

# [NEWS] ICQ Web Portal Multiple Cross Site Scripting Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2001-09/0080.html>

---

*From:* [support@securiteam.com](mailto:support@securiteam.com)

*Date:* 09/24/01

From: [support@securiteam.com](mailto:support@securiteam.com)

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

Subject: [NEWS] ICQ Web Portal Multiple Cross Site Scripting Vulnerability

Message-Id: <20010924192400.B53AB138C1@mail.der-keiler.de>

Date: Mon, 24 Sep 2001 21:24:00 +0200 (CEST)

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

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> – Know that you're safe.

-----

## ICQ Web Portal Multiple Cross Site Scripting Vulnerability

---

### SUMMARY

The ICQ portal suffers from several Cross Site Scripting vulnerabilities. These vulnerabilities allow attackers to force the web site to return arbitrary information that would seem as coming from the original web site.

### DETAILS

The ICQ web portal may inadvertently include malicious HTML tags or script in dynamically generated pages.

Example 1:

<http://search.icq.com/dirsearch.adp?query=>

**>Hello!</h1><script>alert('hello');</script>est&wh=is&u**

Screen Shots:

<<http://www.isecurelabs.com/advisory/icq1.jpg>>

>Hello!</h1><script>alert('hello');</script>est&wh=is&users=1

## Securiteam: [NEWS] ICQ Web Portal Multiple Cross Site Scripting

<http://www.isecurelabs.com/advisory/icq1.jpg>  
<<http://www.isecurelabs.com/advisory/icq2.jpg>>  
<http://www.isecurelabs.com/advisory/icq2.jpg>

Example 2:

<http://web.icq.com/foo/>>alert('hello');</script>

Screen Shots:

<<http://www.isecurelabs.com/advisory/icq3.jpg>>  
<http://www.isecurelabs.com/advisory/icq3.jpg>  
<<http://www.isecurelabs.com/advisory/icq4.jpg>>  
<http://www.isecurelabs.com/advisory/icq4.jpg>

### ADDITIONAL INFORMATION

For more information about CSS (Cross Site Scripting), see:

<<http://www.securiteam.com/exploits/5IP000KOLI.html>>  
<http://www.securiteam.com/exploits/5IP000KOLI.html>

The information has been provided by

<<mailto:aurelien.cabazon@iSecureLabs.com>> Cabazon Aurelien.

=====

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](mailto:list-unsubscribe@securiteam.com)

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

- 
- **Previous message:** [support@securiteam.com](mailto:support@securiteam.com): "[UNIX] Textor Webmasters CGI Allows Remote Command Execution"
  - **Messages sorted by:** [\[ date \]](#) [\[ thread \]](#) [\[ subject \]](#) [\[ author \]](#) [\[ attachment \]](#)