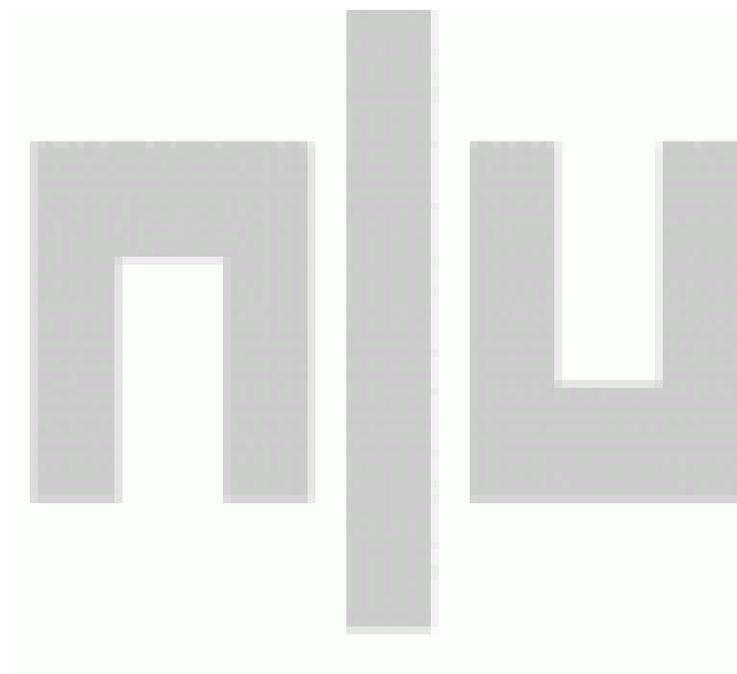


Cross Site Scripting (XSS)  
Vulnerabilities in rediff.com  
IA search, IN search and JOB Search



Author: Aseem Jakhar  
Email: [null@null.co.in](mailto: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: 14<sup>th</sup> 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.

Welcome to rediff.com India - Mozilla Firefox: IBM Edition

File Edit View History Bookmarks Tools Help

http://in.rediff.com/

IBM

rediff.com

Web Images Videos Air Tickets Trains Stocks Jobs Compare Mobiles Cars More...

`<script>alert(document.cookie)</script>` Search

Search today - Varun Gandhi, Gautam Gambhir, Videst, Preity Zinta, IIM A

LocalAds **new** Connect Shopping Mobile More on Rediff

Education Videos Auctions Devotional Stocks Live!  
Travel Blogs Books Hello Tunes Book a Domain  
more.. Rediff Bol Mobiles Wallpapers Rediffmail Pro  
Post Ad **it's free** Toolbar Mp3 Players Ringtones All Services

Rediffmail

Username  
..... Go  
 Secured [Forgot Password?](#)  
**New Users? Sign Up**

Featured Users

**Q&A** Get Answers  
What are your expectations from Windows 7?  
[Answer this](#)

Headlines News Business Movies Sports Get Ahead

April 01, 2009 10:32 IST

- Dawood exemplifies link between terror & crime
- **Net connection speed: India ranks 115th** | Stocks
- That magnificent Brawn and his flying machines
- **Pix: Meet Advani's wizards** | Pawar can still be PM
- PwC struggles to overcome Satyam scandal
- **'Why shouldn't Brahmins get reservation?'**
- **How SL players overcame fear** | Shut ICL: BCCI
- **LFW: 'I'd like Advani as PM'** | Sabya shines
- **Images: Candid Shots @ LFW** | **New beginnings**
- Suriya's hottest Tamil release | Director's cut
- Pics: Malaika Arora Khan brings sexy back

[Most e-mailed](#) | [Just In!](#) | [More](#) | [Video](#) | [Newshound](#)

**Listen to Music**  
Kaise Mujhe

Live: Stock Market Commentary

**Wednesday, 1 April**  
**10:22 AM** - Buy [Bank of Maharashtra](#) with of 5-10% gains, says Anil Singhvi, market expert, on CNBC Awaaz. Keep stop loss 20.50, he adds. The stock is currently trading at Rs 22.50, up 8.4% on the BSE.

more on rediff [MoneyWiz](#)

[BSE NSE Quotes](#) | [Share Bazaar](#)

Shopping Stock Quotes

Get quotes

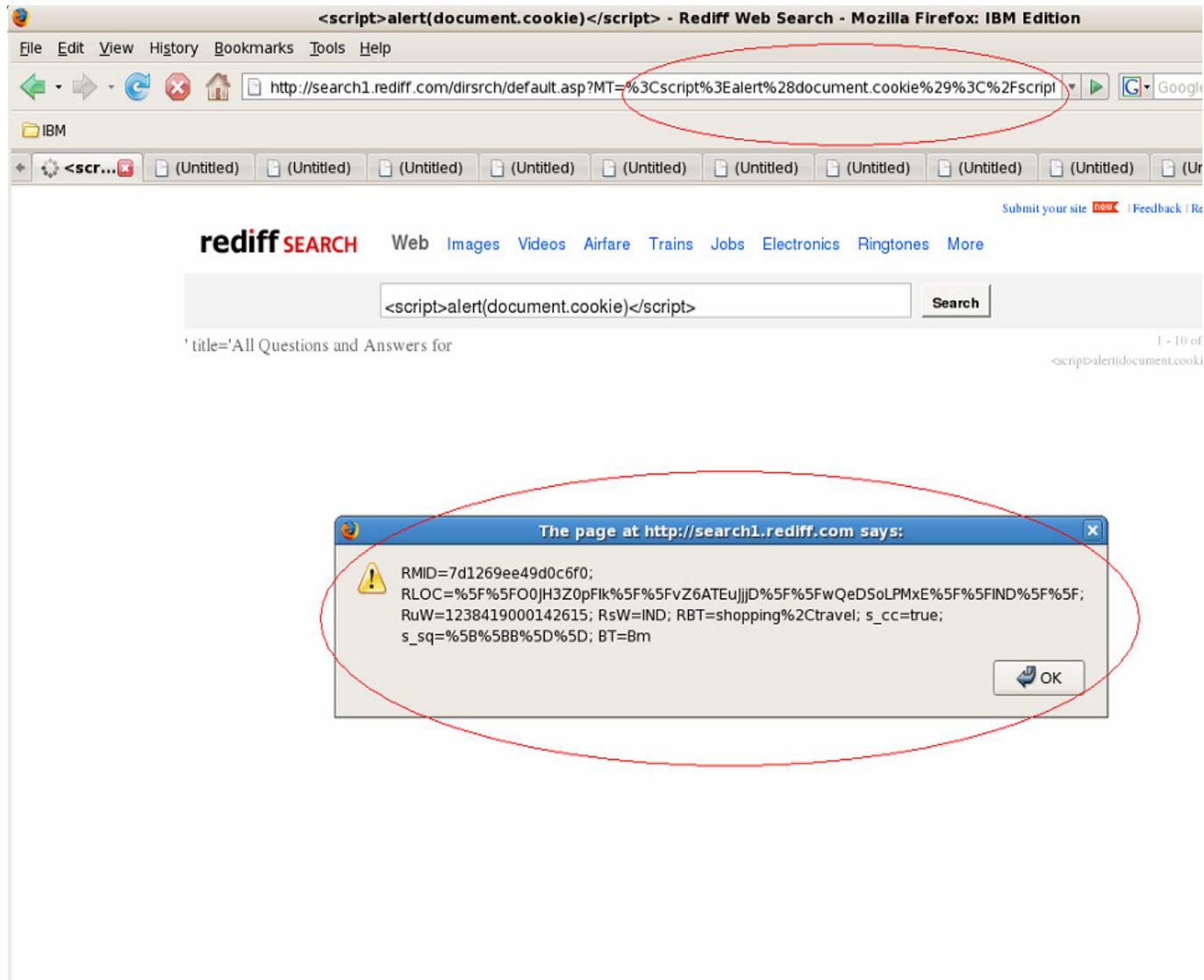
Stock Market commentary | Global Indicators

01 Apr, 10:31:53

BSE	9,632.50
-76.00	-0.78%
NSE	2,979.70

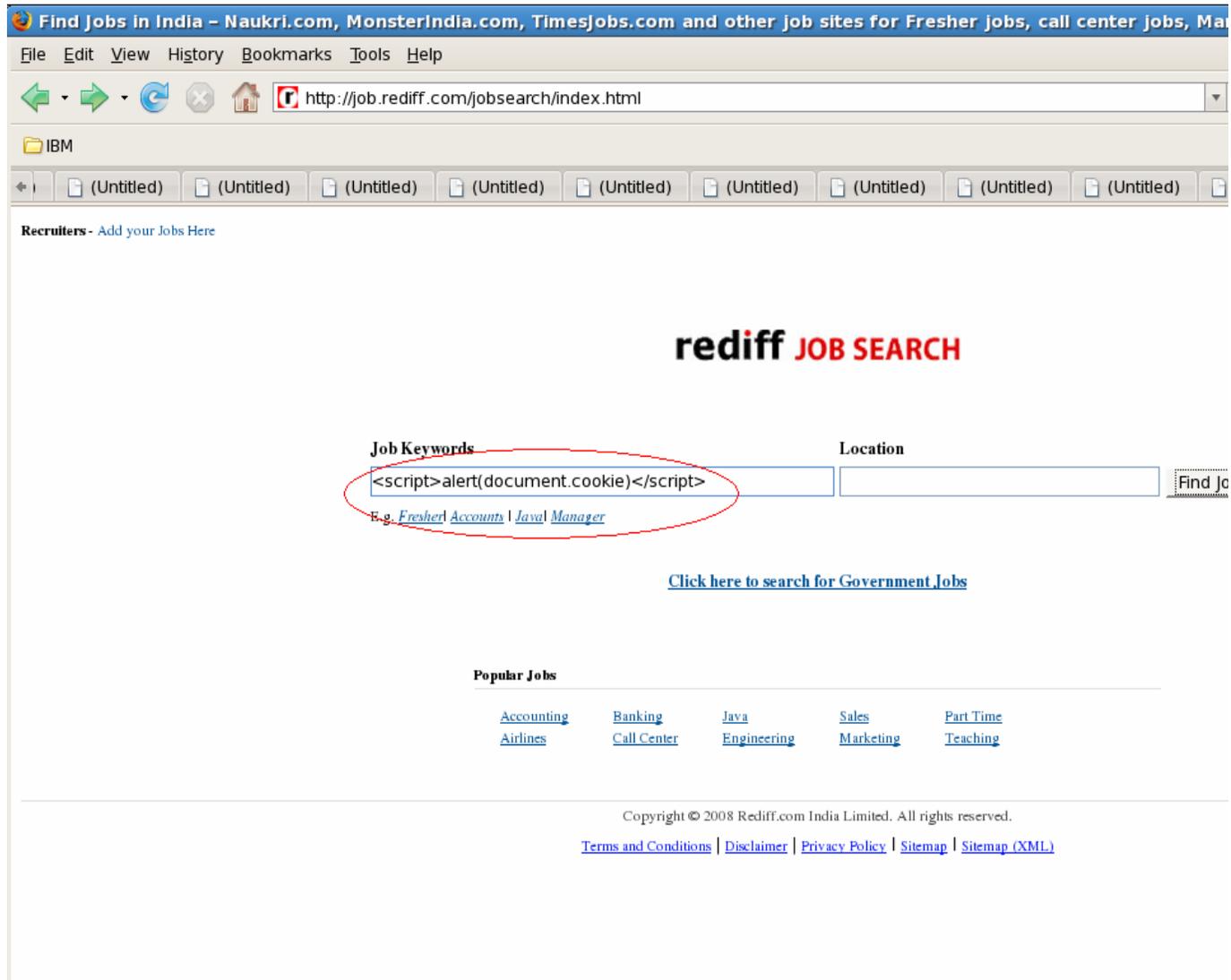
## Home Page Search result:

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



Find Jobs in India - Naukri.com, MonsterIndia.com, Timesjobs.com and other job sites for Fresher jobs, call center jobs, Ma

File Edit View History Bookmarks Tools Help

http://job.rediff.com/jobsearch/index.html

IBM

Recruiters - Add your Jobs Here

# rediff JOB SEARCH

Job Keywords  Location

E.g. [Fresher Accounts](#) | [Java Manager](#)

[Click here to search for Government Jobs](#)

### Popular Jobs

<a href="#">Accounting</a>	<a href="#">Banking</a>	<a href="#">Java</a>	<a href="#">Sales</a>	<a href="#">Part Time</a>
<a href="#">Airlines</a>	<a href="#">Call Center</a>	<a href="#">Engineering</a>	<a href="#">Marketing</a>	<a href="#">Teaching</a>

Copyright © 2008 Rediff.com India Limited. All rights reserved.

[Terms and Conditions](#) | [Disclaimer](#) | [Privacy Policy](#) | [Sitemap](#) | [Sitemap \(XML\)](#)

## Job Search result:

Find Jobs in India â€” Naukri.com, MonsterIndia.com, TimesJobs.com and other job sites for Fresher jobs, call center jobs, Manager jobs

File Edit View History Bookmarks Tools Help

http://job.rediff.com/jobsearch/not\_found.php?keyword=%3Cscript%3Ealert(document.cookie)%3C/script%3E

IBM

Recruiters - Add your Jobs Here

### rediff JOB SEARCH

Oops, we did not find any results for your Query "

The page at http://job.rediff.com says:

⚠ RMD=7d1269ee49d0c6f0;  
RLOC=%5F%5F00jH3Z0pFik%5F%5FvZ6ATEUjjjD%5F%5FwQeDSolPMxE%5F%5FIND%5F%5F;  
RuW=1238419000142615; RsW=IND; RBT=shopping%2Ctravel; s\_cc=true;  
s\_sq=%5B%5B%5D%5D; BT=8m%2CDO

OK