

Advisory : Critical Vulnerabilities in American Online Networks [SQL Injections , Redirection and Phishing Attacks]

Severity : Critical

Dated : 2 March 2007

By: Aditya K Sood [www.secniche.org]

Explanation :

A number of websites in AOL networks are prone to SQL injections and Phishing attacks. An attacker can easily leverage internal information from the server by injecting rogue elements. Also the attacker can perform phishing by manipulating redirection from the domain context.

A number of sites with detailed response is presented as:

Websites Affected :

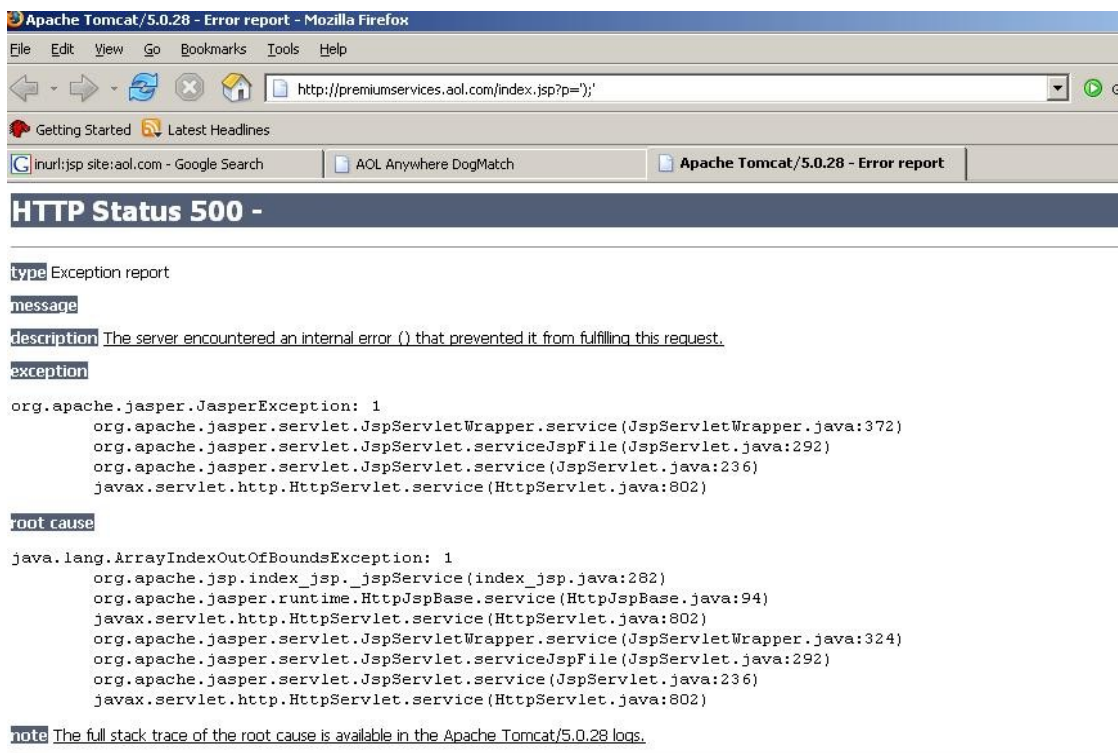
SQL Injections:

`http://premiumservices.aol.com/index.jsp?p=');'`
`http://webcenter.polls.aol.com/modular.jsp?resType=');`
`http://futbolmexicano.deportes.aol.com/apertura2006/equipos/index-notab.php?x='`

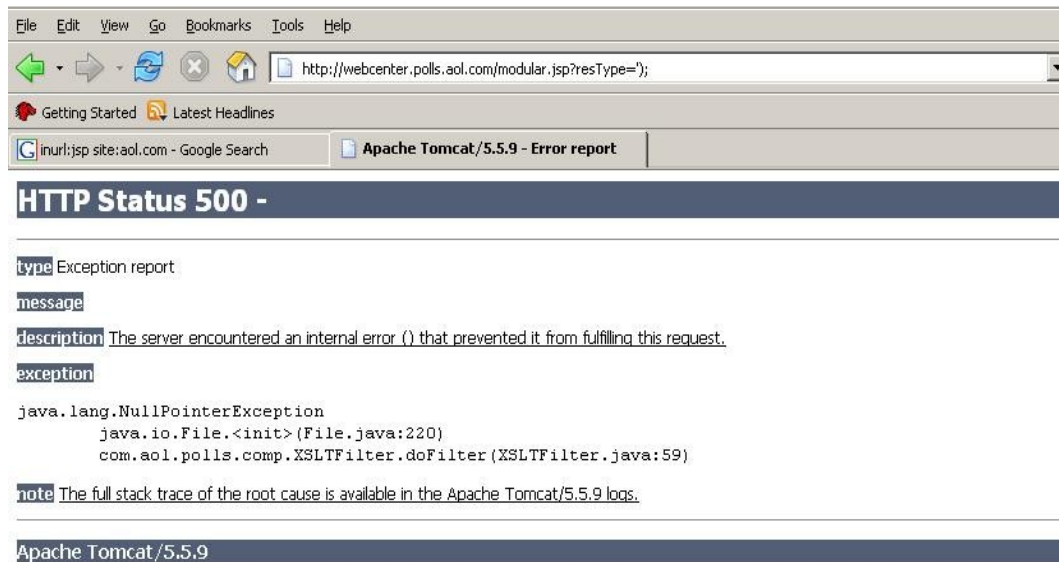
Redirection and Phishing:

`http://music.aol.com/predir.adp?_type=click&_u=<Destination Address>`
`http://groups.aol.com/gm/V4/iFrFPhoto.jsp?url=<Destination Name>=');`

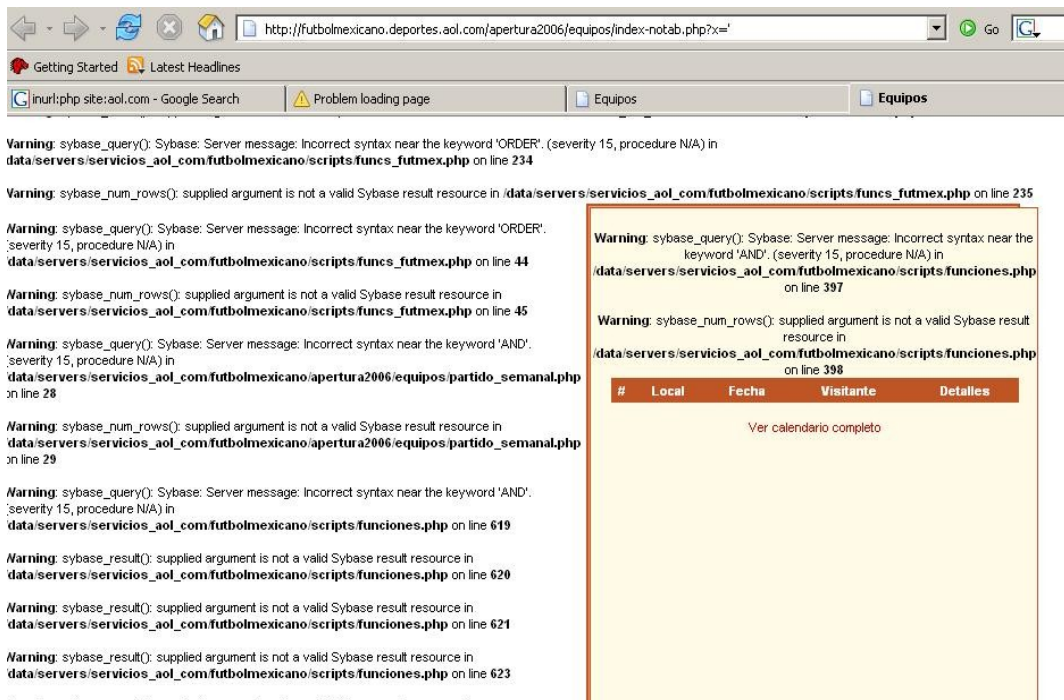
Snapshot: `http://premiumservices.aol.com/index.jsp?p=');`



Snapshot: <http://webcenter.polls.aol.com/modular.jsp?resType=>');



Snapshot : <http://futbolmexicano.deportes.aol.com/apertura2006/equipos/index-notab.php?x=>'



Redirection Examples :

<http://groups.aol.com/gm/V4/iFrFPhoto.jsp?url=http://www.google.com>

http://music.aol.com/pedir.adp?_type=click&_u=http://www.google.com

Vendor Status : Reported. Major Websites Patched.