aberto, Moodle e Drupal, a fim de descobrir como é feito o gerenciamento de anexos através de documentação ou código-fonte. Além disso, outro ponto essencial consistiu no estudo das diretrizes de segurança da OWASP, para que a análise da segurança das plataformas selecionadas pudessem se guiar por parâmetros comparativos. Após a análise, foi possível verificar que o Moodle faz o controle de acesso de anexos por meio de uma função de reescrita de URL, aplicando um hash criptográfico no nome do anexo presente na URL, impedindo o acesso indevido por usuários não pertencentes ao sistema. De outra parte, a documentação do Drupal não faz a descrição de como é realizada tal gerenciamento de anexos. Na sequência, foram feitas as instalações do Drupal e do Moodle em um Servidor Ubuntu a fim de fazer os testes práticos, seguindo o Guia de Testes de Segurança da OWASP. O primeiro ponto de análise prática foi o de enumeração de URLs, e foi observado pequenas diferenças entre ambas, sendo que o logout do sistema por determinado tempo de inatividade e a exigência de uma senha contendo um nível de complexidade mínima para o cadastro de um novo usuário no sistema, são aspectos presentes no Moodle, e ausentes no Drupal. Contudo, foi possível identificar que é feito o controle de acesso nos dois AVAs, através de testes para verificar se a Falha de Restrição de Acesso à URLs era uma vulnerabilidade presente nas plataformas, e foi constatado que o gerenciamento de acesso aos anexos, e o gerenciamento de sessão de usuário é realizada com êxito. Portanto , esses ambientes apresentaram formas seguras de gerenciamento de anexos. Em continuação dos trabalhos, encontra-se a tarefa de verificar o funcionamento do controle de acesso a anexos nesses ambientes, para desenvolvimento de uma biblioteca em Flutter para uso no Vesperto.

Palavras-Chave: controle de acesso a anexos, algoritmos, segurança da informação.
Instituição de Fomento: Conselho Nacional de Desenvolvimento Científico e Tecnológico - CNPq

Link do pitch: https://youtu.be/b9u4zZ2Fzvo