# Cross Site Scripting (XSS) Vulnerabilities in rediff.com IA search, IN search and JOB Search



Author: Aseem Jakhar
Email: null@null.co.in

## Organization
Rediff.com (Nasdaq: REDF) is one of the premier worldwide online providers of news, information, communication, entertainment and shopping services.

Rediff.com provides a platform for Indians worldwide to connect with one another online. Rediff.com is committed to offering a personalized and a secure surfing and shopping environment.
*(Source: http://investor.rediff.com/overview.asp)*

## Vulnerability
Multiple Non-Persistent Cross site scripting (XSS) vulnerabilities were found in different rediff searches.

## Disclosure Timeline
Reported: 14th April 2009
Fixed: ----------

## Credits
Aseem Jakhar (Member NULL security community)
http://null.co.in

## Description

Multiple Non-Persistent Cross site scripting (XSS) vulnerabilities were found in different rediff searches. The tested search options were the search on home page for **in** (India) , **ia** (India Abroad: rediff.com US) and the **job** search page. In the PoC images we will show 2 options out of the three as **ia** and **in** home page searches use the same code which is evident from the fact that both redirect the user to http://search1.rediff.com/..... . A user can be tricked by sending her a rediff url containing the malicious script. On clicking the malicious URL the script will be injected into the users browser and will get executed automatically and can be used to exploit any known vulnerability in the user's browser (or transfer user cookies to the cracker if rediff sets session cookies for home page or job page).

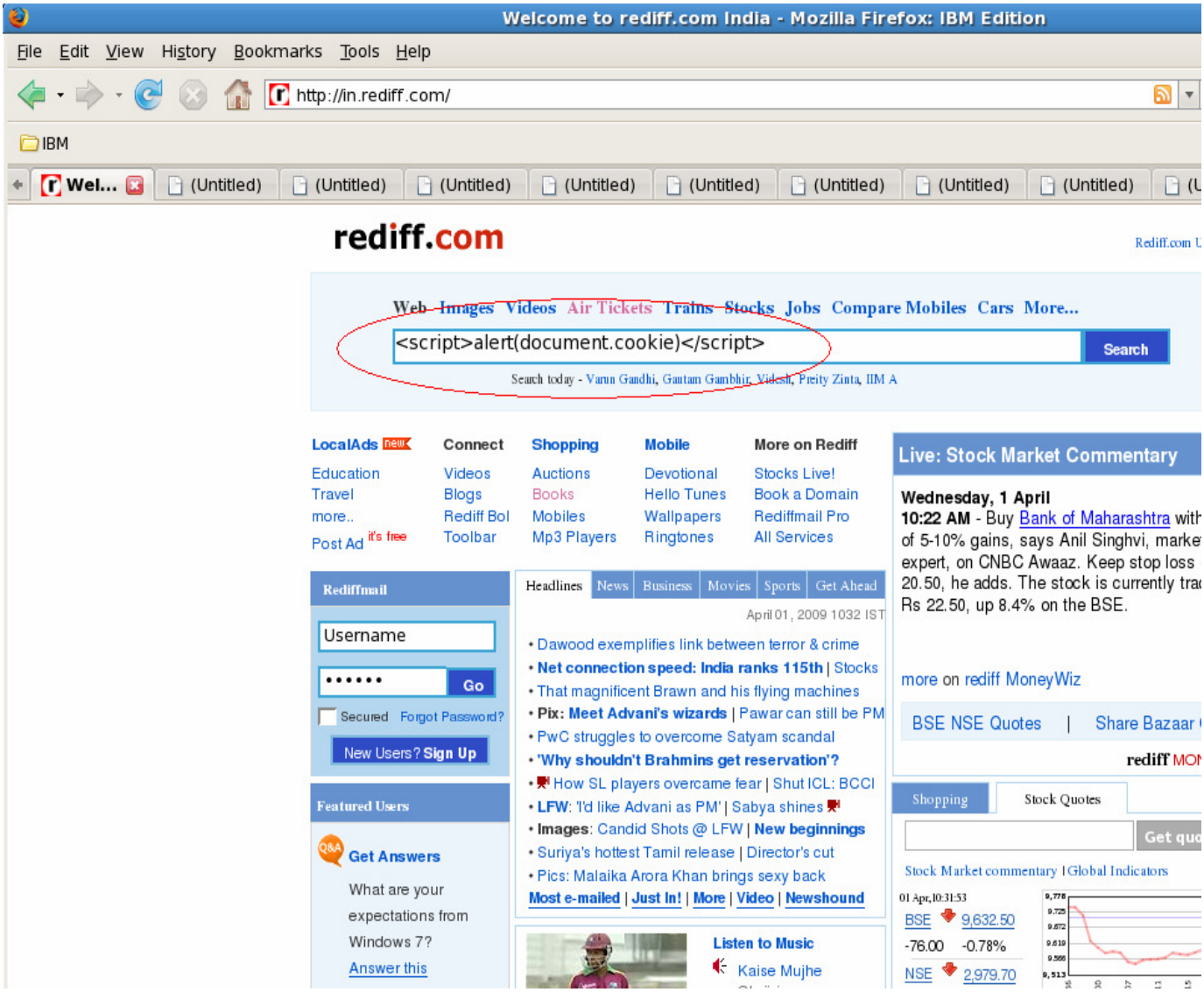
**Two PoC URLs (home and job search):**
1. General Home page search URL:
`http://search1.rediff.com/dirsrch/default.asp?MT=%3Cscript%3Ealert%28document.cookie%29%3C%2Fscript%3E`

2. Job Search URL:
`http://job.rediff.com/jobsearch/not_found.php?keyword=%3Cscript%3Ealert(document.cookie)%3C/script%3E`

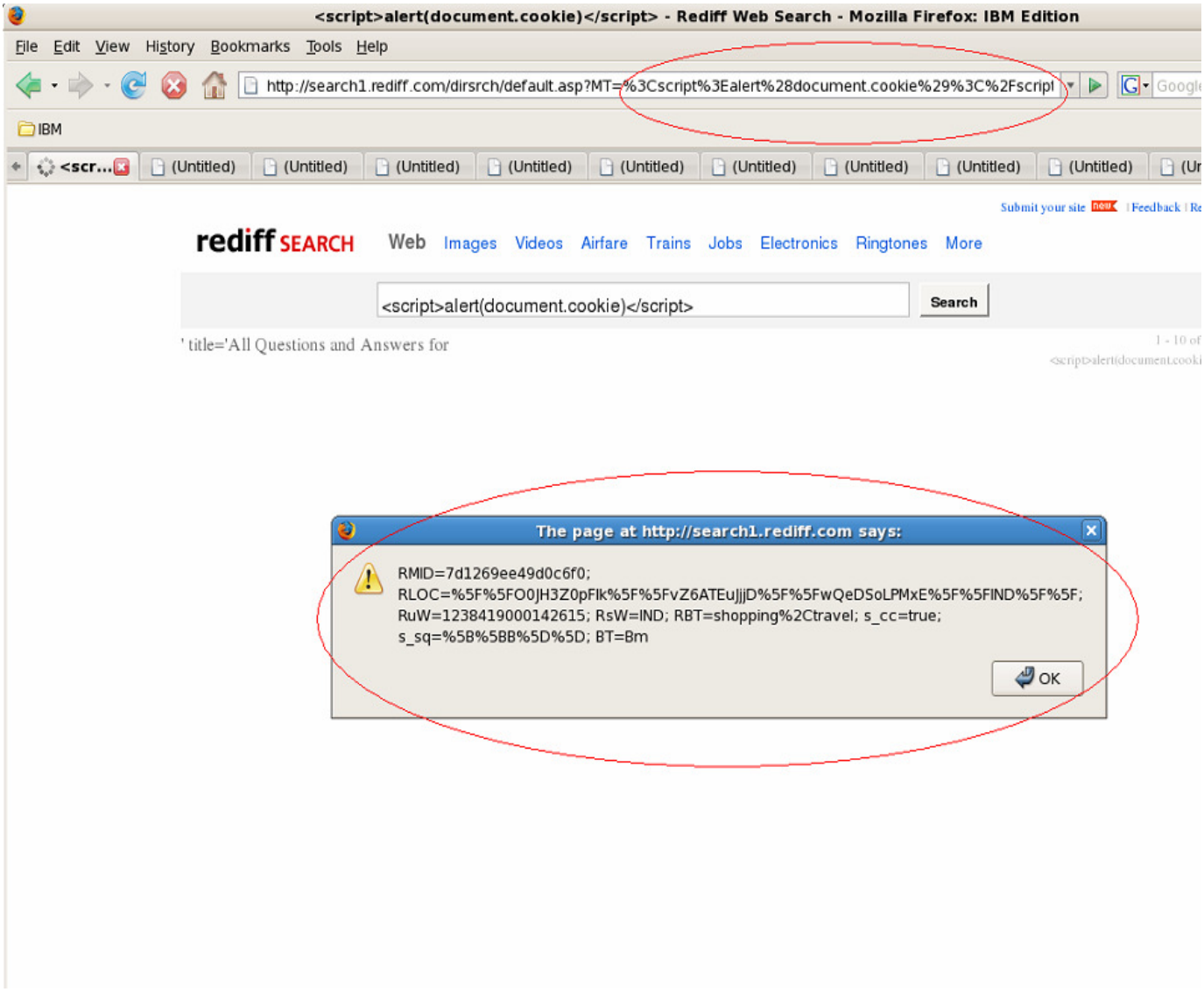
# Proof of Concept Images

**Home page Search:**

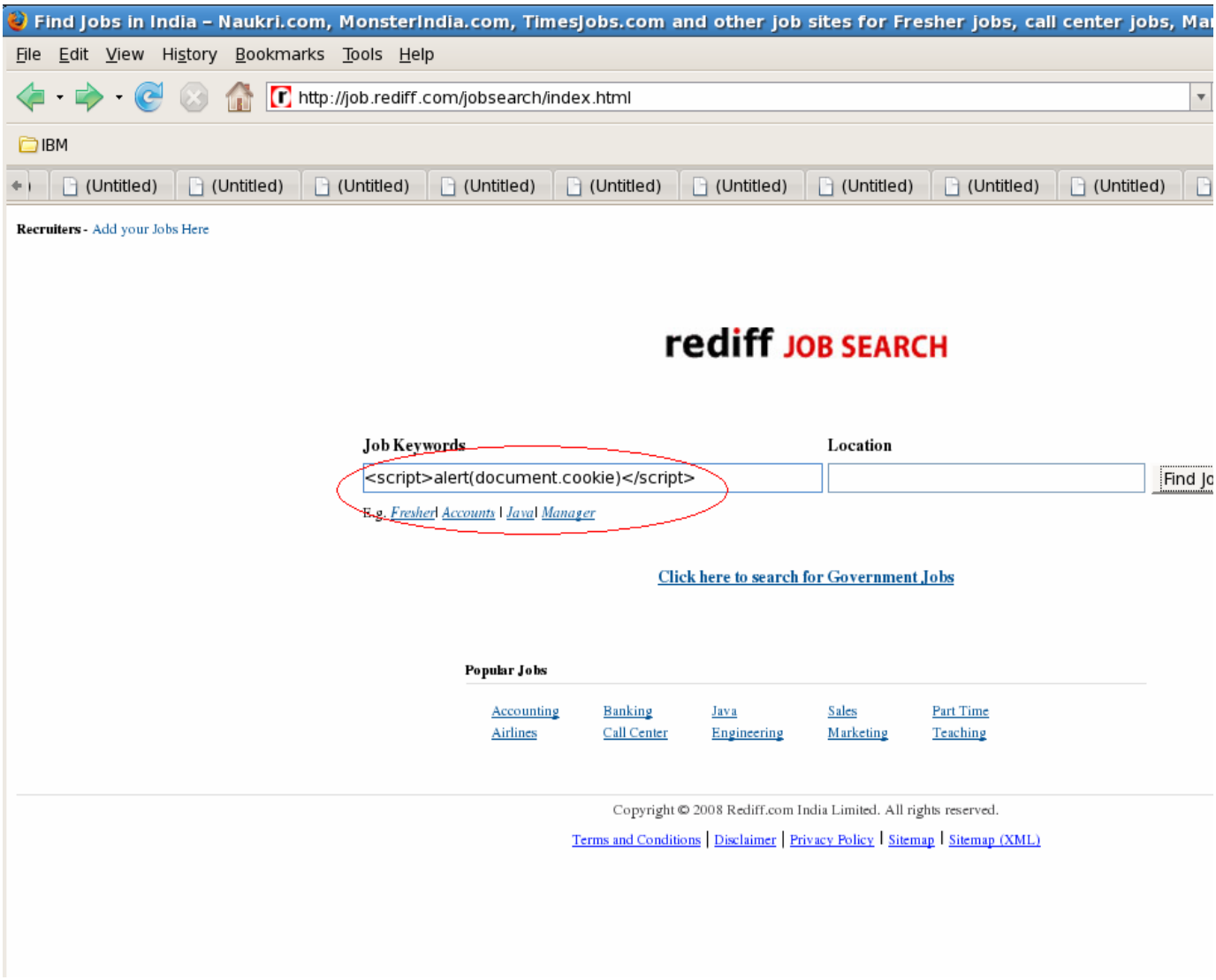
Send the script code as search item.



**Home Page Search result:**
Voila!! We have our URL embedded with malicious script ☺. The server sends the search criteria as is and the browser executes our script code. Another problem is that the search item is embedded “as is” at more than one place in the html and hence our script code gets executed multiple times.



**Job Search:**
Using the same lame script code as job search criteria



**Job Search result:**