

[NEWS] Passing JavaScript/HTML Filters with Special Chars (Multibrowser)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-07/0133.html>

From: SecuriTeam (*support_at_securiteam.com*)

Date: 07/31/03

To: list@securiteam.com

Date: 31 Jul 2003 14:40:22 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

Get Thawte's New Step-by-Step SSL Guide for Apache.

In this guide you will find out how to test, purchase, install and use a Thawte Digital Certificate on you Apache web server.

Throughout, best practices for set-up are highlighted to help you ensure efficient ongoing management of your encryption keys and digital certificates. Get you copy of this new guide now:

<http://ad.doubleclick.net/clk;5903117;8265118;i>

Passing JavaScript/HTML Filters with Special Chars (Multibrowser)

SUMMARY

When web browsers parse HTML they remove certain non-alpha numeric characters, this behavior may be used by an malicious user to fool JavaScript/HTML filters, allowing the execution of malicious HTML or JavaScript code.

DETAILS

To detect what kind of special chars can be used in HTML parameters Ben has set up the following asp-page:

```
-----2.asp-----  
<% @LANGUAGE=JScript%><%  
  
%><script>function a(o){alert(o)}</script><%  
%><%
```

Securiteam: [NEWS] Passing JavaScript/HTML Filters with Special Chars (Multibrowser)

```
for(i=0;i<256;++i){
  uc = "%"+chk(i.toString(16));
  %>
<% }

function chk(sInp){if(sInp.length<2){
  return String("0"+sInp)
}else{return sInp}}
%>
```

The page has been viewed with Mozilla, Opera, and Internet Explorer, an alert-box will pop up in this order:

- * Mozilla 1.3.1 (Win32): 0 (with restrictions)
- * Opera 7.11 (Win32): 0, 9, 10, 13, 173
- * Internet Explorer 5.0: 13, 10, 9, 0

Mozilla doesn't allow the window.alert()-method in "javascript:" images, so Ben had to use his own function "a()". It also returned an error for char 9, 10 and 13: "Error: unterminated regular expression literal".

Demonstration site:

<<http://badwebmasters.net/advisory/012/test.asp>>
<http://badwebmasters.net/advisory/012/test.asp>

ADDITIONAL INFORMATION

The information has been provided by <<mailto:badwebmasters@online.de>> ben moeckel.

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:
list-unsubscribe@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.