

Não sei

Alexandre Yuji Kajihara

2017

1 Introdução

Atualmente, os sistemas estão migrando para Web [1] e são implementados com *bugs* de software críticos que podem ser explorados de forma maliciosa [2]. Com isso as aplicações Web estão sujeitos a ataque de hackers, tentando obter acesso não autorizado ou acessar informações privadas [2]. Uma das técnicas de ataque mais populares é a de injeção SQL em que se as consultas não forem validados, os atacantes podem ter acessos a dados não autorizados, inserir e excluir dados, e até páginas de erro podem revelar qual banco de dados está sendo utilizado e as tabelas presentes [1]. Para prevenir ataques desse tipo, existem técnicas que obrigam o cliente a inserir dados corretos e que podem ser descobertos quando forem inseridos valores ilegais [2]. Além do que, desenvolvedores podem aplicar melhores práticas de codificação ou executar testes de penetração para prevenir ataques em aplicações Web [2]. Necessariamente, também existem alguns testes que podem ser feitos como o teste da caixa branca em que se analisa códigos, porém se feito de forma exaustiva pode ser difícil e não encontrar todas as falhas [2]. Já no teste da caixa preta são testes de penetração, em que o scanner pode não reconhecer os componentes internos da aplicação Web. Porém, queremos prevenir possíveis e detectar possíveis ataques [2].

Referências

- [1] Angelo Ciampa, Corrado Aaron Visaggio, and Massimiliano Di Penta. A heuristic-based approach for detecting SQL-injection vulnerabilities in web applications. In *2010 ICSE Workshop on Software Engineering for Secure Systems - SESS*. ACM, 2010.
- [2] Marco Vieira, Nuno Antunes, and Henrique Madeira. Using web security scanners to detect vulnerabilities in web services. In *2009 IEEE/IFIP International Conference on Dependable Systems & Networks*. IEEE, jun 2009.