

SQL Injection

Are Your Web Applications
Vulnerable?

SQL Injection: Are Your Web Applications Secure?

- SQL Injection
 - Técnica que explora aplicações web que utilizam dados enviados por usuários.

SQL Injection: Are Your Web Applications Secure?

- Tipos mais comuns de ataque
 - SELECT
 - Tenta visualizar os dados utilizando consulta simples com cláusula WHERE.
 - UNION SELECT
 - Tenta visualizar os dados fazendo a SELECT original ser ignorada ou não retornar nenhum resultado, e forçando a execução da *query* injetada.
 - INSERT
 - Similar à WHERE, mas trabalha diretamente com a inserção dos dados.
 - Mais detectável.

SQL Injection: Are Your Web Applications Secure?

- Como evitar
 - Sanitizar as instruções SQL
 - Prefixar e Sufixar as entradas de usuários com aspas.
 - Converter caracteres especiais em seus correspondentes em HTML
 - Limitar os privilégios do usuário utilizado pela aplicação web
 - Criar *stored procedures* para as funções necessárias à aplicação.

SQL Injection: Are Your Web Applications Secure?

- *Stored Procedure*
 - Geralmente considerada o final do beco-sem-saída das injeções
 - O autor não conhece nenhum meio de efetuar as injeções quando são enviadas para as *stored procedures*.

SQL Injection: Are Your Web Applications Secure?

- Injeção de *Stored Procedures*
 - Mais fáceis do que injeções regulares
 - Algumas dão acesso diretamente ao *shell* do banco.
 - Algumas exibem o resultado em forma de páginas web
 - A maioria não retorna o resultado, como as injeções regulares

SQL Injection: Are Your Web Applications Secure?

OI, AQUI É DA ESCOLA
DO SEU FILHO.
ESTAMOS TENDO UM
PROBLEMA COM OS
COMPUTADORES.



ORIGINAL: XKCD.COM

AI MEU DEUS - ELE QUE-
BROU ALGUMA COISA?
MAIS OU
MENOS -



TRADUÇÃO LIVRE TIRINHAS.COM

VOCÊ DEU MESMO AO
SEU FILHO O NOME DE
Roberto'); DROP TABLE
Alunos; -- ?



AH, SIM. O
CHAMAMOS DE
BETINHO
TABLES.

BOM, PERDEMOS TODOS
OS DADOS DOS ALUNOS
DESTE ANO. ESPERO QUE
ESTEJA FELIZ.



E EU ESPERO QUE
VOCÊS TENHAM
APRENDIDO A
SANITIZAR AS
ENTRADAS DOS
SEUS BANCOS
DE DADOS.