Apresentação de Pentest

SQL Injection

IFES - Santa Teresa, 2019

O que é?

O 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.

É uma classe de ataque onde o invasor pode inserir ou manipular consultas criadas pela aplicação, que são enviadas diretamente para o banco de dados relacional via query.

Por que funciona?

Por que a aplicação aceita dados arbitrários fornecidos pelo usuário (“confia” no texto digitado);

O código se torna vulnerável porque não realiza nenhum tipo de validação nos dados que foram digitados pelo usuário. Isso permite que um usuário mal intencionado, que saiba manipular querys, consiga “burlar” a digitação dos campos de login, ou qualquer outro formulario e até mesmo uma URL.

Como evitar?

Uma forma de evitar as injeções é bloquear caracteres perigosos (ou seja, barra invertida, apóstrofo e ponto e vírgula). Existem algumas formas de evitar a inserção de dados hostis pelo usuário, no PHP, uma delas é utilizando a função preg_replace(), como no exemplo a baixo:

- `$senha = preg_replace( ‘/[^[:alpha:]_]/’ , “ , $valorInserido);`

Curiosidade

Em 2011 o site oficial do MySQL (mysql.com) sofreu um ataque de SQL Injection. Os crackers conseguiram realizar o ataque com sucesso, roubando vários dados, inclusive divulgaram as informações de login de um Diretor de produtos, cujo a senha tinha apenas 4 digitos.

Obrigado!

Rai Bizerra Maciel
Benito Marculano
Flávio Gonçalves

Link do código usado no exemplo:
https://github.com/raibm/SQL-INJECTION-PHP