ניר אדר
underwar@hotmail.com

אסף רשף
assaf@fullscreen.co.il

גירסה 1.00 – 17.10.2002

הגבלת הגולשים באתר

מסמך זה הורד מהאתר http://underwar.livedns.co.il.
אין להפיץ מסמך זה במדיה כלשהי, ללא אישור מפורש מאת המחברים.
מחברי המסמך אינם אחראים לכל נזק, ישיר או עקיף, שיגרם עקב השימוש במידע המופיע במסמך, וכן לנכונות התוכן של הנושאים המופיעים במסמך. עם זאת, המחברים עשו את מירב המאמצים כדי לספק את המידע המדויק והמלא ביותר.

Nir Adar
Email: underwar@hotmail.com
Home Page: http://underwar.livedns.co.il

Assaf Reshef
Email: assaf@fullscreen.co.il

אנא שלחו תיקונים והערות אל המחברים.

הקדמה

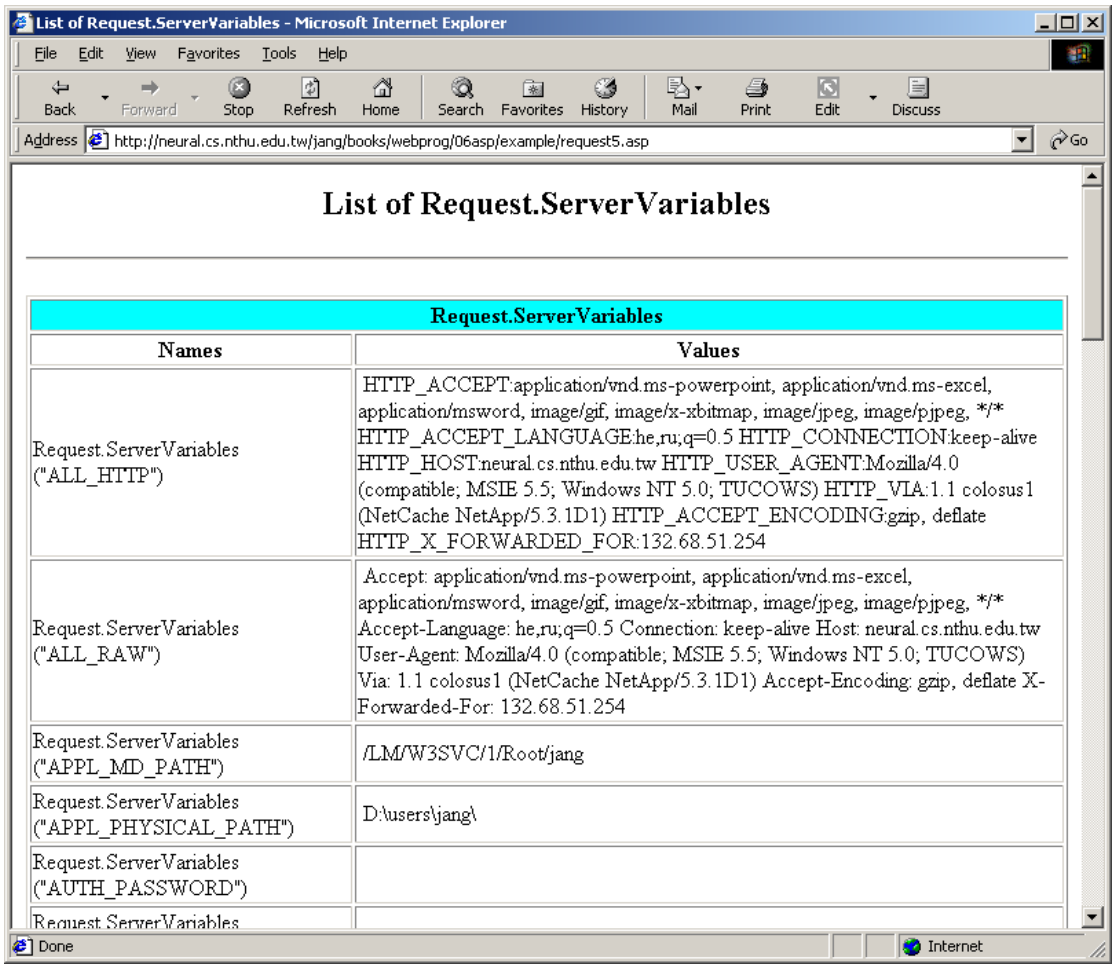
כאשר בעל אתר נותן למבקרים גישה לראות את קוד המקור של דפי האתר שלו, הוא צריך לדאוג גם לאבטחה נכונה של הקוד שמציג אותם, אחרת יהיה אפשר לנצל את זה לרעה.
הבעיה ידועה זמן רב ובשביעי במאי, 1999, אחד מחברי L0pht פרסם מסמך בנושא:
"Web users can view ASP source code and other sensitive files on the web server",
אשר הציגה את הבעיה בפירוט. עם זאת, אפילו בימים אלו, בעיה זו עדיין אקטואלית.
נדגים בעיה זו על אתר אחד, אולם ניתן למצוא את אותה הבעיה ובעיות נוספות באתרים רבים.

הסקריפט הבעייתי שנציג במסמך זה הוא showcode.asp, והוא חלק מחבילת הדוגמאות המצורפת על Microsoft IIS Server.

מציאת אתר עם בעיה

נתחיל בביקור בדף : http://neural.cs.nthu.edu.tw/jang/books/webprog/06asp/example/request5.asp.

דף שימושי זה מאפשר לגולש לראות את משתני השרת השונים שקיימים בשפת ASP.



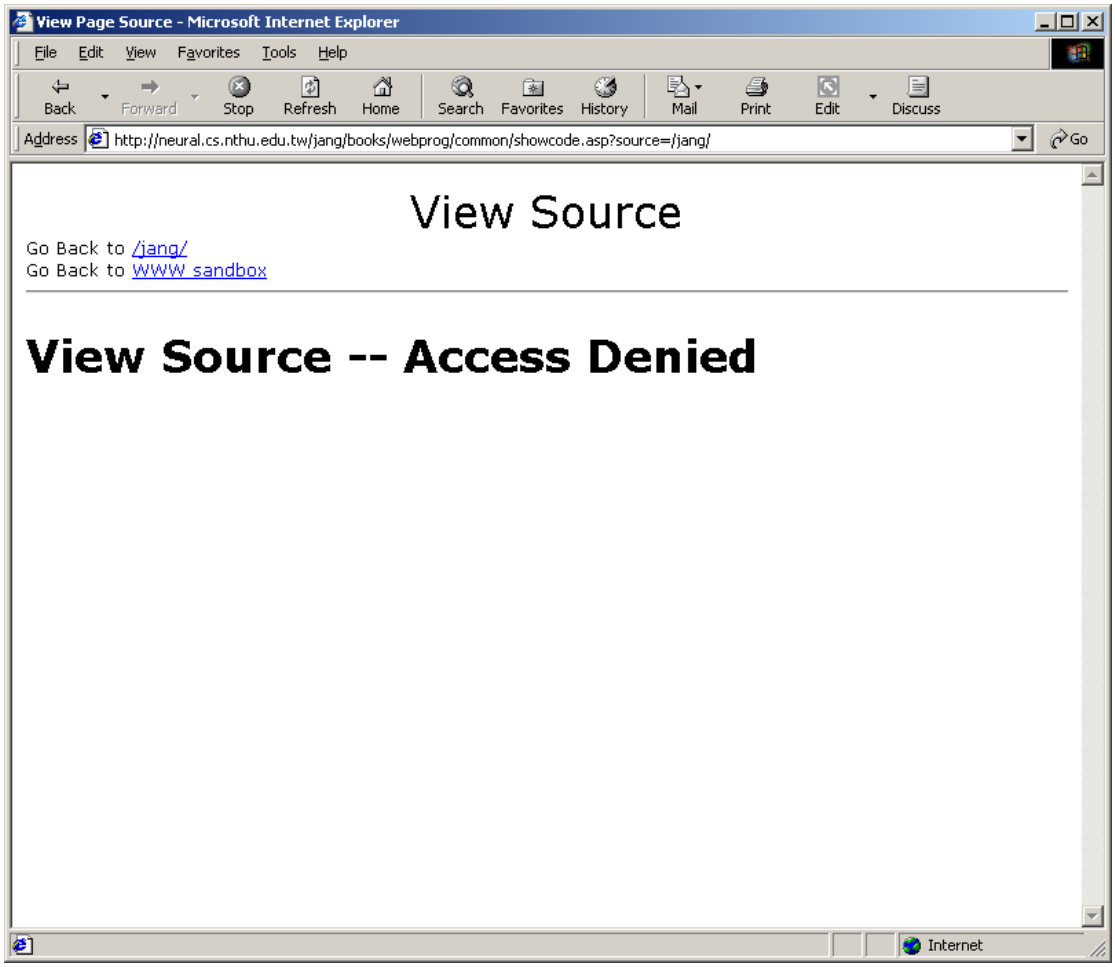
נשים לב שבתחתית הדף, ישנו קישור מעניין – View Source.
נזכיר כי דפי ASP הינם דפים העוברים עיבוד בצד השרת, כלומר, הדף המגיע אלינו לדפדפן אינו הדף המקורי שהמתכנת כתב, אלא אנו מקבלים דף אחרי עיבוד. אם נרצה לאפשר למבקרים לראות את דפי ה ASP המקוריים, נצטרך לכתוב סקריפט מיוחד, שיהיה גם הוא דף ASP שיישב בצד השרת, ושידאג להצגת הקוד של דפי ה-ASP. זהו המקרה באתר שלפנינו. כאשר לחצנו על הקישור View Source, נפתח חלון חדש, עם הכתובת
http://neural.cs.nthu.edu.tw/jang/books/webprog/common/showcode.asp?source=/jang/books/webprog/06asp/example/request5.asp, שם נגלה לפנינו הקוד של הדף.

חקירת הבעיה – האם אנו יכולים לנצל את הדף? האם זוהי בעיית אבטחה?

ננסה לנתח את הכתובת http://neural.cs.nthu.edu.tw/jang/books/webprog/common/showcode.asp
זהו הדף שמציג את הקוד. אנו רואים כי הוא מקבל פרמטר:
.source=/jang/books/webprog/06asp/example/request5.asp
ניתן להבין כי פרמטר זה קובע את הקוד של הדף שיוצג בפנינו.

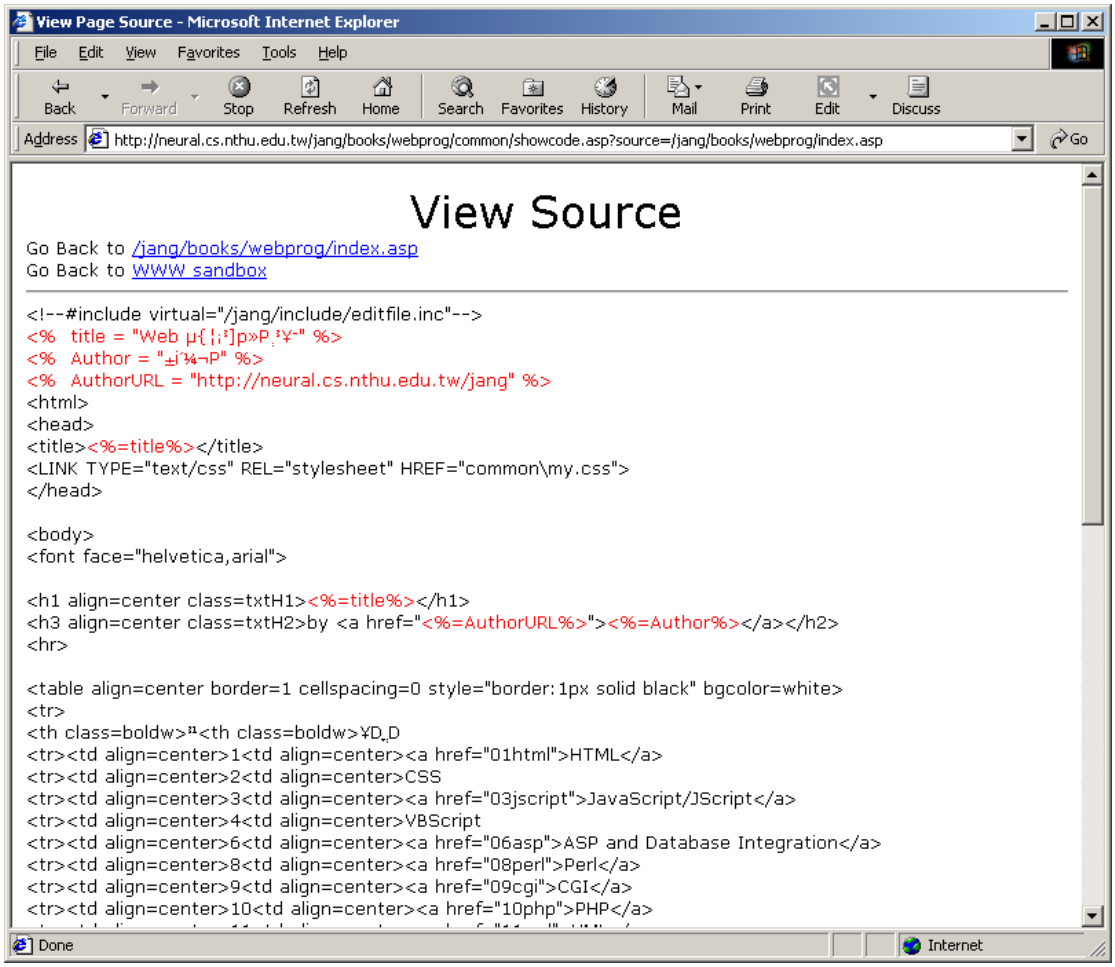
הצגת הקוד של דפים פותחת בעיית אבטחה: נניח כי באתר שלנו יש מערכת משתמשים. אדם בעל גישה לקוד המקור יוכל לגלות היכן מצוי מבנה הנתונים השומר את כל הנתונים של המשתמשים, ולגנוב/להרוס אותו. בעיות אבטחה נוספות עלולות להתגלות, במידה ויש לאדם את הקוד של האתר.
לפיכך, בדרך כלל נרצה למנוע את הצגת הדפים, או לאפשר להציג רק דפים בתיקיה מסוימת, לדוגמא, ייתכן שבאתר שאנו בודקים כעת, נוכל לראות רק את הקוד שתחת הספרייה /jang/books/webprog ואת כל תתי הספריות שלה.
נבדוק זאת.
ניקח את ה-URL המקורי, ונשנה אותו, על מנת להציג את הדף :
http://neural.cs.nthu.edu.tw/jang/index.asp
נכתוב בדפדפן את הכתובת הבאה:
http://neural.cs.nthu.edu.tw/jang/books/webprog/common/showcode.asp?source=/jang/index.asp

בעל האתר אכן חסם את הגישה לכתובת זו, אנו מקבלים מולנו את הדף הבא:



עדיין איננו מוותרים על ההזדמנות להביט בדפי האתר.
ננסה לבדוק האם אנו יכולים לראות את הקוד של דף אחר:
http://neural.cs.nthu.edu.tw/jang/books/webprog/common/showcode.asp?source=/jang/books/webprog/index.asp.

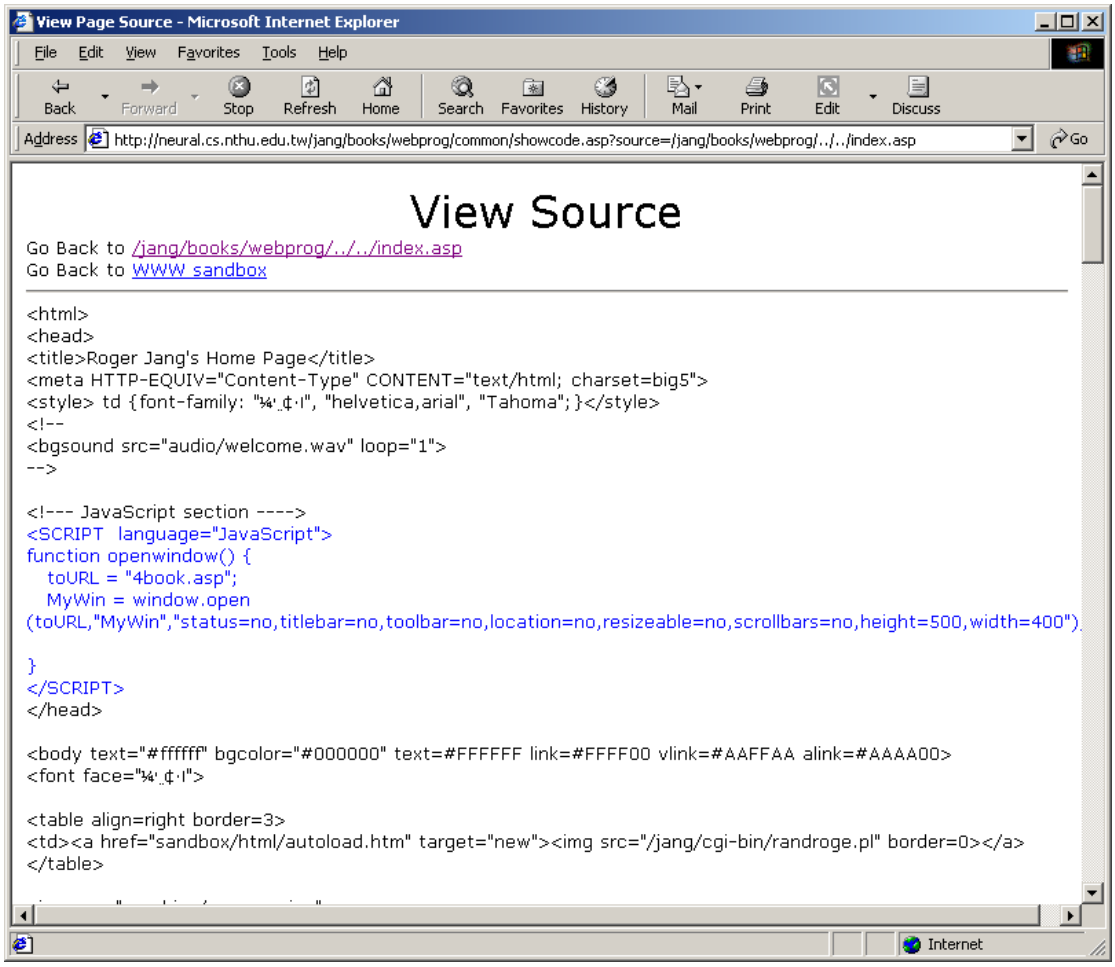
על המסך מופיע הקוד של הדף http://neural.cs.nthu.edu.tw/jang/books/webprog/index.asp.



ידוע כי במערכות הפעלה שונות, המשמעות של הביטוי ".." היא ספרייה אחת כלפי מעלה.
ננסה כעת לראות את הקוד של האתר הבא:
http://neural.cs.nthu.edu.tw/jang/books/webprog/../../index.asp, כלומר את הכתובת הבאה, אותה כתובת שקודם נחסמה אליה הגישה: http://neural.cs.nthu.edu.tw/jang/index.asp

נכתוב בדפדפן את השורה הבאה:

http://neural.cs.nthu.edu.tw/jang/books/webprog/common/showcode.asp?source=/jang/books/webprog/../../index.asp



אכן, הפעם ההגנה של השרת לא פעלה, והקוד של הדף הוצג לפנינו ללא כל מחסום.

שימושים

נוכל כעת לנסות להשיג דברים נוספים.
למשל, ניתן לראות בדף כי כותב האתר משתמש בסקריפט של Perl:

```
<table align=right border=3>
<td><a href="sandbox/html/autoload.htm" target="new"><img src="/jang/cgi-
bin/randroge.pl" border=0></a>
</table>
```

האם אנו יכולים להציג את הקוד של הסקריפט?
ננסה:

http://neural.cs.nthu.edu.tw/jang/books/webprog/common/showcode.asp?source=/jang/books/webprog/../../cgi-bin/randroge.pl

הסקריפט מוצג ללא כל בעיה.

כעת ננסה להציג את הקוד של הדף, שמציג את כל הדפים. נראה האם נוכל למצוא את בעיית האבטחה:
נביט בכתובת:
http://neural.cs.nthu.edu.tw/jang/books/webprog/common/showcode.asp?source=/jang/books/webprog/common/showcode.asp

נשים לב, שלא היינו צריכים לגלות את בעיית האבטחה הנ"ל, על ידי ניסוי וטעייה כפי שעשינו.
אנו מסוגלים לראות את הקוד של הדף showcode.asp באופן חופשי, בלי להשתמש ב "..", ולכן יכלנו לגלות את בעיית האבטחה שהרגע גילינו על ידי הסתכלות בקוד של showcode.asp וחיפוש בעיות אבטחה בקוד.

נעשה זאת כעת.

חקירת הסיבות לבעיה

נביט בקוד של הדף:

```
<SCRIPT  LANGUAGE=VBScript RUNAT=Server>
FUNCTION fValidPath (ByVal strPath)
    If (InStr(1, strPath, "/webbook/javascript", 1) or _
        InStr(1, strPath, "/books/webprog", 1)) Then
        fValidPath = 1
    Else
        fValidPath = 0
    End If
END FUNCTION

REM Returns the minimum number greater than 0
REM If both are 0, returns -1
FUNCTION posMin (iNum1, iNum2)
    If iNum1 = 0 AND iNum2 = 0 Then
        posMin = -1
    ElseIf iNum2 = 0 Then
        posMin = iNum1
    ElseIf iNum1 = 0 Then
        posMin = iNum2
    ElseIf iNum1 <  iNum2 Then
        posMin = iNum1
    Else
        posMin = iNum2
    End If
END FUNCTION

FUNCTION fCheckLine(ByVal strLine)
    fCheckLine = 0
    iTemp = 0

    iPos = InStr(strLine, "<" & "%")
    If posMin(iTemp, iPos) = iPos Then
        iTemp = iPos
        fCheckLine = 1
    End If

    iPos = InStr(strLine, "%" & ">")
    If posMin(iTemp, iPos) = iPos Then
        iTemp = iPos
        fCheckLine = 2
    End If

    iPos = InStr(1, strLine, "<" & "SCRIPT", 1)
    If posMin(iTemp, iPos) = iPos Then
        iTemp = iPos
        fCheckLine = 3
    End If

    iPos = InStr(1, strLine, "<" & "/SCRIPT", 1)
    If posMin(iTemp, iPos) = iPos Then
        iTemp = iPos
```

```
        fCheckLine = 4
    End If
END FUNCTION

SUB PrintHTML(ByVal strLine)
    iSpaces = Len(strLine) - Len(LTrim(strLine))
    i = 1
    While Mid(Strline, i, 1) = Chr(9)
        iSpaces = iSpaces + 5
        i = i + 1
    Wend
    If iSpaces > 0 Then
        For i = 1 to iSpaces
            Response.Write(" ")
        Next
    End If
    iPos = InStr(strLine, "<")
    If iPos Then
        Response.Write(Left(strLine, iPos - 1))
        Response.Write("<")
        strLine = Right(strLine, Len(strLine) - iPos)
        Call PrintHTML(strLine)
    Else
        Response.Write(strLine)
    End If
END SUB

SUB PrintLine (ByVal strLine, iFlag)
    Select Case iFlag
        Case 0
            Call PrintHTML(strLine)
        Case 1
            iPos = InStr(strLine, "<" & "%")
            Call PrintHTML(Left(strLine, iPos - 1))
            Response.Write("<FONT COLOR=#ff0000>")
            Response.Write("<%")
            strLine = Right(strLine, Len(strLine) - (iPos + 1))
            Call PrintLine(strLine, fCheckLine(strLine))
        Case 2
            iPos = InStr(strLine, "%" & ">")
            Call PrintHTML(Left(strLine, iPos -1))
            Response.Write("%>")
            Response.Write("</FONT>")
            strLine = Right(strLine, Len(strLine) - (iPos + 1))
            Call PrintLine(strLine, fCheckLine(strLine))
        Case 3
            iPos = InStr(1, strLine, "<" & "SCRIPT", 1)
            Call PrintHTML(Left(strLine, iPos - 1))
            Response.Write("<FONT COLOR=#0000ff>")
            Response.Write("<SCRIPT")
            strLine = Right(strLine, Len(strLine) - (iPos + 6))
            Call PrintLine(strLine, fCheckLine(strLine))
        Case 4
            iPos = InStr(1, strLine, "<" & "/SCRIPT>", 1)
            Call PrintHTML(Left(strLine, iPos - 1))
```

```
            Response.Write("</SCRIPT>")
            Response.Write("</FONT>")
            strLine = Right(strLine, Len(strLine) - (iPos + 8))
            Call PrintLine(strLine, fCheckLine(strLine))
        Case Else
            Response.Write("FUNCTION ERROR -- CONTACT ADMIN.")
    End Select
END SUB
</SCRIPT>

<%  strVirtualPath=Request("source") %>

<html>
<head><title>View Page Source</title></head>
<body>

<center>
<font face="Verdana, Arial, Helvetica" SIZE=6>View Source</font>
</center>

<font FACE="Verdana, Arial, Helvetica" SIZE=2>
Go Back to <a href="<%=strVirtualPath%>"><%=strVirtualPath%></a><BR>
Go Back to <a href="/jang/sandbox">WWW sandbox</a>
<hr>
<%
If fValidPath(strVirtualPath) Then
    strFilename = Server.MapPath(strVirtualPath)
    Set FileObject = Server.CreateObject("Scripting.FileSystemObject")
    Set oInStream = FileObject.OpenTextFile (strFilename, 1, FALSE)
    While NOT oInStream.AtEndOfStream
        strOutput = oInStream.ReadLine
        Call PrintLine(strOutput, fCheckLine(strOutput))
        Response.Write("<BR>")
    Wend
Else
    Response.Write("<H1>View Source -- Access Denied</H1>")
End If
%>

</body>
</html>
```

הדף מחולק למספר קטעים – החלק הכחול הוא פונקציות עזר, בהם משתמש בדף. פעולת הסקריפט מתחילה בסוף הקטע הכחול.
הקטע שאינו מודגש הינו קוד HTML. הבלוק האדום בסוף הדף – ממנו נתחיל את הניתוח.
נראה כי המתכנת קורא לפונקציה fValidPath(), ולפי הערך שהיא מחזירה, קובע האם להציג למשתמש את הדף המבוקש, או את ההודעה – View Source - Access Denied.

נביט בעיון בקוד של fValidPath(),זוהי הפונקציה האחראית לאבטחה בדף זה:

```
FUNCTION fValidPath (ByVal strPath)
    If (InStr(1, strPath, "/webbook/javascript", 1) or _
        InStr(1, strPath, "/books/webprog", 1)) Then
        fValidPath = 1
    Else
        fValidPath = 0
    End If
END FUNCTION
```

הפונקציה מקבלת מחרוזת המציינת נתיב בשרת.
כותב הסקריפט התכוון לבדוק אם הכתובת /webbook/javascript או הכתובת /books/webprog מופיעות ב-URL, אבל הוא לא חשב על האפשרות של "דילוג אחורה" בנתיבים, על ידי "..". לכן כשהכנסנו את הטקסט שהוא רצה לראות, הפונקציה אישרה לנו את זה, וה ".." בנתיב שחיפשנו גרמו לנו בעצם לבקש את הקוד של סקריפט שהכותב לא התכוונן שנראה

פתרון אפשרי לבעיה

פתרון לבעיה היה יכול להיות למשל:

```
FUNCTION fValidPath (ByVal strPath)
    If (InStr(1, strPath, "/webbook/javascript", 1) or _
        InStr(1, strPath, "/books/webprog", 1)) Then
        fValidPath = 1
    Else
        fValidPath = 0
    End If
    If (InStr(strPath, "..") <> 0) Then fValidPath = 0
END FUNCTION
```

תוספת זו מחפשת את הטקסט ".." בנתיב שלנו ולא מאפשרת לקוד להראות קבצים עם הטקסט הזה בנתיב. מעין זו הייתה חוסמת את ההתקפה שביצענו הרגע.

EOF