

# Outlook Web Access authentication bypass

**Source:** <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2003-05/0255.html>

---

**From:** Chris Robertson ([Chris.Robertson\\_at\\_instill.com](mailto:Chris.Robertson_at_instill.com))

**Date:** 05/23/03

To: "'bugtraq@securityfocus.com'" <bugtraq@securityfocus.com>

Date: Fri, 23 May 2003 01:03:17 -0700

This exploit exhibits the same symptoms as CAN-2002-0507 however I have found it is possible on an Exchange 5.5 (patches current to within ~3 months) single system Outlook Web Access install (IIS and Exchange on the same server) to access any mailbox once the client has been successfully authenticated in Netscape 7.0 on Windows 2k and Redhat 7.2, Mozilla 1.0.1, Galeon 1.2.5, and Konqueror 3.0.3-13 on Redhat 8.0. Additionally under IE 5.50.4807.2300 it is possible to get the same behavior by canceling an attempted login to a non-authorized mailbox and editing the url from ..."isnewwindow=0"... to ..."isnewwindow=1"...

Does anyone have anymore info on this?

Thanks,  
Chris Robertson  
Security Engineer  
Instill Corp.