

## Re: Web session tracking security prob. Vulnerable: IIS and ColdFusion (maybe others)

*Source:* <http://www.derkeiler.com/Mailing-Lists/securityfocus/vuln-dev/2001-09/0013.html>

---

**From:** Jeff Jancula ([Jeff@Jancula.com](mailto:Jeff@Jancula.com))

**Date:** 09/03/01

Message-ID: <00bc01c134ba\$4bb81080\$a600000a@Jancula.com>

From: "Jeff Jancula" <[Jeff@Jancula.com](mailto:Jeff@Jancula.com)>

To: "Hicks, John" <[JHicks@JUSTICE.GC.CA](mailto:JHicks@JUSTICE.GC.CA)>, <[vuln-dev@securityfocus.com](mailto:vuln-dev@securityfocus.com)>

Subject: Re: Web session tracking security prob. Vulnerable: IIS and ColdFusion (maybe others)

Date: Mon, 3 Sep 2001 16:52:07 -0400

John,

I think you miss the point... IIS does issue a session ID, however you do not have to use it! You can make your own ID up! So, forget about "guessing" someone's session ID, just feed a victim with malicious cross-site scripting or a more permanent cookie (ASPSESSION), and you will KNOW the session ID you gave them.

Hijacking becomes easy then.

Jeff

----- Original Message -----

From: "Hicks, John" <[JHicks@JUSTICE.GC.CA](mailto:JHicks@JUSTICE.GC.CA)>

To: <[vuln-dev@securityfocus.com](mailto:vuln-dev@securityfocus.com)>

Sent: Thursday, August 30, 2001 11:23 AM

Subject: RE: Web session tracking security prob. Vulnerable: IIS and ColdFusion (maybe others)

> *I am not too familiar with Cold Fusion, however, if you run ASP (Active  
> Server Page) Applications on your IIS Server, the server issues a Session ID  
> to each new session. This is how ASP maintains state across web pages. I  
>*