Engenharia de Segurança (SSC -0747)

São Carlos, 28 de Abril de 2010

Prática 4 – SQL Injection

1. Introdução

SQL Injection é uma técnica de injeção de código que explora vulnerabilidades no banco de dados. Tipicamente, o não tratamento de sequências de escape gera este tipo de vulnerabilidade.

Nesta prática estudaremos como funciona este ataque funciona e como é possível evitá-lo. Para ilustrar utilizaremos páginas feitas em php5 e o banco de dados mysql.

2. Materiais

Utilizaremos os seguintes materiais:

- Notebook com interface Ethernet/Wireless
- Linux BT4 (Live CD)
- Servidor Apache+PHP+MySQL

3. Descrição da Prática

Os alunos se dividirão em grupos de 4 pessoas, e cada grupo receberá um notebook. Em seguida anote o número do notebook na folha de presença na frente do nome.

Logando no Sistema

a) Acesse o sistema web disponibilizado pelo monitor através de SQL Injection.

b) Crie um usuário no banco de dados através da página, adicionando o seguinte comando no final da string.

CREATE USER test1 IDENTIFIED BY 'pass1'; -- priv

c) Sabendo que o banco de dados foi feito em php, crie uma página Web através do SQL Injection com acesso a comandos do terminal. Isto pode ser feito através da inserção da string:

```
UNION SELECT 'Test',2,3,4 INTO OUTFILE '/tmp/meu_nome.txt'
--
```

Responda as seguintes questões:

1) No PHP é possível tratar as strings de entrada para evitar SQL Injection? Qual o comando para isto?
2) Para que serve a opção magic_quotes do arquivo php.ini?
3) Existe alguma funcionalidade nos bancos de dados SQL Server e Oracle que posibilitam a execução de comandos do shell através de instruções SQL?
4) Discuta como o que pode ser feito pelo desenvolvedor Web e pelo projetista de banco de dados para evitar SQL Injection no sistema.