



Procedimentos de segurança para evitar SQL Injection no Firebird

Luiz Paulo de Oliveira Santos

LPAULO@HARDSQL.COM.BR





Principais incidentes

Quem ataca?

Quem defende?

O que deve ser observado?





Descrição

Técnicas

Vítimas

Ataques

Quem ataca?

Como funciona?





Partes do SQL Injection
Ítems para implementar
O que é necessário?





Que bancos são susceptíveis

Principal agente: Linguagens

Script ou Compilado?

Entrada de dados – o principal caminho





Ítems à observar

Ítems à bloquear

O que verificar?

Exemplo de ferramentas: NESSUS





O que validar?

Como validar?

Principais Injections





Exemplo de código SQL

Exemplo de código PHP

Exemplo de injection



SQL Injection – Como implementar?



```
$query = "SELECT * FROM users WHERE usuario =  
'$user' AND senha = '$senha';";  
$result = ibase_query("sistema", $query);  
if( ibase_fetch_row($result) > 0)  
{ echo "Login OK..."; }  
else  
{ die("usuário ou senha inválidos!"); }
```



SQL Injection – Como implementar?



```
$query = "SELECT * FROM users WHERE  
usuario='adelesio' AND senha='1212a'";  
$result = ibase_query("sistema", $query);  
if( ibase_fetch_row($result) > 0)  
{ echo "Login OK..."; }  
else  
{ die("usuário ou senha inválidos!"); }
```



SQL Injection – Como implementar?



' or '1'='1



SQL Injection – Como implementar?



```
$query = "SELECT * FROM users WHERE  
usuario='adelesio' AND senha='' or '1'='1';";  
$result = ibase_query("sistema", $query);  
if( ibase_fetch_row($result) > 0)  
{ echo "Login OK..."; }  
else  
{ die("usuário ou senha inválidos!"); }
```



SQL Injection – Como implementar?



```
' ; DROP TABLE `usuarios`
```



SQL Injection – Como implementar?



```
$query = "SELECT * FROM users WHERE  
usuario='adelesio' AND senha='' ; DROP TABLE  
'usuarios';";  
$result = ibase_query("sistema", $query);  
if( ibase_fetch_row($result) > 0)  
{ echo "Login OK..."; }  
else  
{ die("usuário ou senha inválidos!"); }
```



SQL Injection – O que é?



- Mass SQL injection
- Blind SQL injection
- Second Order SQL injection
- Code injection
- Command injection
- XPATH injection
- Interpreter injection
- PHP, ASP & outros scripts injections
- XSS - Cross Site Scripting
- Double Encoding
- Resource injection
- XML injection
- LDAP injection
- ORM injection
- Refletion injection
- Log injection
- Top 10 injection flaws
- Avoiding SQL injection





Queries estáticas

Direitos mínimos

SELECT mais precisos





Principais verificações

Certificar conteúdo informado

Certificar origem dos dados

Certificar saída de dados





Testar o código SQL ou os parâmetros
antes de executar!





Proteções nativas do Firebird





Dúvidas?!

