

Re: SQL Security in ASP

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.sqlserver.security/2002-09/2449.html>

From: Refd0m (refdom@xfocus.org)

Date: 09/17/02

From: "Refd0m" <refdom@xfocus.org>
Date: Tue, 17 Sep 2002 09:37:07 +0800

hi,

You must also focus the SQL filter in ASP, it's a serious security problem. You can read some article about "SQL injection".

I write a filter function.

Function Filter_SQL(strData)

```
Dim strFilter
Dim blnFlag
Dim i
```

```
strFilter="";,/,--,@,_,exec,declare" 'character that must be
filtered, ' is a separator.
blnFlag=Flase 'filter flag. TRUE must be filtered.
```

```
Dim arrayFilter
arrayFilter=Split(strFilter,",")
For i=0 To UBound(arrayFilter)
  If Instr(strData,arrayFilter(i))>0 Then
    blnFlag=True
  Exit For
  End If
Next
```

```
If blnFlag Then
  Response.Redirect "wrong.asp"
Else
  Filter_SQL=strData
End If
```

End Function

--

Refd0m

Re: SQL Security in ASP

microsoft.public.sqlserver.security: Re: SQL Security in ASP

Homepage: www.xfocus.org
www.opengram.com

"CJM" <cjmwork@yahoo.co.uk> Ð´ÈëÏÛÏçÐÂÎÁ:eqThtDaxCHA.1788@tkmsftngp12...
> I am developing the the first of several intranet applications that access
> SQL 2000 through ASP. This is my first time doing this; previously I've
> always used Access97/2k.
>
> I'm am trying to settle on a security model, that is effective, but is
> quick
> and not cumbersome. Following on from my Access work, I realise I could
> use
> the same technicque: have users login in to the site and restrict access
> to
> the DB by restricting users access to certain ASPs and by checking the
> user
> credentials on a page by page basis.... basically, keeping unauthorised
> users away from particular application functions.
>
> This has always worked well for me, and would be fine in this scenario.
> However, since I am creating the first of many, and since SQL has fairly
> sophisticated security features (to the layman) built-in, I though now
> would
> be a suitable time to change to a new regime.
>
> So..... do I stick with what I have got, or are there some neat features
> in
> SQL that can help me do a better job?
>
> To re-iterate, I think I'm more interested in function-level security that
> field-level security, so solutions that go down to the nth degree wont be
> appropriate.
>
> Cheers
>
> CJM
>
>
>
>
>