VBScript エスケープ法について

ＮＴＴ コミュニケーションズ株式会社
ＩＴ マネジメントサービス事業部
セキュリティオペレーションセンタ

2009 年 05 月 26 日

Ver. 1.0

1. 調査概要

Microsoft Internet Explorer 上では、JScript(JavaScript 互換)だけではなく、VBScript も動作する。
汚染データを、VBScript 上の文字列リテラルとして用いる場合のサニタイジング法(エスケープ法)について検討した結果をここに記す。

サニタイジング処理の対象文字は、以下の二つが基本である。
- 「"(ダブルクォート)」
- 改行 (Cr 及び Lf)

HTML 内に VBScript を記述する場合には、以下の三つの文字もサニタイジング対象となる。
- 「/(スラッシュ)」
- 「<(小なり記号)」
- 「>(大なり記号)」

これらは、VBScript 中に「</script>」などという文字列を挿入されて、HTML パーサーが誤動作しないために必要である。

念のために、以下の文字もサニタイジングの対象としてもよい。
- 「'(シングルクォート)」

VBScript では、文字列リテラルは「"(ダブルクォート)」で囲むため、「'(シングルクォート)」のサニタイジング処理は必要ないと思われるが、念のためにサニタイジング処理してもよいだろう。

2. HTML 上の JavaScript のエスケープ法

VBScript について検討する前に、HTML 上の JavaScript において、汚染データを文字列リテラルとして使う場合について簡単に検討する。

HTML 上の JavaScript では、以下の文字がサニタイジング処理の対象となっている。

- 「"(ダブルクォート)」
- 「'(シングルクォート)」
- 「\(バックスラッシュ)」
- 「改行コード(Cr 及び Lf)」
- 「/(スラッシュ)」
- 「<(小なり記号)」
- 「>(大なり記号)」

以上の検討内容を、VBScript に対して適用していく。

3. HTML 上の VBScript のエスケープ法

3.1. VBScript での文字列リテラルに対してのサニタイジング処理の基本

VBScript では、文字列リテラルを「"(ダブルクォート)」で囲む。また、文字列リテラル上の「"(ダブルクォート)」は、「""(ダブルクォート二個)」に置換(エスケープ)することで、文字列リテラルとしての(データとしての)「"(ダブルクォート)」を表現することができる。

VBScript では、コードは改行で区切られて記述される。文字列のデータとして改行を示す場合、「vbLf」「vbCr」「vbCrLf」などの定数が用意されているため、それらに置換する。

最後に文字列データの連結には「&」を用いる。

3.2. HTML 上の VBScript の場合の注意点

HTML 上のスクリプト・コードは、基本的には以下の手順でスクリプト・実行エンジンに渡される

1. HTTP レスポンス・メッセージを Web ブラウザが受信
2. HTTP レスポンス・メッセージのボディ部分が、HTML レンダリング・エンジンに渡される
3. HTTP レンダリング・エンジンは、「<script>」から「</script>」までを抜き出し、その部分をスクリプト・実行エンジンに渡す

以上の流れを考えれば、VBScript コード中に「</script>」などのデータが挿入された場合、3 の処理が誤動作する可能性がある。
よって、HTML 上のスクリプト・コードでは「/」「<」「>」をサニタイジング処理しておく必要がある。

VBScript の場合、Chr() 関数を使い、以下の三つの文字を関数に置き換えることでサニタイジング処理することができる。

- 「/(スラッシュ)」　→ Chr(47)
- 「<(小なり記号)」　→ Chr(60)
- 「>(大なり記号)」　→ Chr(62)

3.3. 「'(シングルクォート)」の扱い

VBScript では「'(シングルクォート)」は、コメントの開始を意味する。(JavaScript でいえば「//」と同義と考えてよい)
よって、VBScript に関しては、「'(シングルクォート)」をサニタイジング処理する必要はないといえるが、Chr() 関数に置き換えてもよい。

- 「'(シングルクォート)」→ Chr(39)

3.4. まとめ

HTML 上の VBScript に対して、汚染データを文字列リテラルの一部として埋め込む場合、以下の文字をサニタイジング処理する。

- 「"(ダブルクォート)」→「""」
- CrLf(改行) → vbCrLf
- Cr(改行) → vbCrLf
- Lf(改行) → vbLf
- 「/(スラッシュ)」 → Chr(47)
- 「<(小なり記号)」 → Chr(60)
- 「>(大なり記号)」 → Chr(62)
- 「'(シングルクォート)」→ Chr(39)

(念のため、「'(シングルクォート)」)も含めた

4. 検証結果

4.1. 検証環境

以下の環境で、検証を行った。

- Microsoft WindowsXP 日本語版 SP3 上の IIS5.1 + ASP
- Microsoft WindowsXP 日本語版 SP3 上の Microsoft Internet Explorer 6 SP3

4.2. 検証コード(IIS+ASP)

IIS+ASP のコードは、図 4.2-1 である。
このコードの VBEscape(入力データ、フラグ 1、フラグ 2)が、エスケープ関数である。
(フラグ 1=True の時、「/(スラッシュ)」「<(小なり記号)」「>(大なり記号)」らもエスケープする)
(フラグ 2=True の時、「'(シングルクォート)」もエスケープする)

```
<%
 Option Explicit
 Dim myArg1
 myArg1 = ""
 myArg1 = Request.Form("arg1")
 myArg1 = VBEscape(myArg1,True,True)
%>
<HTML>
 <HEAD><TITLE>VBEscape テスト</TITLE></HEAD>
 <BODY>
  <CENTER>
   <FORM ACTION="" METHOD="post">
    <TEXTAREA NAME="arg1" ROWS="10" COLS="72"><% =
Server.HTMLEncode(Request.Form("arg1")) %></TEXTAREA><BR>
    <INPUT TYPE="submit">
   </FORM>
   <HR>
   <% If 0 < Len(myArg1) Then %>
    <SCRIPT LANGUAGE="VBScript">
     MsgBox("<% = myArg1 %>")
    </SCRIPT>
   <% End If%>
  </CENTER>
 </BODY>
</HTML>
<%
 Function VBEscape(iStr, iFlg1, iFlg2)
  Dim myStr
  myStr = Replace(iStr,"""","""""")
  myStr = Replace(myStr,vbCrLf,""" & vbCrLf & """)
  myStr = Replace(myStr,vbLf,""" & vbLf & """)
  myStr = Replace(myStr,vbCr,""" & vbCr & """)
  If iFlg1 = True Then
   myStr = Replace(myStr,"/",""" & Chr(47) & """)
   myStr = Replace(myStr,"<",""" & Chr(60) & """)
   myStr = Replace(myStr,">",""" & Chr(62) & """)
  End If
  If iFlg2 = True Then
   myStr = Replace(myStr,"'",""" & Chr(39) & """)
  End If
  myStr = Replace(myStr," & """" & "," & ")
  VBEscape = myStr
 End Function
%>
```

図 4.2-1 : VBScript のサニタイジング処理が正しいかどうか検証するための IIS+ASP のコード

4.3. 検証結果

以下の図より、適切にエスケープされていることを確認した。

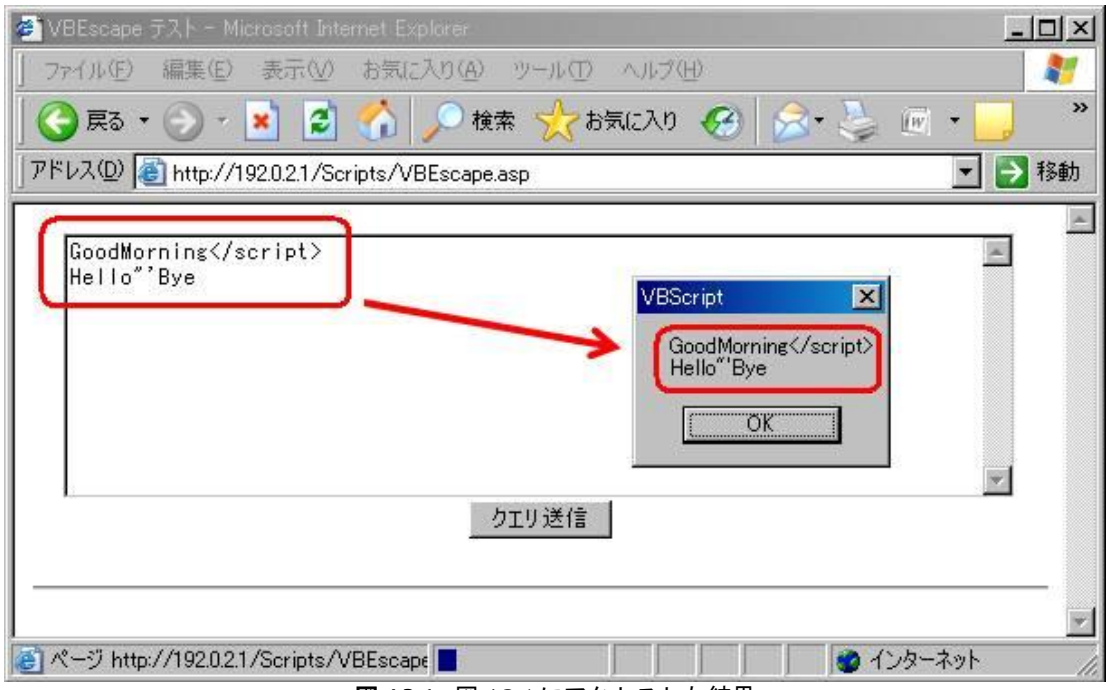

図 4.3-1 : 図 4.2-1 にアクセスした結果

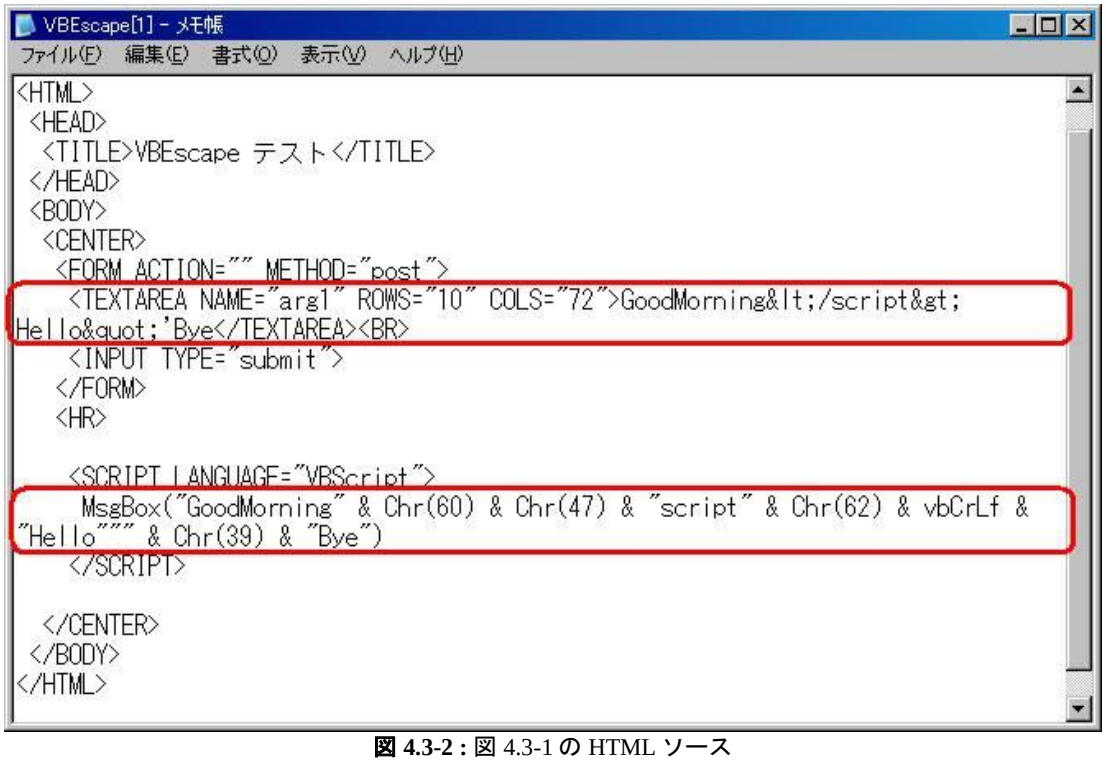

図 4.3-2 : 図 4.3-1 の HTML ソース

5. 検証作業者

NTT コミュニケーションズ株式会社
IT マネジメントサービス事業部ネットワークマネジメントサービス部
セキュリティオペレーションセンター
　佐名木 智貴

6. 参考

- メーリングリスト「Sea Surfers ML」
  http://www.freeml.com/seasurfers

7. 履歴

- 2009 年 05 月 26 日 ： ver1.0 最初の公開

8. 最新版の公開 URL

http://www.ntt.com/icto/security/data/soc.html#security_report

9. 本レポートに関する問合せ先

NTT コミュニケーションズ株式会社
IT マネジメントサービス事業部ネットワークマネジメントサービス部
セキュリティオペレーションセンター

e-mail: scan@ntt.com

以 上