which one of you is being held on sql injection filtering ?

Sql injection filtering

فیلتر کردن عملیات Sql injection

در حدود بیش از ده سال است که از عمر **sql injection** میگذرد ، اما حتی در هنگام بهترین تنظیمات یادآوری این نکته ضروری است که شما همیشه باید به برنامه های خود اعتبار بیافزایید

البته مطالبی که در طی این مقاله ارائه خواهند شد ، صرفا برای همه کاربرد ندارد و برای استفاده بهتر باید آن را متناسب با نیاز خود سازگار کنید !

بنابراین من تلاش خواهم کردم تا یک راهکار عمومی را به همه نشان دهم (استفاده از **vbscript**)

بخطار داشته باشید که شما احتیاج دارید تا ویژگی های وب اپلیکیشن خود را در ذهن نگه دارید و چیزهایی که برای یک مدیریت صحیح بر وب سرور نیاز دارید را پیوسته تغییر دهید .

هدف از این نمونه این است که مردم فقط کمی با نحوه فیلترینگ آشنا شوند !

در اینجا ما یک لیست سیاه تهییه خواهیم کرد و دستورات و کدهای مخربی را که موجب نفوذ هکرها میشود را فیلتر میکنیم

اما باز هم شاید هکر بتواند از خلاقیت خود استفاده کند و مثلا دستور **union** را بصورت **UN/**/ION** استفاده کند !

به هر حال ما فقط راه را نشان خواهیم داد و بقیه خلاقیت ها را به شما واگذار میکنیم ،

البته دنیای هک و امنیت دنیای جالبی است ! گاهی اوقات خبرنگاران و عده ایی از وب مسترها به من و دوستانم ایراد میگیرند که شما ها فقط خرابکاری میکنید و جز نفوذ کار دیگری بلد نیستید !

اما این تصور اشتباه است ، در دنیای هک و امنیت هر روزه ممکن است آسیب پذیری هایی کشف شود ، و قاعدتا عده ایی هم در صدد امن سازی آن برمی آیند ، این کارها برای خیلی از متخصصان امنیتی دوست داشتنی و جالب است ! (البته سر شار از تجربه و

علم اندوزی) تقریبا میتوان گفت مانند یک بازی دو طرفه و پیشرفته است !

Sql injection چیست ؟

اینجکشن یک روش تزریق کدهای مخرب است و چون از پورت 80 استفاده میکند ، هیچگونه ربطی به فایروال یا سایر نرم افزارها و سخت افزارهای امن سازی در سرور ندارد .
در واقع اینجکشن از روشی موذیانه برای سو استفاده از آسیب پذیری های "ورودی های اعتبار سازی نشده" استفاده میکند !
یک هکر میتواند با اجرای دستورات Sql و با تزریق آن ها به سرور به اطلاعات مهمی دست یابد !
بطور مثال : www.site.com/news.asp=12+union+select+1,2,username,password,5+from+news
که در صورت تزریق درست ، نفوذگر به نام کاربری و رمز عبور دست پیدا خواهد کرد !
توضیحات بیشتر در زمینه اینجکشن این مقاله را به حاشیه میراند !

توضیحاتی کوتاه در مورد اسکریپت !

در این اسکریپت ابتدا ما یک لیست از کاراکترهایی که هکرها در تزریق کدهای مخرب استفاده میکنند را جمع آوری میکنیم و سپس برنامه را طوری طراحی میکنیم که در صورت استفاده از این کاراکتر ها بعنوان یک url مجاز ، برنامه url را غیر مجاز بشناسد وهکر را به صفحه خطلا یا همان error page هدایت کند !
توضیح : اگر مایل باشید میتوانید در صفحه خطا فحش هم بنویسید ! (حداقل این طوری یکم حرصتون روی هکرا خالی میشه :d)

SqlCheckInclude.asp

این سورس کد صفحه ایی ست که ورودی ها را تست میکند ! این کد را در یک فایل Aspقرار دهید سپس تغییراتی که متناسب با نیاز خود میبنید را در سورس کد اعمال کنید .
البته فقط لیست سیاه و صفحه خطا را ویرایش کنید و با بقیه کد ها کاری نداشته باشید !

```
<%
'  SqlCheckInclude.asp
'
'  Author: d3c0der
'
'  This is the include file to use with your asp pages to
'  validate input for SQL injection.


Dim BlackList, ErrorPage, s

'
'  Below is a black list that will block certain SQL commands and
'  sequences used in SQL injection will help with input sanitization
'
'  However this is may not suffice, because:
'  1) These might not cover all the cases (like encoded characters)
'  2) This may disallow legitimate input
'
'  Creating a raw sql query strings by concatenating user input is
'  unsafe programming practice. It is advised that you use parameterized
```

```
'  SQL instead. Check http://support.microsoft.com/kb/q164485/ for information
'  on how to do this using ADO from ASP.
'
'  Moreover, you need to also implement a white list for your parameters.
'  For example, if you are expecting input for a zipcode you should create
'  a validation rule that will only allow 5 characters in [0-9].
'

BlackList = Array("--", ";", "/*", "*/", "@@", "+",_
                  "char", "nchar", "varchar", "nvarchar",_
                  "alter", "begin", "cast", "create", "cursor",_
                  "declare", "delete", "drop", "end", "exec",_
                  "execute", "fetch", "insert", "kill", "open",_
                  "select", "sys", "sysobjects", "syscolumns",_
                  "table", "update", "union")

'  Populate the error page you want to redirect to in case the
'  check fails.

ErrorPage = "/ErrorPage.asp"

''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''
'  This function does not check for encoded characters
'  since we do not know the form of encoding your application
'  uses. Add the appropriate logic to deal with encoded characters
'  in here
''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''
Function CheckStringForSQL(str)
  On Error Resume Next

  Dim lstr

  ' If the string is empty, return true
  If ( IsEmpty(str) ) Then
    CheckStringForSQL = false
    Exit Function
  ElseIf ( StrComp(str, "") = 0 ) Then
    CheckStringForSQL = false
    Exit Function
  End If

  lstr = LCase(str)

  ' Check if the string contains any patterns in our
  ' black list
  For Each s in BlackList

    If ( InStr (lstr, s) <> 0 ) Then
      CheckStringForSQL = true
      Exit Function
    End If

  Next

  CheckStringForSQL = false

End Function


''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''
'  Check forms data
''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''

For Each s in Request.Form
  If ( CheckStringForSQL(Request.Form(s)) ) Then

    ' Redirect to an error page
    Response.Redirect(ErrorPage)
```

```
  End If
Next

''''''''''''''''''''''''''''''''''''''''''''''''''''''''
'  Check query string
''''''''''''''''''''''''''''''''''''''''''''''''''''''''

For Each s in Request.QueryString
  If ( CheckStringForSQL(Request.QueryString(s)) ) Then

    ' Redirect to error page
    Response.Redirect(ErrorPage)

    End If

Next


''''''''''''''''''''''''''''''''''''''''''''''''''''''''
'  Check cookies
''''''''''''''''''''''''''''''''''''''''''''''''''''''''

For Each s in Request.Cookies
  If ( CheckStringForSQL(Request.Cookies(s)) ) Then

    ' Redirect to error page
    Response.Redirect(ErrorPage)

  End If

Next


''''''''''''''''''''''''''''''''''''''''''''''''''''''''
'  Add additional checks for input that your application
'  uses. (for example various request headers your app
'  might use)
''''''''''''''''''''''''''''''''''''''''''''''''''''''''

%>
```

TestPage.asp

این صفحه نشان دهنده نحوه include شدن اسکریپت در برنامه است

```
 <%
'  TestPage.asp
'
'  Author: d3c0der
'
'  This is a file to test the SQLCheckInclude file. The idea here is that you add
'  the include file to the beginning of every asp page to get SQL injection
'  input validation


%>

<!--#include file="SqlCheckInclude.asp"-->
<%
Response.Write("Welcome to the Test Page.")
Response.Write("If you are seeing this page then SQL validation succeeded.")
%>
```

ErrorPage.asp

این همان صفحه ایی است که در صورت مشکوک قلمداد شدن توسط لیست سیاه ، هکر به این صفحه هدایت میشود !

```
<%
'  ErrorPage.asp
'
'  Author: d3c0der
'
Response.Write("mage maraz dari ke mikhay site hack koni ? :d ")

'  This is the error page that users will be redirected to if the input cannot
'  be validated


%>
<%Response.Write("ERROR: Invalid Input")%>
```

Translated and Research by : d3c0der

D3c0der@hotmail.com

Data ir security group

www.Datairan.net

منابع :

http://blogs.iis.net/nazim/default.aspx