==========
Achievo-1.3.2-STABLE Cross Site Scripting (XSS)
==========
AUTHOR : ROHIT BANSAL
TITLE: Team Member, EvilFingers.com
DATE : 19th Sept,2008
Mail: RoHiTiSbAcK [at] GmAiL.com
==========
Application: achievo-1.3.2-STABLE
Site: http://www.achievo.org/<http://www.w4ck1ng.com/board/link.php?url=http://www.achievo.org/>
Bug: XSS[Cross Site Scripting]
File: /achievo-1.3.2/dispatch.php

Variable: GET variable 'atknodetype'
==========
Bug explanation - Cross Site Scripting:

Cross site scripting (also referred to as XSS) is a vulnerability that
allows
an attacker to send malicious code (usually in the form of Javascript) to
another user. Because a browser cannot know if the script should be trusted
or not, it will execute the script in the user context allowing the attacker
to access any cookies or session tokens retained by the browser.

==========
Impact of Vulnerability:

Malicious users may inject JavaScript, VBScript, ActiveX, HTML or Flash into
a vulnerable application to fool a user in order to gather data from them.
An
attacker can steal the session cookie and take over the account,
impersonating the user. It is also possible to modify the content of the
page
presented to the user.

==========
PoC:

http://127.0.0.1/achievo-1.3.2/dispatch.php?atknodetype=
>"><script%20%0a%0d>a
lert(document.cookie)%3B</script>&atkaction=adminpim&atklevel=-1&atkprevlevel
=0&achievo=cgvuu4c9nv45ofdq8ntv1inm82

==========
GreeTz

InfySec , EvilFingers, Neo Anderson

==========